Technische Universität Kaiserslautern
Fachbereich Mathematik

Integrality of representations of finite groups

Tommy Hofmann

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. Werner Bley

Tag der Disputation: 10.06.2016

D 386

Preface

Contribution

Integrality of representations of finite groups. Representation theory of finite groups is an area of mathematics closely related to group theory, where an abstract group G is analyzed by means of so-called representations of G over a field k, which are just group homomorphisms $G \to \mathrm{GL}_n(k)$. One can think of representation theory as a linearization tool for finite groups, as the abstract operation in a group is transferred to the well known setting of linear transformations of finite dimensional vector spaces. As all properties of linear transformations are invariant under base change, the following definition is intuitive for representations: We say that two representations $\rho, \tilde{\rho} \colon G \to \mathrm{GL}_n(k)$ are equivalent, if and only if there exists an invertible matrix $X \in \mathrm{GL}_n(k)$ such that $X\rho(g)X^{-1} = \tilde{\rho}(g)$ for all $g \in G$, that is, if and only if we can find a base change $\varphi_X \colon \mathrm{GL}_n(k) \to \mathrm{GL}_n(k),\ A \mapsto XAX^{-1}$ such that $\varphi_X \circ \rho = \tilde{\rho}$.

In case $k = \mathbf{C}$ the representations are so-called complex representations, and the study of these has a long history, beginning with Frobenius at the end of the 19th century. As equivalent representations have the same properties, one might ask whether for a given complex representation one can find a—in some sense—simpler equivalent representation. For example it is known that for every finite group G there exists a number field K, that is, a finite extension K of $\mathbf{Q}$, such that for every complex representation $G \to \mathrm{GL}_n(\mathbf{C})$ there exists an equivalent complex representation $\tilde{\rho}$ with $\tilde{\rho}(g) \in \mathrm{GL}_n(K)$ for all $g \in G$.

Thanks to this rationality result it is reasonable to concentrate on representations $G \to \mathrm{GL}_n(K)$, where K is a number field. A special case of these representations are so-called rational representations $G \to \mathrm{GL}_n(\mathbf{Q})$. For these we have an additional simplification step due to Burnside [Bur08]: Given a representation $G \to \mathrm{GL}_n(\mathbf{Q})$ there exists a conjugate representation $\tilde{\rho}$ such that $\tilde{\rho}(g) \in \mathrm{GL}_n(\mathbf{Z})$ for all $g \in G$, that is, all matrices have integer entries. Coming back to the general case of a representation over a number field K and replacing $\mathbf{Z}$ by the ring of integers $\mathcal{O}_K$ of K, Burnside asked and partly dealt with the natural follow-up question, which we investigate in this thesis:

Question (Burnside): Given a representation $\rho \colon G \to \mathrm{GL}_n(K)$ of a finite group G over a number field K, does there exist a representation $\tilde{\rho}$ conjugate to ρ such that $\tilde{\rho}(g) \in \mathrm{GL}_n(\mathcal{O}_K)$ for all $g \in G$?

In this case we call $\tilde{\rho}$ an integral representation and we say that ρ can be made integral. Using this convention, the above result of Burnside reads: Every representation over $\mathbf{Q}$ can be made integral. While Burnside [Bur08] himself and Schur [Sch11] found sufficient conditions under which a representation over a number field can be made integral, for 70 years it was open whether every representation over a number field can be made integral. By providing two examples, Cliff, Ritter and Weiss [CRW92] (and independently Serre and Feit [Ser08]), finally answered the question of Burnside negatively. As both proofs, the one(s) of Cliff, Ritter and Weiss and the one(s) of Serre and Feit, involve ad hoc methods applicable only in their particular situations, they did not provide an answer to the following question: Is it possible to decide algorithmically whether a representation over a number field can be made integral? The first main contribution of this thesis is an affirmative answer to this problem (see §17):

Theorem. There exists an algorithm that, given a representation of a finite group over a number field, answers Burnside's question, that is, it decides whether this representation can be made integral. Moreover, if this is the case, a conjugate integral representation can be computed.

To describe the second main contribution, we shift our focus from a single representation to families of representations realizing a given character of a finite group. Recall that a character of G is a map $\chi \colon G \to \mathbf{C}$, such that there exists a representation $\rho\colon G \to \mathrm{GL}_n(\mathbf{C})$ with $\mathrm{tr}(\rho(g)) = \chi(g)$ for all $g \in G$. In this case we say that χ is realized by ρ. As conjugate representations have the same character, the aforementioned rationality result implies that every character of G can be realized by a representation over a number field. In fact there are infinitely many different number fields which allow for representations realizing χ and of particular interest are the fields with minimal degree over $\mathbf{Q}$. While a single representation over a number field of minimal degree realizing a given character may fail to be integral, we now ask:

Question: Given a character χ of G, does there exist an integral representation $G \to \mathrm{GL}_n(K)$ with K of minimal degree realizing χ? Can one always find a representation $G \to \mathrm{GL}_n(K)$ with K of minimal degree realizing χ which cannot be made integral? If such fields exist, how many are there?

Building upon the work of Serre, we are able to give an answer under certain conditions on the character (see Theorem 18.18):

Theorem. Let χ be an irreducible character of a finite group with degree $\deg(\chi) = 2$, character field $\mathbf{Q}(\chi) = \mathbf{Q}$ and Schur index $m_{\mathbf{Q}}(\chi) = 2$. Then there are infinitely many number fields K of minimal degree and integral representations ρ over K realizing χ. And there are infinitely many number fields K of minimal degree and representations ρ over K realizing χ which cannot be made integral.

Moreover, based on extensive computations using our developed algorithms, we make various conjectures generalizing this theorem.

Orders and lattices. The first step towards answering integrality questions for representations of finite groups is a change of language: Instead of considering representations $G \to \mathrm{GL}_n(K)$ and $G \to \mathrm{GL}_n(\mathcal{O}_K)$ we investigate K-vector spaces and free $\mathcal{O}_K$-modules with a given operation of G. The question of whether a representation $\rho\colon G \to \mathrm{GL}_n(K)$ can be made integral translates to a question about existence of G-invariant $\mathcal{O}_K$-modules with special properties contained in the KG-module associated to ρ. More precisely, for a fixed KG-module we need to decide whether there exists an $\mathcal{O}_K$-free $\mathcal{O}_K G$-submodule of full rank. While the change of language seems tautological at a first glance, we have now entered the well developed area of orders and lattices over Dedekind domains. As this area is lagging behind on the algorithmic side, we had to address various algorithmic questions in order to decide integrality. In particular for an order Λ over $\mathcal{O}_K$, Λ-lattices M and N and $\mathfrak{p}$ a nonzero prime ideal of $\mathcal{O}_K$, in this thesis we address the following problems:

- Computation of $\mathrm{Hom}_\Lambda(M, N)$, $\mathrm{Hom}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p})$ and reductions thereof.
- Local lattice isomorphism: Decide whether $M_\mathfrak{p} \cong N_\mathfrak{p}$.
- Classifying lattices up to local isomorphism.
- Computation of the different genera of lattices.
- Effective version of the theorem of Jordan–Zassenhaus.
- Decomposition of lattices modulo prime ideals at all prime ideals.
- Computation of Solomon zeta functions of lattices.

Let us digress on the second to last item (all the other problems are straightforward to describe). Let K be a number field and consider an irreducible KG-module V together with an $\mathcal{O}_K G$-lattice M of V. One now might ask how the module $M/\mathfrak{p}M$ (the so-called reduction of V modulo $\mathfrak{p}$, which is to some extent independent of the chosen $\mathcal{O}_K G$-lattice of V) changes, as $\mathfrak{p}$ varies over the nonzero prime ideals of $\mathcal{O}_K$. Will it stay irreducible or not? If not, how large are the composition factors and how do they vary with $\mathfrak{p}$? In case K is a splitting field, the answer is a consequence of a result of Brauer–Nesbitt in the area of modular representation theory: Outside a finite number of prime ideals the reduction of V stays irreducible. In this thesis we address the case where K is an arbitrary number field and show—using class field theory—that the decomposition behavior can be described explicitly allowing us to describe all possible decompositions that can and will occur.

The last item, the computation of the Solomon zeta function, is not directly linked to the question of integrality, but is an immediate application of the previous items. Based on experiments with an algorithm for computing this zeta function, we were able to conjecture and prove the form of the Solomon zeta function for all lattices in the natural representation of the symmetric group.

Modules over ring of integers. The underlying premise of all algorithms dealing with $\mathcal{O}_K G$-lattices is that we can (efficiently) compute with finitely generated, torsion-free modules over $\mathcal{O}_K$. In addition to representing such modules this means computing sums, intersections, testing membership of elements, or testing isomorphism. Assuming for a moment that $K = \mathbf{Q}$ and $\mathcal{O}_K = \mathbf{Z}$, these problems can be addressed using the Hermite normal form, a unique row reduced echelon form for integer matrices. Because of its wide range of applications, research on Hermite normal form algorithms has attracted lots of attention, see [Sto00], resulting in fast (theoretical and practical) polynomial time algorithms.

Because $\mathcal{O}_K$ is in general not a principal ideal domain, the situation in the general case is quite different—both in theory and in practice. While more than 100 years ago Steinitz proved in [Ste11, Ste12] that submodules of $\mathcal{O}_K^n$ can be represented by a combination of matrices and ideals, explicit algorithms were lacking for a long time. Based on the pioneering work of Bosma and Pohst [BP91], the notion of a Hermite normal form was generalized to $\mathcal{O}_K$-modules by Cohen [Coh96]. Moreover by describing algorithms for computing this so-called pseudo-Hermite normal form, the problem of computing with modules over $\mathcal{O}_K$ was finally solved. While Cohen's algorithm was believed to be polynomial time, no proof was provided. In this thesis we present two fundamentally different algorithms for computing the pseudo-Hermite normal form, with polynomial running time. The first one is a modification of Cohen's original algorithm with proven polynomial running time. The second one is quite different, for it uses the Euclidean structure of non-trivial quotient rings of $\mathcal{O}_K$ in a novel way, allowing us to bypass all difficulties occurring when manipulating modules over $\mathcal{O}_K$. As a corollary we also obtain a new algorithm for computing the Hermite normal form of integer matrices.

In order to talk about running time of algorithms manipulating objects associated to algebraic number fields, we first introduce and analyze a model for computing with these objects. After fixing representations for algebraic integers and fractional ideals, we give a detailed exposition of the complexity of a wide range of operations. While most of the used algorithms are well known (see [PZ89, Coh93]), thorough complexity analyses were lacking (see [Bel04] for partial results on element arithmetic).

While in this thesis the pseudo-Hermite normal form and algorithms computing it are only used as a tool for handling lattices and more complicated objects, they have a wide range of applications. Applications come from number theory itself, e.g. working with relative extensions (see [Coh00]). But they also show up in the field of cryptography (see [FS10]) and coding theory (see [BQ12]).

The thesis contains material from the author's (partly) published articles [FH14, Hof16, BFH14]. In particular, the thesis contains joint work with Claus Fieker and Jean-Françoise Biasse. The respective publication is listed at the beginning of the corresponding chapter respectively section it gives contribution to.

Structure

The thesis is structured as follows: In Chapter 1—after recalling elementary facts about number fields and matrix normal forms over rings—we develop a computational model for number fields, including field and ideal arithmetic. In Chapter 2, we describe pseudo-Hermite normal form algorithms and use the model of Chapter 1 to prove polynomial running time. Chapter 3 is purely theoretical and recalls the basic theory of orders and lattices. We also include a new proof of the theorem of Jordan–Zassenhaus for global fields which is in addition constructive. In Chapter 4 we provide algorithms for various problems involving orders and lattices. In Chapter 5, after investigating reductions of modules over group algebras, we finally apply all the machinery to tackle the question of integrality.

Acknowledgement

I would like to thank my supervisor, Claus Fieker, for suggesting me to work on integral representation theory, and his constant guidance and support. I owe special thanks to Prof. Werner Bley for agreeing to act as a referee of my thesis.

Notation and convention

By $\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$ we denote the rational integers, the rational numbers, the real numbers and the complex numbers respectively. By $\mathbf{P}$ we denote the set of (positive) prime numbers. We denote by $\bar{\mathbf{Q}}$ a fixed algebraic closure of $\mathbf{Q}$ inside $\mathbf{C}$. A ring is always a ring with unit and a ring morphism is always unit preserving. Unless otherwise mentioned, all modules are unital left modules.

For a ring R and integers $m, n \in \mathbf{Z}_{\geq 1}$ we denote by $\mathrm{Mat}_{n \times m}(R)$ the R-module of all $n \times m$ matrices with entries in R and by $\mathrm{GL}_n(R)$ the group $\mathrm{Mat}_{n \times n}(R)^\times$ of invertible $n \times n$ matrices. By $\mathbf{0}_{n \times m}$ we denote the zero matrix in $\mathrm{Mat}_{n \times m}(R)$. For $1 \leq i \leq n, 1 \leq j \leq m$ we denote by e_{ij} the matrix $(\delta_{ki}\delta_{lj})_{1 \leq i \leq n, 1 \leq j \leq m}$ in $\mathrm{Mat}_{n \times m}(R)$. We call $(\mathrm{e}_{ij})_{i,j}$ the canonical basis of $\mathrm{Mat}_{n \times m}(R)$. By $\mathbf{1}_n$ we denote the $n \times n$ identity matrix. A diagonal matrix $A = (a_{ij})_{i,j} \in \mathrm{Mat}_{n \times n}(R)$ with $a_{i,j} = 0$ for all i, j with $i \neq j$ is denoted by $\mathrm{diag}(a_{11}, a_{22}, \ldots, a_{nn})$. For a matrix $A \in \mathrm{Mat}_{n \times m}(R)$ we denote by $\mathrm{sp}(A)$ the R-submodule of R^m which is spanned by the rows of A. For $1 \leq j \leq n$, we denote by $\mathrm{sp}_j(A)$ the module $\{(v_1, \ldots, v_m) \in \mathrm{sp}(A) \mid v_m = v_{m-1} = \cdots = v_{m-j+1} = 0\}$.

If $M = (m_{ij})_{i,j} \in \mathrm{Mat}_{n \times m}(\mathbf{Z})$ is an integer matrix, we denote by $|M| = \max\{|m_{ij}| \mid 1 \leq i, j \leq n\}$ the absolute value of the largest entry of M.

To simplify the presentation of complexity results, we use soft-Oh notation $\tilde{O}$: For functions $f, g \colon \mathbf{R}_{\geq 0} \to \mathbf{R}_{\geq 0}$ we have $f \in \tilde{O}(g)$ if and only if there exists $k \in \mathbf{Z}_{>0}$ such that $f \in O(g(\log(g))^k)$.

If $f \colon M \to N$ is a function and $M' \subseteq M$, $N' \subseteq N$ are subsets with $f(M') \subseteq N'$ we denote by $f|_{N'}^{M'} \colon M' \to N'$ the function induced by f.

Let R be a commutative ring, M a free R-module of rank m with R-basis $\mathscr{M}$ and N a free R-module of rank n with R-basis $\mathscr{N}$. Then for an R-morphism $f \colon M \to N$ we denote by $\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(f) \subseteq \mathrm{Mat}_{m \times n}(R)$ the matrix of f with respect to the bases $\mathscr{M}$ and $\mathscr{N}$.

Contents

CHAPTER 1

Computing in number fields

In the long history of (algebraic) number theory, developments on the theoretical side have always been accompanied by explicit constructive methods. In this context algebraic number fields are no exception. Although algorithms for nearly every problem in algebraic number fields have been known for quite a time (see [Coh93, PZ89]), and many implementations can be found (for example [PARI, BCP97, DFK$^+$97]), the inspection of complexity seems schizophrenic: While some problems like the class group computation of (quadratic) number fields, have attracted lots of attention including detailed complexity analyses, lots of areas have been treated negligently.

Among those areas are basic element and ideal arithmetic in number fields. Even though these operation are at the heart of almost all algorithms, apart from the investigation of multiplication by Belabas in [Bel04] the complexity was never an issue. Actually in [PZ89] the authors deliberately decided against an analysis of complexity since “the algorithms under consideration yield good to excellent results for number fields of small degree and not too large discriminants” [PZ89, Preface].

Since then the situation has changed dramatically. With applications coming from cryptography and coding theory, and newly available hardware, the computational bounds are constantly pushed further and further. In particular the credo of small degree/discriminant does not apply anymore. As a consequence we need to understand the dependency of basic arithmetic on the degree and discriminant.

The goal of this chapter is to introduce a simple computational model for algebraic number fields which can be used to analyze more involved algorithms. In particular, this will be applied in Chapter 2 where we evaluate the complexity of computing normal forms of modules over the ring of integers of a number field. In parts results of this chapter have been published in [BFH14] and [FH14].

§1. Background

§1A. Number fields

In this section very basic facts from algebraic number theory are introduced, mainly for notational purpose. We begin with basic properties of number fields, which can be found in any book entitled “algebraic number theory”, see for example [Neu99] or [Lan94].

A *number field* K is a finite extension of $\mathbf{Q}$ contained in $\bar{\mathbf{Q}}$. The degree $[K : \mathbf{Q}]$ of the field extension is called the *degree* of the number field K. The rationals $\mathbf{Q}$ being of characteristic 0, a number field K of degree d admits d embeddings $K \to \mathbf{C}$. We denote by $\Sigma_{K,\infty} = \Sigma_\infty$ the set of all these embeddings. For an element α of K we denote by μ_α the $\mathbf{Q}$-linear map $K \to K$, $\beta \longmapsto \alpha\beta$. If Ω is a $\mathbf{Q}$-basis of K, then the matrix $M_{\alpha,\Omega} \in \operatorname{Mat}_{d\times d}(\mathbf{Q})$ representing μ_α with respect to Ω is called the *regular representation of α (with respect to Ω)*. In case Ω is fixed we drop the Ω in the index and speak of the regular representation of α. As usual we define $\mathrm{N}_{K|\mathbf{Q}}(\alpha) = \det(\mu_\alpha) \in \mathbf{Q}$ and $\mathrm{Tr}_{K|\mathbf{Q}}(\alpha) = \mathrm{tr}(\mu_\alpha) \in \mathbf{Q}$ respectively to be the *norm* of α and the *trace* of α respectively. Note that we have

$$\mathrm{N}_{K|\mathbf{Q}}(\alpha) = \prod_{\sigma\in\Sigma_\infty} \sigma(\alpha) \quad \text{and} \quad \mathrm{Tr}_{K|\mathbf{Q}}(\alpha) = \sum_{\sigma\in\Sigma_\infty} \sigma(\alpha).$$

An embedding $\sigma \in \Sigma_\infty$ is called *real*, if the image of σ is contained in $\mathbf{R}$ and *complex* otherwise. As usual for an embedding $\sigma \in \Sigma_\infty$ we denote by $\overline{\sigma}$ the composition of σ with complex conjugation. Denoting by r

the number of real embeddings and by $2s$ the number of complex embeddings of K, we call the tuple (r, s) the *signature* of K. We can embed K in $K_{\mathbf{R}} = K \otimes_{\mathbf{Q}} \mathbf{R} \simeq \mathbf{R}^r \times \mathbf{C}^s$ and extend all embeddings to $K_{\mathbf{R}}$. The d-dimensional real vector space $K_{\mathbf{R}}$ carries the Hermitian form

$$T_2\colon K_{\mathbf{R}} \times K_{\mathbf{R}} \longrightarrow \mathbf{R}, (\alpha, \beta) \longmapsto \sum_{\sigma \in \Sigma_\infty} \sigma(\alpha)\overline{\sigma}(\beta).$$

The associated norm $\| \;\|$ defined by $\|\alpha\| = \sqrt{T_2(\alpha, \alpha)}$ for $\alpha \in K_{\mathbf{R}}$, turns $K_{\mathbf{R}}$ into a normed vector space over $\mathbf{R}$.

An element $\alpha \in \overline{\mathbf{Q}}$ is called *integral* or an *algebraic integer*, if the minimal polynomial (the monic generator of the kernel of $\mathbf{Q}[X] \to \mathbf{Q}(\alpha), f \mapsto f(\alpha)$) is an element of $\mathbf{Z}[X]$. The *ring of integers* of K is the set of all algebraic integers contained in K. We denote it by $\mathcal{O} = \mathcal{O}_K$. The set $\mathcal{O}$ is a Noetherian, integrally closed subring of K of dimension 1, that is, a Dedekind domain. Moreover it is a free $\mathbf{Z}$-module of rank d with $\mathbf{Q}\mathcal{O} = K$. The *discriminant* $\Delta = \Delta_K$ of the number field K is defined to be $\det(\operatorname{Tr}_{K|\mathbf{Q}}(\omega_i \cdot \omega_j)_{i,j})$, where $\omega_1, \dots, \omega_d$ is any $\mathbf{Z}$-basis of $\mathcal{O}$ (such a $\mathbf{Z}$-basis is called an *integral basis* of $\mathcal{O}$).

A *fractional ideal* of K is a nonzero finitely generated $\mathcal{O}$-submodule of K. The set I_K of fractional ideals of K forms a group with identity element $\mathcal{O}$, where the product $\mathfrak{a}\mathfrak{b}$ of two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ of K is defined to be the $\mathcal{O}$-module generated by the set $\{\alpha\beta \mid \alpha \in \mathfrak{a}, \beta \in \mathfrak{b}\}$, and inversion is given by $\mathfrak{a}^{-1} = \{\alpha \in K \mid \alpha\mathfrak{a} \subseteq \mathcal{O}\}$. Since every fractional ideal $\mathfrak{a}$ can be uniquely written in the form $\mathfrak{a} = \prod_{0 \neq \mathfrak{p} \in \operatorname{Spec}(\mathcal{O})} \mathfrak{p}^{n_\mathfrak{p}}$ with $n_\mathfrak{p} \in \mathbf{Z}$ and $n_\mathfrak{p} = 0$ for almost all $\mathfrak{p}$, the abelian group I_K is free on the set of nonzero prime ideals of $\mathcal{O}$. The integer $n_\mathfrak{p}$ is called the $\mathfrak{p}$*-adic valuation of* $\mathfrak{a}$ and is denoted by $v_\mathfrak{p}(\mathfrak{a})$. A fractional ideal contained in $\mathcal{O}$ is called an *integral ideal* of K, which is in fact a nonzero ideal of the commutative ring $\mathcal{O}$. For every fractional ideal $\mathfrak{a}$ of K, there exists $r \in \mathbf{Z}_{>0}$ such that $r\mathfrak{a}$ is an integral ideal. The minimal positive integer with this property is defined to be the *denominator* of the fractional ideal $\mathfrak{a}$ and is denoted by $\operatorname{den}(\mathfrak{a})$.

In case a fractional ideal is generated (as an $\mathcal{O}$-module) by a single element of K, we call it a *principal fractional ideal.* For an element $\alpha \in K^\times$, this fractional ideal is denoted by (α). We define $v_\mathfrak{p}((\alpha))$ to be the $\mathfrak{p}$*-adic valuation of* α and denote it by $v_\mathfrak{p}(\alpha)$. The set P_K of all principal fractional ideals is a subgroup of the abelian group I_K. The quotient I_K/P_K is a finite abelian group denoted by Cl_K or $\operatorname{Cl}_\mathcal{O}$ and is called the *ideal class group* of K.

As the ring of integers $\mathcal{O}$ is residually finite, the quotient $\mathcal{O}/\mathfrak{a}$ is finite for all nonzero integral ideals $\mathfrak{a}$ of $\mathcal{O}$. We call $|\mathcal{O}/\mathfrak{a}|$ the *ideal norm* of $\mathfrak{a}$ and denote it by $\mathbf{N}(\mathfrak{a})$.

Given an integral ideal $\mathfrak{a}$ of K, the unique positive integer $m \in \mathbf{Z}_{\geq 0}$ with $(m) = \mathbf{Z} \cap \mathfrak{a}$ is called the *minimum of* $\mathfrak{a}$ and is denoted by $\min(\mathfrak{a})$. Note that we have $\min(\mathfrak{a}) = \min\{a \in \mathbf{Z}_{>0} \mid a \in \mathfrak{a}\}$, justifying the naming.

Remark 1.1. The theory of fractional ideals can be developed for arbitrary Dedekind domains $\mathcal{O}$. In this case the number field K has to be replaced by the field of fractions of $\mathcal{O}$. In particular attached to $\mathcal{O}$ we have the ideal class group $\operatorname{Cl}_\mathcal{O}$, an abelian group which no longer has to be finite.

Completions.

Assumption. Let $\mathcal{O}$ be a Dedekind domain with field of fractions K and $\mathfrak{p}$ a nonzero prime ideal of $\mathcal{O}$.

Associated to the prime ideal $\mathfrak{p}$, we have the discrete valuation $v_\mathfrak{p}\colon K^\times \to \mathbf{Z}$ and the non-Archimedean valuation

$$|\;|_\mathfrak{p}\colon K \longrightarrow \mathbf{R}_{\geq 0}, \alpha \longmapsto \begin{cases} 0, & \text{if } \alpha = 0, \\ c^{-v_\mathfrak{p}(\alpha)}, & \text{else,} \end{cases}$$

where $c \in \mathbf{R}_{>1}$ is some fixed real number. We fix a completion of the metric space $(K, |\;|_\mathfrak{p})$ and denote it (by abuse of notation) by $(K_\mathfrak{p}, |\;|_\mathfrak{p})$. We call it the $\mathfrak{p}$*-adic completion* of K or the *completion of K at* $\mathfrak{p}$. The set $\mathcal{O}_\mathfrak{p} = \{\alpha \in K_\mathfrak{p} \mid |\alpha|_\mathfrak{p} \leq 1\}$ is a complete discrete valuation ring with unit group $\mathcal{O}_\mathfrak{p}^\times = \{\alpha \in K_\mathfrak{p} \mid |\alpha|_\mathfrak{p} = 1\}$. We view K and $\mathcal{O}$ respectively as being embedded in $K_\mathfrak{p}$ and $\mathcal{O}_\mathfrak{p}$ respectively. If V is a K-vector space, we denote by $V_\mathfrak{p}$ the $K_\mathfrak{p}$-vector space $K_\mathfrak{p} \otimes_K V$ and view V as a subset of $V_\mathfrak{p}$ via the canonical monomorphism $V \to K_\mathfrak{p} \otimes_K V$. Similarly if M is a torsion-free finitely generated $\mathcal{O}$-module, we define $M_\mathfrak{p}$ to be the $\mathcal{O}_\mathfrak{p}$-module $\mathcal{O}_\mathfrak{p} \otimes_\mathcal{O} M$ and view M as a subset of $M_\mathfrak{p}$. In case $\mathfrak{p}$ is a principal ideal with generator $\pi \in \mathfrak{p}$ and $X \in \{K, \mathcal{O}, V, M\}$, we write X_π instead of $X_\mathfrak{p}$. Note that a different choice for c does not affect the topology induced by the valuation and therefore yields the same completion and associated objects.

Quotients of rings of integers. We now turn to the structure of quotients of rings of integers. Since the presented results are non-standard, for the convenience of the reader we have included proofs.

Assumption. Let K be an algebraic number field with ring of integers $\mathcal{O}$ and $\mathfrak{m}$ a nonzero ideal of $\mathcal{O}$.

Recall that a principal ideal ring is a ring in which every ideal is principal. It is well known that the quotient ring $\mathcal{O}/\mathfrak{m}$ is a principal ideal ring: Since principal ideal rings are closed under direct products (see [ZS75, Ch.IV, Theorem 33]), the Chinese remainder theorem shows that it is sufficient to consider the case of a prime ideal power $\mathfrak{m} = \mathfrak{p}^l$. Since the completion $\mathcal{O}_\mathfrak{p}$ is a discrete valuation ring, the quotient ring $\mathcal{O}_\mathfrak{p}/\mathfrak{p}^l\mathcal{O}_\mathfrak{p}$ is a principal ideal ring. Now the claim follows as $\mathcal{O}/\mathfrak{p}^l$ and $\mathcal{O}_\mathfrak{p}/\mathfrak{p}^l\mathcal{O}_\mathfrak{p}$ are isomorphic rings. In fact, the quotient ring has even more structure.

Recall that a pair (R, φ) consisting of a commutative ring R and a function $\varphi\colon R\backslash\{0\} \to \mathbf{Z}_{\geq 0}$ is called a *Euclidean ring*, if the following property is satisfied: For all $a, b \in R, b \neq 0$ there exist $q, r \in R$ such that

$$a = qb + r \text{ with } \varphi(r) < \varphi(b) \text{ or } r = 0. \tag{1.1}$$

In this case φ is called the *Euclidean function* of this Euclidean ring and (1.1) is called *Euclidean division.*

Remark 1.2. This is not *the* definition of a Euclidean ring but one that suits our purpose. We refer the interested reader to [AF95] for an overview of different definitions and connections between them.

The fact that $\mathcal{O}/\mathfrak{m}$ is a Euclidean ring has also been shown by Fletcher in [Fle71]. The main goal of this section is the description of this Euclidean structure with some minor modifications to the arguments of Fletcher. The first step is the definition of the Euclidean structure in case $\mathfrak{m}$ is a prime ideal power $\mathfrak{p}^l$, exploiting the special properties of the ring $\mathcal{O}/\mathfrak{p}^l$. Finally it is shown that the direct product of these rings is again a Euclidean ring.

Let us recall some facts about the residue ring $\mathcal{O}/\mathfrak{p}^l$, where $\mathfrak{p}^l$ is a prime ideal power. Denote by π an element of $\mathfrak{p}\backslash\mathfrak{p}^2$ (such an element is called a $\mathfrak{p}$-*uniformizer*). The ring $\mathcal{O}/\mathfrak{p}^l$ is a *special principal ideal ring*, that is, a principal ideal ring with unique maximal ideal which is in addition nilpotent. Consequently every ideal is of the form $(\overline{\pi}^k)$ with $0 \leq k \leq l$.

Fixing a set S of coset representatives of $\mathcal{O}$ modulo $\mathfrak{p}$, it is well known that every element $\overline{a}$ of $\mathcal{O}/\mathfrak{p}^l$ can be uniquely written in the form $\overline{a} = \sum_{i=0}^{l-1} \overline{s}_i\overline{\pi}^i$ with $s_i \in S$. Moreover $\overline{a}$ is invertible if and only if s_0 is a unit modulo $\mathfrak{p}$. Using this representation it is easy to compute the cardinality of various objects associated to $\mathcal{O}/\mathfrak{p}^l$.

Lemma 1.3. Let $0 \leq k \leq l$. Then the following hold:
(i) $\#(\mathcal{O}/\mathfrak{p}^l)^\times = \mathbf{N}(\mathfrak{p})^{l-1}(\mathbf{N}(\mathfrak{p}) - 1)$.
(ii) $\#(\overline{\pi}^k) = \mathbf{N}(\mathfrak{p})^{l-k}$.
(iii) If $\mathfrak{a}$ is an ideal of $\mathcal{O}$, then $\overline{\mathfrak{a}} = (\overline{\pi}^{\min(v_\mathfrak{p}(\mathfrak{a}),l)})$ and $\#\overline{\mathfrak{a}} = \mathbf{N}(\mathfrak{p})^{l-\min(v_\mathfrak{p}(\mathfrak{a}),l)}$.
(iv) The number of elements $\alpha \in (\mathcal{O}/\mathfrak{p}^l)$ with $(\alpha) = (\overline{\pi}^k)$ is $\mathbf{N}(\mathfrak{p})^{l-k-1}(\mathbf{N}(\mathfrak{p}) - 1)$ if $0 \leq k < l$ and 1 if $k \geq l$.

Proof. We let S be as in the preceding discussion and assume that $0 \in S$.
(i): Since $\#S = \mathbf{N}(\mathfrak{p})$ and $\overline{a} = \sum_{i=0}^{l-1} \overline{s}_i\overline{\pi}^i$ is a unit if and only if $s_0 \in S\backslash\{0\}$ the result follows.
(ii): Every element of $(\overline{\pi}^k)$ can be uniquely written in the form $\sum_{i=k}^{l-1} \overline{s}_i\overline{\pi}^i$ with $s_i \in S$.
(iii) and (iv): Follow from (i) and (ii). □

We now turn to the Euclidean structure of $\mathcal{O}/\mathfrak{p}^l$. The following result is essentially [Fle71, Proposition 7].

Lemma 1.4. Let

$$\varphi_\mathfrak{p}\colon (\mathcal{O}/\mathfrak{p}^l)\backslash\{\overline{0}\} \longrightarrow \mathbf{Z}_{\geq 0},\ \overline{a} \longmapsto \mathbf{N}(\mathfrak{p})^{v_\mathfrak{p}(a)}.$$

Then $(\mathcal{O}/\mathfrak{p}^k, \varphi_\mathfrak{p})$ is a Euclidean ring.

Proof. Since $\varphi_\mathfrak{p}$ is the composition of $\varphi'\colon (\mathcal{O}/\mathfrak{p}^l)\backslash\{\overline{0}\} \to \mathbf{Z}_{\geq 0}$, $\overline{a} \mapsto v_\mathfrak{p}(a)$ and the strictly increasing function $\mathbf{R}_{\geq 0} \to \mathbf{R}$, $x \mapsto \mathbf{N}(\mathfrak{p})^x$, it is sufficient to show that $(\mathcal{O}/\mathfrak{p}^l, \varphi')$ is a Euclidean ring. But this is already shown in [Fle71, Proposition 7]. For the sake of completeness we sketch the argument: The above representation of elements of $\mathcal{O}/\mathfrak{p}^l$ shows that every element $\overline{a}$ can be written as $\overline{u}_a\overline{\pi}^k$ for some unit $\overline{u}_a$ and integer k (in fact $k = v_\mathfrak{p}(a)$). If $\overline{a}$ and $\overline{b}$ are elements of $\mathcal{O}/\mathfrak{p}^l$ with $\overline{b} \neq \overline{0}$, then

$$\overline{a} = \begin{cases} \overline{0} \cdot \overline{b} + \overline{a}, & \text{if } v_\mathfrak{p}(a) < v_\mathfrak{p}(b), \\ \overline{u}_a\overline{u}_b^{-1}\overline{\pi}^{v_\mathfrak{p}(a)-v_\mathfrak{p}(b)} \cdot \overline{b} + \overline{0}, & \text{if } v_\mathfrak{p}(a) \geq v_\mathfrak{p}(b). \end{cases}$$

is a Euclidean division. □

We extend the function $\varphi_{\mathfrak{p}}$ of Lemma 1.4 to the whole of $\mathcal{O}/\mathfrak{p}^l$ by setting $\varphi_{\mathfrak{p}}(\overline{0}) = \mathbf{N}(\mathfrak{p})^l$. Thus for all $\overline{a} \in \mathcal{O}/\mathfrak{p}^l$ we have $\varphi_{\mathfrak{p}}(\overline{a}) = \mathbf{N}(\mathfrak{p})^{\min(v_{\mathfrak{p}}(a),l)}$. We can now put everything together. For each prime divisor $\mathfrak{p}$ of $\mathfrak{m}$ denote by $\varphi_{\mathfrak{p}} \colon \mathcal{O}/\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})} \to \mathbf{Z}$ the Euclidean function defined in Lemma 1.4 and by $\overline{a}_{\mathfrak{p}} \in \mathcal{O}/\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})}$ the $\mathfrak{p}$-component of an element $\overline{a} \in \mathcal{O}/\mathfrak{m}$ under the natural isomorphism $\mathcal{O}/\mathfrak{m} \cong \prod_{\mathfrak{p}\mid\mathfrak{m}}(\mathcal{O}/\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})})$.

Proposition 1.5. The ring $\mathcal{O}/\mathfrak{m}$ together with

$$\varphi\colon (\mathcal{O}/\mathfrak{m})\backslash\{\overline{0}\} \longrightarrow \mathbf{Z}_{\geq 0},\ \overline{a} \longmapsto \mathbf{N}((a,\mathfrak{m}))$$

is a Euclidean ring.

Proof. The proof of [Fle71, Proposition 6] shows that $\mathcal{O}/\mathfrak{m}$ is a Euclidean ring with Euclidean function $\sum_{\mathfrak{p}\mid\mathfrak{m}} \varphi_{\mathfrak{p}}(\overline{a}_{\mathfrak{p}})$. But it is easy to see that the proof remains valid if the sum is replaced by $f((\varphi_{\mathfrak{p}}(\overline{a}_{\mathfrak{p}}))_{\mathfrak{p}})$, where $f\colon \prod_{\mathfrak{p}\mid\mathfrak{m}} \mathbf{R} \to \mathbf{R}$ is any strictly increasing multivariate function. The result then follows by choosing f to be the product and noting that $\mathbf{N}((a,\mathfrak{m})) = \varphi(\overline{a}) = \prod_{\mathfrak{p}\mid\mathfrak{m}} \varphi_{\mathfrak{p}}(\overline{a}_{\mathfrak{p}})$. □

Example 1.6. Consider the rational integers $\mathbf{Z}$ and an ideal $N\mathbf{Z}$ thereof. For any integer $a \in \mathbf{Z}$ the value $\mathbf{N}((a, N\mathbf{Z}))$ is equal to $\gcd(a, N)$. Thus Proposition 1.4 shows that the ring $\mathbf{Z}/N\mathbf{Z}$ together with

$$\mathbf{Z}/N\mathbf{Z}\backslash\{\overline{0}\} \longrightarrow \mathbf{Z}_{>0},\ \overline{a} \longmapsto \gcd(a,N)$$

is a Euclidean ring. Note that $\mathbf{Z}/N\mathbf{Z}$ being the quotient of the Euclidean ring $\mathbf{Z}$, admits another Euclidean function:

$$\mathbf{Z}/N\mathbf{Z}\backslash\{\overline{0}\} \longrightarrow \mathbf{Z}_{>0},\ \overline{a} \longmapsto \min(\overline{a} \cap \mathbf{Z}_{>0}).$$

For this function the Euclidean division in $\mathbf{Z}/N\mathbf{Z}$ is then defined using lifting to $\mathbf{Z}$, Euclidean division in $\mathbf{Z}$ and projection back to $\mathbf{Z}/N\mathbf{Z}$.

Remark 1.7. Note that due to the presence of zero-divisors the division in $\mathcal{O}/\mathfrak{m}$ is not unique. To illustrate the occurring pitfalls we consider an example in $\mathbf{Z}/30\mathbf{Z}$. It is easy to see that $\overline{a} = \overline{6}$ and $\overline{b} = \overline{10}$ satisfy $(\overline{a}, \overline{b}) = (\overline{g})$ with $g = \overline{2}$. This shows that $\overline{g}$ is a greatest common divisor of $\overline{a}$ and $\overline{b}$. We now want to divide by $\overline{g}$: While the equations $\overline{g} \cdot \overline{18} = \overline{a}$ and $\overline{g} \cdot \overline{20} = \overline{b}$ show that $\overline{18}$ and $\overline{20}$ are valid quotients, they are not coprime in $\mathbf{Z}/30\mathbf{Z}$ as $(\overline{18}, \overline{20}) = (\overline{2})$. This is in total contrast to the situation of integral domains, where dividing by a greatest common divisor produces coprime elements. Nevertheless we can try to find coprime quotients by choosing different ones. Now $\overline{g} \cdot \overline{3} = \overline{a}$ and $\overline{g} \cdot \overline{5} = \overline{b}$ show that $\overline{3}$ and $\overline{5}$ will also do and they are fortunately coprime in $\mathbf{Z}/30\mathbf{Z}$.

The following proposition shows, that by choosing quotients with Euclidean function as small as possible, it is always possible to produce coprime elements.

Proposition 1.8. We set $\varphi = \varphi_{\mathfrak{m}}$. Let $\overline{a}, \overline{b} \in \mathcal{O}/\mathfrak{m}$. Then the following holds:

(i) The element $\overline{b}$ divides $\overline{a}$ if and only if $(a,\mathfrak{m})(b,\mathfrak{m})^{-1}$ is an integral ideal.

(ii) An element $\overline{c} \in \mathcal{O}/\mathfrak{m}$ satisfies $\overline{b}\overline{c} = \overline{a}$ if and only if $(c,\mathfrak{m}) \subseteq (a,\mathfrak{m})(b,\mathfrak{m})^{-1}$.

(iii) If $\overline{c} \in \mathcal{O}/\mathfrak{m}$ satisfies $\overline{b}\overline{c} = \overline{a}$, then $\varphi(\overline{a})/\varphi(\overline{b})$ divides $\varphi(\overline{c})$.

(iv) Let $\overline{c} \in \mathcal{O}/\mathfrak{m}$ such that $\overline{b}\overline{c} = \overline{a}$. Then $\varphi(\overline{a})/\varphi(\overline{b}) = \varphi(\overline{c})$ is equivalent to $(\overline{c}) = \overline{(a,\mathfrak{m})(b,\mathfrak{m})^{-1}}$.

(v) Let $\overline{g} \in \mathcal{O}/\mathfrak{m}$ be a greatest common divisor of $\overline{a}, \overline{b}$, that is, $(\overline{g}) = (\overline{a}, \overline{b})$. Assume that $\overline{e}, \overline{f}$ are elements of $\mathcal{O}/\mathfrak{m}$ such that $\overline{e}\overline{g} = \overline{a}$, $\overline{f}\overline{g} = \overline{b}$, $\varphi(\overline{e}) = \varphi(\overline{a})/\varphi(\overline{g})$ and $\varphi(\overline{f}) = \varphi(\overline{b})/\varphi(\overline{g})$. Then $\overline{e}$ and $\overline{f}$ are coprime, that is, $(\overline{e}, \overline{f}) = \mathcal{O}/\mathfrak{m}$.

Proof. (i): This follows from the fact that $\overline{b} \mid \overline{a}$ is equivalent to $\overline{b}_{\mathfrak{p}} \mid \overline{a}_{\mathfrak{p}}$ for all prime divisors $\mathfrak{p}$ of $\mathfrak{m}$.

(ii): For each prime divisor $\mathfrak{p}$ of $\mathfrak{m}$ we have $\overline{b}_{\mathfrak{p}}\overline{c}_{\mathfrak{p}} = \overline{a}_{\mathfrak{p}}$. If $\overline{a}_{\mathfrak{p}} \neq 0$ (and therefore $\overline{b}_{\mathfrak{p}} \neq 0$) this is equivalent to $v_{\mathfrak{p}}(c) = v_{\mathfrak{p}}(a) - v_{\mathfrak{p}}(b) = v_{\mathfrak{p}}((a,\mathfrak{m})(b,\mathfrak{m})^{-1})$. If $\overline{a}_{\mathfrak{p}} = \overline{b}_{\mathfrak{p}} = 0$ then this is equivalent to $v_{\mathfrak{p}}(c) \geq 0 = v_{\mathfrak{p}}((a,\mathfrak{m})(b,\mathfrak{m})^{-1})$. If $\overline{a}_{\mathfrak{p}} = 0$ and $\overline{b}_{\mathfrak{p}} \neq 0$, then this is equivalent to $v_{\mathfrak{p}}(c) \geq v_{\mathfrak{p}}(\mathfrak{m}) - v_{\mathfrak{p}}(b) = v_{\mathfrak{p}}((a,\mathfrak{m})(b,\mathfrak{m})^{-1})$. Now the claim follows.

(iii) and (iv): This follows from (ii).

(v): Note that $(g,\mathfrak{m}) = (a,b,\mathfrak{m})$. By (ii) the assumption on the Euclidean function implies $(e,\mathfrak{m}) = (a,\mathfrak{m})(a,b,\mathfrak{m})^{-1}$ and $(f,\mathfrak{m}) = (b,\mathfrak{m})(a,b,\mathfrak{m})^{-1}$. From this one deduces that $(e,f,\mathfrak{m}) = \mathcal{O}$, that is, $(\overline{e}, \overline{f}) = \mathcal{O}/\mathfrak{m}$. □

§1B. Modules and normal forms

In this section we will recall the basic theory of modules and matrix normal forms over various rings. References for this section are [Bou03, Chapter VII] (Modules over principal ideal domains), [Coh00, Chapter 1] (Modules and normal forms over Dedekind domains) as well as [Sto00] (Normal forms over principal ideal rings and principal ideal domains). Throughout this section, we will make use of the following notation to obtain unique representatives for various equivalence relations. For a ring R, we denote by $\mathrm{A}(R)$ a complete set of equivalence class representatives with respect to $\sim$, where for $a, b \in R$ we define $a \sim b$, if and only if $a = ub$ for some unit $u \in R^\times$. For every ideal $\mathfrak{a} \subseteq R$ we fix a complete set of coset representatives of $R/\mathfrak{a}$ and denote it by $\mathrm{Rs}(\mathfrak{a})$. In case $\mathfrak{a} = (r)$ is principal with $r \in R$, we write $\mathrm{Rs}(r)$ instead of $\mathrm{Rs}(\mathfrak{a})$.

Principal ideal domains. For principal ideal domains, the theory of finitely generated modules is as simple as it can be:

Theorem and Definition 1.9. Let R be a principal ideal domain and M a finitely generated R-module.

(i) There exists a unique integer $r \in \mathbf{Z}_{\geq 0}$ such that $M \cong R^r \oplus M_{\mathrm{tor}}$. The number r is called the *rank* of M.

(ii) If M is a submodule of a free R-module of rank r, then M is free of rank $\leq r$.

(iii) If M is torsion, then there exist elements $r_1, \dots, r_l \in R$ such that $M \cong \prod_{i=1}^{l} R/r_iR$.

(iv) If N is a R-submodule of M such that M and N have the same rank, then there exist elements $r_1, \dots, r_l \in R$ such that $M/N \cong \prod_{i=1}^{l} R/r_iR$. The ideal $r_1 \cdots r_l R$ is independent of the chosen decomposition. We call it the *index ideal* of N in M and denote it by $(M : N)$.

Remark 1.10. The index ideal obeys the same rules as the ordinary index. Moreover, in case R is residually finite (this means that non-trivial quotients of R are finite), we have $\#R/(M : N) = |M : N|$

To establish the connection to matrix normal forms, consider a $\mathbf{Z}$-module $M \subseteq \mathbf{Z}^m$, which is—as it is often the case in applications—described by a set of generators $A_1, \dots, A_n \in \mathbf{Z}^m$. Using these generators as rows of a matrix $A \in \mathrm{Mat}_{n\times m}(\mathbf{Z})$, the module M is thus determined by A. While in this way we can represent M with its infinitely many elements using only finite space, this way of representing M raises various questions:

(i) Assume that the number of generators is much larger than m. By Lemma 1.9 we know that the module M is a free module of rank at most m. Thus by theory we know that there exists a matrix $A' \in \mathrm{Mat}_{k\times m}(\mathbf{Z})$ with $1 \leq k \leq m$ such that M is generated by the rows of A'. How can we obtain such an A' given A?

(ii) Assume that N is a second $\mathbf{Z}$-module $N \subseteq \mathbf{Z}^m$ which is determined by a matrix $B \in \mathrm{Mat}_{l\times m}(\mathbf{Z})$. How can we decide if $M = N$? How to find generators of the $\mathbf{Z}$-modules $M \cap N$, $M + N$?

This is where the theory of matrix normal forms comes into play: Associated to M or A respectively there exists a unique $\mathbf{Z}$-matrix H with rows spanning M such that certain minimality conditions are satisfied. More importantly there exist algorithms for computing H given A. While the minimality condition will solve question (i), the uniqueness will us help with (ii).

Definition 1.11 (Hermite normal form, [Coh93, 2.4]). Let R be a principal ideal domain. A matrix $H = (h_{ij})_{ij} \in \mathrm{Mat}_{m\times n}(R)$ with r nonzero rows is in *Hermite normal form*, if and only if the following hold:

(i) The first r rows of H are nonzero. For $1 \leq i \leq r$ let h_{i,j_i} be the last nonzero entry in row i. Then $1 \leq j_1 < j_2 < \cdots < j_r \leq m$.

(ii) We have $h_{i,j_i} \in \mathrm{A}(R)$ and $h_{k,i_j} \in \mathrm{Rs}(h_{i,j_i})$ for $1 \leq i < k \leq r$.

Example 1.12. Consider the ring $R = \mathbf{Z}$ together with $\mathrm{A}(\mathbf{Z}) = \mathbf{Z}_{\geq 0}$ and $\mathrm{Rs}(n) = \{0, 1, \dots, n-1\}$ for $n \in \mathbf{Z}_{>0}$. Then one easily checks that of the following matrices,

$$A = \begin{pmatrix} 5 & 0 & 0 & 0 \\ 2 & 3 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 2 & 2 & 2 & 1 \end{pmatrix} \in \mathrm{Mat}_{4\times 4}(\mathbf{Z}), \quad B = \begin{pmatrix} 5 & 0 & 0 & 0 \\ 2 & 3 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{Mat}_{4\times 4}(\mathbf{Z}),$$

the matrix B is in Hermite normal form, while A is not.

Theorem and Definition 1.13. Let R be a principal ideal domain and $A \in \mathrm{Mat}_{n\times m}(R)$. Then there exists a unique matrix $H \in \mathrm{Mat}_{n\times m}(R)$ in Hermite normal form and a unimodular matrix $U \in \mathrm{GL}_n(R)$ such that $UA = H$. We call H the *Hermite normal form of A*.

Example 1.14. Consider again the matrix A of Example 1.12. Then the equation

$$\underbrace{\begin{pmatrix}1&0&0&0\\0&1&-1&0\\0&0&1&0\\0&0&-2&1\end{pmatrix}}_{=U}\cdot A=\begin{pmatrix}1&0&0&0\\0&1&-1&0\\0&0&1&0\\0&0&-2&1\end{pmatrix}\cdot\begin{pmatrix}5&0&0&0\\2&3&1&0\\1&1&1&0\\2&2&2&1\end{pmatrix}=\underbrace{\begin{pmatrix}5&0&0&0\\1&2&0&0\\1&1&1&0\\0&0&0&1\end{pmatrix}}_{=H}$$

together with the fact that $U \in \mathrm{GL}_4(\mathbf{Z})$ shows that H is the Hermite normal form of A.

Principal ideal rings. In case the underlying ring is only a principal ideal ring, that is, zero-divisors may be present, the theory gets more interesting. For residue rings of the form $\mathbf{Z}/N\mathbf{Z}$, $N \in \mathbf{Z}_{>0}$, the idea of attaching a unique matrix normal form to submodules of $(\mathbf{Z}/N\mathbf{Z})^m$ goes back to Howell [How86]. In [Sto00], Storjohann extended this idea to all principal ideal rings. Recall that for a matrix $A \in \mathrm{Mat}_{n\times m}(R)$ we denote by $\mathrm{sp}(A)$ the R-submodule of R^m which is spanned by the rows of A and for $1 \leq j \leq n$, we denote by $\mathrm{sp}_j(A)$ the module $\{(v_1,\dots,v_m) \in \mathrm{sp}(A) \mid v_m = v_{m-1} = \dots = v_{m-j+1} = 0\}$.

Definition 1.15 (Howell normal form). Let R be a principal ideal ring and $H \in \mathrm{Mat}_{m\times n}(R)$ a matrix with r nonzero rows. We say that H is in *Howell normal form*, if and only if the following hold:

(i) The first r rows are nonzero. For $1 \leq i \leq r$ let h_{i,j_i} the last nonzero entry in row i. Then $1 \leq j_1 < j_2 < \dots < j_r \leq m$.

(ii) We have $h_{i,j_i} \in \mathrm{A}(R)$ and $h_{k,j_i} \in \mathrm{Rs}(h_{i,j_i})$ for $1 \leq k < i \leq r$.

(iii) For $1 \leq i \leq r$ the rows $1,\dots,r-i+1$ generate $\mathrm{sp}_{n-j_i+1}(H)$.

Example 1.16. Consider the ring $R = \mathbf{Z}/12\mathbf{Z}$. To illustrate the Howell normal form, let us first look at an example which is not in Howell normal form. The matrix

$$A=\begin{pmatrix}\overline{1}&\overline{0}&\overline{0}\\\overline{0}&\overline{1}&\overline{4}\\\overline{0}&\overline{0}&\overline{0}\end{pmatrix}$$

is in row echelon form, so clearly satisfies property (i). By choosing $\mathrm{A}(R)$ and $\mathrm{Rs}(r)$ appropriately we may also assume that A satisfies (ii). But it does not satisfy (iii): We have $j_1 = 1$ and $j_2 = 3$. Multiplying the second row with $\overline{3}$, we obtain the element $(\overline{0}\ \overline{3}\ \overline{0}) \in \mathrm{sp}_1(A) = \mathrm{sp}_{3-j_2+1}(A)$. If A would be in Howell normal form, then $(\overline{0}\ \overline{3}\ \overline{0})$ would need to be in the span of the first row, which it clearly is not. On the other hand, just replacing the last row of A with $(\overline{0}\ \overline{3}\ \overline{0})$ and permuting the rows yields the matrix

$$\begin{pmatrix}\overline{1}&\overline{0}&\overline{0}\\\overline{0}&\overline{3}&\overline{0}\\\overline{0}&\overline{1}&\overline{4}\end{pmatrix},$$

which now satisfies (ii) and (iii), that is, the matrix is in Howell normal form.

In [Sto00], the following is proven.

Theorem and Definition 1.17. Let R be a principal ideal ring and $A \in \mathrm{Mat}_{m\times n}(R)$. Then there exists a unique matrix $H \in \mathrm{Mat}_{m\times n}(R)$ in Howell normal form such that $\mathrm{sp}(A) = \mathrm{sp}(H)$. The matrix H is called the *Howell normal form* of A.

Example 1.18. In Example 1.16 we, starting with the matrix

$$A=\begin{pmatrix}\overline{1}&\overline{0}&\overline{0}\\\overline{0}&\overline{1}&\overline{4}\\\overline{0}&\overline{0}&\overline{0}\end{pmatrix},$$

after various transformation obtained the matrix

$$\begin{pmatrix}\overline{1}&\overline{0}&\overline{0}\\\overline{0}&\overline{3}&\overline{0}\\\overline{0}&\overline{1}&\overline{4}\end{pmatrix}$$

which is in Howell normal form. Since the operations we applied did not change the span, the matrix H is in fact the Howell normal form of A.

Theorem and Definition 1.19. Let R be a principal ideal ring and $A \in \operatorname{Mat}_{n\times m}(R)$. Then there exist unimodular matrices $U \in \operatorname{GL}_n(R)$, $V \in \operatorname{GL}_m(R)$ and nonzero elements $s_1, \dots, s_r \in R$ such that s_i divides s_{i+1} for $1 \le i \le r-1$ and

$$UAV = \begin{pmatrix} s_1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & & \vdots \\ \vdots & \ddots & s_r & \ddots & & \vdots \\ \vdots & & \ddots & 0 & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 & 0 \end{pmatrix}.$$

The matrix UAV is called a *Smith normal form of A* and $s_1, \dots, s_r$ are called the *elementary divisors of A*. The elementary divisors are unique up to multiplication by units (see [Kap49, Theorem 9.3]).

Example 1.20. Consider the ring $R = \mathbf{Z}$ and the matrix

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \in \operatorname{Mat}_{3\times 3}(\mathbf{Z}).$$

Then the equation

$$\underbrace{\begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 1 & -2 & 1 \end{pmatrix}}_{=U} \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \underbrace{\begin{pmatrix} -1 & 1 & 1 \\ 1 & 1 & -2 \\ 0 & -1 & 1 \end{pmatrix}}_{=V} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

together with the fact that $U, V \in \operatorname{GL}_3(\mathbf{Z})$ shows that $\operatorname{diag}(1, 3, 0)$ is a Smith normal form of A.

Dedekind domains. We now consider the situation where the underlying ring R is a Dedekind domain.

Theorem and Definition 1.21 ([CR81, §4D], [Coh00, Chapter 1]). Let R be a Dedekind domain with field of fractions K and M, N finitely generated R-modules. Then the following hold:

(i) If M is torsion-free, then M is projective.

(ii) There exists a finitely generated projective R-module P such that $M \cong P \oplus M_{\mathrm{tor}}$. The dimension $\dim_K(K \otimes_R M)$ is called the *rank* of M and denoted by $\operatorname{rk}(M)$.

(iii) If M is torsion-free, then there exist fractional ideals $\mathfrak{a}_i$ of K and elements $v_i \in KM$ such that

$$M = \mathfrak{a}_1 v_1 \oplus \mathfrak{a}_2 v_2 \oplus \cdots \oplus \mathfrak{a}_n v_n.$$

The class of $\mathfrak{a}_1 \cdots \mathfrak{a}_n$ in Cl_R is independent of the chosen decomposition. We call it the *(Steinitz) class of M* and denote it by $\operatorname{cl}(M)$.

(iv) If M and N are torsion-free, then $M \cong N$ if and only if $\operatorname{rk}(M) = \operatorname{rk}(N)$ and $\operatorname{cl}(M) = \operatorname{cl}(N)$.

(v) If M is torsion-free, then M is a free R-module if and only if $\operatorname{cl}(M) = 1$.

(vi) If N is a submodule of M such that M and N are torsion-free and have the same rank, then there exist integral ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_l$ such that $M/N \cong \prod_{i=1}^{l} R/\mathfrak{a}_i$. The ideal $\mathfrak{a}_1 \cdots \mathfrak{a}_l$ is independent of the chosen decomposition. We call it the *index ideal* of N in M and denote it by $(M : N)$.

(vii) If N is an R-submodule of M such that M and N are torsion-free and have the same rank, then $\operatorname{cl}(N) = [(M : N)] \cdot \operatorname{cl}(M)$.

(viii) If M is torsion-free, then $M = \bigcap_{0 \ne \mathfrak{p} \in \operatorname{Spec}(R)} (KM \cap M_{\mathfrak{p}})$.

(ix) Assume that $\mathfrak{p}$ is a nonzero prime ideal of R and N is a submodule of M such that M and N are torsion-free and have the same rank. Then $(M : N)_{\mathfrak{p}} = (M_{\mathfrak{p}} : N_{\mathfrak{p}})$.

Already the presence of non-principal ideals implies that finitely generated torsion-free R-modules won't in general be free anymore. For this reason the connection between finitely generated torsion-free modules and matrix normal forms is more subtle than in the principal ideal domain case. While for any R-module $M \subseteq R^m$ there exists—due to M being finitely generated—some matrix $A \in \operatorname{Mat}_{m\times n}(R)$ such that $\operatorname{sp}(A) = M$, we cannot expect to find a triangular shaped matrix with this property. For if this is the case, M is the direct sum of the free R-modules spanned by the rows of A and therefore free itself. To work with R-modules and matrix normal forms over R, Cohen [Coh96] has introduced the notion of pseudo-objects.

Definition 1.22 (Pseudo-generating set and pseudo-basis). Let R be a Dedekind domain with field of fractions K, M a finitely generated torsion-free R-module and $V = KM$. A pair $((\mathfrak{a}_i),(v_i))$ consisting of a family of fractional ideals $\mathfrak{a}_i$ of K and elements $v_i \in V$ with $\sum_{i=1}^{n} \mathfrak{a}_i v_i = M$ is called a *pseudo-generating set of* M. In case $M = \mathfrak{a}_1 v_1 \oplus \mathfrak{a}_2 v_2 \oplus \cdots \oplus \mathfrak{a}_n v_n$, we call $((\mathfrak{a}_i),(v_i))$ a *pseudo-basis* of M. Note that if $((\mathfrak{a}_i),(v_i))$ is a pseudo-basis of M, then (v_i) is necessarily a K-basis of V. For a nonzero prime ideal $\mathfrak{p}$ of R we call the pseudo-basis $((\mathfrak{a}_i),(v_i))$ $\mathfrak{p}$-*free*, if the coefficient ideals $\mathfrak{a}_1,\dots,\mathfrak{a}_n$ have non-negative $\mathfrak{p}$-adic valuation.

Theorem 1.21 shows that every finitely generated torsion-free module over a Dedekind domain has a pseudo-basis.

Definition 1.23 (Pseudo-matrix). Let R be a Dedekind domain with field of fractions K. A pair $\mathcal{A} = ((\mathfrak{a}_i), A)$ consisting of a family $(\mathfrak{a}_i)_{1\leq i\leq m}$ of fractional ideals of K and a matrix $A \in \mathrm{Mat}_{m\times n}(K)$ is called a *pseudo-matrix*. The ideals $\mathfrak{a}_i$, $1 \leq i \leq m$, are called the *coefficient ideals* of the pseudo-matrix. We call $\mathcal{A}$ a *square pseudo-matrix* if A is a square matrix. The rank $\mathrm{rk}(\mathrm{sp}(\mathcal{A}))$ is called the *rank* of $\mathcal{A}$. We say that $\mathcal{A}$ has *full rank* if the rank of $\mathcal{A}$ equals n. In this case we define the *determinantal ideal* of $\mathcal{A}$ to be the ideal $\det(A)\cdot \mathfrak{a}_1 \cdots \mathfrak{a}_m$ and denote it by $\det(\mathcal{A})$. The *span* of the pseudo-matrix $\mathcal{A}$ is defined to be $\mathrm{sp}(\mathcal{A}) = \mathfrak{a}_1 A_1 + \cdots + \mathfrak{a}_m A_m \subseteq K^n$, where $A_1,\dots,A_m$ are the rows of A. The pseudo-matrix $\mathcal{A}$ is called *nice*, if and only if $\mathrm{sp}(\mathcal{A}) = \mathfrak{a}_1 A_1 \oplus \cdots \oplus \mathfrak{a}_m A_m$. (Thus a pseudo-matrix $((\mathfrak{a}_i), A)$ is nice if and only if $((\mathfrak{a}_i),(A_i))$ is a pseudo-basis of $\mathrm{sp}((\mathfrak{a}_i), A)$.)

Remark 1.24. Let R be a Dedekind domain with field of fractions K and $((\mathfrak{a}_i), A)$ a pseudo-matrix with $A \in \mathrm{Mat}_{m\times n}(K)$. Then the pseudo-matrix is usually denoted in the following way:

$$\begin{array}{c} \mathfrak{a}_1 \\ \mathfrak{a}_2 \\ \vdots \\ \mathfrak{a}_m \end{array} \left(\begin{array}{c} A_1 \\ \hline A_2 \\ \hline \vdots \\ \hline A_m \end{array} \right),$$

where $A_1,\dots,A_m$ are the rows of A.

Example 1.25. Let R be a Dedekind domain, $\mathfrak{a}$ a non-principal ideal of R, and $e_1, e_2 \in R^2$ the standard basis of R^2. We consider the R-module $M = \mathfrak{a}e_1 \oplus \mathfrak{a}e_2$. Because $\mathfrak{a}$ is non-principal, there does not exist a matrix $A \in \mathrm{Mat}_{2\times 2}(R)$ such that $\mathrm{sp}(A) = M$. On the other hand, the pseudo-matrix

$$\begin{array}{c} \mathfrak{a} \\ \mathfrak{a} \end{array} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

is nice and does have span M.

Using the theory of pseudo-matrices, the problem of computing a pseudo-basis given a (pseudo-)generating set translates to the problem of computing a nice pseudo-matrix given any pseudo-matrix. Note that a pseudo-matrix $((\mathfrak{a}_i), A)$ is nice if A is of triangular shape. The problem of computing a nice pseudo-matrix goes back to Bosma and Pohst [BP91], but can also be found in O'Meara's theory of adapted bases [O'M63, §81] (although he never mentions "computation" or "algorithm"). Based on similar ideas, Cohen introduced in [Coh96] the notion of a pseudo-Hermite normal form—similar to the Hermite normal form over principal ideal domains.

Theorem and Definition 1.26 (Pseudo-Hermite normal form). Let R be a Dedekind domain with field of fractions K and $\mathcal{A} = ((\mathfrak{a}_i), A)$ a pseudo-matrix with $A = (a_{ij}) \in \mathrm{Mat}_{m\times n}(R)$ such that A has r nonzero rows. We say that $\mathcal{A}$ is in *pseudo-Hermite normal form*, if and only if the following hold:

(i) The first r rows of A are nonzero. For $1 \leq i \leq r$ let a_{i,j_i} be the the last nonzero entry in row i. Then $1 \leq j_1 < j_2 < \cdots < j_r \leq m$.

(ii) We have $a_{i,j_i} = 1$ for $1 \leq i < k \leq r$.

By [Coh96, Theorem 2.5], there exists a pseudo-matrix $\mathcal{H}$ in pseudo-Hermite normal form with the same span as $\mathcal{A}$. We call $\mathcal{H}$ a *pseudo-Hermite normal form* of $\mathcal{A}$ or $\mathrm{sp}(\mathcal{A})$.

Remark 1.27.

(i) The pseudo-Hermite normal form can be made unique adding reduction requirements similar to the second item of the Hermite normal form definition (see [Coh96]). Since ensuring uniqueness is not an obstacle from a computational point of view, we decided to not include uniqueness here.

(ii) Restriction to principal ideal domains and discarding the coefficient ideals does *not* recover the Hermite normal form in Definition 1.11: If $((\mathfrak{a}_i), A)$ is the pseudo-Hermite normal form of a $\mathbf{Z}$-module M, then A will in general not be a Hermite normal form of M. This is due to the different normalizations of the pivot elements. For pseudo-Hermite normal forms they are always 1, while for the Hermite normal form they can be anything. The most simple example is the $\mathbf{Z}$-module $2\mathbf{Z}$ with Hermite normal form $\begin{pmatrix} 2 \end{pmatrix} \in \mathrm{Mat}_{1\times 1}(\mathbf{Z})$ and pseudo-Hermite normal form $((2\mathbf{Z}), \begin{pmatrix} 1 \end{pmatrix})$.

Definition 1.28. Let R be a Dedekind domain with field of fractions K and $M \subseteq R^n$ an R-module. An integral ideal $\mathfrak{m}$ of K is called an *admissible modulus* for M if and only if $\mathfrak{m}R^n \subseteq M$.

Lemma 1.29. Let R be a Dedekind domain and $M \subseteq R^n$ an R-module. The following hold:

(i) There exists an admissible modulus $\mathfrak{m}$ for M if and only if M has rank n.

(ii) If M has rank n, then the index ideal $(R^n : M)$ is an admissible modulus for M.

(iii) Assume that M has rank n and $\mathcal{A}$ is a square pseudo-matrix with span M. Then $\det(\mathcal{A})$ is an admissible modulus for M.

Proof. (i): If $\mathfrak{m}$ is an admissible modulus for M, then $\mathfrak{m}R^n \subseteq M \subseteq R^n$. Hence M has rank n. The other direction follows from (ii).

(ii): Let $\mathfrak{m} = [R^n : M]$. By Theorem 1.21 we can write $R^n/M \cong \prod_{i=1}^m R/\mathfrak{a}_i$ for nonzero ideals $\mathfrak{a}_i$ of R and we know that $\mathfrak{m} = \mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_m$. Since $\mathfrak{m} \subseteq \mathfrak{a}_i$ for all $1 \le i \le m$, we know that $\mathfrak{m}$ annihilates $\prod_{i=1}^m R/\mathfrak{a}_i$. Hence $\mathfrak{m}R^n \subseteq M$.

(iii): This is [Hop98, Proposition 4.8.3]. □

Theorem and Definition 1.30 (Pseudo-Smith normal form, [Coh00, 1.7]). Let R be a Dedekind domain with field of fractions K, $A \in \mathrm{Mat}_{n\times m}(K)$ a matrix and $(\mathfrak{a}_i)_{1\le i\le n}$, $(\mathfrak{b}_j)_{1\le j\le m}$ fractional ideals of K such that $a_{ij} \in \mathfrak{a}_i\mathfrak{b}_j^{-1}$ for $1 \le i \le n$, $1 \le j \le m$. Then there exist fractional ideals $(\mathfrak{a}_i')_{1\le i\le n}$, $(\mathfrak{b}_j')_{1\le j\le m}$ of K and matrices $U = (u_{ij})_{i,j} \in \mathrm{GL}_n(K)$, $V = (v_{ij})_{i,j} \in \mathrm{GL}_m(K)$ with the following properties:

(i) $\prod_{i=1}^n \mathfrak{a}_i = \det(U)\prod_{i=1}^n \mathfrak{a}_i'$ and $\prod_{j=1}^m \mathfrak{b}_j' = \det(V)\prod_{j=1}^m \mathfrak{b}_j$,

(ii) there exists $r \in \mathbf{Z}_{\ge 0}$ such that

$$UAV = \left(\begin{array}{c|c} \mathbf{1}_r & \mathbf{0}_{r,m-r} \\ \hline \mathbf{0}_{n-r,r} & \mathbf{0}_{n-r,m-r} \end{array}\right),$$

(iii) the ideals $\mathfrak{a}_i'(\mathfrak{b}_i')^{-1}$, $1 \le i \le r$, are integral ,

(iv) we have $u_{ij} \in \mathfrak{a}_i\mathfrak{a}_j'^{-1}$ and $v_{ij} \in \mathfrak{b}_i'\mathfrak{b}_j^{-1}$.

We call the triple $(UAV, (\mathfrak{a}_i')_i, (\mathfrak{b}_j')_j)$ a *pseudo-Smith normal form of* $(A, (\mathfrak{a}_i), (\mathfrak{b}_i))$.

Remark 1.31. While we have stated only the existence theorems for matrix normal forms over principal ideal domains, principal ideal rings and Dedekind domains, all theorems admit constructive proofs. That is, as soon as the underlying ring supports certain basic operations, there exist (efficient) algorithms for computing matrix normal forms. For the case of principal ideal domains and principal ideal rings we refer the reader to [Sto00]. The more recent topic of normal forms of modules over Dedekind domains will be covered in Chapter 2.

Saturation of modules. We end this section with an application of the (pseudo-)Smith normal form to the computation of saturations.

Definition 1.32. Let R be an integral domain, M a free R-module and $N \subseteq M$ a submodule. We call N *saturated (in M)*, if and only if for all $r \in R$, $r \ne 0$, and $m \in M$ the inclusion $rm \in N$ implies $m \in N$. The minimal R-module L which is saturated in M and which satisfies $N \subseteq L \subseteq M$ is called the *saturation of N in M*.

Lemma 1.33. Let R be an integral domain with field of fractions K. Assume that N is an R-submodule of a finitely generated torsion-free R-module M. Then the following hold:

(i) The module N is saturated in M if and only if M/N is torsion-free.

(ii) Assume that M and N are R-submodules of a free K-module. Then the saturation of N is $KN \cap M$.

Proof. (i): Assume that N is saturated in M. Consider $r \in R$, $\overline{m} \in M/N$ with $r\overline{m} = \overline{0}$. Then $\overline{rm} = \overline{0}$, that is, $rm \in N$. By assumption this implies $r = 0$ or $m \in N$, that is, $\overline{m} = \overline{0}$. Hence M/N is torsion-free.

Now let M/N be torsion-free. Consider $r \in R$, $r \ne 0$, $m \in M$ with $rm \in N$. Then $r\overline{m} = \overline{rm} = \overline{0}$, which by assumption implies $\overline{m} = \overline{0}$, that is, $m \in N$. Hence N is saturated in M.

(ii): We first show that $KN \cap M$ is saturated in M: Let $m \in M$ and assume that $rm \in KN \cap M$ for some $r \in R$, $r \neq 0$. We can write $rm = kn$ for some $n \in N$ and $k \in K$. Then $m = \frac{k}{r}n \in KN \cap M$. Thus $KN \cap M$ is saturated in M.
Now let $L \subseteq M$ be a saturated R-module with $N \subseteq L \subseteq M$. We want to show that $KN \cap M \subseteq L$. Let $kn \in KN \cap M$ with $k \in K$ and $n \in N$. By writing $k = \frac{r}{s}$ with $r, s \in R$ we obtain $kn = \frac{r}{s}n \in KN \cap M$. Then $kn \in M$ and $s(kn) = rn \in N \subseteq L$. Since L is saturated in M this implies $kn \in L$.

Lemma 1.34. Let R be a principal ideal domain and $M \subseteq R^k$ a free R-module of rank r with basis matrix $B \in \mathrm{Mat}_{r\times k}(R)$. Assume that $S = UBV$ is a Smith normal form of B, where $U \in \mathrm{GL}_r(R)$, $V \in \mathrm{GL}_k(R)$ are transformation matrices. Denote by $w_1, \dots, w_r$ the first r rows of V^{-1}. Then $w_1, \dots, w_r$ is an R-basis of the saturation of M in R^k.

Proof. Let $s_1, \dots, s_r$ be elementary divisors of B. We have $M = \mathrm{sp}(B) = \mathrm{sp}(UB) = \mathrm{sp}(SV^{-1}) = \bigoplus_{i=1}^{r} Rs_iw_i$. As $R^k = \bigoplus_{i=1}^{k} Rw_i$, the claim follows with Lemma 1.33. □

Lemma 1.35. Let R be a Dedekind domain with field of fractions K. Let N be an R-submodule of a finitely generated torsion-free R-module $M \subseteq K^k$. Denote the rank of M by m and the rank of N by n. Assume that $((\alpha_i)_{1\leq i\leq m}, (\mathfrak{a}_i)_{1\leq i\leq m})$ and $((\beta_i)_{1\leq i\leq n}, (\mathfrak{b}_i)_{1\leq i\leq n})$ are pseudo-bases of M and N respectively and that $A \in \mathrm{Mat}_{m\times n}(K)$ is the base change matrix with

$$(\beta_1, \beta_2, \dots, \beta_n) = (\alpha_1, \alpha_2, \dots, \alpha_m)A.$$

Let $(S, (\mathfrak{a}'_i)_{1\leq i\leq m}, (\mathfrak{b}'_i)_{1\leq i\leq n})$ be a pseudo-Smith normal form of $(A, (\mathfrak{a}_i)_{1\leq i\leq m}, (\mathfrak{b}_i)_{1\leq i\leq n})$ and $U \in \mathrm{GL}_m(K)$, $V \in \mathrm{GL}_n(K)$, transformation matrices. Consider the m elements $w_1, \dots, w_m$ definied by

$$(w_1, w_2, \dots, w_m) = (\alpha_1, \alpha_2, \dots, \alpha_m)U^{-1}.$$

Then $((w_i)_{1\leq i\leq n}, (\mathfrak{a}'_i)_{1\leq i\leq n})$ is a pseudo-basis of the saturation of N in M.

Proof. First note that because of the special shape of S we have

$$\begin{aligned}(w_1, w_2, \dots, w_n) &= (w_1, w_2, \dots, w_m)S \\ &= (\alpha_1, \alpha_2, \dots, \alpha_m)U^{-1}S \\ &= (\alpha_1, \alpha_2, \dots, \alpha_m)U^{-1}SV^{-1}V \\ &= (\alpha_1, \alpha_2, \dots, \alpha_m)AV \\ &= (\beta_1, \beta_2, \dots, \beta_n)V.\end{aligned}$$

The matrices U, V satisfy properties (iii) and (i) of Definition 1.30. Hence by [Coh00, Proposition 1.4.2] we know that $((w_i)_{1\leq i\leq m}, (\mathfrak{a}'_i)_{1\leq i\leq m})$ and $((w_i)_{1\leq i\leq n}, (\mathfrak{b}'_i)_{1\leq i\leq n})$ are pseudo-bases of M and N respectively. Thus

$$N = \bigoplus_{i=1}^{n} \mathfrak{b}'_iw_i \quad \text{and} \quad M = \bigoplus_{i=1}^{m} \mathfrak{a}'_iw_i = \bigoplus_{i=1}^{m} \mathfrak{b}'_i(\mathfrak{a}'_i\mathfrak{b}'_i)^{-1}w_i.$$

By Lemma 1.33 the saturation of N in M is $KN \cap M$, which is just $\bigoplus_{i=1}^{n} \mathfrak{a}'_iw_i$. □

Lemma 1.36. Let R be a principal ideal domain and $\mathfrak{a} \subseteq R$ an ideal. Assume that $A \in \mathrm{Mat}_{r\times k}(R)$ is a matrix with span $M \subseteq R^k$ and L is the saturation of M in R^k. Denote by $\overline{}$ the reduction modulo $\mathfrak{a}$ of elements of R as well as $\mathrm{Mat}_{r\times k}(R)$. Let $\hat{S} = \hat{U}\overline{A}\hat{V}$ be a Smith normal form of $\overline{A} \in \mathrm{Mat}_{r\times k}(R/\mathfrak{a})$ with elementary divisors $\overline{s}_1, \dots, \overline{s}_r$. Denote by $\overline{w}_1, \dots, \overline{w}_r$ the nonzero rows of $\hat{V}^{-1}$. Then

$$L/\mathfrak{a}L = \langle \overline{w}_1, \dots, w_r \rangle_{\mathcal{O}/\mathfrak{a}}.$$

Proof. Let $S = UAV$ be a Smith normal form of A over R. Then $\overline{U}^{-1}\overline{SV}^{-1} = \overline{A} = \hat{U}^{-1}\hat{S}\hat{V}^{-1}$. Since $\overline{U}$ and $\hat{U}$ are invertible, the rows of $\overline{SV}^{-1}$ and $\hat{S}\hat{V}^{-1}$ span the same module. As $\overline{S}$ and $\hat{S}$ are diagonal matrices with associated diagonal entries, we conclude that the rows of $\overline{V}^{-1}$ and $\hat{V}^{-1}$ span the same module. Moreover by Lemma 1.34 we know that the rows of V^{-1} span L over R, which finishes the proof. □

§2. A computational model for number field arithmetic

We now want to develop a simple computational model for number field arithmetic, which will then be applied in Chapter 2 to analyze our pseudo-Hermite normal form algorithm.

§2A. On the notion of complexity

As this is not a work in theoretical computer science, we will not give a formal definition of algorithms and complexity. While this can be done using Turing machines, random-access machines or related concepts we think of algorithms in the following colloquial way: An algorithm is a set of instructions that given an appropriate set of data (the input), returns a new set of data (the output). The input as well as the output will always be a family of natural numbers, where each natural number is encoded as follows: We fix a base $b \in \mathbf{Z}_{\geq 2}$ and represent an integer $n \in \mathbf{Z}_{\geq 1}$ using its b-adic expansion $(n_0, \dots, n_k)$. More precisely we have $n_0, \dots, n_k \in \mathbf{Z}_{\geq 0}$, $0 \leq n_i < b$ and $n_k \neq 0$ such that $n = \sum_{i=0}^{k} n_i b^i$. For $* \in \{+, -, \cdot, /\}$ and $x, y \in \mathbf{Z}$ with $0 \leq x, y < b$ the computation of $x * y \in \mathbf{Z}$ (if defined) is referred to as a word operation. Given an algorithm, we call the function, which assigns to each input the number of word operations required to execute the algorithm, the running time or complexity of the algorithm. Although using this notion of complexity we (to some extent) leave the rigorous mathematical world, the advantages outweigh the disadvantages.

Example 2.1. It is easy to see that there exists an algorithm, that given integers $m, n \in \mathbf{Z}_{\geq 1}$ computes $m+n$ with complexity in $O(\max(\log(m), \log(n)))$.

Assumption. We make the following assumption for any forthcoming complexity analysis.

(i) Due to Schönhage–Strassen ([SS71]) there exists an algorithm that given two integers $m, n \in \mathbf{Z}_{\geq 1}$ with $\log(m), \log(n) \leq B$ computes the product $m \cdot n$ with complexity in $\tilde{O}(B)$. Note that the algorithm of Fürer ([Für07]) has lower complexity than the Schönhage-Strassen algorithm, but the $\tilde{O}$ notation is too coarse to capture the difference.

(ii) Bernstein [Ber08] has shown that using the fast multiplication algorithm one can derive fast algorithms for a variety of problems, e.g., there exist algorithms that given $m, n \in \mathbf{Z}$ with $\log(|m|), \log(|n|) \leq B$ compute $\gcd(m, n)$ or a quotient with remainder, with complexity in $\tilde{O}(B)$.

(iii) Due to Dixon [Dix82] there exists an algorithm (Dixon's algorithm), that given a non-singular matrix $A \in \mathrm{Mat}_{n \times n}(\mathbf{Z})$ and $y \in \mathbf{Z}^n$ computes $x \in \mathbf{Q}^n$ such that $Ax = y$ with complexity in $\tilde{O}(n^3(\log(|A|) + \log(|y|)))$.

(iv) In Chapter 2 (see Remark 4.23) we will show that there exists an algorithm that given $A \in \mathrm{Mat}_{n \times m}(\mathbf{Z})$ and $\lambda \in \mathbf{Z}_{\geq 1}$ such that $\lambda \mathbf{Z}^m \subseteq \mathrm{sp}(A)$ computes the Hermite normal form of A with complexity in $\tilde{O}(nm \log(|A|) + nm^2 \log(\lambda))$.

Occasionally we will deal with probabilistic algorithms, which use calls to a random number generator during execution. These probabilistic algorithms come in two flavors. For Las Vegas algorithms the output is always correct, while the running time can vary when the algorithm is applied to the same input. For each input data the running time is now a distribution and the expected running time is the expectation of this distribution. In case of Monte Carlo algorithms neither the running time nor the output are determined by the input alone.

§2B. A notion of size

We first of all need a notion of size that bounds the size required to represent ideals and field elements.

Assumption. Let K be a number field of degree d with ring of integers $\mathcal{O}$. By $\Omega = (\omega_1, \dots, \omega_d)$ we denote a $\mathbf{Z}$-basis of $\mathcal{O}$ with $\omega_1 = 1$.

Size of ideals. An integral ideal $\mathfrak{a}$ of K is a free $\mathbf{Z}$-submodule of $\mathcal{O}$ of rank d and will be represented by the Hermite normal form $M_{\mathfrak{a}} \in \mathrm{Mat}_{d \times d}(\mathbf{Z})$ of any basis matrix of $\mathfrak{a}$ with respect to the fixed integral basis Ω. The size required to store the matrix is therefore bounded by $d^2 \log(|M_{\mathfrak{a}}|)$. Since we assume that ω_1 is equal 1, the value $|M_{\mathfrak{a}}|$, that is, the largest entry in $M_{\mathfrak{a}}$, is actually equal to $\min\{a \in \mathbf{Z}_{>0} \mid a \in \mathfrak{a}\} = \min(\mathfrak{a})$.

Definition 2.2. Let $\mathfrak{a}$ be an integral ideal of K. We define $\mathsf{sz}(\mathfrak{a}) = d^2 \log(\min(\mathfrak{a}))$ to be the *size* of $\mathfrak{a}$. If $\mathfrak{a} = \tilde{\mathfrak{a}}/k$ is a fractional ideal of K, where $\mathfrak{a}$ is integral and $k \in \mathbf{Z}_{>0}$ is the denominator of $\mathfrak{a}$, we define the *size* of $\mathfrak{a}$ by $\mathsf{sz}(\mathfrak{a}) = \mathsf{sz}(\tilde{\mathfrak{a}}) + d^2 \log(k)$.

The weight d^2 on the denominator is introduced to have a nice behavior with respect to the usual ideal operations. Before we show this, we need to recall some basic facts about the minimum of integral ideals. The weight can also be seen as viewing the ideal as given by a rational matrix directly (instead of a pair consisting of an integer matrix and the denominator).

Proposition 2.3. Let $\mathfrak{a}, \mathfrak{b}$ be integral ideals of K and $k \in \mathbf{Z}$. Then the following hold:
(i) $\min(\mathfrak{a} + \mathfrak{b})$ divides $\gcd(\min(\mathfrak{a}), \min(\mathfrak{b}))$.
(ii) $\min(\mathfrak{a}\mathfrak{b})$ divides $\min(\mathfrak{a})\min(\mathfrak{b})$.
(iii) The denominator of $\mathfrak{a}^{-1}$ is equal to $\min(\mathfrak{a})$.
(iv) $\min(k\mathfrak{a}) = |k| \min(\mathfrak{a})$.
(v) $\min(\mathfrak{a})$ divides $\mathbf{N}(\mathfrak{a})$.

Proof. Follows from the definition. □

The properties of the minimum translate directly into corresponding properties of the size of integral ideals. The next proposition shows that in fact the same relations hold also for fractional ideals.

Proposition 2.4. Let $\mathfrak{a}, \mathfrak{b}$ be fractional ideals of K and $m \in \mathbf{Z}$, $m \neq 0$. Then the following hold:
(i) $\mathsf{sz}(m\mathfrak{a}) \leq \mathsf{sz}(\mathfrak{a}) + d^2 \log(|m|)$.
(ii) $\mathsf{sz}(\mathfrak{a} + \mathfrak{b}) \leq 2(\mathsf{sz}(\mathfrak{a}) + \mathsf{sz}(\mathfrak{b}))$.
(iii) $\mathsf{sz}(\mathfrak{a}\mathfrak{b}) \leq \mathsf{sz}(\mathfrak{a}) + \mathsf{sz}(\mathfrak{b})$
(iv) $\mathsf{sz}(\mathfrak{a}^{-1}) \leq 2\,\mathsf{sz}(\mathfrak{a})$.

Proof. Note that if $\mathfrak{a}$ and $\mathfrak{b}$ are integral ideals then (i), (ii) and (iii) follow immediately from the properties of the minimum obtained in Proposition 2.3. Write $\mathfrak{a} = \tilde{\mathfrak{a}}/k$ and $\mathfrak{b} = \tilde{\mathfrak{b}}/l$ with k and l the denominator of $\mathfrak{a}$ and $\mathfrak{b}$ respectively.
(i): We have

$$\mathsf{sz}(m\mathfrak{a}) \leq \mathsf{sz}(m\tilde{\mathfrak{a}}) + d^2\log(k) \leq \mathsf{sz}(\tilde{\mathfrak{a}}) + d^2\log(|m|) + d^2\log(k) = \mathsf{sz}(\mathfrak{a}) + d^2\log(|m|).$$

(ii): As the sum $\mathfrak{a} + \mathfrak{b}$ is equal to $(l\tilde{\mathfrak{a}} + k\tilde{\mathfrak{b}})/kl$ we obtain

$$\begin{aligned}\mathsf{sz}(\mathfrak{a} + \mathfrak{b}) \leq \mathsf{sz}(l\tilde{\mathfrak{a}} + k\tilde{\mathfrak{b}}) + d^2\log(kl) \leq \mathsf{sz}(\tilde{\mathfrak{a}}) + d^2\log(l) + \mathsf{sz}(\tilde{\mathfrak{b}}) + d^2\log(k) + \mathsf{sz}(\mathfrak{a}) + \mathsf{sz}(\mathfrak{b}) \\ = 2(\mathsf{sz}(\mathfrak{a}) + \mathsf{sz}(\mathfrak{b})).\end{aligned}$$

(iii): We have

$$\mathsf{sz}(\mathfrak{a}\mathfrak{b}) \leq \mathsf{sz}(\tilde{\mathfrak{a}}\tilde{\mathfrak{b}}) + d^2\log(k) + d^2\log(l) \leq \mathsf{sz}(\mathfrak{a}) + \mathsf{sz}(\mathfrak{b}).$$

(iv): Consider first the integral case: We know that $\min(\tilde{\mathfrak{a}}) \in \tilde{\mathfrak{a}}$. Thus the principal ideal $(\min(\tilde{\mathfrak{a}}))$ is divided by $\tilde{\mathfrak{a}}$ and there exists an integral ideal $\mathfrak{b}$ with $(\min(\tilde{\mathfrak{a}})) = \tilde{\mathfrak{a}}\mathfrak{b}$, that is, $\tilde{\mathfrak{a}}^{-1} = \frac{\mathfrak{b}}{\min(\tilde{\mathfrak{a}})}$. Note that $\min(\tilde{\mathfrak{a}}) \in \mathfrak{b}$ and therefore $\min(\mathfrak{b}) \leq \min(\tilde{\mathfrak{a}})$. As $\min(\tilde{\mathfrak{a}})$ is the denominator of $\tilde{\mathfrak{a}}^{-1}$ by Proposition 2.3 (iv) we obtain

$$\mathsf{sz}(\tilde{\mathfrak{a}}^{-1}) = \mathsf{sz}(\mathfrak{b}) + d^2\log(\min(\tilde{\mathfrak{a}})) \leq 2\,\mathsf{sz}(\tilde{\mathfrak{a}}).$$

Returning to the general case we have $\mathfrak{a}^{-1} = k\tilde{\mathfrak{a}}^{-1}$. Thus

$$\mathsf{sz}(\mathfrak{a}^{-1}) \leq \mathsf{sz}(\tilde{\mathfrak{a}}^{-1}) + d^2\log(k) \leq 2\,\mathsf{sz}(\tilde{\mathfrak{a}}) + 2d^2\log(k) = 2\,\mathsf{sz}(\mathfrak{a}).$$ □

Size of elements. The integral basis Ω allows us to represent an integral element $\alpha \in \mathcal{O}$ by its coefficient vector $(a_1, \dots, a_d) \in \mathbf{Z}^d$ satisfying $\alpha = \sum_{i=1}^d a_i\omega_i$.

Definition 2.5. The *size* of an integral element $\alpha \in \mathcal{O}$ with respect to the chosen integral basis Ω is defined to be $\mathsf{sz}(\alpha) = d\max_i \log(|a_i|)$. For an element $\alpha \in K$, $\alpha = \tilde{\alpha}/k$ with $k \in \mathbf{Z}_{>0}$ the denominator of α, we define $\mathsf{sz}(\alpha) = \mathsf{sz}(\tilde{\alpha}) + d\log(k)$ to be the *size* of α.

Similarly to the ideals above, we added the weight d to the denominator to achieve a more nice transformation behavior under the standard operations. Its justification also comes from viewing elements in K as rational vectors rather than integral elements with a common denominator.

In order to relate our function sz to the multiplicative structure on K, we need to recall that the notion of size of elements is closely related to norms on the $\mathbf{R}$-vector space $K_{\mathbf{R}}$. More precisely, the fixed integral basis Ω is also an $\mathbf{R}$-basis of $K_{\mathbf{R}}$ and gives rise to an isomorphism

$$\Phi\colon K_{\mathbf{R}} \to \mathbf{R}^d, \sum_{i=1}^{d} a_i\omega_i \longmapsto (a_1, \dots, a_d),$$

onto the d-dimensional real vector space. Let $\| \ \|_\infty$ be the ∞-norm on $\mathbf{R}^d$. We have $d \log(\|\Phi(\alpha)\|_\infty) = \mathsf{sz}(\alpha)$ for $\alpha \in \mathcal{O}$. But this is not the only way to identify $K_{\mathbf{R}}$ with a normed real vector space. Denote the r real embeddings by $(\sigma_i)_{1\le i\le r}$ and the $2s$ complex embeddings by $(\sigma_i)_{r+1\le i\le r+2s}$. We use the usual ordering of the complex embeddings, such that $\sigma_{s+k} = \overline{\sigma}_k$ for $r < k \le r + s$. Using these embeddings we define

$$\begin{aligned}\Psi\colon K_{\mathbf{R}} &\longrightarrow \mathbf{R}^r \times \mathbf{R}^{2s}\\ \alpha &\longmapsto (\sigma_i(\alpha))_{1\le i\le r}, (\operatorname{Re}(\sigma_i(\alpha)) + \operatorname{Im}(\sigma_i(\alpha)), \operatorname{Re}(\sigma_i(\alpha)) - \operatorname{Im}(\sigma_i(\alpha)))_{r<i\le 2s+1},\end{aligned}$$

yielding $\|\Psi(\alpha)\|_2 = \|\alpha\|$ for $\alpha \in K$, where $\| \ \|_2$ denotes the 2-norm on $\mathbf{R}^{r+2s}$. Since $\mathbf{R}$ is complete, any two norms on $K_{\mathbf{R}}$ are equivalent. Thus there exist constants $C_1, C_2 \in \mathbf{R}_{>0}$ depending on K and the chosen basis Ω with

$$\frac{1}{C_2}\|\alpha\|_\infty \le \|\alpha\| \le C_1\|\alpha\|_\infty, \tag{1.2}$$

for all $\alpha \in K$. Moreover we have the inequalities

$$\|\alpha\| \le \sqrt{d} \max_{\sigma\in\Sigma_\infty} |\sigma(\alpha)|, \quad \max_{\sigma\in\Sigma_\infty} |\sigma(\alpha)| \le \|\alpha\|, \tag{1.3}$$

for all $\alpha \in K$ and applying the geometric arithmetic mean inequality yields

$$|\mathrm{N}_{K|\mathbf{Q}}(\alpha)| \le \frac{\|\alpha\|^d}{d^{d/2}}. \tag{1.4}$$

Another important characteristic of an integral basis Ω is the size of the *structure constants* $(m_{i,j,k})_{i,j,k}$, which are defined by the relations

$$\omega_i\omega_j = \sum_{k=1}^{d} m_{i,j,k}\omega_k$$

for $1 \le i, j \le d$. We denote the maximum value $\max_{i,j,k} |m_{i,j,k}|$ by C_3.

Remark 2.6. Note that there is a situation in which we are able to estimate the constants C_1, C_2, C_3 explicitly. Assume that Ω is LLL-reduced with respect to T_2 and LLL parameter c. Then by [Bel04, Proposition 5.1] the basis Ω satisfies

$$\|\omega_i\|^2 \le \left(d^{-(i-1)}c^{d(d-1)/2}|\Delta_K|\right)^{1/(d-i+1)}$$

for all $1 \le i \le d$ but it may happen that $\omega_1 = 1$ is no longer true. Moreover the structure constants satisfy

$$|m_{i,j,k}| \le \frac{c^{3d(d-1)/4}}{d^{d-(1/2)}}|\Delta_K| \quad 1 \le i, j, k \le d,$$

and thus we can choose

$$C_1 = \max_i \left(d^{-(i-1)}c^{d(d-1)/2}|\Delta_K|\right)^{1/2(d-i+1)}, \quad C_3 = \frac{c^{3d(d-1)/4}}{d^{d-(1/2)}}.$$

By [FS10, Lemma 2] we have $\|\alpha\|_\infty \le 2^{3d/2}\|\alpha\|$ for all $\alpha \in K$ allowing for $C_2 = 2^{3d/2}$.

Using the preceding discussion we can now describe the relation between size and the multiplicative structure of $\mathcal{O}$. If $\alpha = \sum_{i=1}^d a_i\omega_i$ and $\beta = \sum_{j=1}^d b_j\omega_j$ are integral elements in $\mathcal{O}$, the product $\alpha\beta$ is equal to $\sum_{k=1}^d c_k\omega_k$ with

$$c_k = \sum_{i=1}^{d} a_i \sum_{j=1}^{d} b_j m_{i,j,k}.$$

Thus for the size of $\alpha\beta$ we obtain

$$\mathsf{sz}(\alpha\beta) \le \mathsf{sz}(\alpha) + \mathsf{sz}(\beta) + 2d\log(d) + d\log(C_3).$$

The constant $2d\log(d) + d\log(C_3)$ therefore measures the increase of size when multiplying two integral elements.

The second multiplicative operation is the inversion of integral elements. Let $\alpha^{-1} = \beta/k$ with $k \in \mathbf{Z}_{>0}$ the denominator of α^{-1} and $\beta \in \mathcal{O}$. Using $k = \operatorname{den}(\alpha^{-1}) = \operatorname{den}((\alpha)^{-1}) = \min((\alpha)) \le \mathbf{N}((\alpha)) = |\mathrm{N}_{K|\mathbf{Q}}(\alpha)|$ and Inequality (1.4) we obtain $\log(k) \le d\log(C_1) + d\log(\|\alpha\|_\infty) - \frac{d}{2}\log(d)$. Since

$$|\sigma(\beta)| = \frac{\sigma(k)}{|\sigma(\alpha)|} = \frac{k}{|\sigma(\alpha)|} \le \frac{|\mathrm{N}_{K|\mathbf{Q}}(\alpha)|}{|\sigma(\alpha)|} = \prod_{\substack{\tau\in\Sigma_\infty\\ \tau\neq\sigma}} |\tau(\alpha)| \le \|\alpha\|^{d-1}$$

for every embedding $\sigma \in \Sigma_\infty$, we get $\|\beta\| \le \sqrt{d}\,\|\alpha\|^{d-1}$ by Inequality (1.3). Combining this with the estimate for the denominator yields

$$\mathsf{sz}(\alpha^{-1}) = d\log(k) + \mathsf{sz}(\beta) \le d\,\mathsf{sz}(\alpha) + d^2\log(C_1) + d\log(C_2).$$

Again we see that there is a constant depending on Ω describing the increase of size during element inversion. We define C_Ω by

$$C_\Omega = \max\{2d\log(d) + d\log(C_3), d^2\log(C_1) + d\log(C_2)\}$$

to obtain a constant incorporating both operations. Since we work with a fixed basis we drop the Ω from the index and denote this constant just by C. So far the obtained bounds on the size are only valid for integral elements and it remains to prove similar relations for the whole of K. We begin with the multiplicative structure.

Proposition 2.7. For all $\alpha, \beta \in K$ and $m \in \mathbf{Z}$ the following hold:
(i) $\mathsf{sz}(m\alpha) = \mathsf{sz}(\alpha) + d\log(|m|)$,
(ii) $\mathsf{sz}(\alpha\beta) \le \mathsf{sz}(\alpha) + \mathsf{sz}(\beta) + C$,
(iii) $\mathsf{sz}(\alpha^{-1}) \le d\,\mathsf{sz}(\alpha) + C$.

Proof. We write $\alpha = \tilde{\alpha}/k$ and $\beta = \tilde{\beta}/l$ with k and l the denominator of α and β respectively. Note that by the choice of C item (i) and (iii) hold for integral elements. (i): From the definition of the size it follows that $\mathsf{sz}(k\tilde{\alpha}) = \mathsf{sz}(\tilde{\alpha}) + d\log(|k|)$. Since the denominator of $m\alpha$ is bounded by k we have

$$\mathsf{sz}(k\alpha) \le \mathsf{sz}(k\tilde{\alpha}) + d\log(k) = \mathsf{sz}(\alpha) + d\log(|m|).$$

(ii): Since the denominator of $\alpha\beta$ is bounded by kl we obtain

$$\mathsf{sz}(\alpha\beta) \le \mathsf{sz}(\tilde{\alpha}\tilde{\beta}) + d\log(kl) \le \mathsf{sz}(\alpha) + \mathsf{sz}(\beta) + C.$$

(iii): The inverse of α is equal to $k\tilde{\alpha}^{-1}$. Therefore using (i) we get

$$\mathsf{sz}(\alpha^{-1}) = \mathsf{sz}(\tilde{\alpha}^{-1}) + d\log(k) = d\log(k) + \mathsf{sz}(\tilde{\alpha}) + C \le d\,\mathsf{sz}(\alpha) + C. \qquad \square$$

We now investigate the additive structure.

Proposition 2.8. If α and β are elements of K then $\mathsf{sz}(\alpha+\beta) \le 2(\mathsf{sz}(\alpha) + \mathsf{sz}(\beta))$.

Proof. It is easy to see that $\mathsf{sz}(\alpha+\beta) \le \mathsf{sz}(\alpha) + \mathsf{sz}(\beta)$ if α and β are integral elements. Now write $\alpha = \tilde{\alpha}/k$ and $\beta = \tilde{\beta}/l$ with k and l the denominator of α and β respectively. Then we obtain $\mathsf{sz}(l\tilde{\alpha} + k\tilde{\beta}) \le \mathsf{sz}(\tilde{\alpha}) + \mathsf{sz}(\tilde{\beta}) + d\log(k) + d\log(l) = \mathsf{sz}(\alpha) + \mathsf{sz}(\beta)$ and finally

$$\mathsf{sz}(\alpha+\beta) \le \mathsf{sz}(l\tilde{\alpha} + k\tilde{\beta}) + d\log(kl) \le 2(\mathsf{sz}(\alpha) + \mathsf{sz}(\beta)). \qquad \square$$

Finally we need the mixed operation between ideals and elements.

Proposition 2.9. Let $\alpha \in K$ and $\mathfrak{a}$ a fractional ideal of K. Then $\mathsf{sz}(\alpha\mathfrak{a}) \le \mathsf{sz}(\mathfrak{a}) + d^2\,\mathsf{sz}(\alpha) + dC$.

Proof. We consider first the integral case with $\alpha \in \mathcal{O}$ and $\mathfrak{a} \subseteq \mathcal{O}$. Using Inequalities (1.2) and (1.4) the minimum of the principal ideal (α) can be bounded by $C_1^d \|\alpha\|_\infty^d$. Thus we have

$$\mathsf{sz}(\alpha\mathfrak{a}) = d^2 \log(\min(\alpha\mathfrak{a})) \le d^2 \log(\min(\alpha)) + d^2 \log(\min(\mathfrak{a})) \le d^2 \,\mathsf{sz}(\alpha) + \mathsf{sz}(\mathfrak{a}) + dC.$$

Now let $\alpha = \tilde{\alpha}/k$ and $\mathfrak{a} = \tilde{\mathfrak{a}}/l$ with k and l the denominator of α and $\mathfrak{a}$ respectively. Using the integral case we obtain

$$\begin{aligned} \mathsf{sz}(\alpha\mathfrak{a}) &\le \mathsf{sz}(\tilde{\alpha}\tilde{\mathfrak{a}}) + d^2\log(kl) \le \mathsf{sz}(\tilde{\mathfrak{a}}) + d^2\log(l) + d^2\,\mathsf{sz}(\tilde{\alpha}) + d^2 \log(k) + dC \\ &= \mathsf{sz}(\mathfrak{a}) + d^2\,\mathsf{sz}(\alpha) + dC. \end{aligned}$$

□

§2C. Complexity of operations

In this section, we evaluate the complexity of the basic operations performed on number field elements and ideals.

Assumption. The input of our pseudo-Hermite normal form algorithm being a pseudo-matrix of a finitely generated torsion-free $\mathcal{O}$-module, we take the following precomputed data for granted:

(i) An integral basis $\Omega = (\omega_i)_{1\le i\le d}$ of the maximal order $\mathcal{O}$ satisfying $\omega_1 = 1$.

(ii) The structure constants $M = (m_{i,j,k})_{i,j,k}$ of Ω.

(iii) The matrix $DT^{-1} \in \mathrm{Mat}_{d\times d}(\mathbf{Z})$, where $T = (\mathrm{Tr}(\omega_i\omega_j))_{i,j}$ and $D = \min\{d \in \mathbf{Z}_{\ge 1} \mid d\cdot T^{-1} \in \mathrm{Mat}_{d\times d}(\mathbf{Z})\}$. Moreover using [FS10, Theorem 3] we compute a HKZ-reduced 2-element representation (δ_1, δ_2) of the ideal generated by the rows of DT^{-1} (see also [Coh93, 4.8.4]) with the property

$$\|\delta_i\| \le 4\left(\frac{1}{2}\sqrt{d+3}\right)^8 |\Delta_K|^{\frac{4}{d}+4}\left(2^C\right)^4, \quad \text{that is} \quad \mathsf{sz}(\delta_i) \in \tilde{O}\left(\frac{1}{d}\log(|\Delta_K|) + C\right)$$

for $i = 1, 2$. In addition we compute the regular representations M_{δ_1} and M_{δ_2}.

Since for large field degree d the computation of HKZ-reduced elements can be quite expensive, we note that it is possible to replace δ_1, δ_2 with an LLL-reduced 2-element representation computable in polynomial time. This only affects the $\tilde{O}$-constant but not the asymptotic complexity of our main algorithm. We do not impose any further restrictions on our integral basis Ω. All dependency on Ω is captured by $C = C_\Omega$.

Remark 2.10. The number field K is almost always given in the form $K = \mathbf{Q}(\alpha)$ for some element $\alpha \in \mathcal{O}$ which is a zero of a monic irreducible polynomial $f \in \mathbf{Z}[X]$. In Section 5 we describe a modular algorithm for computing the determinant of a square matrix over $\mathcal{O}$. For this purpose we need to bound the size of the minimal polynomial f of α and its discriminant. One possibility is to incorporate the minimal polynomial as an additional invariant of the field K. Since we want to keep the number of dependencies low, we choose a different approach. We want to show that given the integral basis $\Omega = (\omega_i)_{1\le i\le d}$ we can find a new primitive element whose discriminant and size of the minimal polynomial can be bounded by the already defined invariant $C = C_\Omega$: By a theorem of Sonn and Zassenhaus [SZ67] there exist $\varepsilon_1, \ldots, \varepsilon_d \in \{0, 1\}$ such that $\alpha = \sum_{i=1}^d \varepsilon_i\omega_i$ is a primitive element of the field extension $K|\mathbf{Q}$. Applying an embedding $\sigma \in \Sigma_\infty$ we obtain

$$|\sigma(\alpha)| \le d \max_i |\sigma(\omega_i)| \le d \max_i \|\omega_i\| \le dC_1.$$

Using these estimates for the conjugates of α we get the following bound on the coefficients of the minimal polynomial $f = X^d + \sum_{i=0}^{d-1} a_i X^i \in \mathbf{Z}[X]$ of α: Let $\Sigma_\infty = \{\sigma_1, \ldots, \sigma_d\}$. Since the elements $\sigma_j(\alpha)$, $1 \le j \le d$, are exactly the roots of f, we obtain

$$|a_i| = |s_i(\sigma_1(\alpha), \ldots, \sigma_d(\alpha))| \le \binom{d}{i} \max_j |\sigma_j(\alpha)|^i \le d^d \max_j |\sigma_j(\alpha)|^d \le d^d d^d C_1^d,$$

for $0 \le i \le d-1$, where $s_i \in \mathbf{Z}[X_1, \ldots, X_d]$ denotes the elementary symmetric polynomial of degree i. Therefore the height of f can be estimated by

$$\log(|f|) = \max_i \log(|a_i|) \le 2d\log(d) + d\log(C_1) \le C.$$

As we have a bound for the absolute values of its roots, we can moreover derive the following estimate for the discriminant of f:

$$|\mathrm{disc}(f)| = \prod_{i<j} |\sigma_i(\alpha) - \sigma_j(\alpha)|^2 \leq |\max_j 2\sigma_j(\alpha)|^{d^2} \leq 2^{d^2} \max_j |\sigma_j(\alpha)|^{d^2}.$$

Taking logarithms on both sides we obtain

$$\log(|\mathrm{disc}(f)|) \in O(d^2 \log(\max_j |\sigma_j(\alpha)|)) \subseteq O(d^2(\log(d) + \log(C_1)) \subseteq \tilde{O}(C).$$

Thus we can assume that we are given a primitive element with minimal polynomial $f \in \mathbf{Z}[X]$ satisfying $\log(|f|) \leq C$ and $\log(|\mathrm{disc}(f)|) \in \tilde{O}(C)$.

Field arithmetic. During our pseudo-Hermite normal form computation we need to perform additions, multiplications, and inversions of elements of K. Although algorithms for these operations are well known (see [Coh93, Bel04]) and many implementations can be found, there is a lack of references on the complexity. While multiplication in $\mathcal{O}$ was investigated by Belabas [Bel04], all the other operations are missing. We address the complexity issues in the rest of this section and begin with the additive structure.

Proposition 2.11. Let $\alpha, \beta \in K$, $\gamma \in \mathcal{O}$ an integral element and $m \in \mathbf{Z}$. We can

(i) compute the product $m\alpha$ with complexity in $\tilde{O}(\mathsf{sz}(\alpha) + d\log(|m|))$,

(ii) compute the quotient α/m with complexity in $\tilde{O}(\mathsf{sz}(\alpha) + \log(|m|))$,

(iii) compute the sum $\alpha + \beta$ with complexity in $O(\mathsf{sz}(\alpha) + \mathsf{sz}(\beta))$.

Proof. Let us write $\alpha = \tilde{\alpha}/k$ and $\beta = \tilde{\beta}/l$ with k and l the denominator of α and β respectively. Denote by $(a_1, \dots, a_d)$ the coefficient vector of $\tilde{\alpha}$.

(i): We have $m\alpha = (m\tilde{\alpha})/k = ((m/g)\tilde{\alpha})/(k/g)$, where g is the GCD of m and k. In addition, k/g is the denominator of $m\alpha$. As $k \leq \mathsf{sz}(\alpha)/d$, the complexity of computing g is in $\tilde{O}(\mathsf{sz}(\alpha)/d + \log(|m|))$. The computation of k/g and m/g has complexity in $\tilde{O}(\mathsf{sz}(\alpha)/d)$ and $\tilde{O}(\log(|m|))$ (as $|g| \leq k$ and $|g| \leq |m|$). Finally we have to compute $(m/g)a_i$ for all $i = 1, \dots, d$. Since $\log(|m/g|) \leq \log(|m|)$ and $\log(|a_i|) \leq \mathsf{sz}(\alpha)/d$, each multiplication has complexity in $\tilde{O}(\log(|m|) + \mathsf{sz}(\alpha)/d)$. As there are d such multiplications, the computation of $(m/g)\alpha$ has complexity in $\tilde{O}(d\log(|m|) + \mathsf{sz}(\alpha)$. By adding up the individual complexities the claim follows.

(ii): Set $g = \gcd(m, a_1, \dots, a_d)$. The quotient α/m is then given by $(\tilde{\alpha}/g)/(k \cdot m/g)$. As the costs of computing g are in $\tilde{O}(\log(|m|) + d\log(\|\tilde{\alpha}\|_\infty))$ and the products can be computed in $\tilde{O}(d\log(\|\tilde{\alpha}\|_\infty))$ and $\tilde{O}(\log(|m|) + \log(k))$ the claim follows.

(iii): The complexity obviously holds for integral elements. By (i) the computation of $l\tilde{\alpha}$ and $k\tilde{\alpha}$ has complexity in $\tilde{O}(\mathsf{sz}(\alpha) + \mathsf{sz}(\beta))$ and the complexity of adding $l\tilde{\alpha}$ and $k\tilde{\beta}$ is in $\tilde{O}(\mathsf{sz}(\alpha) + \mathsf{sz}(\beta))$. Computing kl has complexity in $\tilde{O}(\mathsf{sz}(\alpha)/d + \mathsf{sz}(\beta)/d)$. The last thing we have to do is making sure that the coefficients of the numerator and the denominator are coprime. This is done by d GCD computations and d divisions with complexity in $\tilde{O}(d(\mathsf{sz}(\alpha)/d + \mathsf{sz}(\beta)/d))$. □

Remark 2.12. The previous proposition looks counter-intuitive. More precisely, since addition of two number field elements is just addition of two elements in $\mathbf{Q}^d$, we would expect a (more visible) linear dependency on d to show up. In fact, this is the case, hidden carefully in the definition of sz. Assuming that α and β are integral elements, unraveling the definition of sz shows that the computation of $\alpha + \beta$ has complexity in

$$\tilde{O}(d(\log(\|\alpha\|_\infty) + \log(\|\beta\|_\infty))) = \tilde{O}(d \max(\log(\|\alpha\|_\infty, \log(\|\beta\|_\infty),$$

as we would expect.

Proposition 2.13. Let $\alpha, \beta, \alpha_1, \dots, \alpha_n \in K$, $\gamma \in \mathcal{O}$ an integral element and $m \in \mathbf{Z}$. We can

(i) compute the regular representation M_γ of γ with complexity in $\tilde{O}(d^2\,\mathsf{sz}(\gamma) + d^2C)$,

(ii) compute the product $\alpha\beta$ with complexity in $\tilde{O}(d\,\mathsf{sz}(\alpha) + d\,\mathsf{sz}(\beta) + dC)$ if the regular representation of the numerator of α is known,

(iii) compute the product $\alpha\beta$ with complexity in $\tilde{O}(d^2\,\mathsf{sz}(\alpha) + d\,\mathsf{sz}(\beta) + d^2C)$,

(iv) compute the products $\alpha\alpha_i$, $1 \leq i \leq n$, with complexity in $\tilde{O}(d(d+n)\,\mathsf{sz}(\alpha) + dn\max_i \mathsf{sz}(\alpha_i) + d(d+n)C)$,

(v) compute the inverse α^{-1} with complexity in $\tilde{O}(d^2\,\mathsf{sz}(\alpha) + d^2C)$ if $\alpha \neq 0$.

Proof. Let us write $\alpha = \tilde{\alpha}/k$ and $\beta = \tilde{\beta}/l$ with k and l the denominator of α and β respectively.

(i): If $(c_1, \dots, c_d) \in \mathbf{Z}^d$ denotes the coefficient vector of γ, then the regular representation of γ is given by

$$M_\gamma = \left(\sum_{j=1}^{d} c_j m_{ij}^k \right)_{i,k}.$$

Thus computing M_γ involves d^3 multiplications (and additions) and the overall complexity is in $\tilde{O}(d^2 \,\mathsf{sz}(\gamma) + d^3 \log(C_3)) = \tilde{O}(d^2 \,\mathsf{sz}(\gamma) + d^2 C)$.

(ii): Let $(a_1, \dots, a_d)$ and $(b_1, \dots, b_d)$ be the coefficient vectors of $\tilde{\alpha}$ and $\tilde{\beta}$ respectively. The coefficients of the product $\tilde{\alpha}\tilde{\beta} = \sum_{i=1}^d c_i \omega_i$ are given by

$$(c_1, \dots, c_d) = (b_1, \dots, b_d) M_{\tilde{\alpha}}.$$

Hence the product is obtained by d^2 multiplications. As the matrix $M_{\tilde{\alpha}}$ satisfies $\log(|M_{\tilde{\alpha}}|) \in \tilde{O}\left(\mathsf{sz}(\tilde{\alpha})/d + C/d\right)$ this has complexity in $\tilde{O}(d \,\mathsf{sz}(\tilde{\alpha}) + d \,\mathsf{sz}(\tilde{\beta}) + dC)$. Since taking care of denominators is less expensive this step dominates the computation.

(iii), (iv): Use (i) and (ii).

(v): We fist evaluate the complexity of inverting the integral element $\tilde{\alpha}$. In this case the coefficients $b_1, \dots, b_n$ of the element $\delta \in K$ with $\tilde{\alpha}\delta = 1$ satisfy

$$(b_1, \dots, b_d) M_{\tilde{\alpha}} = (1, 0, \dots, 0).$$

Thus inverting $\tilde{\alpha}$ boils down to calculating the regular representation of $\tilde{\alpha}$ and finding the unique rational solution of a linear system of d integer equations. By (i) the computation of $M_{\tilde{\alpha}}$ has complexity in $\tilde{O}(d^2 \,\mathsf{sz}(\tilde{\alpha}) + d^2 C)$ and the entries of $M_{\tilde{\alpha}}$ satisfy $\log(|M_{\tilde{\alpha}}|) \in O\left(\mathsf{sz}(\tilde{\alpha})/d + C/d\right)$. Using Dixon's algorithm solving the system then has complexity in $\tilde{O}(d^2 \,\mathsf{sz}(\alpha) + d^2 C)$. Now the inverse of α is given by $\alpha^{-1} = k\tilde{\alpha}^{-1}$. Since $\mathsf{sz}(\tilde{\alpha}^{-1}) \leq d \,\mathsf{sz}(\alpha) + C$ the complexity to compute $k\tilde{\alpha}^{-1}$ is in $\tilde{O}(d \,\mathsf{sz}(\alpha) + C)$. □

Ideal arithmetic. By assumption integral ideals are represented by their unique Hermite normal form with respect to the fixed integral basis. Therefore operations with ideals are mainly Hermite normal form computations which are accelerated by the availability of a multiple of the corresponding largest elementary divisor. Consider for a example an integral ideal $\mathfrak{a}$, for which we know only some $A \in \mathrm{Mat}_{r \times d}(\mathbf{Z})$, such that the rows generate A. The goal is now to find the unique Hermite normal form of A. Assume that we know some multiple λ of $\min(\mathfrak{a})$. As $\min(\mathfrak{a})$ and therefore also λ is an element of $\mathfrak{a}$ we conclude that $\lambda\omega_i \in \mathfrak{a}$ for all $1 \leq i \leq d$. On the side of the $\mathbf{Z}$-module structure this implies $\lambda\mathbf{Z}^d \subseteq \mathrm{sp}(A)$, that is, (λ) is an admissible modulus for A, allowing us to efficiently compute the Hermite normal form. The following lemmas show how this idea can be exploited during ideal arithmetic.

Lemma 2.14. Let $\mathfrak{a}$ and $\mathfrak{b}$ be fractional ideals and $m \in \mathbf{Z}$. We can

(i) compute $m\mathfrak{a}$ with complexity in $\tilde{O}(\mathsf{sz}(\mathfrak{a}) + d^2 \log(|m|))$,

(ii) compute the sum $\mathfrak{a} + \mathfrak{b}$ with complexity in $\tilde{O}(d(\mathsf{sz}(\mathfrak{a}) + \mathsf{sz}(\mathfrak{b})))$.

Proof. We write $\mathfrak{a} = \tilde{\mathfrak{a}}/k$ and $\mathfrak{b} = \tilde{\mathfrak{b}}/l$ with k and l the denominator of $\mathfrak{a}$ and $\mathfrak{b}$ respectively.

(i): We first have to compute the GCD g of m and k. Together with the division of k and m by g this has complexity in $\tilde{O}(\log(|m|) + \log(k))$. Finally we have to multiply the Hermite normal form matrix of $\tilde{\mathfrak{a}}$ with m/g taking d^2 multiplications with integers of size bounded by $\mathsf{sz}(\tilde{\mathfrak{a}})/d^2 + \log(|m|)$. In total we obtain a complexity in $\tilde{O}(\mathsf{sz}(\mathfrak{a}) + d^2 \log(|m|))$.

(ii): We first consider the case of integral ideals $\tilde{\mathfrak{a}}$ and $\tilde{\mathfrak{b}}$. The Hermite normal form basis of $\tilde{\mathfrak{a}} + \tilde{\mathfrak{b}}$ is obtained by computing the Hermite normal form of the concatenation $(M_{\tilde{\mathfrak{a}}}^t | M_{\tilde{\mathfrak{b}}}^t)^t$. As the minimum of $\tilde{\mathfrak{a}} + \tilde{\mathfrak{b}}$ divides $\gcd(\min(\tilde{\mathfrak{a}}), \min(\tilde{\mathfrak{b}}))$ this computation can be done with complexity in

$$\tilde{O}((2d)d(\log(\min(\tilde{\mathfrak{a}})) + \log(\min(\tilde{\mathfrak{b}}))) + (2d)d^2 \log(\gcd(\min(\tilde{\mathfrak{a}}), \min(\tilde{\mathfrak{b}})))) \subseteq \tilde{O}(d \min(\mathsf{sz}(\tilde{\mathfrak{a}}), \mathsf{sz}(\tilde{\mathfrak{b}}))).$$

Now consider the fractional case. By (i) and the integral case computing $l\tilde{\mathfrak{a}} + k\tilde{\mathfrak{b}}$ has complexity in $\tilde{O}(d(\mathsf{sz}(\mathfrak{a}) + \mathsf{sz}(\mathfrak{b})))$. Since this dominates the denominator computation we obtain an overall complexity as claimed. □

Proposition 2.15. Let $\alpha \in K$ and $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}$ be integral ideals. We can

(i) compute $\mathfrak{a}\mathfrak{b}$ with complexity in $\tilde{O}(d^2 \,\mathsf{sz}(\mathfrak{a}) + d^2 \,\mathsf{sz}(\mathfrak{b}) + d^3 C)$.

(ii) compute $\alpha\mathfrak{a}$ with complexity in $\tilde{O}(d^3\,\mathsf{sz}(\alpha) + d\,\mathsf{sz}(\mathfrak{a}) + d^2C)$.

Proof. We write $\mathfrak{a} = \tilde{\mathfrak{a}}/k$, $\mathfrak{b} = \tilde{\mathfrak{b}}/l$ and $\alpha = \tilde{\alpha}/m$ with k, l and m the denominator of $\mathfrak{a}$, $\mathfrak{b}$ and α respectively.

(i): As $\mathfrak{a}\mathfrak{b} = \tilde{\mathfrak{a}}\tilde{\mathfrak{b}}/(kl)$ we first evaluate the complexity of computing $\tilde{\mathfrak{a}}\tilde{\mathfrak{b}}$. Denoting by $(\alpha_i)_i$ and $(\beta_j)_j$ the Hermite normal form bases of $\tilde{\mathfrak{a}}$ and $\tilde{\mathfrak{b}}$ respectively we know that $\mathsf{sz}(\alpha_i) \leq \mathsf{sz}(\tilde{\mathfrak{a}})/d$ and $\mathsf{sz}(\beta_i) \leq \mathsf{sz}(\tilde{\mathfrak{b}})/d$ respectively. The d^2 elements $(\alpha_i\beta_j)_{i,j}$ form a $\mathbf{Z}$-generating system of $\tilde{\mathfrak{a}}\tilde{\mathfrak{b}}$ and their computation has complexity in

$$\tilde{O}(d^2(\mathsf{sz}(\tilde{\mathfrak{a}})/d + \mathsf{sz}(\tilde{\mathfrak{b}})/d) + d^3C) \subseteq \tilde{O}(d^2\,\mathsf{sz}(\tilde{\mathfrak{a}}) + d^2\,\mathsf{sz}(\tilde{\mathfrak{b}}) + d^3C).$$

The matrix M of this generating system then satisfies $\log(|M|) \leq \mathsf{sz}(\tilde{\mathfrak{a}})/d^2 + \mathsf{sz}(\tilde{\mathfrak{b}})/d^2 + C/d$. As the minimum of $\tilde{\mathfrak{a}}\tilde{\mathfrak{b}}$ divides $\min(\tilde{\mathfrak{a}})\min(\tilde{\mathfrak{b}})$ the final Hermite normal form computation has complexity in

$$\tilde{O}(d^2\,\mathsf{sz}(\tilde{\mathfrak{a}}) + d^2\,\mathsf{sz}(\tilde{\mathfrak{b}}) + d^3C).$$

As denominator computation is dominated by these steps the claim holds.

(ii): If we denote the basis of $\tilde{\mathfrak{a}}$ corresponding to the Hermite normal form by $(\alpha_i)_i$ we know that $(\tilde{\alpha}\alpha_i)_i$ forms a $\mathbf{Z}$-generating system of the ideal $\tilde{\alpha}\tilde{\mathfrak{a}}$. Computing the d products $\tilde{\alpha}\alpha_i$ for $1 \leq i \leq d$ has complexity in $\tilde{O}(d^2\,\mathsf{sz}(\tilde{\alpha}) + d\,\mathsf{sz}(\tilde{\mathfrak{a}}) + d^2C)$ since we have to compute the regular representation of $\tilde{\alpha}$ only once. If M denotes the matrix corresponding to this generating system of $\tilde{\alpha}\tilde{\mathfrak{a}}$ we know that $\log(|M|) \leq \mathsf{sz}(\tilde{\alpha})/d + \mathsf{sz}(\tilde{\mathfrak{a}})/d^2 + C/d$. Before computing the Hermite normal form matrix, we take care of the denominator. Computing kl, the GCD of kl and the entries of the matrix M and dividing kl and M by the GCD has complexity in $\tilde{O}(d\,\mathsf{sz}(\alpha) + \mathsf{sz}(\mathfrak{a}) + dC)$. As we know the regular representation of $\tilde{\alpha}$ we also know the minimum of the principal ideal (α). In particular we know $\min((\tilde{\alpha}))\min(\tilde{\mathfrak{a}})$ which is a multiple of $\min(\tilde{\alpha}\tilde{\mathfrak{a}})$. Using the estimate $\mathsf{sz}((\tilde{\alpha})) \leq d^2\,\mathsf{sz}(\tilde{\alpha}) + dC$ (see proof of Proposition 2.9) the final Hermite normal form computation has complexity in

$$\tilde{O}(d^3\,\mathsf{sz}(\alpha) + d\,\mathsf{sz}(\mathfrak{a}) + d^2C). \qquad \square$$

Remark 2.16. As for field arithmetic, the previous proposition looks counter-intuitive. Since ideal multiplication is just d^2 multiplications followed by the computation of a Hermite normal form of a $d^2 \times d$ matrix, we would expect a factor d^4 to show up. Again this is hidden carefully in the definition of sz. Assuming that $\mathfrak{a}$ and $\mathfrak{b}$ are integral ideals of K, unraveling the definition of sz shows that the computation of $\mathfrak{a}\cdot\mathfrak{b}$ has complexity in

$$\tilde{O}(d^4\max(\log(\min(\mathfrak{a})), \log(\min(\mathfrak{b}))) \subseteq \tilde{O}(d^4\log(\mathbf{N}(\mathfrak{a}\mathfrak{b}))),$$

as we would expect.

Finally we need to invert ideals. We use a slightly modified version of [Bel04, Algorithm 5.3] (which itself is a modified version of [Coh93, Algorithm 4.8.21]), exploiting the fact that

$$\mathfrak{a}^{-1} = \left\{\alpha \in K \,\middle|\, \mathrm{Tr}(\alpha\mathfrak{D}^{-1}\mathfrak{a}) \subseteq \mathbf{Z}\right\},$$

where $\mathfrak{D}$ denotes the different of K. Recall that $\mathfrak{D}^{-1}$ is a fractional ideal with (fractional) basis matrix $T^{-1} \in \mathrm{Mat}_{d\times d}(\mathbf{Z})$, where $T = (\mathrm{Tr}(\omega_i\omega_j))_{i,j}$. In order to evaluate the complexity of ideal inversion we need a bound on the size of mT^{-1} where m denotes the denominator of T^{-1}, that is, $m = \min(\mathfrak{D})$. Since by Cramer's rule we know that $|mT^{-1}| \leq d^d|T|^d$ it remains to consider $|T|$. By definition the trace of an element $\alpha \in K$ is given by the trace of its regular representation, $\mathrm{Tr}_{K|\mathbf{Q}}(\alpha) = \mathrm{Tr}(M_\alpha)$. In case of a basis element $\alpha = \omega_k$ for some $1 \leq k \leq d$ the entries of M_α are just structure constants m_{ij}^k and therefore $|\mathrm{Tr}_{K|\mathbf{Q}}(\omega_k)| \leq dC_3$. Applying this to $\mathrm{Tr}_{K|\mathbf{Q}}(\omega_i\omega_j)$ for $1 \leq i, j \leq d$ yields

$$|\mathrm{Tr}_{K|\mathbf{Q}}(\omega_i\omega_j)| \leq \sum_{k=1}^{d}|m_{ij}^k||\mathrm{Tr}_{K|\mathbf{Q}}(\omega_k)| \leq d^2C_3^2$$

and therefore

$$\log(|mT^{-1}|) \leq 2d\log(d) + 2d\log(C_3) \in O(C).$$

In addition note that $\min(\mathfrak{D})$ divides the norm of $\mathfrak{D}$, which is just $|\Delta_K|$.

Proposition 2.17. Let $\mathfrak{a}$ be a fractional ideal. Then we can compute $\mathfrak{a}^{-1}$ with complexity in $\tilde{O}(d\,\mathsf{sz}(\mathfrak{a}) + d^3\log(|\Delta_K|) + d^2C)$.

Proof. We use the same notation as in the preceding discussion. Let us first consider the integral case $\mathfrak{a} \subseteq \mathcal{O}$. Recall that the denominator of $\mathfrak{a}^{-1}$ is just $\min(\mathfrak{a})$ and need not be computed. Denote by $(\alpha_i)_i$ the Hermite normal form basis of $\mathfrak{a}$ and by $\mathfrak{B}$ the integral ideal $m\mathfrak{D}^{-1}$. We first have to compute $\mathfrak{a}\mathfrak{B}$. Using the precomputed 2-element representation $\mathfrak{B} = (\delta_1, \delta_2)$ this amounts to compute $2d$ products $\alpha_i\delta_j$, $1 \leq i \leq d$, $1 \leq j \leq 2$. As we have also precomputed the regular representation of δ_1 and δ_2 this has complexity in $\tilde{O}(d\,\mathsf{sz}(\mathfrak{a}) + d\log(|\Delta_K|) + d^2C)$ and yields a matrix $M \in \mathrm{Mat}_{2d\times d}(\mathbf{Z})$ with $\log(|M|) \leq \mathsf{sz}(\mathfrak{a})/d^2 + \log(|\Delta_K)/d^2 + C/d$. The cost of computing the Hermite normal form H of M is therefore in $\tilde{O}(d\,\mathsf{sz}(\mathfrak{a}) + d^3\log(|\Delta_K|) + dC)$, where we use that the minimum of $\mathfrak{a}\mathfrak{b}$ divides $\min(\mathfrak{a})|\Delta_K|$. A transposed basis matrix of the numerator of $\mathfrak{a}^{-1}$ is then obtained as the solution $X \in \mathrm{Mat}_{d\times d}(\mathbf{Z})$ of the equation $HX = \min(\mathfrak{a})(mT^{-1})$. Note that the triangular shape of H allows us to recover X by back substitution. Since $\min(\mathfrak{a})^2$ is contained in the span of X we can work modulo $\min(\mathfrak{a})^2$. The estimates $\log(|H|) \leq \log(\min(\mathfrak{a})|\Delta_K|)$ and $\log(mT^{-1}) \in O(C)$ show that the initial reduction has complexity in $\tilde{O}(\mathsf{sz}(\mathfrak{a}) + d^2\log(|\Delta_K|) + d^2C)$. For each column of X the back substitution itself then has a complexity in $\tilde{O}(d^2\min(\mathfrak{a}))$ yielding a complexity of $\tilde{O}(d\,\mathsf{sz}(\mathfrak{a}))$ in total for obtaining X. Finally we need to compute the Hermite normal form of X^t which has complexity in $\tilde{O}(d^2\log(|X|) + d^3\log(\min(\mathfrak{a}))) \subseteq \tilde{O}(d\,\mathsf{sz}(\mathfrak{a}))$.

Now let $\mathfrak{a} = \tilde{\mathfrak{a}}/k$ be a fractional ideal with denominator k. As $\mathsf{sz}(\tilde{\mathfrak{a}}^{-1}) \leq 2\,\mathsf{sz}(\tilde{\mathfrak{a}})$ the computation of $k\tilde{\mathfrak{a}}^{-1}$ has complexity in $\tilde{O}(\mathsf{sz}(\tilde{\mathfrak{a}}) + d^2\log(k)) = \tilde{O}(\mathsf{sz}(\mathfrak{a}))$ and the claim follows. □

§2D. Summary

For the readers convenience we summarize the complexity results obtained in this chapter. In Table 1.1 we have listed the various operations of field elements together with the complexity and the size of the output. While the first column is self-explanatory, the last two columns should be read as follows: If, in a row with operation $o\colon X \to Y$, c and s denote the functions of the second and third column respectively, then the computation of $o(x)$, $x \in X$, has complexity in $\tilde{O}(c(x))$ and $\mathsf{sz}(o(x)) \in O(s(x))$. In Table 1.2 we do the same for all basic ideal operations. We have also included Table 1.3, to show how the complexity looks like after unraveling the definition of sz. Here $I_{\mathcal{O}}$ denotes the set of integral ideals of K.

Operation $o\colon X \to Y$	Complexity $c\colon X \to \mathbf{Z}_{>0}$	Size $s\colon X \to \mathbf{Z}_{>0}$	Reference
$K \times \mathbf{Z} \to K$, $(\alpha, m) \mapsto m\alpha$	$(\alpha, m) \mapsto \mathsf{sz}(\alpha) + d\log(\lvert m\rvert)$	$(\alpha, m) \mapsto \mathsf{sz}(\alpha) + d\log(\lvert m\rvert)$	Proposition 2.11(i)
$K \times \mathbf{Z} \to K$, $(\alpha, m) \mapsto \alpha/m$	$(\alpha, m) \mapsto \mathsf{sz}(\alpha) + \log(\lvert m\rvert)$	$(\alpha, m) \mapsto \mathsf{sz}(\alpha) + d\log(\lvert m\rvert)$	Proposition 2.11(ii)
$K \times K \to K$, $(\alpha, \beta) \mapsto \alpha + \beta$	$(\alpha, \beta) \mapsto \mathsf{sz}(\alpha) + \mathsf{sz}(\beta)$	$(\alpha, \beta) \mapsto \mathsf{sz}(\alpha) + \mathsf{sz}(\beta)$	Proposition 2.11(iii)
$\mathcal{O} \to \mathrm{Mat}_{d\times d}(\mathbf{Z})$, $\gamma \mapsto M_\gamma$	$\gamma \mapsto d^2\,\mathsf{sz}(\gamma) + d^2C$		Proposition 2.13(i)
$K \times K \to K, (\alpha, \beta) \mapsto \alpha\beta$, $M_{\tilde{\alpha}}$ known, $\alpha = \tilde{\alpha}/k$	$(\alpha, \beta) \mapsto d\,\mathsf{sz}(\alpha) + d\,\mathsf{sz}(\beta) + dC$	$(\alpha, \beta) \mapsto \mathsf{sz}(\alpha) + \mathsf{sz}(\beta) + C$	Proposition 2.13(ii)
$K \times K \to K$, $(\alpha, \beta) \to \alpha\beta$	$(\alpha, \beta) \mapsto d^2\,\mathsf{sz}(\alpha) + d\,\mathsf{sz}(\beta) + d^2C$	$(\alpha, \beta) \mapsto \mathsf{sz}(\alpha) + \mathsf{sz}(\beta) + C$	Proposition 2.13(iii)
$K \times K^n \to K^n$, $(\alpha, (\alpha_i)) \mapsto (\alpha\alpha_i)$	$(\alpha, (\alpha_i)) \mapsto d(d+n)\,\mathsf{sz}(\alpha) + d(d+n)C$	$(\alpha, (\alpha_i)) \mapsto n\,\mathsf{sz}(\alpha) + n\,\mathsf{sz}(\alpha_i) + nC$	Proposition 2.13(iv)
$K \to K$, $\alpha \to \alpha^{-1}$	$\alpha \mapsto d^2\,\mathsf{sz}(\alpha) + d^2C$	$\alpha \mapsto d\,\mathsf{sz}(\alpha) + C$	Proposition 2.13(v)

Table 1.1.: Complexity of field arithmetic

Operation $o\colon X \to Y$	Complexity $c\colon X \to \mathbf{Z}_{>0}$	Size $s\colon X \to \mathbf{Z}_{>0}$	Reference
$I_K \times \mathbf{Z} \to I_K$, $(\mathfrak{a}, m) \mapsto m\mathfrak{a}$	$(\mathfrak{a}, m) \mapsto \mathsf{sz}(\mathfrak{a}) + d^2\log(\lvert m\rvert)$	$(\mathfrak{a}, m) \mapsto \mathsf{sz}(\mathfrak{a}) + d^2\log(\lvert m\rvert)$	Lemma 2.14(ii)
$I_K \times I_K \to I_K$, $(\mathfrak{a}, \mathfrak{b}) \mapsto \mathfrak{a} + \mathfrak{b}$	$(\mathfrak{a}, \mathfrak{b}) \mapsto d(\mathsf{sz}(\mathfrak{a}) + \mathsf{sz}(\mathfrak{b}))$	$(\mathfrak{a}, \mathfrak{b}) \mapsto \mathsf{sz}(\mathfrak{a}) + \mathsf{sz}(\mathfrak{b})$	Lemma 2.14(ii)
$I_K \times I_K \to I_K$, $(\mathfrak{a}, \mathfrak{b}) \mapsto \mathfrak{a}\mathfrak{b}$	$(\mathfrak{a}, \mathfrak{b}) \mapsto d^2\,\mathsf{sz}(\mathfrak{a}) + d^2\,\mathsf{sz}(\mathfrak{b}) + d^3C$	$(\mathfrak{a}, \mathfrak{b}) \mapsto \mathsf{sz}(\mathfrak{a}) + \mathsf{sz}(\mathfrak{b})$	Proposition 2.15(i)
$I_K \times K \to I_K$, $(\mathfrak{a}, \alpha) \mapsto \alpha\mathfrak{a}$	$(\mathfrak{a}, \alpha) \mapsto d^3\,\mathsf{sz}(\alpha) + d\,\mathsf{sz}(\mathfrak{a}) + d^2C$	$(\mathfrak{a}, \alpha) \mapsto \mathsf{sz}(\mathfrak{a}) + d^2\,\mathsf{sz}(\alpha) + dC$	Proposition 2.15(ii)
$I_K \to I_K$, $\mathfrak{a} \mapsto \mathfrak{a}^{-1}$	$\mathfrak{a} \mapsto d\,\mathsf{sz}(\mathfrak{a}) + d^3\log(\lvert\Delta_K\rvert) + d^2C$	$\mathfrak{a} \mapsto \mathsf{sz}(\mathfrak{a})$	Proposition 2.17

Table 1.2.: Complexity of ideal arithmetic

Operation $o\colon X \to Y$	Complexity $c\colon X \to \mathbf{Z}_{>0}$
$\mathcal{O} \times \mathbf{Z} \to \mathcal{O}$, $(\alpha, m) \mapsto m\alpha$	$(\alpha, m) \mapsto d(\log(\lVert\alpha\rVert_\infty) + \log(\lvert m\rvert))$
$\mathcal{O} \times \mathcal{O} \to \mathcal{O}$, $(\alpha, \beta) \mapsto \alpha + \beta$	$(\alpha, \beta) \mapsto d(\log(\lVert\alpha\rVert_\infty) + \log(\lVert\beta\rVert_\infty))$
$\mathcal{O} \to \mathrm{Mat}_{d\times d}(\mathbf{Z})$, $\gamma \mapsto M_\gamma$	$\gamma \mapsto d^3\log(\lVert\gamma\rVert_\infty) + d^2C$
$\mathcal{O} \times \mathcal{O} \to \mathcal{O}$, $(\alpha, \beta) \mapsto \alpha\beta$, M_α known	$(\alpha, \beta) \mapsto d^2(\log(\lVert\alpha\rVert_\infty + \log(\lVert\beta\rVert_\infty))) + dC$
$\mathcal{O} \times \mathcal{O} \to \mathcal{O}$, $(\alpha, \beta) \mapsto \alpha\beta$	$(\alpha, \beta) \mapsto d^3\log(\lVert\alpha\rVert_\infty) + d^2\log(\lVert\beta\rVert_\infty) + d^2C$
$\mathcal{O} \to K$, $\alpha \mapsto \alpha^{-1}$	$\alpha \mapsto d^3\log(\lVert\alpha\rVert_\infty) + d^2C$
$I_{\mathcal{O}} \times \mathbf{Z} \to I_{\mathcal{O}}$, $(\mathfrak{a}, m) \mapsto m\mathfrak{a}$	$(\mathfrak{a}, m) \mapsto d^2\log(\mathbf{N}(\mathfrak{a})) + d^2\log(\lvert m\rvert)$
$I_{\mathcal{O}} \times I_{\mathcal{O}} \to I_{\mathcal{O}}$, $(\mathfrak{a}, \mathfrak{b}) \mapsto \mathfrak{a} + \mathfrak{b}$	$(\mathfrak{a}, \mathfrak{b}) \mapsto d^3\log(\mathbf{N}(\mathfrak{a}\mathfrak{b}))$
$I_{\mathcal{O}} \times I_{\mathcal{O}} \to I_{\mathcal{O}}$, $(\mathfrak{a}, \mathfrak{b}) \mapsto \mathfrak{a}\mathfrak{b}$	$(\mathfrak{a}, \mathfrak{b}) \mapsto d^4\log(\mathbf{N}(\mathfrak{a}\mathfrak{b})) + d^3C$
$I_{\mathcal{O}} \times K \to I_{\mathcal{O}}$, $(\mathfrak{a}, \alpha) \mapsto \alpha\mathfrak{a}$	$(\mathfrak{a}, \alpha) \mapsto d^4\log(\lVert\alpha\rVert_\infty) + d^3\log(\mathbf{N}(\mathfrak{a})) + d^2C$
$I_{\mathcal{O}} \to I_K$, $\mathfrak{a} \mapsto \mathfrak{a}^{-1}$	$\mathfrak{a} \mapsto d^3\log(\mathbf{N}(\mathfrak{a})) + d^3\log(\lvert\Delta_K\rvert) + d^2C$

Table 1.3.: Complexity without sz

CHAPTER 2

Normal forms of modules over rings of integers

The pseudo-Hermite normal form is for module theory over Dedekind domains as important as the Hermite normal form is for module theory over the integers (or any other principal ideal domain): Normal forms provide us with algorithmic means to get finitely generated modules fully under control. Applications include testing membership, the decision of equality of modules, computation of the sum of modules, intersection of modules or quotient of modules. In case of Dedekind domains, using the pseudo-Hermite normal form it is moreover possible to test whether a module is free or not. In the following chapters, this powerful tool will be applied in the context of lattices over orders, where the objects of interest are modules over Dedekind domains with additional structure. As a consequence, the pseudo-Hermite normal form is at the heart of all algorithms dealing with orders and lattices and efficient algorithms to compute it are a necessity.

In Chapter 1 we already touched the topic of normal forms of modules over Dedekind domains while discussing pseudo-matrices and pseudo-Hermite normal forms. Using the computational model developed in the aforementioned chapter, we will now show that there exists an algorithm, which given a pseudo-matrix computes a pseudo-Hermite normal form with running time polynomial in the size of the input. Note that the emphasis lies on polynomial running time, as already Cohen in [Coh96] showed that there exists some algorithm for this task. The basic idea is as follows: Recall that given a matrix $A \in \mathrm{Mat}_{2\times 2}(\mathbf{Z})$, due to $\mathbf{Z}$ being a GCD domain, there exists a unimodular transformation $U \in \mathrm{GL}_2(\mathbf{Z})$ such that

$$UA = \begin{pmatrix} * & 0 \\ * & * \end{pmatrix},$$

that is, UA is a lower triangular matrix. Now for pseudo-matrices, a similar statement was obtained by Cohen in [Coh96]: Consider the pseudo-matrix

$$\begin{array}{c} \mathfrak{a} \\ \mathfrak{b} \end{array} \begin{pmatrix} a & * \\ b & * \end{pmatrix}$$

over a number field K and set $\mathfrak{d} = a\mathfrak{a} + b\mathfrak{b}$. Then it can be shown that there exists a pseudo-matrix

$$\begin{array}{c} \mathfrak{d} \\ \mathfrak{a}\mathfrak{b}\mathfrak{d}^{-1} \end{array} \begin{pmatrix} 1 & 0 \\ * & * \end{pmatrix}$$

such that both pseudo-matrices have the same span. By iterating this process beginning in the lower right corner, any pseudo-matrix can be transformed into pseudo-Hermite normal form with the same span. As this imitates the classical Hermite normal form algorithm over $\mathbf{Z}$, this approach has the same disadvantage: coefficient growth during the algorithm. In this chapter we will present two solutions to this problem by providing algorithms with proven polynomial running time.

§3. The classical modular pseudo-Hermite normal form algorithm

The contents of this section has been published as [BFH14].

Assumption. Let K be an algebraic number field of degree d with ring of integers $\mathcal{O}$.

There are different strategies for dealing with coefficient explosion in classical Hermite normal form algorithms over $\mathbf{Z}$. One strategy, which is used by Hafner and McCurley [HM91] exploits the fact, that the whole computation can be done modulo some multiple of the determinant of the associated lattice (in case of a square non-singular matrix, this is just the determinant of the matrix): Consider a matrix $A \in \operatorname{Mat}_{n\times m}$ with admissible modulus (λ), that is, $\lambda\mathbf{Z}^m \subseteq \operatorname{sp}(A)$. Then adding multiples of $(\lambda e_i)_{1\leq i\leq n}$ to the rows of A, where $(e_i)_{1\leq i\leq m}$ is the canonical basis of $\mathbf{Z}^m$, does not change the span of A. Thus we can use λ to reduce the entries during any unimodular transformation applied to A. Similarly the same holds for pseudo-matrices, where (λ) has to be replaced by an admissible modulus. As a consequence we can use reduction modulo (different) integral ideals involving the determinantal ideal. On the other hand, these ideals we are allowed to reduce with, are in general not generated by a single rational integer, making the notion of reduction much more difficult.

We will use the approach of Cohen [Coh96, Algorithm 2.12] with a different reduction algorithm and provide a rigorous complexity analysis. The reduction is accompanied by a normalization algorithm, which bounds the size of the coefficient ideals. Note that both techniques—reduction and normalization—rely on lattice basis reduction of lattices in the Euclidean space $(K_{\mathbf{R}}, \|\ \|)$

Choice of a lattice reduction algorithm. There are various lattice basis reduction algorithms and in general the smaller the resulting basis the worse the complexity of the algorithm. Thus one has to balance between smallness and efficiency. Instead of the L^2 algorithm of Nguyen and Stehlé [NS09], which has complexity quadratic in the size of the input, we rely on the nearly linear $\tilde{\mathrm{L}}^1$-algorithm of Novocin, Stehlé and Villard, which provides a lattice basis satisfying a weakened LLL condition. More precisely, for an *LLL-parameter* $\Xi = (\delta, \eta, \theta)$ with $\eta \in [\frac{1}{2}, 1)$, $\theta \geq 0$ and $\delta \in (\eta^2, 1]$, the notion of a Ξ-LLL reduced basis is defined in [CSV12]. Setting $\ell = (\theta\eta + \sqrt{(1+\theta^2)\delta - \eta^2})(\delta-\eta^2)^{-1}$ it is proved in [CSV12, Theorem 5.4] that a Ξ-LLL reduced basis $(b_1, \dots, b_n)$ of a lattice L of rank n in a Euclidean space with norm $\|\ \|$ satisfies

$$\begin{aligned} \|b_1\| &\leq \ell^{n-1}\lambda(L), \\ \|b_1\| &\leq \ell^{\frac{n-1}{2}}|\det(L)|^{\frac{1}{n}}, \\ \prod_{j=1}^{n} \|b_j\| &\leq \ell^{\frac{n(n-1)}{2}}|\det(L)|, \end{aligned} \tag{2.1}$$

where $\det(L)$ and $\lambda(L)$ denote the determinant and the first minimum of the lattice L respectively. Using this weakened LLL condition, Novocin, Stehlé and Villard [NSV11] construct an algorithm, named $\tilde{\mathrm{L}}^1$, with the following property ([NSV11, Theorem 7]): Given a matrix $B \in \operatorname{Mat}_{d\times d}(\mathbf{Z})$ with rows $B_1, \dots, B_j$ satisfying $\max_j \|B_j\| \leq 2^\beta$, the $\tilde{\mathrm{L}}^1$ algorithm returns a Ξ-reduced basis of the lattice associated to B using $\tilde{O}(d^5\beta)$ bit operations.

In the following, we fix LLL-parameter $\Xi = (\delta, \eta, \theta)$ and regard the associated parameter ℓ as a constant, which we ignore during the complexity analysis.

§3A. Reduction with respect to fractional ideals

Consider an integral ideal $\mathfrak{a}$ of K and an integral element $\alpha \in \mathcal{O}$. The goal of the reduction algorithm is to replace the element α by $\overline{\alpha} \in K$ such that $\alpha - \overline{\alpha}$ is an element of $\mathfrak{a}$ and the T_2-norm of $\overline{\alpha}$ is small compared to $\mathbf{N}(\mathfrak{a})$. Let $(\alpha_i)_{1\leq i\leq d}$ be a $\mathbf{Z}$-basis of $\mathfrak{a}$ and $\alpha = \sum_{i=1}^d a_i\alpha_i$ the representation of α in the $\mathbf{Q}$-basis $(\alpha_i)_{1\leq i\leq d}$ of K. The element $\overline{\alpha}$, defined as $\overline{\alpha} = \sum_{i=1}^d (a_i - \lceil a_i \rfloor)\alpha_i$ satisfies

$$\alpha - \overline{\alpha} = \sum_{i=1}^{d} \lceil a_i \rfloor \alpha_i \in \mathfrak{a} \quad \text{and} \quad \|\overline{\alpha}\| \leq \sum_{i=1}^{d} |a_i - \lceil a_i \rfloor| \, \|\alpha_i\| \leq \frac{1}{2}\sum_{i=1}^{d} \|\alpha_i\| \leq \frac{d}{2}\max_i \|\alpha_i\|\,.$$

Here, as usual, for a real number $z \in \mathbf{R}$ we denote by $\lceil z \rfloor = \lfloor z + \frac{1}{2} \rfloor$ rounding to the nearest integer. By the arithmetic-geometric mean inequality we have

$$\|\alpha_j\| \geq \sqrt{d}\,|\mathrm{N}_{K|\mathbf{Q}}(\alpha_j)|^{\frac{1}{d}} \geq \sqrt{d}\,\mathbf{N}(\mathfrak{a})^{\frac{1}{d}}$$

for all $1 \leq j \leq d$ and assuming that $(\alpha_i)_i$ is Ξ-LLL reduced, we obtain by (2.1)

$$\prod_{i=1}^{d} \|\alpha_i\| \leq \ell^{\frac{d(d-1)}{2}} \det(L_{\mathfrak{a}}),$$

where $L_{\mathfrak{a}}$ denotes the lattice associated to $\mathfrak{a}$ in $(K_{\mathbf{R}}, \| \ \|)$ and $\det(L_{\mathfrak{a}})$ its determinant. Using both inequalities we obtain

$$d^{\frac{d-1}{2}}\, \mathbf{N}(\mathfrak{a})^{\frac{d-1}{d}}\, \|\alpha_j\| \leq \prod_{i=1}^{d} \|\alpha_i\| \leq \ell^{\frac{d(d-1)}{2}} \det(L_{\mathfrak{a}})$$

and thus

$$\|\alpha_j\| \leq \ell^{\frac{d(d-1)}{2}} d^{-\frac{d-1}{2}}\, \mathbf{N}(\mathfrak{a})^{-\frac{d-1}{d}} \det(L_{\mathfrak{a}}) \leq \sqrt{d}\ell^{\frac{d(d-1)}{2}}\, \mathbf{N}(\mathfrak{a})^{\frac{1}{d}} \sqrt{|\Delta_K|} \tag{2.2}$$

for all $1 \leq j \leq d$. Hence we are able to bound $\|\overline{\alpha}\|$ in terms of $\mathbf{N}(\mathfrak{a})$ and field invariants only.

Consider now the general case with $\alpha \in K$ and a fractional ideal $\mathfrak{a}$ of K. We write $\alpha = \beta/k \in K$ and $\mathfrak{a} = \mathfrak{b}/l$ with $k, l \in \mathbf{Z}_{>0}$ the denominator of α and $\mathfrak{a}$ respectively. Then the above consideration applied to $l\beta \in \mathcal{O}$ and the integral ideal $k\mathfrak{b}$ yields an element $\overline{\alpha}$ with

$$\alpha - \overline{\alpha}/(kl) \in \mathfrak{a}$$

and

$$\|\overline{\alpha}/(kl)\| \leq d^{\frac{3}{2}} \ell^{\frac{d(d-1)}{2}}\, \mathbf{N}(\mathfrak{a})^{\frac{1}{d}} \sqrt{|\Delta_K|}.$$

To compute $\overline{\alpha}/(kl)$ we proceed as follows. First of all let $L \in \mathrm{Mat}_{d\times d}(\mathbf{Z})$ be the basis matrix of a Ξ-LLL reduced basis of the lattice attached to $\mathfrak{b}$. Denote by $A = (a_1, \dots, a_n)$ the coefficient vector of β with respect to the integral basis Ω. There exists $Y \in \mathbf{Q}^d$ such that $YL = lA$, that is, Y is the coefficient vector of $l\beta$ with respect to the basis matrix $L \in \mathrm{Mat}_{d\times d}(\mathbf{Z})$ of $\mathfrak{b}$. Dividing by k we obtain Y/k, which is then the coefficient vector of $l\beta$ with respect to the basis matrix kL of $k\mathfrak{b}$. Finally the coefficient vector of $\overline{\alpha}/(kl)$ is given by

$$\frac{1}{kl}(kL)\Big(\frac{Y}{k} - \Big\lceil\frac{Y}{k}\Big\rceil\Big) = \frac{1}{kl} L\tilde{Y},$$

where $\lceil \ \rceil$ is applied entrywise and $\tilde{Y} \in \mathbf{Z}^d$ is the vector with entries in $\{0, 1, \dots, k-1\}$ such that $Y \equiv \tilde{Y} \bmod k\mathbf{Z}^d$. This procedure is summarized in Algorithm 3.1.

Algorithm 3.1 (Reduction modulo fractional ideals). Given an element $\alpha \in K$ and a fractional ideal $\mathfrak{a}$ of K, the following steps return $\tilde{\alpha} \in K$ such that $\alpha - \tilde{\alpha} \in \mathfrak{a}$ and $\|\tilde{\alpha}\| \leq d^{3/2}\ell^{d(d-1)/2}\mathbf{N}(\mathfrak{a})^{1/d}\sqrt{|\Delta_K|}$.

```
(1) Let $\alpha = \beta/k$ and $\mathfrak{a} = \mathfrak{b}/l$.
(2) Compute the basis matrix $L$ of a $\Xi$-reduced basis of $\mathfrak{b}$ using the $\widetilde{\mathrm{L}}^1$-algorithm.
(3) Solve $YL = lA$ for $Y \in \mathbf{Q}^n$, where $A$ is the coefficient vector of $\beta$.
(4) Compute $\tilde{Y}$ and $Z = 1/(kl)L\tilde{Y}$.
(5) Return the element corresponding to $Z$.
```

Proposition 3.2. Algorithm 3.1 is correct and has complexity in

$$\tilde{O}(d^3 \,\mathsf{sz}(\mathfrak{a}) + d^2 \,\mathsf{sz}(\alpha) + d^3 \log(|\Delta_K|) + d^3 C).$$

The size of the output $\tilde{\alpha}$ satisfies

$$\|\tilde{\alpha}\| \leq d^{\frac{3}{2}} \ell^{\frac{d(d-1)}{2}} \mathbf{N}(\mathfrak{a})^{\frac{1}{d}} \sqrt{|\Delta_K|}.$$

Moreover if a Ξ-LLL reduced basis of the numerator of $\mathfrak{a}$ is known, then the reduction of α has complexity in

$$\tilde{O}(d \,\mathsf{sz}(\mathfrak{a}) + d^2 \,\mathsf{sz}(\alpha) + d^2 C + d^3 \log(|\Delta_K|)).$$

Proof. As correctness was already shown, we just have to do the cost analysis. The $\widetilde{\mathrm{L}}^1$-algorithm allows us to compute L with complexity in $\tilde{O}(d^5(\min(\mathfrak{a}) + \log(C_1)))$. Write $B_L = \log(|L|)$ and $B_\beta = \log(\|\beta\|_\infty)$. Applying Dixon's algorithm to compute Y has costs in $\tilde{O}(d^3(B_L + B_\beta + \log(l)))$ and invoking Cramer's rule yields $|Y| \leq d^d B_L^d B_\beta \log(l)$, that is, $\log(|Y|) \in \tilde{O}(dB_L + B_\beta + \log(l))$. Therefore the d divisions required to compute $Y \bmod k$ have complexity in $\tilde{O}(d(dB_L + B_\beta + \log(l)))$. Since $|Y \bmod k| \leq k$ the matrix vector multiplications consist of d^2 multiplications of integers of size bounded by $\tilde{O}(B_L + \log(k))$ and the output satisfies $\log(|L(Y \bmod k)|) \in \tilde{O}(\log(k) + B_L)$. Finally the product kl, as well as d GCDs and divisions with $L(Y \bmod k)$ need to be computed with complexity in $\tilde{O}(d(B_L + \log(k) + \log(l)))$. Without the computation of the reduced basis we have in total a complexity in

$$\tilde{O}(d^3 B_L + d^3 B_\beta + d\log(k) + d\log(l))$$

which simplifies to

$$\tilde{O}(d\,\mathsf{sz}(\mathfrak{a}) + d^2\,\mathsf{sz}(\alpha) + d^3\log(|\Delta_K|) + d^2C)$$

using the bound $B_L \in \tilde{O}(\min(\mathfrak{b}) + d^2 + \log(C_2) + \log(|\Delta|))$ derived from (2.2). Since the complexity of the $\widetilde{\mathrm{L}}^1$-algorithm is in $\tilde{O}(d^3\,\mathsf{sz}(\mathfrak{a}) + d^3C)$ the claim follows. □

Remark 3.3. Let $\mathfrak{a}$ be a fractional ideal of K.

(i) Note that the computation of the reduced basis gives a big contribution to the overall complexity of Algorithm 3.1. It is therefore important to compute the reduced basis only once, when reducing lots of elements of K modulo $\mathfrak{a}$. More precisely the reduction of n elements $\alpha_1, \ldots, \alpha_n \in K$ can be done in

$$\tilde{O}(d^3\,\mathsf{sz}(\mathfrak{a}) + nd\,\mathsf{sz}(\mathfrak{a}) + nd^2\max_i \mathsf{sz}(\alpha_i) + (n+d)d^2C + nd^3\log(|\Delta_K|)).$$

(ii) A reduced element is not necessarily of small size since the T_2-norm of a number field element alone does not control the size of the element. More precisely if α is in K and $k \in \mathbf{Z}_{>0}$ is the denominator of α then we have

$$\mathsf{sz}(\alpha) = d\log(\|k\alpha\|_\infty) + \log(k) \leq (d+1)\log(k) + C + \log(\|\alpha\|).$$

Thus in addition we need to control the size of the denominator to ensure that the reduced element is small with respect to sz.

§3B. Normalization

The normalization is the key difference between our approach and the one of Cohen [Coh96]. It is the strategy that—together with the reduction—prevents the coefficient swell by making sure that the coefficient ideals are integral with size bounded by invariants of the field. The connection between the size of the integral coefficient ideals and denominators of the matrix entries is seen as follows. Assume that $((\mathfrak{a}_i)_i, A)$ is a pseudo-matrix with span $M \subseteq \mathcal{O}^n$ and that A_i is the i-th row of A. As $M \subseteq \mathcal{O}^n$ we see that $\mathfrak{a}_iA_i \subseteq \mathcal{O}^n$. In particular, as $\min(\mathfrak{a}_i) \in \mathfrak{a}_i \cap \mathbf{Z}_{>0}$ and $\min(\mathfrak{a}_i)A_i \subseteq \mathcal{O}^n$, the denominators of the entries of A_i are bounded by $\min(\mathfrak{a}_i)$.

Since $\mathfrak{a}_iA_i = \alpha\mathfrak{a}_i(1/\alpha)A_i$ we can adjust our coefficient ideals by scalars from K (while multiplying the row with the inverse). Therefore the task is to find, given an integral ideal $\mathfrak{a}$ of K, an integral ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b}^{-1}$ is principal and $\mathbf{N}(\mathfrak{b})$ is bounded by field invariants only. Basically we just have to find a small integral representative of the ideal class of $\mathfrak{a}$. The usual proof of the finiteness of the class number provides us with such a small representative and a norm bound involving Minkowski's constant. As this is not suited for algorithmic purposes we handle this problem using Ξ-LLL reduced bases.

We write $\mathfrak{a} = \mathfrak{b}/k$ and $\mathfrak{b}^{-1} = \mathfrak{c}/l$ with k and l the denominator of $\mathfrak{a}$ and $\mathfrak{b}^{-1}$ respectively. Applying the $\widetilde{\mathrm{L}}^1$ algorithm to $\mathfrak{c}$ we find an element $\alpha \in \mathfrak{c}$ satisfying

$$\|\alpha\| \leq \ell^{\frac{d-1}{2}}|\Delta_K|^{\frac{1}{2d}}\,\mathbf{N}(\mathfrak{c})^{\frac{1}{d}}, \tag{2.3}$$

that is

$$|\mathrm{N}_{K|\mathbf{Q}}(\alpha)| \leq \ell^{d^2}\sqrt{|\Delta_K|}\,\mathbf{N}(\mathfrak{c}).$$

Then the ideal $\tilde{\mathfrak{a}}$ defined by $\tilde{\mathfrak{a}} = (\alpha/l)k\mathfrak{a}$ is integral since $\alpha \in \mathfrak{c} = l\mathfrak{b}^{-1} = l(k\mathfrak{a})^{-1}$. Moreover its norm satisfies

$$\mathbf{N}(\tilde{\mathfrak{a}}) = \frac{|\mathrm{N}_{K|\mathbf{Q}}(\alpha)|}{\mathbf{N}(\mathfrak{c})} \leq \ell^{d^2}\sqrt{|\Delta_K|}.$$

and is therefore bounded by invariants of the field.

Algorithm 3.4 (Normalization of a one-dimensional module). Given $A = (\alpha_1, \ldots, \alpha_n) \in K^n$ and a fractional ideal $\mathfrak{a}$ of K with denominator k, the following steps return $\tilde{A} \in K^n$ and an integral ideal $\tilde{\mathfrak{a}}$ of K such that $\mathbf{N}(\tilde{\mathfrak{a}}) \leq \ell^{d^2}\sqrt{|\Delta_K|}$ and $\mathfrak{a}A = \tilde{\mathfrak{a}}\tilde{A}$.

(1) Compute $\mathfrak{b}^{-1} = \mathfrak{c}/l$ where $\mathfrak{b}$ is the numerator of $\mathfrak{a}$.
(2) Let α be the first element of a Ξ-LLL reduced basis of $\mathfrak{c}$.
(3) Return $\tilde{A} = l/(k\alpha)A$ and $\tilde{\mathfrak{a}} = (\alpha/l)k\mathfrak{a}$.

Proposition 3.5. Algorithm 3.4 is correct and its output satisfies

$$\mathsf{sz}(\tilde{\alpha}) \in \tilde{O}\left(\mathsf{sz}(\mathfrak{a}) + \max_i \mathsf{sz}(\alpha_i) + d\log(|\Delta_K|) + dC\right),$$
$$\mathsf{sz}(\tilde{\mathfrak{a}}) \in \tilde{O}\left(d^4 + d^2\log(|\Delta_K|)\right),$$

where $\tilde{\alpha} \in K$ is an entry of $\tilde{A}$. Its complexity is in

$$\tilde{O}(d(d^2+n)\,\mathsf{sz}(\mathfrak{a}) + dn \max_i(\mathsf{sz}(\alpha_i)) + d^2(d+n)(\log(|\Delta_K|) + C)).$$

Proof. The correctness of the algorithm follows from the preceding discussion. Computing the inverse of $\mathfrak{b}$ can be done in $\tilde{O}(d\,\mathsf{sz}(\mathfrak{b}) + d^3\log(|\Delta_K|) + d^2C)$. The output satisfies $\mathsf{sz}(\mathfrak{c}) \leq \mathsf{sz}(\mathfrak{b})$ as well as $l \leq \min(\mathfrak{b})$. The second step invokes the $\widetilde{\mathrm{L}}^1$-algorithm whose complexity is in $\tilde{O}(d^3\,\mathsf{sz}(\mathfrak{c}) + d^3C)$ and which computes a small element $\alpha \in \mathfrak{c}$ with the property as in (2.3). Now this bound on the T_2-norm translates into $\mathsf{sz}(\alpha) \in \tilde{O}(\mathsf{sz}(\mathfrak{b})/d + \log(|\Delta_K|) + C)$ as follows: Using the definition of C_2 (see page 12) we get

$$\|\alpha\|_\infty \leq C_2 \ell^{\frac{d-1}{2}} |\Delta_K|^{\frac{1}{2d}}\,\mathbf{N}(\mathfrak{c})^{\frac{1}{d}}.$$

Now

$$\mathsf{sz}(\alpha) = d\log(\|\alpha\|_\infty) = \underbrace{d\log(C_2) + \frac{d(d-1)}{2}\log(\ell)}_{\in O(C)} + \underbrace{\frac{1}{2}\log(|\Delta_K|)}_{\in O(\log(|\Delta_K|))} + \log(\mathbf{N}(\mathfrak{c})).$$

We have $\mathbf{N}(\mathfrak{c}) \leq \min(\mathfrak{c})^d$ (the minimum is the largest elementary divisor of the basis matrix and the norm its determinant) and thus

$$\log(\mathbf{N}(\mathfrak{c})) \leq d\log(\min(\mathfrak{c})) = \mathsf{sz}(\mathfrak{c})/d \leq \mathsf{sz}(\mathfrak{b})/d.$$

The element α/l can be computed with complexity in $\tilde{O}(\mathsf{sz}(\alpha)+\log(l))$ and satisfies $\mathsf{sz}(\alpha/l) \leq \mathsf{sz}(\alpha) + d\log(l)$. Thus computing the new coefficient ideal $(\alpha/l)k\mathfrak{a} = (\alpha/l)\mathfrak{b}$ costs $\tilde{O}(d^3\,\mathsf{sz}(\alpha/l) + d\,\mathsf{sz}(\mathfrak{b}) + d^2C) \subseteq \tilde{O}(d^2\,\mathsf{sz}(\mathfrak{a}) + d^3(\log(|\Delta_K|) + C))$.

It remains to consider the multiplication of A by $l/(k\alpha)$. Inverting α and multiplying α^{-1} by l/k has complexity in $\tilde{O}(d^2\,\mathsf{sz}(\alpha) + d^2C + \log(k) + d\log(l))$. Since $\mathsf{sz}(l/(k\alpha)) \in \tilde{O}(d\,\mathsf{sz}(\alpha) + d\log(l) + d\log(k) + C)$ the multiplication with A has complexity in

$$\tilde{O}(d(d+n)(d\,\mathsf{sz}(\alpha) + d\log(l) + d\log(k)) + dn\max_i(\mathsf{sz}(\alpha_i)) + d(d+n)C),$$

which reduces to $\tilde{O}(d(d+n)\,\mathsf{sz}(\mathfrak{a}) + dn\max_i(\mathsf{sz}(\alpha_i)) + d^2(d+n)(\log(|\Delta_K|) + C))$. Now the claim follows. □

§3C. Constructing idempotents

In order to compute the pseudo-Hermite normal form over Dedekind domains, we use the constructive version of the Chinese remainder theorem introduced by Cohen in [Coh96]. Given coprime integral ideals $\mathfrak{a}$ and $\mathfrak{b}$ of K, we have to find $\alpha \in \mathcal{O}$ such that $\alpha \in \mathfrak{a}$ and $1-\alpha \in \mathfrak{b}$. This problem is closely connected to the computation of the sum of $\mathfrak{a}$ and $\mathfrak{b}$: The Hermite normal form of the matrix

$$A = \left(\begin{array}{c|c} M_{\mathfrak{a}} & M_{\mathfrak{a}} \\ \hline \mathbf{0} & M_{\mathfrak{b}} \end{array}\right)$$

is equal to

$$\left(\begin{array}{c|c} * & \mathbf{0} \\ \hline U & M_{\mathfrak{a}+\mathfrak{b}} \end{array}\right) = \left(\begin{array}{c|c} * & \mathbf{0} \\ \hline U & \mathbf{1}_d \end{array}\right)$$

for some $U \in \mathrm{Mat}_{d\times d}(\mathbf{Z})$ since $\mathfrak{a} + \mathfrak{b} = \mathcal{O}$. Denoting by $v \in \mathbf{Z}^d$ the first row of U we see that the element $\alpha = \sum_{i=1}^d v_i\omega_i$ of $\mathcal{O}$ satisfies $\alpha \in \mathfrak{a}$ and $1 - \alpha \in \mathfrak{b}$.

Lemma 3.6. Given coprime integral ideals $\mathfrak{a}$, $\mathfrak{b}$ of $\mathcal{O}$, there exists a deterministic algorithm which computes elements $\alpha \in \mathfrak{a}$ and $\beta \in \mathfrak{b}$ such that $\alpha + \beta = 1$. Moreover the output satisfies $\mathsf{sz}(\alpha), \mathsf{sz}(\beta) \in \tilde{O}((\mathsf{sz}(\mathfrak{a}) + \mathsf{sz}(\mathfrak{b}))/d)$ and the complexity of the algorithm is in $\tilde{O}(d(\mathsf{sz}(\mathfrak{a}) + \mathsf{sz}(\mathfrak{b})))$.

Proof. We use the same notation as in the preceding discussion. Note that $\lambda = \min(\mathfrak{a})\min(\mathfrak{b})$ satisfies $\lambda\mathbf{Z}^{2d} \in \mathrm{sp}(A)$ allowing us to compute the Hermite normal form with complexity in $\tilde{O}(d^3\log(\min(\mathfrak{a})\min(\mathfrak{b}))) = \tilde{O}(d(\mathsf{sz}(\mathfrak{a}) + \mathsf{sz}(\mathfrak{b}))$. Moreover as $\log(|U|) \leq 2\log(\lambda)$ we know that $\mathsf{sz}(\alpha) = d\log(|v|) \in O((\mathsf{sz}(\mathfrak{a}) + \mathsf{sz}(\mathfrak{b}))/d)$. □

Using this construction we can now describe an algorithm which plays the same role as the extended GCD algorithm over the integers. It is the workhorse of the pseudo-Hermite normal form algorithm and is accompanied by the normalization and reduction procedures.

Algorithm 3.7 (Euclidean Step). Given fractional ideals $\mathfrak{a}$, $\mathfrak{b}$ of K and elements $\alpha, \beta \in K$, the following steps return $\mathfrak{g} = \alpha\mathfrak{a} + \beta\mathfrak{b}$, $\mathfrak{g}^{-1}$, $\gamma \in \mathfrak{a}\mathfrak{g}^{-1}$ and $\delta \in \mathfrak{b}\mathfrak{g}^{-1}$ such that $\alpha\gamma + \beta\delta = 1$.

```
(1) Compute $\mathfrak{g} = \alpha\mathfrak{a} + \beta\mathfrak{b}$, $\mathfrak{g}^{-1}$, $\mathfrak{a}\mathfrak{g}^{-1}$ and $\mathfrak{b}\mathfrak{g}^{-1}$.
(2) Apply Lemma 3.6 to $\alpha\mathfrak{a}\mathfrak{g}^{-1}$ and $\beta\mathfrak{b}\mathfrak{g}^{-1}$ and denote the output by $\tilde{\gamma}$, $\tilde{\delta}$.
(3) Return $\gamma = \tilde{\gamma}\alpha^{-1}$ and $\delta = \tilde{\delta}\beta^{-1}$.
```

Proposition 3.8. Algorithm 3.7 is correct and has complexity in

$$\tilde{O}(d^2(\mathsf{sz}(\mathfrak{a}) + \mathsf{sz}(\mathfrak{b})) + d^4(\mathsf{sz}(\alpha) + \mathsf{sz}(\beta)) + d^3 C + d^3 \log(|\Delta_K|)).$$

The output satisfies $\mathsf{sz}(\gamma), \mathsf{sz}(\delta) \in \tilde{O}((\mathsf{sz}(\mathfrak{a}) + \mathsf{sz}(\mathfrak{b}))/d + d(\mathsf{sz}(\alpha) + \mathsf{sz}(\beta)) + C)$.

Proof. Correctness is clear. The first step consists of the computation of $\alpha\mathfrak{a}$ and $\beta\mathfrak{b}$, which has complexity in $\tilde{O}(d^3(\mathsf{sz}(\alpha)+\mathsf{sz}(\beta))+d(\mathsf{sz}(\mathfrak{a})+\mathsf{sz}(\mathfrak{b}))+d^2C)$. Denote by B the value $\mathsf{sz}(\alpha\mathfrak{a})+\mathsf{sz}(\beta\mathfrak{b}) \in O(\mathsf{sz}(\mathfrak{a})+\mathsf{sz}(\mathfrak{b})+d^2\,\mathsf{sz}(\alpha)+d^2\,\mathsf{sz}(\beta)+dC)$. While the computation of $\mathfrak{g}$ has complexity in $\tilde{O}(dB)$ the inversion costs $\tilde{O}(dB+d^3\log(|\Delta_K|)+d^3C)$. As $\mathsf{sz}(\mathfrak{g}) \in O(B)$ the inverse ideal $\mathfrak{g}^{-1}$ also satisfies $\mathsf{sz}(\mathfrak{g}^{-1}) \in O(B)$. Finding the product $\beta\mathfrak{b}\mathfrak{g}^{-1}$ and $\alpha\mathfrak{a}\mathfrak{g}^{-1}$ then has complexity in $\tilde{O}(d^2B + d^3C)$ and the size of both integral ideals is in $\tilde{O}(B)$. Hence invoking Lemma 3.6 has a complexity in $\tilde{O}(dB)$ and the resulting elements satisfy $\mathsf{sz}(\tilde{\gamma}), \mathsf{sz}(\tilde{\delta}) \in \tilde{O}(B/d)$. Finally we have to compute inverses and products. While α^{-1} and β^{-1} can be computed in $\tilde{O}(d^2\,\mathsf{sz}(\alpha)+d^2\,\mathsf{sz}(\beta)+d^2C)$ the costs of the products are in $\tilde{O}(d^2\,\mathsf{sz}(\tilde{\gamma})+d^2\,\mathsf{sz}(\tilde{\delta})+d^2\,\mathsf{sz}(\alpha)+d^2\,\mathsf{sz}(\beta)+d^2C)$. Thus the ideal product dominates the complexity of the algorithm and the claim follows. Note that $\mathsf{sz}(\gamma) = \mathsf{sz}(\tilde{\gamma}\alpha^{-1}) \leq \mathsf{sz}(\tilde{\gamma}) + d\,\mathsf{sz}(\alpha) + C \in \tilde{O}(B/d + d\,\mathsf{sz}(\alpha))$ and a similar result holds for $\mathsf{sz}(\delta)$. □

§3D. The main algorithm and its complexity

We now describe a polynomial time algorithm for computing a pseudo-Hermite normal of a square pseudo-matrix with full rank. The algorithm is a variant of the so-called modular algorithm of Cohen, the big difference being the normalization of the coefficient ideals. Using this extra feature we are able to bound the denominators of the coefficients of the matrix. Together with the reduction procedure this will allow us to prove polynomial running time. We assume that the determinantal ideal is known (this case often occurs, for example when computing with ideals in relative extensions). If this is not the case, we have to invoke Algorithm 5.14.

Algorithm 3.9 (Pseudo-Hermite normal form algorithm). Given a pseudo-matrix $\mathcal{A} = ((\mathfrak{a}_i)_i, A)$ of full rank with A a square matrix and $\mathfrak{d} = \det(\mathcal{A})$, the following steps return a pseudo-Hermite normal form with the same span as $\mathcal{A}$.

```
(1) Set $((\mathfrak{b}_i)_i, B) \leftarrow ((\mathfrak{a}_i)_i, A)$. Normalize $(B_i, \mathfrak{b}_i)_{1 \leq i \leq n}$ with Algorithm 3.4.
(2) Reduce $B_i$ modulo $\mathfrak{d}\mathfrak{b}_i^{-1}$ using Algorithm 3.1 for $1 \leq i \leq n$.
(3) Set $\mathfrak{D} \leftarrow \mathfrak{d}$.
(4) For $i = n, \ldots, 2$ do the following:
    (5) For $j = i - 1, \cdots, 1$ do the following:
        (6) Set $\mathfrak{g} \leftarrow \beta_{j,i}\mathfrak{b}_j + \beta_{i,i}\mathfrak{b}_i$.
        (7) Compute $\gamma \in \mathfrak{b}_j\mathfrak{g}^{-1}$ and $\delta \in \mathfrak{b}_i\mathfrak{g}^{-1}$ such that $\beta_{j,i}\gamma + \beta_{i,i}\delta = 1$ using Algorithm 3.7.
        (8) Set $(\mathfrak{b}_j, \mathfrak{b}_i) \leftarrow (\mathfrak{b}_j\mathfrak{b}_i\mathfrak{g}^{-1}, \mathfrak{g})$.
        (9) Set $(B_j, B_i) \leftarrow (\beta_{i,i}B_j - \beta_{j,i}B_i, \gamma B_j + \delta B_i)$.
        (10) Normalize $(B_j, \mathfrak{b}_j)$ and $(B_i, \mathfrak{b}_i)$ using Algorithm 3.4
        (11) Reduce $B_j$ modulo $\mathfrak{d}\mathfrak{b}_j^{-1}$ and $B_i$ modulo $\mathfrak{d}\mathfrak{b}_i^{-1}$ using Algorithm 3.1.
    (13) Set $\mathfrak{g} = \beta_{i,i}\mathfrak{b}_i + \mathfrak{D}$. Compute $\gamma \in \mathfrak{b}_i\mathfrak{g}^{-1}$ and $\delta \in \mathfrak{D}\mathfrak{g}^{-1}$ such that $\gamma\beta_{i,i} + \delta = 1$.
    (14) Set $B_i \leftarrow \gamma B_i \bmod \mathfrak{D}\mathfrak{g}^{-1}$ using Algorithm 3.1 and $\mathfrak{b}_i \leftarrow \mathfrak{g}$, $\beta_{i,i} \leftarrow 1$.
    (15) Set $\mathfrak{D} \leftarrow \mathfrak{D}\mathfrak{g}^{-1}$.
(16) Return $(B, (\mathfrak{b}_i)_i)$.
```

First of all, we want to show that at the beginning of the inner loop at Step 6 the sizes of B_i, B_j and $\mathfrak{b}_i, \mathfrak{b}_j$ respectively are bounded. We use an inductive argument and begin with the size of the objects at Step 3. Let $i, j \in \{1, \ldots, n\}$. As the ideal $\mathfrak{b}_i$ is normalized it satisfies

$$\min(\mathfrak{b}_i) \leq \mathbf{N}(\mathfrak{b}_i) \leq \ell^{d^2}\sqrt{|\Delta_K|}.$$

By Proposition 3.2 the reduction of Step 2 yields

$$\|\beta_{i,j}\| \leq d^{3/2}\ell^{d^2}\,\mathbf{N}(\mathfrak{d}\mathfrak{b}_i^{-1})^{1/d}\sqrt{|\Delta_K|} \leq d^{3/2}\ell^{d^2}\min(\mathfrak{d})\sqrt{|\Delta_K|}.$$

As $\beta_{i,j}\mathfrak{b}_\mathfrak{i} \subseteq \mathcal{O}$ the denominator $l \in \mathbf{Z}_{>0}$ of $\beta_{i,j}$ satisfies $l \leq \min(\mathfrak{b}_i)$. In particular

$$\begin{aligned}\mathsf{sz}(\beta_{i,j}) &= d\log(\|l\beta_{i,j}\|_\infty) + d\log(l)\\ &= 2d\log(l) + d\log(\|\beta_{i,j}\|_\infty) \in \tilde{O}(\mathsf{sz}(\mathfrak{d})/d + \mathsf{sz}(\mathfrak{b}_i)/d + C).\end{aligned}$$

We define $B_{\mathrm{id}} = d^4 + d^2\log(|\Delta_K|)$ and $B_{\mathrm{e}} = \mathsf{sz}(\mathfrak{d})/d + B_{\mathrm{id}}/d + C$ respectively. The inequalities $B_{\mathrm{id}} \leq dB_{\mathrm{e}}$ and $C + d\log(|\Delta_K|) + d^3 \leq B_{\mathrm{e}}$ will be used throughout the following complexity analysis.

Proposition 3.10. Let $2 \leq i \leq n$ and $i-1 \leq j \leq n$. At the beginning of the inner loop at Step 7 the size of the coefficient ideals $\mathfrak{b}_i$, $\mathfrak{b}_j$ is bounded by B_{id} and the size of the elements of rows B_i, B_j is in $\tilde{O}(B_{\mathrm{e}})$.

Proof. This follows from Step 10 and 11. □

We are now in a position to analyze the complexity of the algorithm. In order to improve readability we split up the analysis according to the single steps. Let us first take care of the steps in the loops.

Lemma 3.11. Let $(A, (\mathfrak{a}_i)_i)$ be as in the input of Algorithm 3.9.
(i) Steps 6–7 have complexity in $\tilde{O}(d^4B_{\mathrm{e}})$.
(ii) Step 8 has complexity in $\tilde{O}(d^4B_{\mathrm{e}})$.
(iii) Step 9 has complexity in $\tilde{O}(d^2(d+n)B_{\mathrm{e}})$.
(iv) Step 10 has complexity in $\tilde{O}(d^5B_{\mathrm{e}} + d^3nB_{\mathrm{e}})$.
(v) Step 11 has complexity in $\tilde{O}(d^3\,\mathsf{sz}(\mathfrak{d}) + dn\,\mathsf{sz}(\mathfrak{d}) + d^4nB_{\mathrm{e}})$.
(vi) Step 13 has complexity in $\tilde{O}(d^2\,\mathsf{sz}(\mathfrak{d}) + d^4B_{\mathrm{e}})$.
(vii) Step 14 has complexity in $\tilde{O}(d^3\,\mathsf{sz}(\mathfrak{d}) + dn\,\mathsf{sz}(\mathfrak{d}) + d^3nB_{\mathrm{e}})$.
Thus the inner loop in Steps 6–11 as well as Steps 13–15 is dominated by normalization and reduction yielding an overall complexity in

$$\tilde{O}(d^3(d+n)(\mathsf{sz}(\mathfrak{d}) + d^4 + d^2\log(|\Delta_K|) + dC)).$$

Proof. (i): Steps 6–7 are just an application of Algorithm 3.7 with complexity in $\tilde{O}(d^2B_{\mathrm{id}} + d^4B_{\mathrm{e}} + d^3C + d^3\log(|\Delta_K|)) \subseteq \tilde{O}(d^4B_{\mathrm{e}})$. The size of γ and δ is in $\tilde{O}(B_{\mathrm{id}}/d + dB_{\mathrm{e}} + C) \subseteq \tilde{O}(dB_{\mathrm{e}})$.

(ii): The size of $\mathfrak{g}$ and therefore also the size of $\mathfrak{g}^{-1}$ is in $\tilde{O}(B_{\mathrm{id}} + d^2B_{\mathrm{e}} + dC) \subseteq \tilde{O}(d^2B_{\mathrm{e}})$. As we have already computed $\mathfrak{g}^{-1}$ in Algorithm 3.7, the computation of $\mathfrak{b}_i\mathfrak{b}_j\mathfrak{g}^{-1}$ has complexity in $\tilde{O}(d^2B_{\mathrm{id}} + d^2(d^2B_{\mathrm{e}}) + d^3C) \subseteq \tilde{O}(d^4B_{\mathrm{e}})$. Note that $\mathsf{sz}(\mathfrak{b}_i\mathfrak{b}_j\mathfrak{g}^{-1}) \in \tilde{O}(B_{\mathrm{id}} + d^2B_{\mathrm{e}}) \subseteq \tilde{O}(d^2B_{\mathrm{e}})$.

(iii): Since $\mathsf{sz}(\gamma), \mathsf{sz}(\delta) \in \tilde{O}(dB_{\mathrm{e}})$, computing the scalar vector products has complexity in $\tilde{O}(d(d+n)(dB_{\mathrm{e}}) + dnB_{\mathrm{e}} + d(d+n)C) \subseteq \tilde{O}(d^2(d+n)B_{\mathrm{e}})$. The size of the new elements in row i and j is in $\tilde{O}(dB_{\mathrm{e}})$.

(iv): The normalization has complexity in $\tilde{O}(d(d^2+n)(d^2B_{\mathrm{e}}) + dn(dB_{\mathrm{e}}) + d(d^2+n)(\log(|\Delta_K|) + C))$ which simplifies to $\tilde{O}(d^5B_{\mathrm{e}} + d^3nB_{\mathrm{e}})$. While by definition the new ideals have size bounded by B_{id}, the size of the new elements is in $\tilde{O}(d^2B_{\mathrm{e}} + dB_{\mathrm{e}} + d\log(|\Delta_K|) + dC) = \tilde{O}(d^2B_{\mathrm{e}})$.

(v): Inverting $\mathfrak{b}_i$ and $\mathfrak{b}_j$ has complexity in $\tilde{O}(dB_{\mathrm{id}} + d^3\log(|\Delta_K|) + d^2C)$ and the multiplication with $\mathfrak{d}$ is in $\tilde{O}(d^2(B_{\mathrm{id}} + \mathsf{sz}(\mathfrak{d})) + d^3C)$. The reduction itself then has complexity in $\tilde{O}(d(d^2+n)(B_{\mathrm{id}} + \mathsf{sz}(\mathfrak{d})) + d^2n(d^2B_{\mathrm{e}}) + d^2(d+n)C + d^3n\log(|\Delta_K|))$ which is in $\tilde{O}(d^3\,\mathsf{sz}(\mathfrak{d}) + dn\,\mathsf{sz}(\mathfrak{d}) + d^4nB_{\mathrm{e}})$.

(vi): Step 13 is again an application of Algorithm 3.7 with complexity in $\tilde{O}(d^2(B_{\mathrm{id}} + \mathsf{sz}(\mathfrak{d})) + d^4B_{\mathrm{e}} + d^3C + d^3\log(|\Delta_K|)) \subseteq \tilde{O}(d^2\,\mathsf{sz}(\mathfrak{d}) + d^4B_{\mathrm{e}})$ and again the size of γ and δ is in $\tilde{O}(\mathsf{sz}(\mathfrak{d})/d + dB_{\mathrm{e}})$. Here we have used that $\mathsf{sz}(\mathfrak{D}) \leq \mathsf{sz}(\mathfrak{d})$ since $\mathfrak{D}$ is a divisor of $\mathfrak{d}$.

(vii): While the product $\mathfrak{D}\mathfrak{g}^{-1}$ was already computed in Algorithm 3.7, the computation of γB_i has complexity in $\tilde{O}(d(d+n)\,\mathsf{sz}(\gamma) + dnB_{\mathrm{e}} + d(d+n)C) = \tilde{O}((d+n)\,\mathsf{sz}(\mathfrak{d}) + d^2(d+n)B_{\mathrm{e}})$. Since the entries of γB_i have size in $\tilde{O}(\mathsf{sz}(\mathfrak{d})/d + dB_{\mathrm{e}})$ the final reduction is in $\tilde{O}(d^3\,\mathsf{sz}(\mathfrak{d}) + dn\,\mathsf{sz}(\mathfrak{d}) + d^2n(\mathsf{sz}(\mathfrak{d})/d + dB_{\mathrm{e}}) + d^2(d+n)C + d^3n\log(|\Delta_K|))$ which simplifies to $\tilde{O}(d^3\,\mathsf{sz}(\mathfrak{d}) + dn\,\mathsf{sz}(\mathfrak{d}) + d^3nB_{\mathrm{e}})$. □

Theorem 3.12. Algorithm 3.9 is correct and the complexity is in

$$\tilde{O}(d^2n(d+n)\max_i \mathsf{sz}(\mathfrak{a}_i) + d^2n^2\max_{i,j}\mathsf{sz}(\alpha_{i,j}) + d^3n^2(d+n)(\mathsf{sz}(\mathfrak{d}) + d^4 + d^2\log(|\Delta_K|) + dC)).$$

Proof. The correctness was proven in [Coh96]. Since the inner loop is executed $O(n^2)$ times we conclude using Lemma 3.11 that Steps 5–18 have complexity in $\tilde{O}(d^3n^2(d+n)(\mathsf{sz}(\mathfrak{d}) + d^4 + d^2\log(|\Delta_K|) + dC))$. Now we consider the initialization in Step 1–3. Denote $\max_{i,j} \mathsf{sz}(\alpha_{i,j})$ and $\max_i \mathsf{sz}(\mathfrak{a}_i)$ by B_A and $B_\mathfrak{a}$ respectively. By Proposition 3.5 Step 1 has complexity in $\tilde{O}(dn(d^2+n)B_\mathfrak{a} + dn^2B_A + nd(d^2+n)(\log(|\Delta_K|)+C))$ and the new elements have size in $\tilde{O}(B_\mathfrak{a} + B_A + d\log(|\Delta_K|) + dC)$. As in the proof of Lemma 3.11, computing the product $\mathfrak{b}_i^{-1}\mathfrak{d}$ has complexity in $\tilde{O}(dB_{\mathrm{id}} + d^3\log(|\Delta_K|) + d^2(B_{\mathrm{id}} + \mathsf{sz}(\mathfrak{d})) + d^3C)$. Since this is repeated n times this has complexity in $\tilde{O}(d^2nB_{\mathrm{id}} + d^2n\,\mathsf{sz}(\mathfrak{d}) + nd^3C)$. The reductions then cost $\tilde{O}(d(d^2+n)(B_{\mathrm{id}} + \mathsf{sz}(\mathfrak{d})) + d^2n(B_\mathfrak{a} + B_A + d\log(|\Delta_K|) + dC) + d^2(d+n)C + d^3n\log(|\Delta_K|))$ per row, that is, $\tilde{O}(dn(d^2+n)\,\mathsf{sz}(\mathfrak{d}) + d^2n^2B_A + d^2n^2B_\mathfrak{a})$ in total neglecting C and $\log(|\Delta_K|)$. □

Remark 3.13. Although using lattice reduction in the normalization step we are able to bound the size of the coefficient ideals, the size already contains a factor d^4. Together with the expensive ideal operations this explains the strong dependency on d. In addition, the normalization and reduction steps themselves involve a costly lattice reduction algorithm. Unfortunately the dependency of the overall complexity of Algorithm 3.9 on the chosen lattice reduction algorithm is rather involved. We find ourselves on the horns of a dilemma—we have to make sure that the lattice reduction is not too expensive, but at the same time, we need small lattice bases to bound the size of elements and ideals during our algorithm.

§3E. Relative versus absolute computations

We now want to compare the modular pseudo-Hermite normal form algorithm (Algorithm 3.9) with the Hermite normal form algorithm over the integers in situations where we can "choose" the structure we work with. We describe two examples to illustrate the idea.

In practice number fields of large degree are constructed carefully as towers of extensions of type $L \supseteq K \supseteq \mathbf{Q}$ where K is a number field of degree d and L is an extension of K of degree n. The ring of integers $\mathcal{O}_L$ of L as well as the fractional ideals of L are naturally finitely generated modules of rank n over the Dedekind domain $\mathcal{O}_K$. On the other hand, $\mathcal{O}_L$ as well as the fractional ideals of L are naturally free of rank dn over the principal ideal domain $\mathbf{Z}$. Thus the computation with ideals in $\mathcal{O}_L$ can either rely on the pseudo-Hermite normal form over $\mathcal{O}_K$ or on the Hermite normal form over $\mathbf{Z}$ and it is not clear which to prefer.

The second situation we have in mind is quite different. Assume that we are in a situation where we have two finitely generated torsion free $\mathcal{O}$-modules M and N and we are faced with the problem of deciding whether $M \subseteq N$ or $M = N$. After imposing further properties on a pseudo-Hermite normal form yielding uniqueness the problem can be settled using the pseudo-Hermite normal form algorithm. But as the question only depends on the underlying sets of M and N (discarding the $\mathcal{O}$-structure) the problem can be sorted out using the Hermite normal form over the integers. Again it is not clear which method to prefer.

We consider $((\mathfrak{a}_i)_i, A)$, a full-rank pseudo-matrix over $\mathcal{O}$ with $A \in K^{n\times n}$ and associated module $M \subseteq \mathcal{O}^n$. To compute the structure over the integers we have to turn this pseudo-matrix into a $dn \times dn$ matrix over the integers. As each fractional ideal $\mathfrak{a}_i$ is isomorphic to $\mathbf{Z}^d$ as a $\mathbf{Z}$-module, we have $M = A_1\mathfrak{a}_1 + \dots + A_n\mathfrak{a}_n \cong \mathbf{Z}^{dn}$, the isomorphism being induced by the isomorphisms $\mathfrak{a}_i \to \mathbf{Z}^d$. Assume that $\beta \in K$ is an element of the i-th row of A and $\mathfrak{a} = \mathfrak{a}_i$ is the corresponding coefficient ideal of this row. Denote by $\alpha_1, \dots, \alpha_d$ the Hermite normal form basis of $\mathfrak{a}$. The coefficients of the d products $\beta\alpha_1, \dots, \beta\alpha_d$ form a $d \times d$ $\mathbf{Z}$-matrix, with which we replace β. Applying this procedure to all matrix entries of A we obtain a $dn \times dn$ matrix B over the integers, which corresponds to a basis of the free $\mathbf{Z}$-module M of rank dn. These are n^2 computations each having complexity in $\tilde{O}(d^2\max(\mathsf{sz}(\alpha_{i,j})) + d\max(\mathsf{sz}(\mathfrak{a}_i)) + d^2C)$. As $\mathsf{sz}(\beta\alpha_i) \le \mathsf{sz}(\beta) + \mathsf{sz}(\mathfrak{a})/d + C$ the matrix B satisfies $\log(|B|) \le \max(\mathsf{sz}(\alpha_{ij}))/d + \max(\mathsf{sz}(\mathfrak{a}_i))/d^2 + C/d$. Since we know that the matrix B has determinant $\mathbf{N}(\mathfrak{d})$, where $\mathfrak{d}$ denotes the determinantal ideal of $((\mathfrak{a}_i)_i, A)$, computing the Hermite normal form over the integers has complexity in

$$\tilde{O}((dn)^2\log(|B|) + (dn)^3\log(\mathbf{N}(\mathfrak{d}))) \subseteq \tilde{O}(dn^2\max\mathsf{sz}(\alpha_{i,j}) + n^2\max\mathsf{sz}(\mathfrak{a}_i) + d^2n^3\,\mathsf{sz}(\mathfrak{d}) + d^2nC).$$

Combining this with the complexity of computing B we get an overall complexity in

$$\tilde{O}(d^2n^2\max\mathsf{sz}(\alpha_{i,j}) + dn^2\max\mathsf{sz}(\mathfrak{a}_i) + d^2n^3\,\mathsf{sz}(\mathfrak{d}) + d^3n^2C).$$

While the dependency on n is the same as in the pseudo-Hermite normal form case (see Theorem 3.12), the powers of d are slightly lower due to the absence of ideal arithmetic involving normalization and reduction. We conclude: Always use the Hermite normal form over the rational integers if possible. But note that this discussion depends on the chosen pseudo-Hermite normal form algorithm and not on the notion of the pseudo-Hermite normal form itself and of course it is possible that more sophisticated approaches, as for example in the next section, yield different conclusions.

§4. Residue techniques

Assumption. Let K be an algebraic number field of degree d with ring of integers $\mathcal{O}$.

Consider a pseudo-matrix over K with admissible modulus $\mathfrak{m}$. In the previous section we have shown that by reducing intermediate results modulo $\mathfrak{m}\mathfrak{a}^{-1}$, where $\mathfrak{a}$ is a coefficient ideal, and by normalizing the coefficient ideals, we can control the size of the pseudo-matrix entries during the pseudo-Hermite normal form computation. While carefully adjusting the coefficient ideals ensuring that the span does not change, we transformed the pseudo-matrix into lower triangular form yielding a pseudo-Hermite normal form in the end.

When considering the complexity, we see that this approach has two major drawbacks. First of all, the normalization and the reductions modulo $\mathfrak{m}\mathfrak{a}^{-1}$ are extremely costly since they are based on reduced bases and therefore involve lattice reduction algorithms. While the LLL-algorithm and successors thereof show that the problem has polynomial complexity in the size of the input, the dependency on the rank is unhealthily large. On the other hand the necessary modifications of the coefficient ideals themselves are very costly, as they include multiplications and inversions of ideals.

In this chapter we suggest a new approach in the spirit of the original modular Hermite normal form computation over $\mathbf{Z}$. One of the most natural techniques to prevent coefficient swell during the Hermite normal form computation over the integers is the use of residual methods, which goes back to Iliopoulos [Ili89] and Domich, Kannan and Trotter [DKT87]: Instead of computing the Hermite normal form over $\mathbf{Z}$, one computes a normal form over $\mathbf{Z}/m\mathbf{Z}$ for some suitable $m \in \mathbf{Z}$ and lifts the result back to $\mathbf{Z}$. We will show that the same can be done for pseudo-matrices. Instead of working over $\mathcal{O}$ and reducing the entries in the pseudo-matrix modulo ideals now and then, we literally work with modules and matrices over $\mathcal{O}/\mathfrak{m}$.

Working in $\mathcal{O}/\mathfrak{m}$ has two advantages: First of all, as this ring is a Euclidean ring (see §1A), we can rely on a variant of the Howell form making coefficient ideals superfluous. Secondly, we do not have to use lattice reductions to keep the size of the entries bounded. We will show that using probabilistic algorithms we can efficiently work within $\mathcal{O}/\mathfrak{m}$ and with modules over $\mathcal{O}/\mathfrak{m}$.

This section is joint work with Claus Fieker and has been published in [FH14].

§4A. Basic operations

In order to describe the complexity of our algorithms we will rely on a modified notion of basic operations introduced by Mulders and Storjohann in [SM98]. Let (R, φ) be a Euclidean ring and $a, b \in R$. Then a *basic operation* is one of the following:

(B1) For $* \in \{+, -, \cdot\}$ return $a * b$.

(B2) If b divides a in R return an element $\mathsf{div}(a, b) = c \in R$ such that $bc = a$.

(B3) If $b \neq 0$ return $\mathsf{eudiv}(a, b) = (q, r) \in R^2$ such that $a = qb + r$ with $r = 0$ or $\varphi(r) < \varphi(b)$.

(B4) Return $\mathsf{xgcd}(a, b) = (g, s, t, u, v) \in R^5$ such that $(g) = (a, b)$, $g = sa + tb$, $ua + vb = 0$ and $sv - ut = 1$, i.e.,

$$\begin{pmatrix} g & 0 \end{pmatrix} = \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} s & u \\ t & v \end{pmatrix}$$

and the transformation matrix is unimodular.

(B5) Return $\mathsf{Ann}(a) = c$ such that $(c) = \mathrm{Ann}(a) = \{r \in R \mid ra = 0\}$.

Remark 4.1. In [SM98] it is shown that in case of $R = \mathbf{Z}/N\mathbf{Z}$ operations (B1) through (B5) can be performed using $O(M(\log(N)\log(\log(N))))$ bit operations, where $M(t)$ is a bound on the number of bit operations required to multiply two $\lceil t \rceil$-bit integers.

Assumption. Let $\mathfrak{m}$ be a nonzero integral ideal of K with norm N.

We now turn to the case $R = (\mathcal{O}/\mathfrak{m})$, for which there exists an additional basic operation.

(B6) Given an integral ideal $\mathfrak{a}$ of $\mathcal{O}$, return an element $\mathsf{gen}(\mathfrak{a}) = \overline{c} \in (\mathcal{O}/\mathfrak{m})$ such that $\overline{\mathfrak{a}} = (\overline{c})$ in $(\mathcal{O}/\mathfrak{m})$.

We now want to show how each basic operation (Bi) in $(\mathcal{O}/\mathfrak{m})$, $1 \le i \le 6$, can be solved algorithmically using basic operations in $\mathbf{Z}/N\mathbf{Z}$, where $N = \mathbf{N}(\mathfrak{m})$ is the norm of $\mathfrak{m}$. We assume that we are given $\mathbf{Z}$-bases $(\omega_i)_{1 \le i \le d}$ and $(\nu_i)_{1 \le i \le d}$ of $\mathcal{O}$ and $\mathfrak{m}$ respectively such that $\nu_i = n_i \omega_i$ with integers $n_i \in \mathbf{Z}_{\ge 1}$, $1 \le i \le d$, i.e., the basis matrix of $\mathfrak{m}$ is diagonal. Then the map

$$(\mathcal{O}/\mathfrak{m}) \longrightarrow (\mathbf{Z}/n_1\mathbf{Z}) \times \cdots \times (\mathbf{Z}/n_d\mathbf{Z}),\ \overline{\sum_i a_i \omega_i} \longmapsto (\overline{a}_1, \ldots, \overline{a}_d)$$

is an isomorphism of abelian groups which we use to identify $(\mathcal{O}/\mathfrak{m})$ with $\prod_i \mathbf{Z}/n_i\mathbf{Z}$.

Evaluating the canonical map $\mathcal{O} \to (\mathcal{O}/\mathfrak{m})$ at an element $\sum_i a_i\omega_i$ consists of d divisions with remainder and the addition of two elements in $(\mathcal{O}/\mathfrak{m})$ consists of d additions in $\mathbf{Z}/n_i\mathbf{Z}$. As the above map is not multiplicative, multiplication of two elements $\overline{a} = (\overline{a}_1, \dots, \overline{a}_d)$, $\overline{b} = (\overline{b}_1, \dots, \overline{b}_d) \in (\mathcal{O}/\mathfrak{m})$ is more involved. More precisely the element $\overline{c} = (\overline{c}_1, \dots, \overline{c}_d) \in (\mathcal{O}/\mathfrak{m})$ with $\overline{a}\overline{b} = \overline{c}$ is given by

$$\overline{c}_k = \overline{\sum_i \sum_j a_i b_j \Gamma_{i,j}^k} \in (\mathbf{Z}/n_k\mathbf{Z}),$$

where $(\Gamma_{i,j}^k)_{i,j,k}$ denotes the structure constants of the $\mathbf{Z}$-algebra $\mathcal{O}$ with respect to the basis $(\omega_i)_{1 \leq i \leq d}$. Thus for each $1 \leq k \leq d$ we need $O(d^2)$ basic operations in $(\mathbf{Z}/n_k\mathbf{Z})$ to compute $\overline{c}_k$.

To accomplish (B2), denote by $M_b \in \mathrm{Mat}_{d\times d}(\mathbf{Z})$ the representation matrix of $\mathcal{O} \to \mathcal{O}, x \mapsto bx$ with respect to (ω_i), where each entry is reduced modulo N, and by $M_\mathfrak{m}$ the diagonal basis matrix of $\mathfrak{m}$. Then $\overline{a} = \overline{b}\overline{c}$ for some element $c \in (\mathcal{O}/\mathfrak{m})$ if and only if the equation $(M_b|M_\mathfrak{m})X = a$ is solvable. As this linear system can be solved modulo N, we need $O(d^3)$ basic operations in $\mathbf{Z}/N\mathbf{Z}$. Note that the kernel of this matrix is (the lift) of $\mathrm{Ann}(\overline{b})$, the annihilator of $\overline{b}$ in $(\mathcal{O}/\mathfrak{m})$.

So far we have shown that operations (B1) and (B2) can be performed using $O(d^3)$ basic operations in $\mathbf{Z}/N\mathbf{Z}$ (for the sake of simplicity a basic operation in $\mathbf{Z}/k\mathbf{Z}$ with $1 \leq k \leq N$ is counted as a basic operation in $\mathbf{Z}/N\mathbf{Z}$).

We now turn to the more involved operations (Bi), $3 \leq i \leq 6$, the big difference to (B1) being the non-uniqueness of the operations (again mainly due to the presence of zero-divisors). Using the Chinese remainder theorem we will see that the defining properties of the operations can be stated purely in terms of valuations at each prime ideal dividing $\mathfrak{m}$. Therefore the main task will be the construction of integral elements with prescribed behavior at a finite set of prime ideals. While there exist deterministic algorithms for this problem, they have the major flaw that they need a costly prime ideal factorization of $\mathfrak{m}$. To overcome this difficulty, we will pursue the idea of probabilistic algorithms. More precisely our algorithms will be of Las Vegas type with expected polynomial running time, which can be easily turned into Monte Carlo algorithms if wished. The running time of our algorithms will depend on the value

$$p_\mathfrak{m} = \frac{|(\mathcal{O}/\mathfrak{m})^\times|}{|(\mathcal{O}/\mathfrak{m})|} = \prod_{\mathfrak{p}|\mathfrak{m}} \left(1 - \frac{1}{\mathbf{N}(\mathfrak{p})}\right),$$

which we will use throughout this section.

We assume that we have access to an oracle producing random elements in any finite ring of the form $\mathbf{Z}/k\mathbf{Z}$, $k \in \mathbf{Z}_{>0}$. During the complexity analysis we will omit the costs of calling this oracle.

Lemma 4.2. Let $\overline{a} \in (\mathcal{O}/\mathfrak{m})$. Computing $\varphi(\overline{a})$ can be done using $O(d^3)$ basic operations in $\mathbf{Z}/N\mathbf{Z}$, where φ is the Euclidean function of Proposition 1.4.

Proof. We first compute the d products $\overline{a\omega_i}$ for $1 \leq i \leq d$ using $O(d^3)$ basic operations in $\mathbf{Z}/N\mathbf{Z}$. Denoting by $\gamma_1, \dots, \gamma_d$ the canonical lifts of these elements we know that $\gamma_1, \dots, \gamma_d, \nu_1, \dots, \nu_d$ constitute a $\mathbf{Z}$-generating system of $(a) + \mathfrak{m}$. Computing the Hermite normal form basis of this generating system then can be done using $O(d^3)$ basic operations in $\mathbf{Z}/N\mathbf{Z}$ while the norm computation takes $O(d)$ such operations. □

Algorithm 4.3 (Probabilistic Euclidean division). Let $\overline{a}, \overline{b} \in (\mathcal{O}/\mathfrak{m})$, $\overline{b} \neq \overline{0}$. The following steps return $\mathsf{eucdiv}(\overline{a}, \overline{b})$.

(1) Choose $\overline{q} \in (\mathcal{O}/\mathfrak{m})$ uniformly distributed and compute $\overline{r} = \overline{a} - \overline{q}\overline{b}$.
(2) If $\varphi(\overline{r}) \geq \varphi(\overline{a})$ go to Step 1.
(3) Return $(\overline{q}, \overline{r})$.

Lemma 4.4. Let $\overline{a}, \overline{b} \in (\mathcal{O}/\mathfrak{m})$ such that $\overline{b}$ does not divide $\overline{a}$. For each prime divisor $\mathfrak{p}$ of $\mathfrak{m}$ define

$$S_\mathfrak{p} = \begin{cases} (\mathcal{O}/\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})}), & \text{if } 0 < v_\mathfrak{p}(a) < v_\mathfrak{p}(b), \\ (\mathcal{O}/\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})})^\times, & \text{if } v_\mathfrak{p}(b) < v_\mathfrak{p}(a), \\ \{\overline{x} \in (\mathcal{O}/\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})} \mid \mathbf{N}((a + xb), \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})}) \leq \mathbf{N}(b, \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})})\}, & \text{if } v_\mathfrak{p}(a) = v_\mathfrak{p}(b). \end{cases}$$

Then the following holds:

(i) If $\overline{c} \in (\mathcal{O}/\mathfrak{m})$ is an element such that $\overline{c}_\mathfrak{p} \in S_\mathfrak{p}$ for all prime divisors $\mathfrak{p}$ of $\mathfrak{m}$, then $\varphi(\overline{a} + \overline{b}\overline{c}) < \varphi(\overline{b})$.

(ii) We have $\{\overline{c} \in (\mathcal{O}/\mathfrak{m}) \mid \varphi(\overline{a}+\overline{b}\overline{c}) < \varphi(\overline{b})\} \geq |(\mathcal{O}/\mathfrak{m})^\times|$.

(iii) If $\overline{q} \in (\mathcal{O}/\mathfrak{m})$ is uniformly distributed in $(\mathcal{O}/\mathfrak{m})$, then the probability that $\overline{a} = \overline{q}\overline{b} + (\overline{a} - \overline{q}\overline{b})$ is a Euclidean division is at least $p_\mathfrak{m}$.

Proof. (i): Let $\overline{c}_\mathfrak{p} \in S_\mathfrak{p}$. In the second and third case we have $v_\mathfrak{p}(a+bc) \leq v_\mathfrak{p}(b)$ while in the first case we have $v_\mathfrak{p}(a+bc) = v_\mathfrak{p}(a) < v_\mathfrak{p}(b)$. Since $\overline{b}$ does not divide $\overline{a}$ there exists a prime divisor $\mathfrak{p}$ of $\mathfrak{m}$ such that $0 < v_\mathfrak{p}(a) < v_\mathfrak{p}(b)$ implying that $\mathbf{N}((a+bc), \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})}) < \mathbf{N}(b, \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})})$. Thus we have $\varphi(\overline{a}+\overline{b}\overline{c}) < \varphi(\overline{b})$.

(ii): It remains to show $\# S_\mathfrak{p} \geq \#(\mathcal{O}/\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})})^\times$ in the case $v_\mathfrak{p}(a) = v_\mathfrak{p}(b)$. If $v_\mathfrak{p}(b) \geq v_\mathfrak{p}(\mathfrak{m})$, then $S_\mathfrak{p} = \mathcal{O}/\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})}$ and we are done. Therefore let $v_\mathfrak{p}(b) < v_\mathfrak{p}(\mathfrak{m})$ and consider the natural map $\pi\colon (\mathcal{O}/\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})}) \to (\mathcal{O}/\mathfrak{p}^{v_\mathfrak{p}(b)+1})$. The set $\pi(S_\mathfrak{p})$ is the complement of the set of solutions $\overline{a} = -\overline{b}\overline{x}$ with $\overline{x} \in (\mathcal{O}/\mathfrak{p}^{v_\mathfrak{p}(b)+1})$. As this equation has $\mathbf{N}((b), \mathfrak{p}^{v_\mathfrak{p}(b)+1}) = \mathbf{N}(\mathfrak{p}^{v_\mathfrak{p}(b)})$ solutions we have $\#\pi(S_\mathfrak{p}) = \mathbf{N}(\mathfrak{p}^{v_\mathfrak{p}(b)+1}) - \mathbf{N}(\mathfrak{p}^{v_\mathfrak{p}(b)})$. It follows that $\# S_\mathfrak{p} = \mathbf{N}(\mathfrak{p})^{v_\mathfrak{p}(\mathfrak{m})-(v_\mathfrak{p}(b)+1)} \#\pi(S_\mathfrak{p}) = \#(\mathcal{O}/\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})})^\times$.

(iii): This follows from (ii). □

Proposition 4.5. Algorithm 4.3 is correct. The expected number of basic operations in $\mathbf{Z}/N\mathbf{Z}$ is $O((1/p_\mathfrak{m})d^3))$.

Proof. We need to count the expected number of repetitions of Step 1. It is easy to see that for $i \in \mathbf{Z}_{\geq 1}$, with probability $p_\mathfrak{m}(1-p_\mathfrak{m})^{i-1}$ the number of repetitions of Step 1 is i. Thus the expected number is $p_\mathfrak{m} \sum_{i=1}^\infty i(1-p_\mathfrak{m})^{i-1} = p_\mathfrak{m}(1/p_\mathfrak{m} + (1-p_\mathfrak{m})/p_\mathfrak{m}^2) = 1/p_\mathfrak{m}$. Now the claim follows as Step 1 needs $O(d^3)$ basic operations in $\mathbf{Z}/N\mathbf{Z}$. □

Finding a generator of an ideal and computing the annihilator. Let $\mathfrak{a}$ be an ideal of $\mathcal{O}$. It is easy to see that for an element $c \in \mathcal{O}$ the equation $(\overline{c}) = \overline{\mathfrak{a}}$ holds if and only if for all prime divisors $\mathfrak{p}$ of $\mathfrak{m}$ we have $v_\mathfrak{p}(c, \mathfrak{m}) = v_\mathfrak{p}(\mathfrak{a}, \mathfrak{m})$, that is, $\min(v_\mathfrak{p}(c), v_\mathfrak{p}(\mathfrak{m})) = \min(v_\mathfrak{p}(\mathfrak{a}), v_\mathfrak{p}(\mathfrak{m}))$.

Algorithm 4.6. Let $\mathfrak{a}$ be an integral ideal of $\mathcal{O}$. The following steps return $\overline{c} \in (\mathcal{O}/\mathfrak{m})$ such that $(\overline{c}) = \overline{\mathfrak{a}}$.

(1) Compute $(\mathfrak{a}, \mathfrak{m})$.
(2) Choose $\overline{c} \in (\mathfrak{a}, \mathfrak{m})/(N^2)$ uniformly distributed.
(3) If $(\mathfrak{a}, \mathfrak{m}) \neq (\mathfrak{m}, c)$ go to Step 2.
(4) Return $\overline{c} \in (\mathcal{O}/\mathfrak{m})$.

Lemma 4.7. Algorithm 4.6 is correct and the expected number of basic operations in $\mathbf{Z}/N\mathbf{Z}$ is $O((1/p_\mathfrak{m})d^3)$.

Proof. We prove the following: If $\mathfrak{a}$ is an integral ideal of $\mathcal{O}$ and $\overline{c}$ is chosen uniformly in $(\mathfrak{a}, \mathfrak{m})/(N^2)$, then the probability that $(\mathfrak{a}, \mathfrak{m}) = (N, c)$ is $p_\mathfrak{m}$. Let $\mathfrak{b} = (\mathfrak{a}, \mathfrak{m})$ and fix one prime divisor $\mathfrak{p}$ of $\mathfrak{m}$. We want to count the elements $\overline{c} \in \mathfrak{b}/(N^2)$ such that $v_\mathfrak{p}(c) = v_\mathfrak{p}(\mathfrak{b})$. Note that $v_\mathfrak{p}(N^2) > v_\mathfrak{p}(\mathfrak{b})$ and therefore $c \in \mathfrak{b}\backslash\mathfrak{b}\mathfrak{p}$ is equivalent to $\overline{c} \in \mathfrak{b}/(N^2)\backslash\mathfrak{b}\mathfrak{p}/(N^2)$. Counting the elements in these sets we see that the probability that an element $\overline{c} \in \mathfrak{b}/(N^2)$ satisfies $v_\mathfrak{p}(c) = v_\mathfrak{p}(\mathfrak{b})$ is $(1 - 1/\mathbf{N}(\mathfrak{p}))$.

Note that Step 1 needs $O(d^3)$ basic operations in $\mathbf{Z}/N\mathbf{Z}$. We have already shown that the expected number of executions of Step 3 is $1/p_\mathfrak{m}$. As each execution consists of $O(d^3)$ basic operations in $\mathbf{Z}/N\mathbf{Z}$, the claim follows. □

Lemma 4.8. Let $\overline{b} \in (\mathcal{O}/\mathfrak{m})$. Then we can compute $\overline{c} = \mathsf{Ann}(\overline{b})$ with an expected number of $O((1/p_\mathfrak{m})d^3)$ basic operations in $\mathbf{Z}/N\mathbf{Z}$.

Proof. After computing the annihilator as the kernel of M_b modulo N (as for (B2)) using $O(d^3)$ basic operations, we apply Algorithm 4.6 to obtain a generator. □

Extended GCD computation. We now turn to the xgcd problem. In case of the rational integers $\mathbf{Z}$ the task is easy: If g is a greatest common divisor of two integers $a, b \in \mathbf{Z}$ we can compute $s, t \in \mathbf{Z}$ such that $g = sa + tb$. Then

$$\begin{pmatrix} g & 0 \end{pmatrix} = \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} s & -b/g \\ t & a/g \end{pmatrix}$$

and we are done. While we can of course just use the normal Euclidean algorithm to find the cofactors, this is, in our case, rather expensive as each Euclidean division requires a random search. On the other hand, computing the GCD directly using ideals takes only *one* random search.

As the underlying idea is that dividing by a greatest common divisor produces coprime elements, the example at the end of Section §1A shows that we cannot blindly adapt this in the presence of zero-divisors. Fortunately Proposition 1.8 shows that there exist minimal quotients $\overline{e}, \overline{f}$ with respect to the Euclidean function such that

$\overline{eg} = \overline{a}$, $\overline{fg} = \overline{b}$ and $(\overline{e}, \overline{f}) = (\mathcal{O}/\mathfrak{m})$. In particular there exist $\overline{u}, \overline{v} \in (\mathcal{O}/\mathfrak{m})$ such that $\overline{eu} + \overline{fv} = 1$. A quick calculation shows that

$$\begin{pmatrix} \overline{g} & \overline{0} \end{pmatrix} = \begin{pmatrix} \overline{a} & \overline{b} \end{pmatrix} \begin{pmatrix} \overline{u} & -\overline{f} \\ \overline{v} & \overline{e} \end{pmatrix}$$

is a unimodular transformation implying that $\mathsf{xgcd}(\overline{a}, \overline{b}) = (\overline{g}, \overline{u}, \overline{v}, -\overline{f}, \overline{e})$ is valid.

In order to apply this we need to explain how to find minimal quotients and how to express a greatest common divisor as a linear combination.

Lemma 4.9. (i) Let $\overline{b}$ be a divisor of $\overline{a}$. An element $\overline{c} \in (\mathcal{O}/\mathfrak{m})$ with $\overline{cb} = \overline{a}$ and $\varphi(\overline{c}) = \varphi(\overline{a})/\varphi(\overline{b})$ can be computed using an expected number of $O((1/p_{\mathfrak{m}})d^3)$ basic operations in $\mathbf{Z}/N\mathbf{Z}$.

(ii) Let $\overline{e}, \overline{f} \in (\mathcal{O}/\mathfrak{m})$ be such that $(\overline{e}, \overline{f}) = (\mathcal{O}/\mathfrak{m})$. Then $\overline{u}, \overline{v}$ with $\overline{ue} + \overline{vf} = 1$ can be computed using $O(d^3)$ basic operations in $\mathbf{Z}/N\mathbf{Z}$.

(iii) Let $\overline{a}, \overline{b} \in (\mathcal{O}/\mathfrak{m})$. Then $\mathsf{xgcd}(\overline{a}, \overline{b})$ can be computed with an expected number of $O((1/p_{\mathfrak{m}})d^3)$ basic operations.

Proof. (i): Using (B2) we can compute a fixed quotient $\overline{c}_0$. Moreover we have seen that at the same time we obtain a basis of an ideal $\mathfrak{a}$ of $\mathcal{O}$ with $\overline{\mathfrak{a}} = \operatorname{Ann}(\overline{b})$. Invoking (B6) we can compute a generator of the ideal $\overline{\mathfrak{a}}$. Now we choose uniformly distributed elements $\overline{q} \in \overline{\mathfrak{a}}$ until $\varphi(\overline{c}_0 + \overline{q}) = \varphi(\overline{a})/\varphi(\overline{b})$. If this is the case then $\overline{c}_0 + \overline{q}$ is a quotient which is minimal with respect to the Euclidean function. Proposition 1.8 shows that if $\overline{q}$ is uniformly distributed in $\operatorname{Ann}(\overline{b})$, then $\overline{c}_0 + \overline{q}$ is uniformly distributed in $\overline{(a, \mathfrak{m})(b, \mathfrak{m})^{-1}}$. Now the claim follows from Lemma 1.3.

(ii): As in the case of division, we see that the set of tuples $(\overline{x}, \overline{y}) \in (\mathcal{O}/\mathfrak{m})^2$ with $\overline{xe} + \overline{yf} = \overline{1}$ is the set of integer solutions of a system of d linear equations with $3d$ variables over $\mathbf{Z}$. As in addition this system can be solved modulo N, the task of finding a suitable tuple $(\overline{x}, \overline{y})$ can be solved using $O(d^3)$ basic operations in $\mathbf{Z}/N\mathbf{Z}$.

(iii): Follows from (i) and (ii). □

Corollary 4.10. Any basic operation in $(\mathcal{O}/\mathfrak{m})$ can be performed with an expected number of $O((1/p_{\mathfrak{m}})d^3)$ basic operations in $\mathbf{Z}/N\mathbf{Z}$ and with an expected complexity in $\tilde{O}((1/p_{\mathfrak{m}})d^3 \log(N))$.

§4B. Applications to matrix normal forms

The aim of this section is to introduce residual methods for the computation of normal forms of $\mathcal{O}$-modules by passing to a quotient ring $(\mathcal{O}/\mathfrak{m})$ for some suitable integral ideal $\mathfrak{m}$ and by lifting the result back to $\mathcal{O}$.

Strong echelon form for principal ideal rings.

Definition 4.11. Let R be a commutative ring. Let $M \subseteq R^m$ be an R-module. A matrix $H = (h_{ij}) \in \operatorname{Mat}_{n\times m}(R)$, $n \geq m$, is called *strong echelon form* of M if and only if

(S1) for $1 \leq i \leq m$ the i-th row of H is zero or $i = \max\{1 \leq j \leq m \mid h_{ij} \neq 0\}$. For $i > m$ the i-th row of H is zero.

(S2) For $1 \leq i \leq m$ the rows $1, \ldots, i$ generate $\operatorname{sp}_{m-i}(M)$.

To illustrate the definitions consider the following matrices over $\mathbf{Z}/6\mathbf{Z}$:

$$A = \begin{pmatrix} \overline{0} & \overline{0} \\ \overline{1} & \overline{3} \end{pmatrix}, \quad B = \begin{pmatrix} \overline{2} & \overline{0} \\ \overline{5} & \overline{3} \end{pmatrix}, \quad C = \begin{pmatrix} \overline{0} & \overline{0} \\ \overline{2} & \overline{0} \\ \overline{5} & \overline{3} \end{pmatrix}. \quad D = \begin{pmatrix} \overline{2} & \overline{0} \\ \overline{5} & \overline{3} \\ \overline{0} & \overline{0} \end{pmatrix}.$$

It is easy to see that the rows have the same span $M \subseteq (\mathbf{Z}/6\mathbf{Z})^2$. While the matrix A has a minimal number of nonzero rows the element $(\overline{2}, \overline{0}) \in \operatorname{sp}(A)$ shows that A does not satisfy (S2). On the other hand the matrix C violates (S1). Thus only B and D are strong echelon forms of M.

Remark 4.12. A few words on the relation between the strong echelon form and the Howell normal form:

(i) In contrast to the Howell normal form we now "order" the basis elements. This will be important in Section §4B where we describe the combination of strong echelon forms.

(ii) Note that we will use the strong echelon form over $(\mathcal{O}/\mathfrak{m})$ only as an auxiliary step to obtain normal forms over $\mathcal{O}$. Since this does not require the strong echelon form to be unique, this explains the absence of appropriate restrictions in the definition. For working with $(\mathcal{O}/\mathfrak{m})$-modules themselves we can recover

uniqueness easily by the following steps. We have to show how to find a fixed representative modulo $(\mathcal{O}/\mathfrak{m})^\times$ and modulo $(\overline{d})$ for some $\overline{d} \in (\mathcal{O}/\mathfrak{m})$. The former problem can be solved by noting that if $\overline{a}$ is an element of $(\mathcal{O}/\mathfrak{m})$, then the coset of $\overline{a}$ modulo $(\mathcal{O}/\mathfrak{m})^\times$ is equal to the set of all $\overline{b} \in (\mathcal{O}/\mathfrak{m})$ with $(b, \mathfrak{m}) = (a, \mathfrak{m})$. Thus given an ideal $\mathfrak{a}$ of $\mathcal{O}$, we need a way to fix a generator of $\overline{\mathfrak{a}}$. By replacing step (2) of Algorithm 4.6 with a deterministic loop through all elemens of $(\mathfrak{a}, \mathfrak{m})/(N^2)$ one obtains an algorithm for computing a generator with the property that it yields the same result for ideals $\mathfrak{a}$, $\mathfrak{b}$ with $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$. Hence using this modified algorithm we can fix generators of ideals of $\mathcal{O}/\mathfrak{m}$.
By reducing the off-diagonal elements modulo the unique Hermite normal form basis of $(d, \mathfrak{m})$, where d is the corresponding diagonal entry, we obtain unique representatives for the off-diagonal elements.

Based on Howell's approach, Storjohann and Mulders describe in [SM98] a simple algorithm for computing the Howell normal form over $\mathbf{Z}/N\mathbf{Z}$, which easily generalizes to any ring supporting basic operations (Bi), $1 \leq i \leq 6$. The following modified version yields a strong echelon form. Note that we assume that the matrix has at least as many rows as columns, which can always be achieved by padding the matrix with zero rows.

Algorithm 4.13 (Strong echelon form over principal ideal rings). Let $A \in \mathrm{Mat}_{n\times m}(R)$ be a matrix with $n \geq m$, where R is a ring supporting (B1)–(B6). The following steps return a strong echelon form of A.

```
(1) (This puts $A$ into triangular form). For $1 \leq i < j \leq n$ compute $(g, s, t, u, v) = \mathsf{xgcd}(a_{j,i}, a_{j,j})$ and set
        $\begin{pmatrix} A_j \\ A_i \end{pmatrix} = \begin{pmatrix} s & t \\ u & v \end{pmatrix} \begin{pmatrix} A_j \\ A_i \end{pmatrix}.$
(2) Augment $A$ with one zero row.
(3) For $1 \leq j \leq m$ do the following:
    (4) If $a_{j,j} \neq 0$ compute $c = \mathsf{Ann}(a_{j,j})$ and set $A_{n+1} = cA_j$. If $a_{j,j} = 0$ then set $A_{n+1} = A_j$.
    (5) For $j + 1 \leq i \leq m$ compute $(g, s, t, u, v) = \mathsf{xgcd}(a_{i,i}, a_{n+1,i})$ and set
        $\begin{pmatrix} A_i \\ A_{n+1} \end{pmatrix} = \begin{pmatrix} s & t \\ u & v \end{pmatrix} \begin{pmatrix} A_i \\ A_{n+1} \end{pmatrix}.$
(6) Sort the rows of $A$ such that (S1) is satisfied.
(7) Return $A$.
```

Theorem 4.14. Algorithm 4.13 is correct and requires $O(m^2 \max(n, m))$ basic operations in R.

Proof. See [SM98, Theorem 3]. □

Remark 4.15. If, in Algorithm 4.13, we perform only step (1) on a matrix $A \in \mathrm{Mat}_{n\times n}(R)$, we end with a lower triangular matrix $B \in \mathrm{Mat}_{n\times n}(R)$, and there exists a matrix $T \in \mathrm{Mat}_{m\times m}(R)$ with determinant 1 such that $B = TA$. Thus in case $m = n$, that is, A is a square matrix, we can transform A into triangular form using $O(n^3)$ basic operations in R.

Modular computation of a strong echelon form. One of the reasons why we have introduced the strong echelon form is the important fact that it allows for efficient residual computations. To be more precise let R be a principal ideal ring and $a, b, e, f \in R$ elements such that $ab = 0$ and $1 = ea + fb$. Denote by π_a and π_b the canonical projections of R onto $R/(a)$ and $R/(b)$ respectively. By abuse of notation we denote the induced projections $R^m \to (R/(a))^m$ and $\mathrm{Mat}_{n\times n}(R) \to \mathrm{Mat}_{n\times n}(R/(a))$ also by π_a; we do the same for π_b. Then for any R-module $M \subseteq R^m$ the equation

$$M = 1M = eaM + fbM = ea(M + bR^m) + fb(M + aR^m) \tag{2.4}$$

holds. As $M + aR^n = \pi_a^{-1}(\pi_a(M))$ and $M + bR^n = \pi_b^{-1}(\pi_b(M))$ we see that M can be obtained by lifting the modules $\pi_a(M)$ and $\pi_b(M)$, which are now living over the (hopefully "smaller") rings $R/(a)$ and $R/(b)$, back to R. The following lemma shows that by using the strong echelon form the lifting procedure comes for free.

Lemma 4.16. Assume that $A = (a_{ij})_{i,j} \in \mathrm{Mat}_{n\times m}(R)$ is a matrix such that $\pi_a(A) \in \mathrm{Mat}_{n\times m}(R/(a))$ is a strong echelon form of $\pi_a(M)$. Furthermore we assume that all diagonal elements a_{ii}, $1 \leq i \leq m$, are divisors of a and $a_{ij} = 0$ whenever $j > i$. Then A is a strong echelon form of $M + aR^m$.

Proof. Property (S1) is clear. We prove property (S2) by induction on i and begin with $i = 1$. We need to show that A_1, the first row of A, generates $\mathrm{sp}_{m-1}(M + aR^m)$.

Thus let $v = (v_1, 0, \dots, 0) \in \mathrm{sp}_{m-1}(M + aR^m)$. We have $\pi_a(v) \in \mathrm{sp}_{m-1}(\pi_a(M))$, which is generated by $\pi_a(A_1)$. Thus we can find $r \in R$ with $\pi_a(v_1) = r\pi_a(A_1)$, that is, $v_1 - rA_1 \in aR^m$. Because A_1 is of the form $(a_{11}, 0, \dots, 0)$ we have $v_1 - rA_1 = (c, 0, \dots, 0)$ for some $c \in aR$. As a_{11} is a divisor of a, we can find $r \in R$ with $c = r'a_{11}$. In particular $v_1 - rA_1 - r'A_1 = 0$.

Now let $2 \leq i \leq m-1$ and assume (S2) holds for $i-1$. Let $v = (v_1, v_2, \dots, v_i, 0, \dots, 0) \in \mathrm{sp}_{m-i}(M + aR^m)$. If $\pi_a(v_1) \neq 0$, then $\pi_a(v) \in \mathrm{sp}_{m-1}(\pi_a(M))$, and we can find $r_1, \dots, r_i \in R$ such that $\pi_a(v) = r_1\pi_a(A_1) + \dots + r_i\pi_a(A_i)$, that is, $v - r_1A_1 - \dots - r_iA_i \in aR^m$. Because there are only zeros above the diagonal of A we have

$$v - r_1A_1 - \dots - r_iA_i = (c_1, \dots, c_i, 0, \dots, 0) \in aR^m.$$

As in the base case of the induction, we can find $r \in R$ such that $c_i = ra_{ii}$, implying that

$$v' = v - r_1A_1 - \dots - r_iA_i - rA_i = (c_1, \dots, c_{i-1}, 0, \dots) \in \mathrm{sp}_{m-(i-1)}(M).$$

Now the claim follows by applying the induction hypothesis to v'. □

Thus by computing strong echelon forms over $R/(a)$ and $R/(b)$ we can compute strong echelon forms of $M + aR^n$ and $M + bR^n$. We now turn to the recombination step. Let A and B be strong echelon forms of $M + aR^n$ and $M + bR^n$ respectively. By padding A or B with zero rows we may assume that A and B have the same number of rows.

Lemma 4.17. The matrix $fbA + eaB$ is a strong echelon form of M.

Proof. Firstly we show $M = \mathrm{sp}(fbA + eaB)$. Equation (2.4) implies that M is generated by fbA_i, eaB_i, $1 \leq i \leq n$. Therefore it is sufficient to prove $fbA_i, eaB_i \in \mathrm{sp}(fbA + eaB)$. As fb is an idempotent, i.e., $(fb)^2 = fb$, we have $fbA_i = (fb)^2A_i + (fb)(ea)B_i = fb(fbA_i + eaB_i) \in \mathrm{sp}(fbA + eaB)$ and analogously $eaB_i \in \mathrm{sp}(fbA + eaB)$.

Since eaB and fbA have property (S1), so does the sum. Property (S2) follows by decomposing an element $v \in M$ into $v = fbv + eav$ and applying property (S2) of eaB and fbA. □

Now let $\mathfrak{m}$ and $\mathfrak{n}$ be coprime integral ideals of $\mathcal{O}$. We want to apply the preceding discussion to the computation of a strong echelon form of an $(\mathcal{O}/\mathfrak{mn})$-module M. Denote by $\overline{a}$ and $\overline{b}$ generators of the ideals $\overline{\mathfrak{m}}$ and $\overline{\mathfrak{n}}$ in $(\mathcal{O}/\mathfrak{mn})$. Then $\overline{ab} = 0$, and $(\mathcal{O}/\mathfrak{mn})/(\overline{a})$ and $(\mathcal{O}/\mathfrak{mn})/(\overline{b})$ are isomorphic to $\mathcal{O}/\mathfrak{m}$ and $\mathcal{O}/\mathfrak{n}$ respectively. We have canonical projections $\pi_a = \pi_{\mathfrak{m}} \colon (\mathcal{O}/\mathfrak{mn}) \to (\mathcal{O}/\mathfrak{m})$ and $\pi_b = \pi_{\mathfrak{n}} \colon (\mathcal{O}/\mathfrak{mn}) \to (\mathcal{O}/\mathfrak{n})$. As $\overline{a}$ and $\overline{b}$ are coprime, we can compute $\overline{e}, \overline{f} \in (\mathcal{O}/\mathfrak{mn})$ such that $\overline{ea} + \overline{fb} = 1$. Thus we are in a situation where we can apply Lemma 4.16 and 4.17. The only missing step is the normalization of the diagonal elements in the assumption of Lemma 4.17.

We assume that A' is a matrix over $(\mathcal{O}/\mathfrak{mn})$ such that $\pi_{\mathfrak{m}}(A')$ is a strong echelon form of $\pi_{\mathfrak{m}}(M)$. We define a new matrix A over $(\mathcal{O}/\mathfrak{mn})$ by setting the i-th row A_i to be

$$A_i = \overline{b}A'_i + (\overline{a}\delta_{i,j})_{1 \leq j \leq n}$$

for $1 \leq i \leq n$, where $\delta_{i,j}$ denotes the Kronecker delta. As $\overline{b}$ is a unit modulo $\mathfrak{m}$ and $\pi_{\mathfrak{m}}(\overline{a}) = 0$, the matrix $\pi_{\mathfrak{m}}(A)$ is also a strong echelon form of $\pi_{\mathfrak{m}}(M)$. We claim that A satisfies the assumption of Lemma 4.16. To prove this we show that for all $\overline{d} \in (\mathcal{O}/\mathfrak{mn})$ the element $\overline{bd} + \overline{a}$ is a divisor of $\overline{a}$ in $(\mathcal{O}/\mathfrak{mn})$. Note that this is equivalent to $\min(v_{\mathfrak{p}}(bd + a), v_{\mathfrak{p}}(\mathfrak{mn})) \leq \min(v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(\mathfrak{mn}))$ for all prime divisor $\mathfrak{p}$ of $\mathfrak{mn}$. If $\overline{d} = 0$ this holds obviously. Therefore we may assume $\overline{d} \neq 0$. But then the claim follows easily by noting that $v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(\mathfrak{m})$ if $\mathfrak{p} \mid \mathfrak{m}$ and $v_{\mathfrak{p}}(b) > 0 = v_{\mathfrak{p}}(a)$ if $\mathfrak{p} \mid \mathfrak{n}$.

We now apply this to the pseudo-Hermite normal form computation.

Assumption. We assume that $\mathcal{P} = ((\mathfrak{a}_i)_i, A)$ is a pseudo-matrix of full rank with $A \in \mathrm{Mat}_{n\times m}(K)$ and span $M = \mathrm{sp}(\mathcal{P}) \subseteq \mathcal{O}^m$. By $\mathfrak{m}$ we denote an admissible modulus of $\mathcal{P}$, that is, $\mathfrak{m}\mathcal{O}^m \subseteq M$.

Denote by $\pi_{\mathfrak{m}}$ the canonical projection $\mathcal{O} \to \mathcal{O}/\mathfrak{m}$ and the induced projections on $\mathcal{O}^m$ and $\mathrm{Mat}_{n\times n}(\mathcal{O})$.

Algorithm 4.18. The following steps return a matrix $\overline{B} \in \mathrm{Mat}_{m\times m}(\mathcal{O}/\mathfrak{m})$ such that $\mathrm{sp}(\overline{B}) = \pi_{\mathfrak{m}}(\mathrm{sp}(\mathcal{P}))$.

(1) For $1 \leq i \leq n$ find elements $a_i \in K$ such that $\mathfrak{b}_i = a_i\mathfrak{a}_i$ is integral and coprime to $\mathfrak{m}$, and divide row A_i by a_i.

(2) For $1 \leq i, j \leq m$ write $A_{ij} = a_{ij}/b_{ij}$ with $a_{ij}, b_{ij} \in \mathcal{O}$ and b_{ij} coprime to $\mathfrak{m}$.
(3) return $\overline{B} = (\overline{a}_{ij}\overline{b}_{ij}^{-1})_{i,j}$.

A few remarks on the correctness. Step 1 does not change the span and the new coefficient ideals $\mathfrak{b}_i$—being coprime to $\mathfrak{m}$—satisfy $\pi_{\mathfrak{m}}(\mathfrak{b}_i) = (\mathcal{O}/\mathfrak{m})$. Moreover the relation $\mathfrak{m}\mathcal{O}^m \subseteq M \subseteq \mathcal{O}^m$ implies that the denominators of all matrix entries can be chosen to be coprime to $\mathfrak{m}$. Finding the elements a_i in Step 1 is just an application of the approximation theorem (see [Coh00, Corollary 1.3.9]).

Applying Algorithm 4.13 to the matrix $\overline{B}$ obtained in the preceding algorithm we arrive—after removing zero rows—at a matrix $C \in \mathrm{Mat}_{m\times m}(\mathcal{O})$ such that $\pi_{\mathfrak{m}}(C)$ is a strong echelon form of $\pi_{\mathfrak{m}}(M)$. The connection to the original module M is given by the following lemma.

Lemma 4.19. Assume that $C \in \mathrm{Mat}_{m\times m}(\mathcal{O})$ is a matrix such that $\pi_{\mathfrak{m}}(C)$ is a strong echelon form of $\pi_{\mathfrak{m}}(M)$. Then the pseudo-matrix $\mathcal{P}' = (I, D)$ with $I = (\mathcal{O}, \dots, \mathcal{O}, \mathfrak{m}, \dots, \mathfrak{m})$ and $D = (C^t | \mathbf{1}_m)^t$ satisfies $\mathrm{sp}(\mathcal{P}') = M$.

Proof. Let v be an element of M. As $\pi_{\mathfrak{m}}(v) \in \pi_{\mathfrak{m}}(M) = \mathrm{sp}(\pi_{\mathfrak{m}}(C))$, there exist $a_i \in \mathcal{O}$ such that $v - \sum_{i=1}^{n} a_i C_i \in \mathfrak{m}\mathcal{O}^m$. Now the claim follows. □

Thus by computing a preimage $C = (c_{ij})$ of a strong echelon form over the ring $(\mathcal{O}/\mathfrak{m})$, we arrive at the following pseudo-matrix spanning the original module (we write the coefficient ideals in front of the corresponding rows):

$$\mathcal{P}' = \begin{array}{cc} \begin{array}{c} \mathcal{O} \\ \mathcal{O} \\ \mathcal{O} \\ \mathcal{O} \\ \mathcal{O} \\ \mathfrak{m} \\ \mathfrak{m} \\ \mathfrak{m} \\ \mathfrak{m} \\ \mathfrak{m} \end{array} & \left(\begin{array}{ccccc} c_{1,1} & & & & \\ * & c_{2,2} & & 0 & \\ * & * & \cdots & & \\ * & * & \cdots & \cdots & \\ * & * & \cdots & * & c_{m,m} \\ \hline 1 & & & & \\ & 1 & & 0 & \\ & & \cdots & & \\ & 0 & & \cdots & \\ & & & & 1 \end{array} \right) \end{array}. \tag{2.5}$$

We now apply the classical pseudo-Hermite normal form algorithm of Cohen to this pseudo-matrix. The special shape allows us to skip most of the steps and we actually never have to work with all of $\mathcal{P}'$.

Algorithm 4.20 (Demodularization). Let $C \in \mathrm{Mat}_{m\times m}(\mathcal{O})$ be a matrix such that $\pi_{\mathfrak{m}}(C)$ is a strong echelon form of $\pi_{\mathfrak{m}}(M)$. The following steps return a pseudo-Hermite normal form with span equal to M.

```
(1) For $i = m, \dots, 1$ do the following:
(2) Let $\mathfrak{g} = (c_{i,i}, \mathfrak{m})$ and compute $x \in (c_{i,i})\mathfrak{g}^{-1}$, $y \in \mathfrak{m}\mathfrak{g}^{-1}$ such that $1 = x + y$.
(3) Set $\mathfrak{b}_i = \mathfrak{g}$, $B_i = xA_i/c_{i,i}$ and $B_{i,i} = 1$.
(4) return $((\mathfrak{b}_i)_{1\leq i\leq m}, B)$.
```

Theorem 4.21. Algorithm 4.20 is correct.

Proof. For the proof it is convenient to think of all operations applied to the pseudo-matrix $\mathcal{P}'$ in (5.2), which actually spans the module M by Lemma 4.19. We now take a look at Step 2 and Step 3. For the sake of convenience we consider only the case $i = m$. By [Coh96, Prop. 1.3] the pseudo-matrices

$$\begin{array}{cc} \begin{array}{c} (c_{m,m}) \\ \mathfrak{m} \end{array} & \left(\begin{array}{cccc} c_{m,1}/c_{m,m} & \cdots & c_{m,m-1}/c_{m,m} & 1 \\ 0 & \cdots & 0 & 1 \end{array} \right) \end{array}$$

and

$$\begin{array}{cc} \begin{array}{c} \mathfrak{g} \\ \mathfrak{m}\mathfrak{g}^{-1} \end{array} & \left(\begin{array}{cccc} x(c_{m,1}/c_{m,m}) & \cdots & x(c_{m,m-1}/c_{m,m}) & 1 \\ -c_{m,1} & \cdots & -c_{m,m-1} & 0 \end{array} \right) \end{array}$$

span the same module. We need to show that the second row of the latter pseudo-matrix is superfluous. Let v be in the span of the second row. In particular $v \in \mathrm{sp}(M)$ and $\pi_{\mathfrak{m}}(v) \in \pi_{\mathfrak{m}}(M) = \mathrm{sp}(\pi_{\mathfrak{m}}(C))$. As the last entry is zero we have $\pi_{\mathfrak{m}}(v) \in \mathrm{sp}_1(\pi_{\mathfrak{m}}(C))$. As $\pi_{\mathfrak{m}}(C)$ is a strong echelon form this implies that there exists $r_j \in \mathcal{O}$ such that $v - \sum_{j=1}^{m-1} r_j C_j \in \mathrm{sp}_1(\mathfrak{m}\mathcal{O}^m)$. Thus $v = \sum_{j=1}^{m-1} r_j C_j + \sum_{j=1}^{m-1} s_j e_j$ for some $s_j \in \mathfrak{m}$ and $e_j = (\delta_{ji})_{1\leq i\leq m}$. □

A few remarks on the complexity. While the inversion of ideals requires at most $O(d^3)$ operations using a precomputed 2-element representation of the codifferent, the multiplication requires $O(d^4)$ operations if both ideals are given by their $\mathbf{Z}$-bases. Therefore a naive approach to Step 2 requires $O(d^4)$ operations. But we can do better by noting that

$$\mathfrak{m}\mathfrak{g}^{-1} = (\mathfrak{m}(a)^{-1} \cap \mathcal{O}) \text{ and } (a)\mathfrak{g}^{-1} = (\mathfrak{m}(a)^{-1} \cap \mathcal{O})^{-1} \cap \mathcal{O}.$$

Now the ideal product involves a principal ideal and can be performed using at most $O(d^3)$ operations. Since the artificially introduced inversions and intersections with $\mathcal{O}$ require at most $O(d^3)$ operations, the whole step requires at most $O(d^3)$ operations. Note that the naive application of the pseudo-Hermite normal form algorithm of Cohen would have required $O(n^2)$ operations similar to Step 2 involving growing ideals. Let us summarize our algorithm.

Algorithm 4.22. Given an $\mathcal{O}$-module M and a pseudo-matrix $\mathcal{P}$ with $\operatorname{sp}(\mathcal{P}) = M$, the following steps return a pseudo-Hermite normal form of M.

(1) Find an ideal $\mathfrak{m}$ such that $\mathfrak{m}\mathcal{O}^m \subseteq M$ (see Section 5).
(2) Compute $C \in \operatorname{Mat}_{m\times m}(\mathcal{O})$ such that $\pi_\mathfrak{m}(C)$ is a strong echelon form of $\pi_\mathfrak{m}(M)$ using Algorithm 4.13 and Algorithm 4.24
(3) Return the result of Algorithm 4.20 applied to C.

Let $\mathcal{P} = ((\mathfrak{a}_i), A)$ be a pseudo-matrix with $A \in \operatorname{Mat}_{m\times m}(K)$ and span $M \subseteq \mathcal{O}^m$. Note that in order for the modular algorithm to be applicable, it is crucial that there exists some integral ideal $\mathfrak{m}$ such that $\mathfrak{m}\mathcal{O}^m \subseteq M \subseteq \mathcal{O}^m$, which is equivalent to A being of rank m. As in the case $\mathcal{O} = \mathbf{Z}$ without this assumption this modular technique won't work.

Remark 4.23. It is worthwhile to mention the special case $\mathcal{O} = \mathbf{Z}$, for which we can recover the classical Hermite normal form over $\mathbf{Z}$. Let $M \subseteq \mathbf{Z}^m$ be a $\mathbf{Z}$-module of rank m and $A \in \operatorname{Mat}_{n\times m}(\mathbf{Z})$ a matrix with $\operatorname{sp}(A) = M$. Moreover let $\lambda \in \mathbf{Z}_{>0}$ be an element with $\lambda\mathbf{Z}^m \subseteq M$ and $C \in \operatorname{Mat}_{m\times m}(\mathbf{Z})$ such that C modulo $\lambda\mathbf{Z}$ is a strong echelon form of $\pi_\lambda(M) \subseteq (\mathbf{Z}/\lambda\mathbf{Z})^m$. Note that by multiplying the rows of $C \bmod \lambda\mathbf{Z}$ with suitable elements of $(\mathbf{Z}/\lambda\mathbf{Z})^\times$ and by adding suitable elements, we can achieve that the diagonal elements of C actually divide λ. Thus the whole demodularization step is superfluous and C is the Hermite normal form of M. This is in total contrast to the classical modular Hermite normal form algorithms, where after a computation in $\mathbf{Z}/\lambda\mathbf{Z}$ one has to compute again a non-modular Hermite normal form of a matrix similar to (5.2) (see [HM91, Section 2.1]). Hence we obtain an algorithm, that given A together with λ computes the Hermite normal form of A with complexity in $\tilde{O}(nm\log(|A|) + nm^2\log(\lambda))$.

§4C. Splitting the modulus

In order to speed up computations, we would like, if possible to split the modulus, the idea being that if $\mathfrak{m} = \mathfrak{a}\mathfrak{b}$ with $\mathfrak{a}, \mathfrak{b}$ coprime, then, by the Chinese remainder theorem, $(\mathcal{O}/\mathfrak{m}) = (\mathcal{O}/\mathfrak{a}) \times (\mathcal{O}/\mathfrak{b})$ and thus "everything" modulo $\mathfrak{m}$ can be done more efficiently by computing in $(\mathcal{O}/\mathfrak{a})$ and $(\mathcal{O}/\mathfrak{b})$. If we allow for a complete factorization, we of course achieve $(\mathcal{O}/\mathfrak{m}) = \prod_\mathfrak{p}(\mathcal{O}/\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{m})})$, however, for general $\mathfrak{m}$, a factorization is prohibitively expensive. We observe that the complete factorization would result in the best complexity!

Furthermore, for any prime $\mathfrak{p}$ of degree one we have

$$(\mathcal{O}/\mathfrak{p}^k) \cong \mathbf{Z}/p^k\mathbf{Z}$$

for p the rational prime with $\mathfrak{p} \cap \mathbf{Z} = p\mathcal{O}$. Again, the Chinese remainder theorem, this time for $\mathbf{Z}$, allows us to combine any degree one prime ideals with distinct underlying rational primes into one, thus obtaining:

$$(\mathcal{O}/\mathfrak{m}) \cong (\mathbf{Z}/m\mathbf{Z}) \times (\mathcal{O}/\mathfrak{m}')$$

with some potentially much smaller ideal $\mathfrak{m}'$ and a suitable integer $m \in \mathbf{Z}$. Once such a decomposition is obtained, much faster algorithms for $\mathbf{Z}/m\mathbf{Z}$ can be applied for hopefully a large part of the ring.

Unfortunately, without the use of factorization such a complete splitting is difficult to achieve. We propose the following simple algorithm which is aimed at computing a large portion of the "degree one part" while still being fast.

Algorithm 4.24 (Z-split). Let $\mathfrak{m}$ be an integral ideal. The following steps will produce coprime integral ideals $\mathfrak{a}$, $\mathfrak{b}$ with $\mathfrak{a}\mathfrak{b} = \mathfrak{m}$ and a rational integer $m \in \mathbf{Z}$ such that $(\mathcal{O}/\mathfrak{a}) \cong \mathbf{Z}/m\mathbf{Z}$

(1) Let $m = \min(\mathbf{Z}_{\geq 1} \cap \mathfrak{m})$ and $b = \mathbf{N}(\mathfrak{m})/m$.
(2) Repeat $g \leftarrow \gcd(m, b)$, $m \leftarrow m/g$ and $b \leftarrow b^2 \bmod m$ until $g = 1$.
(3) Compute $\mathfrak{a} = m\mathcal{O} + \mathfrak{m}$ and $\mathfrak{b} = (\mathbf{N}(\mathfrak{m})/m)\mathcal{O} + \mathfrak{m}$.
(4) Return $\mathfrak{a}, \mathfrak{b}$.

Note that this algorithm will not necessarily find the largest ideal $\mathfrak{a} \mid \mathfrak{m}$ such that $(\mathcal{O}/\mathfrak{a}) \cong \mathbf{Z}/m\mathbf{Z}$ and $\mathfrak{a}$, $\mathfrak{m}\mathfrak{a}^{-1}$ are coprime: Let $\mathfrak{m} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{q}_1\mathfrak{q}_2$ where $\mathfrak{p}_i$, $\mathfrak{q}_i$ are primes of degree one lying above distinct rational primes p and q respectively. Then $\min(\mathfrak{m}) = pq$ and $\mathbf{N}(\mathfrak{m}) = p^2q^2$, so the algorithm will terminate with $\mathfrak{a} = \mathcal{O}$. However, $\mathfrak{a} = \mathfrak{p}_1\mathfrak{q}_1$ would be a correct result—but we need to actually factorize $\mathfrak{m}$ to find this decomposition.

Proof (of correctness). For any integral ideal $\mathfrak{a}$ the minimum $\min(\mathfrak{a}) = \min(\mathbf{Z}_{\geq 1} \cap \mathfrak{a})$ is equal to $\exp(\mathcal{O}/\mathfrak{a})$ (the exponent of the abelian group $(\mathcal{O}/\mathfrak{a})$): Clearly, $\min(\mathfrak{a}) \in \mathfrak{a}$ and $\operatorname{ord}(1) = \min \mathfrak{a}$ where ord is the order of the element. Thus if $\mathbf{N}(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}| = \min(\mathfrak{a})$, then $(\mathcal{O}/\mathfrak{a}) \cong \mathbf{Z}/\min(\mathfrak{a})\mathbf{Z}$, generated by 1.

From the decomposition above we see that if $\mathbf{N}(\mathfrak{a}) \neq \min(\mathfrak{a})$, then we either have a prime $\mathfrak{q}$ dividing $\mathfrak{a}$ of degree greater than one, we have at least two distinct prime ideals $\mathfrak{q}_i \mid \mathfrak{a}$ $(i = 1, 2)$ lying above the same rational prime or for some ramified prime $\mathfrak{q}$ we have $\mathfrak{q}^2 \mid \mathfrak{a}$. In the first case $(\mathcal{O}/\mathfrak{q}, +)$ is a non-cyclic group, in the second case we have a product of 2 cyclic groups with non-coprime orders while in the last case clearly $\min(\mathfrak{q}) = \min(\mathfrak{q}^2)$, but $\mathbf{N}(\mathfrak{q}) \neq \mathbf{N}(\mathfrak{q}^2)$. In all other cases $\mathfrak{a}$ is composed of powers of degree one prime ideals over distinct rational primes as well as ramified primes with exponent 1.

In the algorithm b initially contains all rational primes q such that either $\mathfrak{q} \mid q$ for some prime of degree greater than one, $\mathfrak{q}_i \mid q$ with $i = 1, 2$ or $\mathfrak{q}^2 \mid \mathfrak{a}$ for some ramified prime $\mathfrak{q} \mid q$. During the loop, we remove all those rational primes from m and in the final step we then split $\mathfrak{m}$ accordingly. The squaring of b ensures that the total time is polynomially bounded in $N = \mathbf{N}(\mathfrak{m})$. □

Remark 4.25. Let $\mathfrak{m} = \mathfrak{a}\mathfrak{b}$ be the splitting obtained by this algorithm. Experimentally, we have $\mathbf{N}(\mathfrak{b}) \ll \mathbf{N}(\mathfrak{a})$, in fact frequently, $\mathbf{N}(\mathfrak{b}) = 1$, thus the effort to compute a pseudo-Hermite normal form over a number field is mostly independent of it's degree and depends almost *only* on the dimension of the matrix.

§4D. Experimental results

We have implemented both the Euclidean structure and the improved pseudo-Hermite normal form computation in the computer algebra system MAGMA [BCP97]. To illustrate the efficiency of our techniques, we computed pseudo-Hermite normal forms for random matrices over a range of fields. We used $K = \mathbf{Q}[t]/(t^d - 10)$ for $d = 2$, 4, 8, and generated matrices of dimensions n up to 300, depending on d. More specifically, starting at $k = 1$, we computed for two random matrices A of dimension $n = 10 \cdot k$ a pseudo-Hermite normal form of the pseudo-matrix $((\mathcal{O})_{1 \leq i \leq n}, A)$ both using our method and MAGMA's implementation of Cohen's algorithm (available through the command HermiteForm) until a single computation took more than one hour. By random matrices we mean matrices over $\mathcal{O}$, where the coefficients (with respect to a fixed integral basis) of the matrix entries are chosen uniformly in $\{-2^B, \dots, 2^B\}$ for the times t_1, t_2 and rounded normally distributed with mean 0 and variance 2^{2B} for the times g_1, g_2. Table 2.1 shows the results for different choices of parameters d, n and B, where t_1 (resp. g_1) denotes the running time (in seconds) using Algorithm 4.22 and t_2 (resp. g_2) the running time (in seconds) using MAGMA's implementation of Cohen's algorithm. We briefly note that the longer running times for the normal distributed matrix entries are a consequence of them being larger: By Hadamard's inequality, the size of the determinant depends mainly on the largest entry in each row or column respectively. Using normal distributed entries, this maximum value will usually be larger than 2^B, which is reflected in the runtime.

While for very small parameters ($d = 2$, $B = 10$, $n \leq 40$) Algorithm 4.22 is slower then HermiteForm, we see that our algorithm clearly outperforms MAGMA'S algorithm for number fields of large degree.

§5. Computation of determinants over rings of integers

Assumption. Let K be an algebraic number field of degree d with ring of integers $\mathcal{O}$.

As already noted, an important ingredient in our pseudo-Hermite normal form algorithms is an admissible modulus of the module under consideration. The algorithms presented in this section describe how to obtain such an ideal in case it is not known in advance. More precisely, we will show how to compute the determinantal ideal of a square pseudo-matrix. For this we first describe a polynomial algorithm for computing the determinant of a square matrix over $\mathcal{O}$. Already for matrices over $\mathbf{Z}$ computing determinants is a rather

Table 2.1.: Algorithm 4.22 versus MAGMA's HermiteForm

d	B	n	t_1	t_2	t_2/t_1	g_1	g_2	g_2/g_1
2	10	10	0.095	0.020	0.210	0.030	0.010	0.333
		20	0.130	0.065	0.500	0.335	0.080	0.238
		30	0.375	0.210	0.560	0.465	0.155	0.333
		40	0.325	0.300	0.923	0.405	0.360	0.888
		200	107.715	143.975	1.336	128.335	165.475	1.289
		300	580.370	1031.430	1.777	842.675	1210.775	1.436
2	100	10	0.075	0.155	2.066	0.055	0.090	1.636
		20	0.380	0.655	1.723	0.400	0.740	1.850
		30	1.245	2.490	2.000	1.455	2.890	1.986
		40	3.265	6.985	2.139	3.155	10.630	3.369
		80	47.945	107.115	2.234	51.495	107.320	2.084
		140	549.080	1194.445	2.175	540.660	1008.665	1.865
4	10	10	0.080	0.055	0.687	0.055	0.085	1.545
		20	0.260	0.390	1.500	0.195	0.385	1.974
		30	0.525	1.040	1.980	0.640	1.325	2.070
		40	1.955	3.080	1.575	0.945	3.440	3.640
		80	10.080	37.970	3.515	12.165	48.505	3.987
		140	77.640	346.315	4.460	107.005	402.735	3.763
8	10	10	0.290	0.850	2.931	0.160	0.660	4.125
		20	0.620	5.345	8.620	1.445	6.955	4.813
		30	1.605	26.470	16.492	1.785	33.190	18.593
		40	5.675	57.535	10.138	7.355	96.797	13.160
		80	48.445	746.120	15.401	44.720	917.765	20.522

involved task, see [KV04] for a survey of different approaches and their complexity. Performing very well in practice and being a deterministic polynomial algorithm we present a determinant algorithm for matrices over $\mathcal{O}$ which is based on the small primes modular approach.

§5A. Bounding the size of the output

The underlying idea of a modular determinant algorithm is the possibility to bound the size of the result before the actual computation. For a matrix $A = (a_{ij})_{i,j} \in \mathrm{Mat}_{n\times n}(\mathcal{O})$ denote by $|A|$ the number $\max_{i,j}\{\|a_{ij}\|_\infty\}$.

Lemma 5.1. For a matrix $A = (a_{ij})_{i,j} \in \mathrm{Mat}_{n\times n}(\mathcal{O})$ we have the inequality $\|\det(A)\|_\infty \leq n^n C_1 C_2^n |A|^n$, that is, $\log(\|\det(A)\|_\infty) \in O(n\log(n|A|) + nC)$. Here C_1, C_2 are the constants of §2B, page 12.

Proof. We have $\det(A) = \sum_{\sigma\in\mathfrak{S}_n} \mathrm{sgn}(\sigma)\prod_{i=1}^n a_{i,\sigma(i)}$ and therefore

$$\|\det(A)\|_\infty \leq C_1 \|\det(A)\| \leq n! \max_{i,j}(\|a_{ij}\|)^n \leq C_1 C_2^n n^n |A|.$$

□

Lemma 5.2. Let $\alpha = \sum_{i=1}^d a_i\omega_i$ and $\beta = \sum_{i=1}^d b_i\omega_i$ be two algebraic integers in $\mathcal{O}$. Assume there exists $B \in \mathbf{R}_{>0}$ such that $|a_i|, |b_j| < B/2$ for all $1 \leq i, j \leq d$ and $\alpha \equiv \beta \mod (B)$. Then $\alpha = \beta$.

Proof. Since $(\omega_i)_i$ is a $\mathbf{Z}$-basis of $\mathcal{O}$, the family $(B\omega_i)_i$ is a $\mathbf{Z}$-basis of the principal ideal (B). Hence $\alpha \equiv \beta \mod (B)$ is equivalent to the divisibility of $a_i - b_i$ by B for all $1 \leq i \leq d$. Using the coefficient bound we obtain

$$0 \leq |a_i - b_i| \leq |a_i| + |b_i| < B.$$

We conclude that $a_i = b_i$ for all $1 \leq i \leq d$, that is, $\alpha = \beta$. □

We now proceed as in the integer case. After computing the determinant modulo several rational primes p we combine the results via the Chinese remainder theorem. As soon as the product of the rational primes exceeds the a priori bound from Lemma 5.1 we can recover the actual value using Lemma 5.2. We will give two different algorithms for this task. The first one computes directly in $\mathcal{O}/p\mathcal{O}$ and uses the residue techniques introduced in the previous section. For this reason the result will be a Las Vegas algorithm with expected polynomial complexity. For the sake of completeness we will also formulate a deterministic algorithm with polynomial complexity. The idea is to decompose $p\mathcal{O}$ into prime ideals $\mathfrak{p}$ of $\mathcal{O}$ allowing for computations in the finite field $\mathcal{O}/\mathfrak{p}$. Again the result modulo $p\mathcal{O}$ can be obtained invoking the Chinese remainder theorem.

§5B. Probabilistic determinant computation

In this section, for a rational prime $p \in \mathbf{Z}$, we denote by π_p the canonical projection $\mathcal{O} \to \mathcal{O}/p\mathcal{O}$. We first consider the computation of the reductions.

Lemma 5.3. Let $P \subseteq \mathbf{Z}$ be a finite set of rational integers and $\beta \in \mathcal{O}$.

(i) For $\beta \in \mathcal{O}$, the computation of of $\pi_p(\beta) \in \mathcal{O}/p\mathcal{O}$ for all $p \in P$ has complexity in $\tilde{O}(d\sum_{p\in P}\log(p) + d\log(\|\beta\|_\infty))$.

(ii) For $A \in \mathrm{Mat}_{n\times n}(\mathcal{O})$ the computation of $\pi_p(A) \in \mathrm{Mat}_{n\times n}(\mathcal{O}/p\mathcal{O})$ for all $p \in P$ has complexity in $\tilde{O}(n^2 d(\#P)\max_{p\in P}\log(p) + n^2 d\log(|A|))$.

Proof. (i): Using the remainder tree of Bernstein [Ber08, 18.7] the computation for each coefficient of β is in $\tilde{O}(\sum_{p\in P}\log(p) + \log(\|\beta\|_\infty))$. □

Now let us turn to the determinant computation over rings of the form $\mathcal{O}/p\mathcal{O}$ with $p \in \mathbf{Z}$. Fortunately, in Remark 4.15 we already described how to transform matrices over residue rings of $\mathcal{O}$ into triangular form. It remains to analyze the complexity.

Corollary 5.4. Let $p \in \mathbf{Z}$ and $B \in \mathrm{Mat}_{n\times n}(\mathcal{O}/p\mathcal{O})$. Then we can compute $\det(B) \in \mathcal{O}/p\mathcal{O}$ with complexity in $\tilde{O}((1/p_{p\mathcal{O}}))n^3 d^4 \log(p))$, where $p_{p\mathcal{O}} = \prod_{\mathfrak{p}|(p)}(1 - 1/\mathbf{N}(\mathfrak{p}))$.

Proof. Remark 4.15 shows that we can transform A into triangular form using $O(n^3)$ basic operations in $\mathcal{O}/p\mathcal{O}$. As each basic operation has complexity $\tilde{O}((1/p_{p\mathcal{O}})d^3\log(\mathbf{N}(p\mathcal{O})))$ by Corollary 4.10, the result follows since $\mathbf{N}(p\mathcal{O}) = p^d$. □

Note that here—in contrast to the application of residue techniques in Section 4—we can actually choose the quotient rings we work with. Thus we can choose $p \in \mathbf{Z}$ such that $p_{p\mathcal{O}}$ is at least 1/2. More precisely let $p \in \mathbf{Z}$ be a rational prime with $p > 2d$. Then we have

$$p_{p\mathcal{O}} = \prod_{\mathfrak{p}|p\mathcal{O}}\left(1 - \frac{1}{\mathbf{N}(\mathfrak{p})}\right) \geq \left(1 - \frac{1}{p}\right)^d \geq 1 - \frac{d}{p} > 1/2$$

using Bernoulli's inequality.

To find enough rational prime numbers we rely on the following classical result on the computation and size of the first r primes. It is an application of the detailed analysis of Rosser and Schoenfeld [RS62] as well as the sieve of Eratosthenes and can be found in [vzGG03, Theorem 18.10].

Proposition 5.5. Let $r \in \mathbf{Z}_{>0}$. The first r prime numbers $p_1, \dots, p_r \in \mathbf{Z}_{>0}$ can be computed with complexity in $O(r(\log(r))^2\log\log(r))$ and if $r \geq 2$ each prime satisfies $p_i \leq 2r\ln(r)$, that is, $\log(p_i) \in \tilde{O}(\log(r))$.

Finally we have to apply the Chinese remainder theorem.

Proposition 5.6. Let $P \subseteq \mathbf{Z}$ be a finite set of rational prime numbers with $\#P = r$, $\max_{p\in P} p \leq B$ and $\alpha_p \in \mathcal{O}/p\mathcal{O}$ for all $p \in P$. Then we can find $\alpha \in \mathcal{O}$ such that $\pi_p(\alpha) = \alpha_p$ for all $p \in P$ with complexity in $\tilde{O}(r\log(B)d)$.

Now we can state and analyze the probabilistic determinant algorithm.

Algorithm 5.7 (Probabilistic determinant computation over $\mathcal{O}$). Given $A \in \mathrm{Mat}_{n\times n}(\mathcal{O})$ the following steps return $\det(A)$.

(1) Compute a bound $B \in \mathbf{R}_{>0}$ on $\|\det(A)\|_\infty$ as in Lemma 5.1 and set $r = \lceil\log(B)\rceil \in \mathbf{Z}_{>0}$.
(2) Compute the first $\lceil\log(B)\rceil + 2d$ primes $2 = p_l < \cdots < p_1$.
(3) Compute $\pi_{p_i}(A)$ for $1 \leq i \leq r$.
(4) Compute $\det(\pi_{p_i}(A))$ for $1 \leq i \leq r$.
(5) Compute $\delta \in \mathcal{O}$ such that $\pi_{p_i}(\delta) = \det(\pi_{p_i}(A))$.

(6) Return δ.

Theorem 5.8. Algorithm 5.7 is correct and has expected complexity in $\tilde{O}(d^4 n^4 \log(|A|) + n^4 d^4 C)$.

Proof. As δ is congruent to $\det(A)$ modulo $\prod_{i=1}^r p_i > B$, correctness follows from Lemma 5.2. By Proposition 5.5, Step 2 has complexity in $\tilde{O}(\log(B) + d)$ and all primes satisfy $\log(p_i) \in \tilde{O}(\log(\log(B) + d)) = \tilde{O}(1)$. Thus Step 3 has complexity in $\tilde{O}(n^2 d \log(B) + n^2 d \log(|A|))$ by Lemma 5.3. Since $p_i > 2d$ for $1 \leq i \leq r$, Step 4 has expected complexity in $\tilde{O}(\log(B) n^3 d^4)$. Finally Step 5 has complexity $\tilde{O}(rd)$ by Proposition 5.6. Now the claim follows since $\log(B) \in \tilde{O}(n \log(|A|) + nC)$. □

In case we fix the number field K, that is, we ignore the constants coming from field arithmetic, the expected complexity of Algorithm 5.7 reduces to $\tilde{O}(n^4 \log(|A|))$, which is similar to the integer case: The determinant of a matrix $A \in \mathbf{Z}^{n \times n}$ can be computed with complexity in $\tilde{O}(n^4 \log(|A|))$ (see [vzGG03]).

§5C. Deterministic determinant computation

While the algorithm presented in the previous section has a good complexity, it has the major flaw that it is only probabilistic. Although from a practical point of view this is not a problem, to show that a pseudo-Hermite normal form can be computed in deterministic polynomial time, we still need to give a deterministic polynomial time determinant algorithm. To overcome the "randomness" of Algorithm 5.7, we will decompose $\mathcal{O}/p\mathcal{O}$, p a rational prime, into rings, with which we can compute deterministically. The rings we have in mind are precisely the residue fields $\mathcal{O}/\mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of $\mathcal{O}$.

Let $p \in \mathbf{Z}$ be a rational prime and

$$p\mathcal{O} = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$$

the factorization of $p\mathcal{O}$ into pairwise different prime ideals $\mathfrak{p}_i$ of $\mathcal{O}$ with exponents $e_i \in \mathbf{Z}_{>0}$. The degrees of the residue field extensions $f_i = \dim_{\mathbf{F}_p} \mathcal{O}/\mathfrak{p}_i$, $1 \leq i \leq g$ satisfy

$$\sum_{i=1}^{g} e_i f_i = d.$$

The Chinese remainder theorem now implies

$$\mathcal{O}/p\mathcal{O} \cong \prod_{i=1}^{g} \mathcal{O}/\mathfrak{p}_i^{e_i}.$$

Note that we are only interested in unramified primes p where all e_i's are equal to 1, or else we would have to compute the determinant over $\mathcal{O}/\mathfrak{p}^{e_i}$, a ring containing zero-divisors. Thus we restrict ourselves to the unramified case, where we have $\sum_{i=1}^{g} f_i = d$. Note that there are only finitely many ramified primes, since these are exactly the prime divisors of Δ_K. Thus for almost all primes the problem of determinant computations over $\mathcal{O}/p\mathcal{O}$ is reduced to the equivalent problems over at most d residue fields $\mathcal{O}/\mathfrak{p}$ and the prime ideal factorization of $p\mathcal{O}$.

Let us now investigate the problem of computing in residue fields of $\mathcal{O}$ and the factorization of $p\mathcal{O}$. Fortunately, if we restrict ourselves to rational primes p not dividing the index $[\mathcal{O} \colon \mathbf{Z}[\alpha]]$ there is an elegant answer to both problems due to the following beautiful theorem of Dedekind–Kummer, see [Coh93, Theorem 4.8.13.]. Recall that f is the defining polynomial of the number field K chosen as in Remark 2.10.

Proposition 5.9. Let p be a rational prime not dividing $[\mathcal{O} \colon \mathbf{Z}[\alpha]]$ and $\overline{f} = \prod_{i=1}^{g} \overline{f}_i^{e_i}$ the factorization of $\overline{f} \in \mathbf{F}_p[X]$ into irreducible polynomials. Then

$$\mathcal{O}/p\mathcal{O} \cong \mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha] \cong \mathbf{F}_p[X]/(\overline{f}) \cong \prod_{i=1}^{g} \mathbf{F}_p[X]/(\overline{f}_i).$$

Computing the factorization of $p\mathcal{O}$ in $\mathcal{O}$ is therefore equivalent to the factorization of a polynomial over $\mathbf{F}_p$. We now describe the complexity of passing to the residue field and of working in them. Assume that p is a fixed rational prime, unramified and not dividing $[\mathcal{O} : \mathbf{Z}[\alpha]]$. The first task is the factorization of f modulo p which can be achieved by the deterministic algorithm of Shoup [Sho90, Theorem 3.1].

Proposition 5.10. Let $p \in \mathbf{Z}_{>0}$ be a rational prime. The number of $\mathbf{F}_p$ operations needed to compute the factorization of $\overline{f} \in \mathbf{F}_p[X]$ into irreducible polynomials is in $\tilde{O}(p^{1/2}\log(p)^2 d^2)$. Thus this has complexity in $\tilde{O}(p^{1/2}d^2\log(p)^3)$.

For each irreducible factor $\overline{f}_i \in \mathbf{F}_p[X]$ of $\overline{f}$ we obtain the diagram

$$\mathcal{O} \longrightarrow \mathcal{O}/p\mathcal{O} \xrightarrow{\pi} \mathbf{F}_p[X]/(\overline{f}) \xrightarrow{\pi_i} \mathbf{F}_p[X]/(\overline{f}_i),$$

where π and π_i are the corresponding projections. We now determine the complexity of passing from $\mathcal{O}$ to $\mathbf{F}_p[X]/(\overline{f}_i)$. Let $\beta = \sum_{i=1}^d b_i\omega_i$ be an integral element. Since π is a ring homomorphism we obtain

$$\pi(\beta) = \sum_{j=1}^d \overline{b_i}\pi(\omega_j)$$

where $^-$ denotes reduction $\mathbf{Z} \to \mathbf{F}_p$. Therefore we need to evaluate π only on the integral basis $(\omega_j)_j$. Denote by α the primitive element of K chosen as in Remark 2.10 with minimal polynomial f. We consider the transformation matrix $M = (m_{ij})_{i,j} \in \mathrm{Mat}_{d\times d}(\mathbf{Z})$ between the power basis $(\alpha^j)_{1\leq j\leq d}$ and the integral basis Ω, which is defined by the equations

$$\alpha^j = \sum_{i=1}^d m_{ij}\omega_i$$

for $1 \leq j \leq d$. Then $\pi(\omega_i)$ is just the i-th column of $\overline{M}^{-1} \in \mathrm{Mat}_{d\times d}(\mathbf{F}_p)$, where $\overline{M} \in \mathrm{Mat}_{d\times d}(\mathbf{F}_p)$ is the matrix obtained by reducing each entry of M modulo p. For the complexity analysis we need a bound on the size of M. As $\alpha = \sum_{i=1}^d \varepsilon_i\omega_i$ with $\varepsilon_i \in \{0,1\}$ we have $\mathsf{sz}(\alpha) = d$ and therefore $\mathsf{sz}(\alpha^j) \leq j\,\mathsf{sz}(\alpha) + jC \leq d\,\mathsf{sz}(\alpha) + dC$, that is, $\log(\|\alpha^j\|_\infty) \leq d + C$. This implies $\log(|M|) \leq C + d$ for the size of the entries of M.

Proposition 5.11. Let p, $\overline{f}_1, \dots, \overline{f}_g$, π, π_i and β as in the preceding discussion.

(i) The $d \cdot g$ many images $\pi_i(\omega_j)$, $1 \leq j \leq d$, $1 \leq i \leq g$, can be computed with complexity in $\tilde{O}(d^3\log(p) + d^2C)$.

(ii) Let P be a finite set of primes. The reduction of the coefficient vector of β modulo all primes in P costs $\tilde{O}(d\sum_{p\in P}\log(p) + \mathsf{sz}(\beta))$.

(iii) Assuming that $\pi_i(\omega_j)$, $1 \leq j \leq d$, $1 \leq i \leq g$ as well as the reduction of the coefficient vector of β modulo p is known, the computation of $\pi_i(\beta)$, $1 \leq i \leq g$, has complexity in $\tilde{O}(d^2\log(p))$.

Proof. (i): The reduction of M modulo p has complexity in $\tilde{O}(d^2(\log(p) + C))$ and inverting the reduced matrix over the finite field $\mathbf{F}_p$ has complexity in $\tilde{O}(d^3(\log(p)))$. Then for each $1 \leq j \leq d$ we have to reduce the elements $\pi_i(\omega_j)$ modulo $\overline{f}_i$ for $1 \leq i \leq g$. By [Sho90, Lemma 3.2] this has complexity in $d\tilde{O}(d\log(g)) \subseteq \tilde{O}(d^2)$.

(ii): Using the remainder tree of Bernstein [Ber08, 18.6] the computation for each coefficient has complexity in $\tilde{O}(\sum_{p\in P}\log(p) + \log(\|\beta\|_\infty))$.

(iii): We just have to compute d products $\overline{a}_j\pi_i(\omega_j)$, $1 \leq j \leq d$ and d additions of elements in $\mathbf{F}_p[X]/(\overline{f}_i)$. The last two steps have complexity in $\tilde{O}(d\deg(\overline{f}_i)\log(p))$. Thus summing over all $1 \leq i \leq g$ we obtain a complexity in $\tilde{O}(d^2\log(p))$. □

Working in the residue fields is just polynomial arithmetic over $\mathbf{F}_p$. For the sake of completeness we recall the necessary complexity, see for example [Sho90, Lemma 3.2].

Remark 5.12. (i) Let $a, b \in \mathbf{F}_p$ and $\star \in \{+,-,\cdot,\div\}$. The complexity of computing $a \star b$ (if defined) is in $\tilde{O}(\log(p))$.

(ii) Multiplication of two polynomials of degree $\leq d$ in $\mathbf{F}_p[X]$ can be performed using $\tilde{O}(d)$ operations in $\mathbf{F}_p$.

(iii) Let $f, g \in \mathbf{F}_p[X]$ be two polynomials of degree $\leq d$. Then $f \mod g$ as well as $\gcd(f,g)$ can be computed using $\tilde{O}(d)$ operations in $\mathbf{F}_p$.

(iv) Let $h \in \mathbf{F}_p[X]$ be a polynomial of degree bounded by d. Assume we have $\overline{g}, \overline{f} \in \mathbf{F}_p[X]/(h)$ and $\star \in \{+,-,\cdot,\div\}$. Then (if defined) $\overline{g \star f}$ can be computed using $\tilde{O}(d)$ operations in $\mathbf{F}_p$, that is, the operation has complexity in $\tilde{O}(d\log(p))$.

Finally we describe how to combine the computations in the finite fields to obtain a result in $\mathcal{O}/N\mathcal{O}$. Assume that we have a finite set P of rational primes and $N = \prod_{p\in P} p$. For each prime p we have a factorization of f

modulo p into irreducible factors $\overline{f}_i \in \mathbf{F}_p[X]$, $1 \leq i \leq g$. Using the Chinese remainder theorem for polynomials we can construct a preimage under the map

$$\mathbf{F}_p[X]/(\overline{f}) \to \prod_{i=1}^{g} \mathbf{F}_p[X]/(\overline{f}_i).$$

The next step is an application of the Chinese remainder theorem for rational integers for each coefficient yielding a preimage under the map

$$\mathbf{Z}[X]/(\overline{f}, N) \longrightarrow \prod_{p \in P} \mathbf{F}_p[X]/(\overline{f}).$$

Finally we have to compute a preimage under the map $\mathcal{O}/N\mathcal{O} \to \mathbf{Z}[X]/(\overline{f}, N)$.

Proposition 5.13. Using the notation from the preceding paragraphs the following holds:

(i) Let $\overline{h}_i \in \mathbf{F}_p[X]/(\overline{f}_i)$ for $1 \leq i \leq d$. Computing $\overline{h} \in \mathbf{F}_p[X]/(\overline{f})$ such that $\pi_i(\overline{h}) = \overline{h}_i$, $1 \leq i \leq g$ has complexity in $\tilde{O}(d \log(p))$.

(ii) Assume we are given $\overline{g}_p \in \mathbf{F}_p[X]/(\overline{f})$ for $p \in P$. Then we can compute $\overline{h} \in \mathbf{Z}[X]/(f, N)$ with $\overline{h} = \overline{g}_p$ in $\mathbf{F}_p[X]/(\overline{f})$ for $p \in P$ with complexity in $\tilde{O}(d \log(B) r)$ where $B \in \mathbf{R}_{\geq 0}$ is such that $p \leq B$ for all $p \in P$ and $\#P = r \geq 2$ is the number of involved primes.

(iii) Given $\overline{g} \in \mathbf{Z}[X]/(f, N)$ the computation of a preimage under the map $\mathcal{O}/N\mathcal{O} \to \mathbf{Z}[X]/(f, N)$ has complexity in $\tilde{O}(d^2(d + C + \log(N)))$.

Proof. (i): This is Corollary 10.23 in [vzGG03].

(ii): Due to Bernstein [Ber08, §23] Chinese remaindering involving r moduli of size bounded by B has complexity in $\tilde{O}(\log(B) r)$. Since we have d coefficients, the result follows.

(iii): This is just a matrix vector product between the coefficients of g and M. □

We still need to describe how many primes we need and of which size they are. By Lemma 5.1 the number $B = n^n C_1 C_2^n |A|^n \in \mathbf{R}_{>0}$ satisfies $\|\det(A)\|_\infty \leq B$. Choosing the first $r' = \lceil \log(B) \rceil$ primes we obtain $\prod_{i=1}^{r'} p_i > 2B$. As we have seen there is a finite number of bad primes we need to avoid. More precisely we are only interested in primes not dividing Δ_K and $[\mathcal{O} \colon \mathbf{Z}[\alpha]]$. As Δ_K and $[\mathcal{O} \colon \mathbf{Z}[\alpha]]$ have at most $\log(|\Delta_K|) + \log([\mathcal{O} \colon \mathbf{Z}[\alpha]])$ prime factors we see that the set of first $r = \log(B) + \log(|\Delta_K|) + \log(|\mathrm{disc}(f)|))$ primes P' contains a subset P such that $\prod_{p \in P} p > B$ and no element of P divides Δ_K or $[\mathcal{O} \colon \mathbf{Z}[\alpha]]$. Here we have used that $[\mathcal{O} \colon \mathbf{Z}[\alpha]]$ divides $|\mathrm{disc}(f)|$.

Algorithm 5.14 (Determinstic determinant computation over $\mathcal{O}$). Given $A \in \mathrm{Mat}_{n \times n}(\mathcal{O})$, the following steps return $\det(A)$.

```
(1) Set $B = n^n C_1 C_2^n |A|^n \in \mathbf{R}_{>0}$ and $r = \lceil (\log(B) + \log(\Delta_K) + \log(|\mathrm{disc}(f)|) \rceil \in \mathbf{Z}_{>0}$.
(2) Compute the first $r$ primes and choose $r' = \lceil \log(B) \rceil$ many $P = \{p_1, \dots, p_{r'}\}$ among these not dividing $\Delta_K$ and $|\mathrm{disc}(f)|$.
(3) For $p \in P$ do the following:
    (4) Compute irreducible $\overline{f}_1, \dots, \overline{f}_g \in \mathbf{F}_p[X]$ such that $\overline{f} = \overline{f}_1 \cdots \overline{f}_g$.
    (5) Compute $\pi_j(\omega_i)$ for $1 \leq i \leq d$ and $1 \leq j \leq g$.
    (6) Compute $\pi_j(A) \in (\mathbf{F}_p[X]/(\overline{f}_j))^{n \times n}$ for $1 \leq j \leq g$.
    (7) Compute $d_j = \det(\pi(A)) \in \mathbf{F}_p[X]/(\overline{f}_j)$ for $1 \leq j \leq g$.
    (8) Compute $\overline{g}_p \in \mathbf{F}_p[X]/(f)$ such that $g_p = d_j$ in $\mathbf{F}_p[X]/(\overline{f}_j)$ for $1 \leq j \leq g$.
(10) Compute $\overline{g} \in \mathbf{Z}[X]/(f, N)$ such that $\overline{g} = g_p$ in $\mathbf{F}_p[X]/(\overline{f})$ for all $p \in P$.
(11) Return the preimage of $\overline{g}$ under $\mathbf{Z}[X]/(f, N) \to \mathcal{O}/N\mathcal{O}$ where $N = \prod_{p \in P} p$.
```

Theorem 5.15. Algorithm 5.14 is correct and has complexity in $\tilde{O}(d^2 r' r^{1/2} + r'(d^2 C + d^3 + dn^3 + d^2 n^2))$, where $r = n \log(|A|) + \log(|\Delta_K|) + nC$ and $r' = n \log(|A|) + nC$.

Proof. The correctness follows from the preceding paragraphs. By Proposition 5.5, Step 2 has costs in $\tilde{O}(r)$ and every $p \in P$ satisfies $p \leq 2r \ln(r)$. As $\log(p) \in \tilde{O}(\log(r)) = \tilde{O}(1)$ we will ignore all polynomial terms in $\log(p)$. Let us now consider the loop in Steps 3–8 excluding Step 5. As already noticed the factorization of f modulo p has complexity in $\tilde{O}(p^{1/2} d^2 + dC) \subseteq \tilde{O}(r^{1/2} d^2 + dC)$. By Proposition 5.11 computing the image of $(\omega_i)_i$ under the various π_j has complexity in $\tilde{O}(d^3 + d^2 C)$. Each determinant computation consists of $O(n^3)$ operations in

$\mathbf{F}_p[X]/(\overline{f}_i)$ taking $\tilde{O}(n^3\deg(\overline{f}_i))$ bit operations in total. Consequently by summing over all $1 \leq i \leq g$ we see that Step 7 has complexity in $\tilde{O}(dn^3)$. By virtue of Proposition 5.13, Step 8 has complexity in $\tilde{O}(d)$. Since these steps are repeated r' times we obtain a complexity in $\tilde{O}(r'(d^2r^{1/2} + d^2C + d^3 + dn^3))$. Now consider the missing Step 5. Reducing the coefficients of all entries of A modulo all primes $p \in P$ has complexity in $\tilde{O}(dn^2\sum_{p\in P}\log(p) + dn^2\log(|A|)) \subseteq \tilde{O}(dn^2r' + dn^2\log(|A|))$ by Proposition 5.11 (ii). To compute $\pi_j(A)$ we apply item (iii) of the same proposition and arrive at a complexity of $\tilde{O}(d^2n^2r)$ since we have to do it r' times. In total the inner loop in Steps 3–8 has a complexity in

$$\tilde{O}(r'(d^2r^{1/2} + d^2C + d^3 + dn^3 + d^2n^2) + dn^2\log(|A|)).$$

As Steps 10 and 11 have complexity in $\tilde{O}(dr')$ and $\tilde{O}(d^2(C + d + \log(N)) \subseteq \tilde{O}(d^2(C + d + r'))$ respectively, we get an overall complexity in

$$\tilde{O}(r'(d^2r^{1/2} + d^2C + d^3 + dn^3 + d^2n^2) + dn^2\log(|A|) + d^2C + d^3 + d^2r').$$

Finally we use the fact that $r \in O(\log(B) + \log(|\mathrm{disc}(f)|) + \log(|\Delta_K|)) \subseteq \tilde{O}(n\log(|A|) + nC + \log(|\Delta_K|))$ and $r' = \lceil\log(B)\rceil$ to conclude that the complexity of Algorithm 5.14 is in

$$\tilde{O}(d^2r'r^{1/2} + r'(d^2C + d^3 + dn^3 + d^2n^2)). \qquad \square$$

Remark 5.16.

(i) In case we fix the number field K, that is, we ignore the constants coming from field arithmetic, the complexity of Algorithm 5.14 reduces to $\tilde{O}((n\log(|A|))^{3/2} + n^4\log(|A|))$.

(ii) Note that in contrast to the integer case our algorithm is not softly linear in $\log(|A|)$ which can be explained as follows: Recall that our small primes approach needs at least $\log(|A|)$ primes which are roughly of the same order as $\log(|A|)$. As the deterministic factorization in $\mathbf{F}_p$ has costs in $\tilde{O}(p^{1/2})$ (ignoring the dependency on the degree), the complexity of all factorizations contains at least a factor of $\log(|A|)\log(|A|)^{1/2} = \log(|A|)^{3/2}$. Consequently we see that the exponential factorization algorithm is the bottleneck of our determinant algorithm. While there exist various probabilistic polynomial algorithms for the factorization over $\mathbf{F}_p$, they are unusable for us, since we are aiming at a deterministic polynomial pseudo-Hermite normal form algorithm.

§5D. Determinantal ideals

We can now address the problem of computing the determinantal ideal. Since we already addressed the problem of computing the determinant of a matrix over $\mathcal{O}$, we just have to deal with the computation of an ideal product.

Lemma 5.17. *Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be fractional ideals of K. Then $\mathfrak{a}_1 \cdots \mathfrak{a}_n$ can be computed with complexity in $\tilde{O}(d^2n\max_i \mathsf{sz}(\mathfrak{a}_i) + d^3nC)$.*

Proof. We may assume that n is a power of 2. A divide and conquer approach shows that the product can be computed with complexity in $\tilde{O}(d^2n\log(n)\max_i \mathsf{sz}(\mathfrak{a}_i) + d^3nC)$. □

By combining this with Theorem 5.8 and Theorem 5.15 we obtain the following results.

Corollary 5.18. *There exists a probabilistic algorithm which computes, given a pseudo-matrix $\mathcal{A} = (A, (\mathfrak{a}_i))$ with $A \in \mathrm{Mat}_{n\times n}(\mathcal{O})$, the determinantal ideal $\det(\mathcal{A})$ with expected complexity in*

$$\tilde{O}(d^4n^4\log(|A|) + d^2n\max_i \mathsf{sz}(\mathfrak{a}_i)).$$

Corollary 5.19. *There exists a deterministic algorithm which computes, given a pseudo-matrix $\mathcal{A} = (A, (\mathfrak{a}_i))$ with $A \in \mathrm{Mat}_{n\times n}(\mathcal{O})$, the determinantal ideal $\det(\mathcal{A})$ with expected complexity in*

$$\tilde{O}(d^2r'r^{1/2} + r'(d^2C + d^3 + dn^3 + d^2n^2) + d^2nB),$$

where $r = n\log(|A|) + \log(|\Delta_K|) + nC$, $r' = n\log(|A|) + nC$ and $B = \max_i \mathsf{sz}(\mathfrak{a}_i)$.

CHAPTER 3

Orders and lattices

In this chapter we recall the basic theory of orders and lattices over Dedekind domains. The aim is to build the theoretical foundations, on which the more algorithmic topics in the succeeding chapters will rest upon. While Sections §6 and §7 deal with basic concepts found in the literature and contain no new material, in §8 we investigate the structure of sublattices. Probably all these statements are either folklore or straightforward generalizations and do not qualify as original either. The same remark applies to Section §9, where we describe the theory of zeta functions of lattices (over non-maximal orders). On the other hand, in Section §10 will give a new constructive proof of the celebrated theorem of Jordan–Zassenhaus in case the field of fractions of the ground ring is a global field.

§6. Generalities

In this section very basic facts about orders and lattices are introduced. We refer the reader to [RHD70, CR81, Rei03] for a detailed exposition of the material.

Assumption 6.1. Let $\mathcal{O}$ be a Dedekind domain with field of fractions K and A a separable finite dimensional K-algebra.

Definition 6.2 (Orders). An *$\mathcal{O}$-order* of A is a subring Λ of A such that

(i) the center of Λ contains $\mathcal{O}$,
(ii) Λ is a finitely generated $\mathcal{O}$-module and
(iii) $K\Lambda = A$.

When there is no confusion about the underlying ring $\mathcal{O}$, we just speak of orders instead of $\mathcal{O}$-orders.

Let us give some examples to illustrate this definition.

Example 6.3.

(i) If K is an algebraic number field with ring of integers $\mathcal{O}$, then $\mathcal{O}$ is a $\mathbf{Z}$-order in the $\mathbf{Q}$-algebra K. Moreover for all integral elements $\alpha \in \overline{\mathbf{Q}}$ the ring $\mathbf{Z}[\alpha]$ is a $\mathbf{Z}$-order in the $\mathbf{Q}$-algebra $\mathbf{Q}(\alpha)$.
(ii) The ring of square matrices $\mathrm{Mat}_n(\mathcal{O})$ is an $\mathcal{O}$-order in the K-algebra $\mathrm{Mat}_n(K)$.
(iii) Let G be a finite group and KG the group algebra of K over G. Then the group ring $\mathcal{O}G$ is an $\mathcal{O}$-order in the K-algebra KG.

Definition 6.4 (Lattices over orders). Let Λ be an $\mathcal{O}$-order of A and V a finitely generated A-module. A Λ-module M is called *Λ-lattice*, if M is a finitely generated projective $\mathcal{O}$-module. A Λ-lattice M is called *Λ-lattice* of V if $M \subseteq V$ is a Λ-submodule and $KM = V$.

For Λ-lattices M and N, a morphism of Λ-modules $\varphi\colon M \to N$ is called a *morphism of Λ-lattices.*

Warning. Unfortunately, in mathematics the word “lattice” is overloaded with various different meanings. While in most cases, the meaning can be derived from the context, the following alternative definition of a lattice can cause severe confusion: Some authors (for example [GP00]) define a Λ-lattice to be Λ-module which is a finitely generated *free* $\mathcal{O}$-module. While for principal ideal domains both notions coincide, for arbitrary Dedekind domains our definition of lattice is strictly weaker. In particular the following statement is just wrong using the stronger definition.

Lemma 6.5. Let Λ be an $\mathcal{O}$-order of A and V a finite-dimensional A-module. Then there exists a Λ-lattice of V.

Proof. [RHD70, IV, 1.12 Lemma] □

Example 6.6. In case of a group algebra $A = KG$, where G is a finite group, an $\mathcal{O}G$-lattice can be found as follows. Let V be a KG-module and $(v_i)_{1 \leq i \leq n}$ a K-basis of V. As $M' = \sum_{i=1}^{n} \mathcal{O}v_i \subseteq V$ is torsion-free and $\mathcal{O}$ is a Dedekind domain, the $\mathcal{O}$-module M' is finitely generated and projective. Since $M = \sum_{g \in G} gM'$ is G-invariant, the set M is an $\mathcal{O}G$-module contained in V. Moreover, M is again a finitely generated, projective $\mathcal{O}$-module and satisfies $KM = V$. Thus M is an $\mathcal{O}G$-lattice of V.

Definition 6.7. An $\mathcal{O}$-order of A is called *maximal*, if it is not properly contained in any other $\mathcal{O}$-order of A.

Theorem 6.8. Any $\mathcal{O}$-order of A is contained in a maximal $\mathcal{O}$-order of A. In particular, there exists a maximal $\mathcal{O}$-order in A.

Proof. [RHD70, IV, 4.6 Theorem] □

Definition 6.9. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}$, Λ an $\mathcal{O}$-order of A and M a Λ-lattice of a finite dimensional A-module V. We define $A_\mathfrak{p} = K_\mathfrak{p} \otimes_K A$ to be the $\mathfrak{p}$-adic completion of A, $\Lambda_\mathfrak{p}$ to be the $\mathfrak{p}$-adic completion of Λ, $M_\mathfrak{p}$ to be the $\mathfrak{p}$-adic completion of M and $V_\mathfrak{p} = K_\mathfrak{p} \otimes_K V$ to be the $\mathfrak{p}$-adic completion of V.

There are natural isomorphism $M_\mathfrak{p} \cong \mathcal{O}_\mathfrak{p} \otimes_\mathcal{O} M$, $\Lambda_\mathfrak{p} \cong \mathcal{O}_\mathfrak{p} \otimes_\mathcal{O} \Lambda$, which we use to identify these objects. We then have inclusions

$$M \subseteq M_\mathfrak{p} \subseteq K_\mathfrak{p} M_\mathfrak{p} = K_\mathfrak{p} M = V_\mathfrak{p}.$$

Lemma 6.10. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}$, Λ an $\mathcal{O}$-order of A and M a Λ-lattice of a finite dimensional A-module V. Then the following hold:

(i) The ring $A_\mathfrak{p}$ is a separable $K_\mathfrak{p}$-algebra.
(ii) The ring $\Lambda_\mathfrak{p}$ is an $\mathcal{O}_\mathfrak{p}$-order of the $K_\mathfrak{p}$-algebra $A_\mathfrak{p}$.
(iii) The $\Lambda_\mathfrak{p}$-module $M_\mathfrak{p}$ is a $\Lambda_\mathfrak{p}$-lattice of the $A_\mathfrak{p}$-module $V_\mathfrak{p}$.

Proof. (i): Follows from the fact that A is separable. (ii) and (iii): [RHD70, IV, 1.7 Lemma]. □

Theorem 6.11. Let Λ be an $\mathcal{O}$-order of A and V an A-module. Then the following hold:

(i) If M is a Λ-lattice of V, then $M = \bigcap_\mathfrak{p}(M_\mathfrak{p} \cap V)$, where the intersection is over all nonzero prime ideals of $\mathcal{O}$.
(ii) If M and N are Λ-lattices of V, then $M_\mathfrak{p} = N_\mathfrak{p}$ for almost all prime ideals $\mathfrak{p}$ of $\mathcal{O}$.
(iii) Assume that $(M^\mathfrak{p})_{0 \neq \mathfrak{p} \in \operatorname{Spec}(\mathcal{O})}$ is a family of $\Lambda_\mathfrak{p}$-lattices $M^\mathfrak{p}$ of $V_\mathfrak{p}$. Assume that there exists a K-basis $v_1, \ldots, v_n$ of V such that $M^\mathfrak{p} = \mathcal{O}_\mathfrak{p} v_1 + \cdots \mathcal{O}_\mathfrak{p} v_n$ for almost all prime ideals $\mathfrak{p}$ of $\mathcal{O}$. Then the Λ-lattice $M = \bigcap_\mathfrak{p}(M^\mathfrak{p} \cap V)$ satisfies $M_\mathfrak{p} = M^\mathfrak{p}$ for all nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}$.
(iv) If $N \subseteq M$ are Λ-lattices of V, then

$$M/N \cong \bigoplus_\mathfrak{p} M_\mathfrak{p}/N_\mathfrak{p} \text{ as } \Lambda\text{-modules},$$

where the product runs over all nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}$.

Proof. (i), (ii) and (iii): [Tak59, Propositions 1.1, 1.2 and 1.3]. (iv): [RHD70, IV, 1.8 Theorem]. □

Corollary 6.12. Let Λ be an $\mathcal{O}$-order of A and V an A-module. Assume that M is a Λ-lattice of V and for prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ we are given $\Lambda_{\mathfrak{p}_i}$-lattices $M^{(\mathfrak{p}_i)}$ of $V_{\mathfrak{p}_i}$. Then there exists a unique Λ-lattice N of V such that $N_\mathfrak{p} = M_\mathfrak{p}$ for all $\mathfrak{p} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ and $N_{\mathfrak{p}_i} = M^{(\mathfrak{p}_i)}$ for $i = 1, \ldots, r$. Moreover if $M^{(\mathfrak{p}_i)} \subseteq M_{\mathfrak{p}_i}$ for $i = 1, \ldots, r$, then N satisfies $N \subseteq M$.

Proof. Using Theorem 6.11 (iii) we can construct N and using (i) we can show the inclusion $N \subseteq M$. □

Lemma 6.13 (Locality of maximality). Let Λ be an $\mathcal{O}$-order of A. Then Λ is maximal if and only if $\Lambda_\mathfrak{p}$ is a maximal order of $A_\mathfrak{p}$ for all nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}$.

Proof. [RHD70, IV, 4.8 Lemma] □

Definition 6.14. Let Λ be an $\mathcal{O}$-order of A. We define $S(\Lambda)$ to be the set of all prime ideals $\mathfrak{p}$ of $\mathcal{O}$, such that $\Lambda_{\mathfrak{p}}$ is not a maximal order of $A_{\mathfrak{p}}$.

Remark 6.15. Based on the existence of maximal overorders and Lemma 6.13 it is easy to see that $S(\Lambda)$ is a finite set: Let Λ_0 be a maximal overorder of Λ. As Λ and Λ_0 span A over K, they have the same rank as $\mathcal{O}$-modules. Thus the order ideal $(\Lambda_0 : \Lambda)$ is defined and we have

$$(\Lambda_0 : \Lambda)\Lambda_0 \subseteq \Lambda \subseteq \Lambda_0.$$

In particular for all prime ideals $\mathfrak{p}$ not dividing $(\Lambda_0 : \Lambda)$ we have $(\Lambda_0)_{\mathfrak{p}} = (\Lambda_0 : \Lambda)_{\mathfrak{p}}(\Lambda_0)_{\mathfrak{p}} \subseteq \Lambda_{\mathfrak{p}} \subseteq (\Lambda_0)_{\mathfrak{p}}$, that is $\Lambda_{\mathfrak{p}} = (\Lambda_0)_{\mathfrak{p}}$. Since $(\Lambda_0)_{\mathfrak{p}}$ is maximal (locality of maximality) we conclude that $S(\Lambda)$ is contained in the set of all prime divisors of $(\Lambda : \Lambda_0)$ and therefore $S(\Lambda)$ is finite.

Example 6.16. Consider the integral group ring $\Lambda = \mathcal{O}G \subseteq KG$ of a finite group G, such that $\operatorname{char}(K)$ does not divide $\#G$. As $\mathcal{O}G$ is maximal if and only if $\#G$ is a unit in $\mathcal{O}$ (see [CR81, (27.1) Proposition]), it follows that $S(\mathcal{O}G) = \{\mathfrak{p} \in \operatorname{Spec}(\mathcal{O}) \mid \#G \in \mathfrak{p}\}$.

Definition 6.17. Let Λ be an $\mathcal{O}$-order, M and N two Λ-lattices and $\mathfrak{p}$ a nonzero prime ideal of $\mathcal{O}$. We say that M and N are $\mathfrak{p}$-*isomorphic* or *locally isomorphic at* $\mathfrak{p}$, if $M_{\mathfrak{p}} \cong N_{\mathfrak{p}}$ as $\Lambda_{\mathfrak{p}}$-lattices. In this case we write $M \sim_{\mathfrak{p}} N$. We say that M and N lie in the same *genus*, if $M \sim_{\mathfrak{p}} N$ for all nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}$. In this case we write $M \vee N$. For a Λ-lattice M we denote by $g(M)$ the set of all Λ-lattices with $KM = KN$ and $M \vee N$. The set $g(M)$ is called the *genus of* M.

While the definition of the genus involves all nonzero prime ideals, it is actually a condition at only a finite set of prime ideals. To see this, we need the following property of maximal orders.

Lemma 6.18. Let Λ an $\mathcal{O}$-order and $\mathfrak{p}$ a nonzero prime ideal of $\mathcal{O}$ such that $\Lambda_{\mathfrak{p}}$ is maximal. Then the following hold:
(i) Every $\Lambda_{\mathfrak{p}}$-lattice is projective.
(ii) Two $\Lambda_{\mathfrak{p}}$-lattices M and N are isomorphic if and only if $K_{\mathfrak{p}}M \cong K_{\mathfrak{p}}N$ as $A_{\mathfrak{p}}$-modules.

Proof. (i): An order with this property is called hereditary. As maximal orders are hereditary, see [RHD70, IV, 4.19 Theorem], the claim follows. (ii): [CR81, Exercise 26.11]. □

Theorem 6.19. Let M and N be Λ-lattices and $S \subseteq \operatorname{Spec}(\mathcal{O})$ a superset of $S(\Lambda)$. Then the following hold:
(i) The relation $M \vee N$ implies $KM \cong KN$ as A-modules.
(ii) If $\Lambda_{\mathfrak{p}}$ is maximal, then $M \sim_{\mathfrak{p}} N$ is equivalent to $KM \cong KN$ as A-modules.
(iii) We have $M \vee N$ if and only if $M \sim_{\mathfrak{p}} N$ for all $\mathfrak{p} \in S$.

Proof. (i): Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}$. From $M_{\mathfrak{p}} \sim_{\mathfrak{p}} N_{\mathfrak{p}}$ we conclude $K_{\mathfrak{p}}M = K_{\mathfrak{p}}M_{\mathfrak{p}} \cong K_{\mathfrak{p}}N_{\mathfrak{p}} = K_{\mathfrak{p}}N$ as $A_{\mathfrak{p}}$-modules. The claim now follows from the theorem of Noether–Deuring (see [CR62, (29.12) Theorem]). (ii) and (iii) follow from $S(\Lambda) \subseteq S$ and Lemma 6.18. □

§7. Homomorphism rings

Assumption 7.1. Let $\mathcal{O}$ be a Dedekind domain with field of fractions K and A a separable K-algebra.

Warning. We will use the following (non-standard) notation for restricting the domain and codomain of a map. Let X, Y be sets with subsets $X' \subseteq X$ and $Y' \subseteq Y$. For a function $f\colon X \to Y$ with $f(X') \subseteq Y'$ we define $f|_{X'}^{Y'}$ to be the function $X' \to Y'$ induced by f.

Lemma 7.2. Let Λ be an $\mathcal{O}$-order of A and M, N two Λ-lattices. Then the following hold:
(i) The $\mathcal{O}$-module $\operatorname{Hom}_\Lambda(M, N)$ is finitely generated and torsion-free.
(ii) We have $\operatorname{Hom}_\Lambda(M, N) = \{\varphi|_M^N \mid \varphi \in \operatorname{Hom}_A(KM, KN) \text{ such that } \varphi(M) \subseteq N\}$.
(iii) If Γ is an $\mathcal{O}$-order with $\Gamma \subseteq \Lambda$, then $\operatorname{Hom}_\Gamma(M, N) = \operatorname{Hom}_\Lambda(M, N)$.

Proof. (i): Clear. (ii): This follows from the fact that every morphism in $\operatorname{Hom}_\Lambda(M, N)$ extends to a morphism in $\operatorname{Hom}_A(KM, KN)$. (iii): Follows from (ii). □

Now let R be a ring extension of $\mathcal{O}$ and Λ an $\mathcal{O}$-order of A. For Λ-lattices M and N, extension of scalars induces naturally an R-morphism $R \otimes_{\mathcal{O}} \mathrm{Hom}_\Lambda(M,N) \longrightarrow \mathrm{Hom}_{R\otimes_{\mathcal{O}}\Lambda}(R \otimes_{\mathcal{O}} M, R \otimes_{\mathcal{O}} N)$, which is in general neither injective nor surjective. Nevertheless, in cases of most interest to us the map is an isomorphism due to the following theorem.

Theorem 7.3. Assume that R is a flat ring extension of $\mathcal{O}$. Then the natural map $R \otimes_{\mathcal{O}} \mathrm{Hom}_\Lambda(M,N) \longrightarrow \mathrm{Hom}_{R\otimes_{\mathcal{O}}\Lambda}(R \otimes_{\mathcal{O}} M, R \otimes_{\mathcal{O}} N)$ is an R-isomorphism.

Proof. As $\mathcal{O}$ is noetherian and Λ is finitely generated over $\mathcal{O}$, the ring Λ is also noetherian. Thus M and N—being finitely generated $\mathcal{O}$-modules—are finitely presented and thus the result follows from [Rei03, (2.38) Theorem]. □

Corollary 7.4. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}$. Then the natural map $\mathcal{O}_\mathfrak{p} \otimes_{\mathcal{O}} \mathrm{Hom}_\Lambda(M,N) \to \mathrm{Hom}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p})$ is an $\mathcal{O}_\mathfrak{p}$-isomorphism.

Proof. As $\mathcal{O}$ is noetherian, the completion at $\mathfrak{p}$ is flat ([Rei03, (5.1) Theorem]). Now the result follows from Theorem 7.3 □

Remark 7.5. In case $\mathcal{O}$ is a principal ideal domain, the above corollary also has a constructive interpretation: Any $\mathcal{O}$-basis of $\mathrm{Hom}_\Lambda(M,N)$ yields an $\mathcal{O}_\mathfrak{p}$-basis of $\mathrm{Hom}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p})$. As usual, in case $\mathcal{O}$ is merely a Dedekind domain, the situation is not hopeless but requires pseudo-bases. If $(\mathfrak{a}_i, \varphi_i)$ is a pseudo-basis of $\mathrm{Hom}_\Lambda(M,N)$ with $\varphi_i \in \mathrm{Hom}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p})$ for all i, then extensions of the φ_i to $\mathrm{Hom}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p})$ form an $\mathcal{O}_\mathfrak{p}$-basis.

Besides $S(\Lambda)$, another important invariant of the lattice Λ is the annihilator ideal of the extension modules. By this we mean an integral ideal $\mathfrak{h}$ of $\mathcal{O}$ satisfying

$$\mathfrak{h} \cdot \mathrm{Ext}^1_\Lambda(M,N) = 0$$

for all Λ-lattices M and N. Here $\mathrm{Ext}^1_\Lambda(M,N)$ denotes the first extension module (see [CR81, §25]). Note that an ideal $\mathfrak{h}$ with the above property is readily available once we know a maximal overorder Λ_0 of Λ: By [CR81, (29.4) Theorem] we have $(\Lambda_0 : \Lambda) \cdot \mathrm{Ext}^1_\Lambda(M,N) = 0$ for all Λ-lattices M and N implying that $\mathfrak{h} = (\Lambda_0 : \Lambda)$ is an admissible choice for $\mathfrak{h}$.

Example 7.6. Let $\Lambda = \mathcal{O}G$ be the group ring of a finite group G. Then [CR81, (25.12) Theorem] says that $\#G \cdot \mathrm{Ext}^1_\Lambda(M,N) = 0$ for all $\mathcal{O}G$-lattices M and N. Thus in this case $\mathfrak{h} = \#G \cdot \mathcal{O}$ is a valid choice. Another possibility is the use of the so called central conductor, which for integral group rings can be computed using Jacobinski's formula, see [CR81, (27.8) Theorem].

§8. The lattice of sublattices

Assumption 8.1. Let $\mathcal{O}$ be a Dedekind domain with field of fractions K, Λ an $\mathcal{O}$-order in a separable K-algebra A and M a Λ-lattice.

Definition 8.2. A proper Λ-sublattice N of M is called *maximal*, if there is no Λ-lattice L with $N \subsetneq L \subsetneq M$. For a prime ideal $\mathfrak{p}$ of $\mathcal{O}$ we call a Λ-sublattice N of M a $\mathfrak{p}$-*sublattice*, if $(M : N)$ is a $\mathfrak{p}$-power. A maximal $\mathfrak{p}$-sublattice is also called $\mathfrak{p}$-*maximal*.

Lemma 8.3. Let N be a maximal Λ-sublattice of M. Then there exists a (unique) prime ideal $\mathfrak{p}$ of $\mathcal{O}$ such that the index ideal $(M : N)$ is a $\mathfrak{p}$-power, that is, N is $\mathfrak{p}$-maximal. Moreover we have $\mathfrak{p}M \subsetneq N \subsetneq M$.

Proof. Since N is properly contained in M, the index ideal $(M : N)$ is not trivial. Let $\mathfrak{p}$ be a prime ideal dividing $(M : N)$. Then the sum $N + \mathfrak{p}M$ is a Λ-module with $N \subseteq N + \mathfrak{p}M \subseteq M$. By the maximality of N we have $N = N + \mathfrak{p}M$ or $M = N + \mathfrak{p}M$. Since the former implies $\mathfrak{p}M \subseteq N$ we will show that $M = N + \mathfrak{p}M$ is impossible. Therefore assume that $M = N + \mathfrak{p}M$. Localizing at $\mathfrak{p}$ we obtain $M_\mathfrak{p} = N_\mathfrak{p} + \mathfrak{p}_\mathfrak{p} M_\mathfrak{p}$ and applying the Lemma of Krull–Azumaya (aka Lemma of Nakayama) to these modules over the local ring $\mathcal{O}_\mathfrak{p}$ yields $N_\mathfrak{p} = M_\mathfrak{p}$. Now the completion of the index ideal $(M : N)_\mathfrak{p}$ is just $(M_\mathfrak{p} : N_\mathfrak{p}) = \mathcal{O}_\mathfrak{p}$. This contradicts the fact that $\mathfrak{p}$ divides $(M : N)$.

Now assume that a prime ideal $\mathfrak{q} \neq \mathfrak{p}$ of $\mathcal{O}$ divides $(M : N)$. Then the same argument as in the first part of the proof shows $\mathfrak{q}M \subseteq N$. Since $\mathfrak{p}$ and $\mathfrak{q}$ are coprime, that is, $\mathcal{O} = \mathfrak{p} + \mathfrak{q}$, we conclude that $M = \mathfrak{q}M + \mathfrak{p}M \subseteq N$ holds, a contradiction. □

The important ingredient for computing all $\mathfrak{p}$-maximal Λ-sublattices of M is the following lemma, which describes the structure of these objects completely:

Lemma 8.4. Let $\mathfrak{p}$ be nonzero prime ideal of $\mathcal{O}$ and $\pi\colon M \to M/\mathfrak{p}M$ the canonical projection. Then the following hold:

(i) Assume that C is a simple $\Lambda/\mathfrak{p}\Lambda$-module and $f \in \operatorname{Hom}_{\Lambda/\mathfrak{p}\Lambda}(M/\mathfrak{p}M, C)$ is a nonzero morphism. Denote by N the preimage of $\ker(f)$ under π. Then N is a $\mathfrak{p}$-maximal Λ-sublattice of M with $(M : N) = \mathfrak{p}^s$, where s is the $k_\mathfrak{p}$-dimension of C.

(ii) Conversely, let N be a $\mathfrak{p}$-maximal Λ-sublattice of M with $(M : N) = \mathfrak{p}^s$. Then there exists a simple $\Lambda/\mathfrak{p}\Lambda$-module C of $k_\mathfrak{p}$-dimension s and a nonzero morphism $f \in \operatorname{Hom}_{\Lambda/\mathfrak{p}\Lambda}(M/\mathfrak{p}M, C)$ such that N is the preimage of $\ker(f)$ under π.

Proof. (i): Regard C as a Λ-module. Then by construction, $f \circ \pi$ is a Λ-morphism and the sequence

$$0 \to N \xrightarrow{\iota} M \xrightarrow{f\circ\pi} C \longrightarrow 0$$

is exact, where ι is the inclusion. It follows that $C \cong M/N$ as Λ-modules and since C and therefore M/N are annihilated by $\mathfrak{p}$, we obtain $\mathfrak{p}M \subseteq N$. This shows that M/N is a $\Lambda/\mathfrak{p}\Lambda$-module. Since M/N is $\mathcal{O}$-isomorphic to $\dim_{k_\mathfrak{p}}(C)$ many copies of $\mathcal{O}/\mathfrak{p}$, the index ideal $(M : N)$ is equal to $\mathfrak{p}^s$, where $s = \dim_{k_\mathfrak{p}}(C)$. Finally, C being simple implies that N is a maximal Λ-sublattice of M.

(ii): If N is such a $\mathfrak{p}$-maximal Λ-sublattice of M, it is easy to see that choosing f to be the projection $M/\mathfrak{p}M \to (M/\mathfrak{p}M)/(N/\mathfrak{p}M)$ has the required properties. □

Remark 8.5. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}$.

(i) In case $M/\mathfrak{p}M$ itself is a simple $\Lambda/\mathfrak{p}\Lambda$-module, any nonzero element of $\operatorname{Hom}_{\Lambda/\mathfrak{p}\Lambda}(M/\mathfrak{p}M, C)$ has kernel equal to $\{0\}$. In particular, the only $\mathfrak{p}$-maximal Λ-sublattice of M is $\mathfrak{p}M$.

(ii) Note that if C is a simple $\Lambda/\mathfrak{p}\Lambda$-module and $\operatorname{Hom}_{\Lambda/\mathfrak{p}\Lambda}(M/\mathfrak{p}M, C) \neq \{0\}$, then C is necessarily isomorphic to a composition factor of $M/\mathfrak{p}M$. It is therefore natural to ask whether all composition factors admit non-trivial morphisms onto them or if not, which composition factors have this property. Denote by $\operatorname{rad}(M/\mathfrak{p}M)$ the radical of $M/\mathfrak{p}M$, which is the intersection of all maximal $\Lambda/\mathfrak{p}\Lambda$-submodules of $M/\mathfrak{p}M$. Then it is well known that for a simple $\Lambda/\mathfrak{p}\Lambda$-module C, the set $\operatorname{Hom}_{\Lambda/\mathfrak{p}M}(M/\mathfrak{p}M, C)$ is nonzero if and only if C is isomorphic to a composition factor of the (semisimple) $\Lambda/\mathfrak{p}\Lambda$-module $(M/\mathfrak{p}M)/\operatorname{rad}(M/\mathfrak{p}M)$ (the latter object is known as the head of $M/\mathfrak{p}M$). See also [NT89].

(iii) If $M/\mathfrak{p}M$ is semisimple, then $\operatorname{rad}(M/\mathfrak{p}M) = 0$ and $M/\mathfrak{p}M$ is the direct sum of its simple submodules. In particular, for a simple $\Lambda/\mathfrak{p}\Lambda$-module C we then have $\operatorname{Hom}_{\Lambda/\mathfrak{p}M}(M/\mathfrak{p}M, C) \neq \{0\}$ if and only if C is isomorphic to a simple submodule of $M/\mathfrak{p}M$.

Definition 8.6. We denote by $\mathcal{L}(M)$ the set of all Λ-sublattices of M and by $\mathcal{L}^{\max}(M)$ the set of all maximal Λ-sublattices of M. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}$. Then we define $\mathcal{L}_\mathfrak{p}(M) = \{N \subseteq M \text{ a } \mathfrak{p}\text{-sublattice}\}$, $\mathcal{L}_\mathfrak{p}^{\max}(M) = \mathcal{L}^{\max}(L) \cap \mathcal{L}_\mathfrak{p}(M)$ to be the set of $\mathfrak{p}$-maximal Λ-sublattices of M. Moreover we define $\operatorname{rad}_\mathfrak{p}(M) = \bigcap_N N$, where N runs through all elements of $\mathcal{L}_\mathfrak{p}^{\max}(M)$, to be the $\mathfrak{p}$-*radical of* M. We define

$$\Phi_\mathfrak{p}(M) = \{L \in \mathcal{L}(M) \mid \operatorname{rad}_\mathfrak{p}(M) \subseteq L \subseteq M\},$$

and if N is any Λ-lattice we set $\Phi_\mathfrak{p}(M,N) = \{L \in \Phi_\mathfrak{p}(M) \mid M \sim_\mathfrak{p} N\}$. Now assume that $\mathcal{L}_\mathfrak{p}^{\max}(M) = \{L_1, \dots, L_h\}$ is finite. For $N \in \Phi_\mathfrak{p}(M)$ we define $\mu_\mathfrak{p}(M,N) = \sum_J (-1)^{\#J}$, where J runs through all subsets of $\{1,\dots,h\}$ with the property that $\bigcap_{i\in J} L_i = N$.

Lemma 8.7. The triple $(\mathcal{L}_\mathfrak{p}(M), +, \cap)$ is a lattice (in the sense of posets).

Proof. Since $(\mathcal{L}(M), +, \cap)$ is a lattice it is sufficient to show that $\mathcal{L}_\mathfrak{p}(M)$ is closed with respect to the binary relations $+$ and $\cap$. For this let N and L be two elements $\mathcal{L}_\mathfrak{p}(M)$. Then there exist $n, l \in \mathbf{Z}_{\geq 1}$ such that $\mathfrak{p}^n M \subseteq N$ and $\mathfrak{p}^l M \subseteq L$. Thus we have $\mathfrak{p}^{\max(n,l)} M \subseteq N \cap L$ and $\mathfrak{p}^{\min(n,l)} M \subseteq N + L$, implying that $N \cap L$, as well as $N + L$, are elements of $\mathcal{L}_\mathfrak{p}(M)$. □

Lemma 8.8. Let M be a Λ-lattice. Then the following hold:

(i) The map $\Psi\colon \mathcal{L}_\mathfrak{p}(M) \to \mathcal{L}(M_\mathfrak{p})$, $N \mapsto N_\mathfrak{p}$ is a lattice isomorphism.

(ii) The map $\Psi\colon \mathcal{L}_\mathfrak{p}^{\max}(M) \to \mathcal{L}^{\max}(M_\mathfrak{p})$, $N \mapsto N_\mathfrak{p}$ is a bijection with $\Psi(N \cap L) = \Psi(N) \cap \Psi(L)$ for all $N, L \in \mathcal{L}_\mathfrak{p}^{\max}(M)$.

Proof. (i): It is sufficient to show that Ψ is an isomorphism of partially ordered sets. Now the inverse of Ψ is given by $\hat{N} \longmapsto V \cap \hat{N}$, where $V = KM$, and it is immediate that Ψ, as well as its inverse, are order preserving.

(ii): This follows from (i). □

Lemma 8.9. Let N be a Λ-lattice and $\mathfrak{p}$ a nonzero prime ideal of $\mathcal{O}$. Assume that $\mathcal{L}_{\mathfrak{p}}^{\max}(M)$ is finite. Then the following hold:

(i) We have $\mathrm{rad}_{\mathfrak{p}}(M)_{\mathfrak{p}} = \mathrm{rad}(M)_{\mathfrak{p}}$.

(ii) The map $\Psi\colon \Phi_{\mathfrak{p}}(M) \to \Phi(M_{\mathfrak{p}})$, $L \mapsto L_{\mathfrak{p}}$ is a bijection.

(iii) The map $\Psi\colon \Phi_{\mathfrak{p}}(M, N) \to \Phi(M_{\mathfrak{p}}, N_{\mathfrak{p}})$, $L \mapsto L_{\mathfrak{p}}$ is a bijection.

(iv) If $N \in \Phi_{\mathfrak{p}}(M)$, then $\mu_{\mathfrak{p}}(M, N) = \mu(M_{\mathfrak{p}}, N_{\mathfrak{p}})$.

Proof. (i): We have

$$\mathrm{rad}_{\mathfrak{p}}(M)_{\mathfrak{p}} = \Psi\Big(\bigcap_{N \in \mathcal{L}_{\mathfrak{p}}^{\max}(M)} N\Big) = \bigcap_{N \in \mathcal{L}_{\mathfrak{p}}^{\max}(M)} \Psi(N) = \bigcap_{N \in \Psi(\mathcal{L}_{\mathfrak{p}}^{\max}(M))} N = \bigcap_{N \in \mathcal{L}^{\max}(M_{\mathfrak{p}})} N = \mathrm{rad}(M_{\mathfrak{p}}).$$

(ii): Since $\Psi\colon \mathcal{L}_{\mathfrak{p}}(M) \to \mathcal{L}(M_{\mathfrak{p}})$, $N \mapsto N_{\mathfrak{p}}$ is a lattice isomorphism and $\Psi(\mathrm{rad}_{\mathfrak{p}}(M)) = \mathrm{rad}(\Psi(M))$ by (i), the map Ψ induces a bijection from $\Phi_{\mathfrak{p}}(M) = \{L \in \mathcal{L}_{\mathfrak{p}}(M) \mid \mathrm{rad}_{\mathfrak{p}}(M) \subseteq L \subseteq M\}$ onto the set

$$\{L \in \Psi(\mathcal{L}(M_{\mathfrak{p}})) \mid \Psi(\mathrm{rad}_{\mathfrak{p}}(M)) \subseteq L \subseteq \Psi(M)\} = \{L \in \mathcal{L}(M_{\mathfrak{p}}) \mid \mathrm{rad}(M_{\mathfrak{p}}) \subseteq L \subseteq M_{\mathfrak{p}}\} = \Phi(M_{\mathfrak{p}}).$$

(iii): By (ii) we know that $L \in \Phi_{\mathfrak{p}}(M, N)$ is equivalent to $\Phi(L) \in \Phi(M_{\mathfrak{p}}, N_{\mathfrak{p}})$. Moreover, by definition $N \sim_{\mathfrak{p}} L$ is equivalent to $\Psi(N) \cong \Psi(L)$.

(iv): Follows from (i), (ii) and (iii). □

§9. Theory of Solomon zeta functions

The exposition basically follows [Sol77] with the appropriate generalizations introduced in [BR80a, BR80b]. Note that here we only scratch the surface of the theory of Solomon zeta functions. Since the work of Solomon in [Sol77, Sol79], much more theoretical work has been done. Most notable is the series of papers [BR80a, BR80b, BR84, BR86, BR87] by Bushnell and Reiner, where they prove Solomon's first conjecture and investigate analytic properties of zeta functions, and the proof of Solomon's second conjecture by Iyama in [Iya03].

Definition 9.1. Let K be either an algebraic number field or a p-adic field and $\mathcal{O}$ the ring of integers of K or the valuation ring of K respectively. Let A be a semisimple K-algebra and Λ an $\mathcal{O}$-order in A. Given a Λ-lattice M, for $n \in \mathbf{Z}_{\geq 1}$ we set $a_n = \#\{N \subseteq M \ \Lambda\text{-sublattice} \mid |M : N| = n\}$ and define the formal Dirichlet series

$$\zeta_\Lambda(M, s) = \sum_{n \in \mathbf{Z}_{\geq 1}} a_n n^{-s}, \quad s \in \mathbf{C}.$$

We call $\zeta_\Lambda(M, s)$ the *Solomon zeta function* of the Λ-lattice M.

Remark 9.2. Consider the case of K being an algebraic number field, $A = K$ as well as $M = \Lambda = \mathcal{O}$. Then $\zeta_{\mathcal{O}}(\mathcal{O}, s)$ is equal to the Dedekind zeta function $\zeta_K(s)$ of the number field K. In particular we have an Euler product

$$\zeta_{\mathcal{O}}(\mathcal{O}, s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{\mathbf{N}(\mathfrak{p})^s}\right)^{-1}$$

for $\mathrm{Re}(s) > 1$, where the product extends over all nonzero prime ideals of $\mathcal{O}$. Recall that for a nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$ the set of ideals of the completion $\mathcal{O}_{\mathfrak{p}}$ is just $\{\mathfrak{p}^n \mathcal{O}_{\mathfrak{p}} \mid n \in \mathbf{Z}_{\geq 0}\}$ and therefore

$$\zeta_{\mathcal{O}_{\mathfrak{p}}}(\mathcal{O}_{\mathfrak{p}}, s) = \sum_{n \in \mathbf{Z}_{\geq 0}} \frac{1}{\mathbf{N}(\mathfrak{p})^{ns}} = \left(1 - \frac{1}{\mathbf{N}(\mathfrak{p})^s}\right)^{-1}$$

for $\mathrm{Re}(s) > 1$. This allows us to rewrite the Euler product in the form

$$\zeta_{\mathcal{O}}(\mathcal{O}, s) = \prod_{0 \neq \mathfrak{p} \in \mathrm{Spec}(\mathcal{O})} \zeta_{\mathcal{O}_{\mathfrak{p}}}(\mathcal{O}_{\mathfrak{p}}, s)$$

for $\operatorname{Re}(s) > 1$. This identity suggests that we should think of the Euler product as a product formula relating local and global properties of $\mathcal{O}$, which fortunately generalizes to our more general setting of noncommutative orders.

Assumption 9.3. For the rest of the section we fix an algebraic number field K with ring of integers $\mathcal{O}$, a finite dimensional semisimple K-algebra A, an $\mathcal{O}$-order Λ of A and a Λ-lattice M. Moreover we let V be the semisimple A-module KM.

For each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$ we obtain an associated $\Lambda_{\mathfrak{p}}$-lattice $M_{\mathfrak{p}}$ with Solomon zeta function $\zeta_{\Lambda_{\mathfrak{p}}}(M_{\mathfrak{p}}, s)$.

Lemma 9.4 (Euler product for Solomon zeta functions). For $\operatorname{Re}(s) > \dim_K(V)$ we have

$$\zeta_\Lambda(M, s) = \prod_{\mathfrak{p}} \zeta_{\Lambda_{\mathfrak{p}}}(M_{\mathfrak{p}}, s),$$

where the product extends over all nonzero prime ideals of $\mathcal{O}$.

Proof. While this is proven in [Sol77, Lemma 6] only for the case $K = \mathbf{Q}$, the generalization to arbitrary K is immediate. □

Definition 9.5. For a nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$ the factor $\zeta_{\Lambda_{\mathfrak{p}}}(M_{\mathfrak{p}}, s)$ is called the $\mathfrak{p}$*-part* or the *Euler factor at* $\mathfrak{p}$ of $\zeta_\Lambda(M, s)$.

One of the fundamental observations of Solomon was the fact that for almost all prime ideals $\mathfrak{p}$, the Euler factor of $\zeta_\Lambda(M, s)$ at $\mathfrak{p}$ depends only on the A-module $V = KM$ and not on the particular Λ-lattice M of V.

Definition 9.6. Write $A = \prod_{i=1}^r A_i$ with simple K-algebras A_i and set $V_i = A_i V$. Let W_i be the unique simple A_i-module and $k_i \in \mathbf{Z}_{>0}$ such that $V_i \cong W_i^{k_i}$. By the Artin–Wedderburn theorem we can write $A_i = \operatorname{Mat}_{m_i \times m_i}(D_i)$ for some division algebra D_i with center K_i (which is a number field containing K). Finally set $e_i^2 = \dim_{K_i}(D_i)$. Then we define

$$\zeta_V(s) = \prod_{i=1}^r \prod_{j=0}^{k_i e_i - 1} \zeta_{K_i}(m_i e_i s - j)$$

to be the *zeta function of* V. If F is a number field containing K and $\mathfrak{p}$ a nonzero prime ideal of $\mathcal{O}$, we define

$$\zeta_{F,\mathfrak{p}}(s) = \prod_{\mathfrak{P} \mid \mathfrak{p}} \left(1 - \frac{1}{\mathbf{N}(\mathfrak{P})^s}\right)^{-1}$$

to be the $\mathfrak{p}$*-part of* ζ_F, where $\mathfrak{P}$ runs through all prime ideals of $\mathcal{O}_F$ lying above $\mathfrak{p}$. Moreover we define

$$\zeta_{V,\mathfrak{p}}(s) = \prod_{i=1}^r \prod_{j=0}^{k_i e_i - 1} \zeta_{K_i,\mathfrak{p}}(m_i e_i s - j)$$

to be the $\mathfrak{p}$*-part of* $\zeta_V(s)$.

Example 9.7. We use the same notation as in the preceding definition. Assume that V is an absolutely irreducible A-module of dimension n. Then there exists a unique i with $A_i V = V \neq \{0\}$ and $A_i \cong \operatorname{Mat}_{n \times n}(K)$. Thus $k_i = 1$, $D_i = K$, $e_i = 1$ and therefore

$$\zeta_V(s) = \zeta_K(ns).$$

Using $\zeta_V(s)$ we can now write

$$\zeta_\Lambda(M, s) = \zeta_V(s) \prod_{\mathfrak{p}} \frac{\zeta_{\Lambda_{\mathfrak{p}}}(M_{\mathfrak{p}}, s)}{\zeta_{V,\mathfrak{p}}(s)}$$

for $\operatorname{Re}(s) > \dim_K(V)$, expressing $\zeta_\Lambda(M, s)$ as a product of Dedekind zeta functions of extensions of K (coming from $\zeta_V(s)$) and potentially infinitely many nontrivial quotients of local factors.

Lemma 9.8. Assume that $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}$ such that $\Lambda_{\mathfrak{p}}$ is a maximal $\mathcal{O}_{\mathfrak{p}}$-order of $A_{\mathfrak{p}}$ and $A_{\mathfrak{p}}$ is a sum of full matrix algebras over fields. Then

$$\frac{\zeta_{\Lambda_{\mathfrak{p}}}(M_{\mathfrak{p}}, s)}{\zeta_{V,\mathfrak{p}}(s)} = 1$$

for $\mathrm{Re}(s) > \dim_K(V)$.

Proof. See [BR80a]. □

Remark 9.9.

(i) To some extent, Lemma 9.8 explains the rather ad hoc definition of ζ_V. It actually emerges from a deep understanding of zeta functions of maximal orders in semisimple K-algebras and is chosen in such a way that for almost all primes the $\mathfrak{p}$-part of ζ_V and the $\mathfrak{p}$-part of the Solomon zeta function of the unique lattice over the maximal order are equal. We don't give any details here but refer the reader to [Sol77] and [BR80a, BR80b].

(ii) The condition on $A_{\mathfrak{p}}$ being the direct sum of full matrix algebras over fields is equivalent to $\mathfrak{p}$ not dividing the discriminant of A. The discriminant of Λ is defined to be the $\mathcal{O}$-ideal $(\det(\mathrm{tr}(x_i x_j)_{i,j}) \mid x_1, \ldots, x_k \in \Lambda)$, where k is the dimension of A and $\mathrm{tr}\colon A \to K$ is the reduced trace. The discriminant $\mathrm{disc}(A)$ is defined to be $\mathrm{disc}(\Lambda_0)$, where Λ_0 is any maximal $\mathcal{O}$-order of A. See also [Rei03, Section 25].

Corollary 9.10. Denote by B the set of prime ideals $\mathfrak{p}$ of $\mathcal{O}$ which either divide $\mathrm{disc}(A)$ or for which $\Lambda_{\mathfrak{p}}$ is not maximal. Then we have

$$\zeta_\Lambda(M, s) = \zeta_V(s) \prod_{\mathfrak{p} \in B} \frac{\zeta_{\Lambda_{\mathfrak{p}}}(M_{\mathfrak{p}}, s)}{\zeta_{V,\mathfrak{p}}(s)}$$

for $\mathrm{Re}(s) > \dim_K(V)$.

While this shows that in order to determine $\zeta_\Lambda(M, s)$ we have to compute only the Euler factors for a finite set of prime ideals, we still do not know whether these factors have a reasonable form which we can actually compute. Using ingenious combinatorial arguments, Solomon ([Sol77]) was able to give a constructive proof of the following fact:

Theorem 9.11. Let $\mathfrak{p}$ be a nonzero prime ideal and p the rational prime lying below $\mathfrak{p}$. Then there exists $\psi_{\mathfrak{p}} \in \mathbf{Q}(X)$ such that

$$\zeta_{\Lambda_{\mathfrak{p}}}(M_{\mathfrak{p}}, s) = \psi_{\mathfrak{p}}(p^{-s}).$$

As the same holds also for $\zeta_{V,\mathfrak{p}}(s)$ ([Sol77]), the theorem shows that there exists $\varphi_{\mathfrak{p}} \in \mathbf{Q}(X)$ such that

$$\frac{\zeta_{\Lambda_{\mathfrak{p}}}(M_{\mathfrak{p}}, s)}{\zeta_{V,\mathfrak{p}}(s)} = \varphi_{\mathfrak{p}}(p^{-s}),$$

that is, the quotient is always a rational function in p^{-s}. Using this theorem we can now formulate a well-defined algorithmic problem concerning the computation of Solomon zeta functions: Does there exists an algorithm for computing $\varphi_{\mathfrak{p}}$?

Moreover, based on numerical data, Solomon conjectured that the quotient is always a polynomial in p^{-s} with integer coefficients. The latter conjecture, also known as Solomon's first conjecture, was proven by Bushnell and Reiner using the theory of zeta integrals.

Theorem 9.12 (Solomon's First Conjecture, Bushnell–Reiner). For each nonzero prime ideal $\mathfrak{p}$ there exists $\varphi_{\mathfrak{p}} \in \mathbf{Z}[X]$ such that

$$\frac{\zeta_{\Lambda_{\mathfrak{p}}}(M_{\mathfrak{p}}, s)}{\zeta_{V,\mathfrak{p}}(s)} = \varphi_{\mathfrak{p}}(p^{-s}),$$

where p is the rational prime lying below $\mathfrak{p}$.

Proof. This is [BR80b, §4.2 Corollary], [BR80a, Theorem 2]. □

Let us now elaborate on the case of group algebras and the set of primes ideals one needs to take care of.

Lemma 9.13. Let G be a finite group, $A = KG$ and $\Lambda = \mathcal{O}G$. Assume that $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}$ such that $\#G \notin \mathfrak{p}$. Then the following hold:

(i) The prime ideal $\mathfrak{p}$ does not divide $\operatorname{disc}(A)$.

(ii) We have

$$\frac{\zeta_{\Lambda_\mathfrak{p}}(M_\mathfrak{p}, s)}{\zeta_{V,\mathfrak{p}}(s)} = 1.$$

Proof. (i): Let Λ_0 be a maximal order of KG containing $\mathcal{O}G$. Since $\operatorname{disc}(\mathcal{O}G) = \operatorname{disc}(\Lambda_0)(\Lambda_0 : \mathcal{O}G)^2 = \operatorname{disc}(A)(\Lambda_0 : \mathcal{O}G)^2$, it is sufficient to show that $\mathfrak{p}$ does not divide $\operatorname{disc}(\mathcal{O}G)$. As $KG = \mathbf{Q}G \otimes_\mathbf{Q} K$ and $\mathcal{O}G = \mathbf{Z}G \otimes_\mathbf{Z} \mathcal{O}$ we have $\operatorname{disc}(\mathcal{O}G) = \operatorname{disc}(\mathbf{Z}G)\mathcal{O}$. Now the claim follows since $\operatorname{disc}(\mathbf{Z}G)$ divides $\#G^{\#G}$ (see [Sol77, Section 4, Remark]). (ii): Since $(\mathcal{O}G)_\mathfrak{p}$ is maximal by Lemma 6.13, the claim follows using (i) and Lemma 9.8. □

Theorem 9.14. Let G be a finite group, $A = KG$ and $\Lambda = \mathcal{O}G$. Then for each prime ideal $\mathfrak{p}$ of $\mathcal{O}$ with $\#G \in \mathfrak{p}$ there exists a polynomial $\varphi_\mathfrak{p} \in \mathbf{Z}[X]$ such that

$$\zeta_\Lambda(M, s) = \zeta_V(s) \prod_{\mathfrak{p}\colon \#G\in\mathfrak{p}} \varphi_\mathfrak{p}(p^{-s})$$

for all $\operatorname{Re}(s) > \dim_K(V)$, where p is the rational prime lying below $\mathfrak{p}$.

Proof. This follows from Lemma 9.4, 9.12 and Theorem 9.12. □

§10. An effective version of the theorem of Jordan–Zassenhaus

Let $\mathcal{O}$ be a Dedekind domain such that the field of fractions K is a global field, that is an algebraic number field or a function field of transcendence degree 1 over a finite field, and Λ an $\mathcal{O}$-order in a semisimple finite-dimensional K-algebra A. Then the famous theorem of Jordan–Zassenhaus states—in its most general setting—that given any A-module V, there are up to Λ-isomorphisms only finitely many Λ-lattices M such that the A-module KM is isomorphic to V. To say that this theorem is important in the theory of orders (that is, in noncommutative number theory) is a massive understatement as the countless applications show. Among those is the finiteness of the class number of number fields (specialize $A = K$ and $\Lambda = \mathcal{O} = \mathcal{O}_K$ the ring of integers of K) and the finiteness of the locally free class group. However the applications are not limited to the theory of orders alone, but also to seemingly unrelated topics. For example, Brauer's original proof of the class number relation for Galois number fields [Bra51] uses the theorem of Jordan–Zassenhaus applied to the group ring of the Galois group. And in general applications can be found everywhere in the theory of Galois modules. Lastly let us mention the classification of conjugacy classes of finite subgroups of $\mathrm{GL}_n(\mathbf{Z})$, for which the theorem of Jordan–Zassenhaus is the underlying theoretical foundation (see [PP77]).

The origins of this theorem date back to Jordan [Jor80]. In his paper Jordan uses the theory of reduced forms to show that quadratic forms decompose into finitely many equivalence classes under integral transformations. The result, which was later reproved by Minkowski in his famous paper [Min06], implies the theorem in the case $\Lambda = \mathbf{Z}G$, where G is a finite group. Motivated by the work on space groups, Bieberbach gave in [Bie12] a streamlined proof of Jordan–Zassenhaus for $\Lambda = \mathbf{Z}G$, still using the theory of quadratic forms. The special cases where G is cyclic or V absolutely irreducible was proved—without appealing to quadratic forms—by Speiser in his book [Spe23]. The goal of freeing Jordan–Zassenhaus from the shackles of quadratic forms was completed by Zassenhaus in [Zas37] where he also extended the result to $\Lambda = \mathcal{O}G$, where $\mathcal{O}$ is any order in an algebraic number field. The final form we stated in the beginning was proven by Swan and Evans in [Swa70]. For a modified proof strategy of this result see also [Rei03]. We call it the final form since it is well known that none of the assumptions can be weakened.

Gaschütz—unhappy about the state of the art proofs for the case $\Lambda = \mathbf{Z}G$—gave in [Gas06] a conceptually much easier proof based on Schur's lemma and Minkowski's theorem on linear forms. In addition, his proof gave in the case of V being irreducible a fairly explicit bound on the index of a set of representatives for the $\mathbf{Z}G$-isomorphism classes relative to a fixed $\mathbf{Z}G$-lattice of V. The aim of this section is the generalization of Gaschütz's ideas to the more general setting of group rings over Dedekind domains with field of fractions a global field.

Assumption 10.1. We let G be a finite group, $\mathcal{O}$ a Dedekind domain such that the field of fractions K is a global field and $A = KG$ is semisimple.

Note that the semisimplicity of KG forces $\#G$ to be a unit in K, that is, the characteristic of K does not divide $\#G$.

Definition 10.2. Let Λ be an $\mathcal{O}$-order of A. For a Λ-lattice M and $c \in \mathbf{R}$ we say that *Jordan–Zassenhaus holds for M with constant c*, if and only if for each Λ-lattice N with $KM \cong KN$ as A-modules there exists a Λ-lattice L of M such that $M \subseteq L$, $L \cong N$ as Λ-lattices and $|L : M| \leq c$.

Lemma 10.3. Let M, N be two $\mathcal{O}G$-lattices of V and $\sigma\colon V \to V$ a K-linear map with $M\sigma \subseteq N$ as well as $\operatorname{Tr}(\sigma) \neq 0$. Then the element $\tau = \sum_{g \in G} g\sigma g^{-1}$ satisfies the following properties:

(i) $M\tau \subseteq N$,

(ii) $\tau h = h\tau$ for all $h \in G$,

(iii) $\operatorname{Tr}(\tau) = \#G \cdot \operatorname{Tr}(\sigma) \neq 0$.

Proof. (i) and (ii): Clear. (iii): This follows from the fact that conjugate linear transformations have the same trace. We have $\#G \neq 0$ in K since KG is semisimple. □

§10A. Algebraic number fields

Assumption 10.4. We now assume that $\mathcal{O} = \mathcal{O}_K$ is the ring of integers of a number field K of degree d.

As $K|\mathbf{Q}$ is separable, we have d embeddings $K \to \mathbf{C}$ giving rise to Archimedean absolute values on K denoted by $|\ |_1, |\ |_2, \dots, |\ |_d$. Recall the following classical results from the geometry of numbers.

Lemma 10.5. The following hold:

(i) Let $A \in \operatorname{Mat}_{n\times n}(\mathbf{R})$ be a real matrix and $c_1, \dots, c_n \in \mathbf{R}_{>0}$ such that $c_1 c_2 \cdots c_n \geq |\det(A)|$. Then there exist $m_1, \dots, m_n \in \mathbf{Z}$ not all equal zero with

$$\left| \sum_{j=1}^{n} a_{ij} m_j \right| \leq c_i,$$

for all $i = 1, \dots, n$.

(ii) Let M be a free $\mathbf{Z}$-module with basis $a_1, a_2, \dots, a_n$ and $N \subseteq M$ a $\mathbf{Z}$-submodule of the same rank. Then there exist $s_i \in \mathbf{Z}$, $1 \leq i \leq n$, not all equal to zero with $|s_i| \leq \sqrt[n]{|M : N|}$ and $\sum_{i=1}^{n} s_i a_i \subseteq N$.

Proof. While claim (i) is Minkowski's famous theorem on linear forms (proven for example in [PZ89, Theorem (4.4)]), the second part follows from (i) by choosing A to be a basis matrix of N with respect to $a_1, \dots, a_n$ and $c_i = \sqrt[n]{|M : N|}$ for $i = 1, \dots, n$. □

We now want to extend this result to modules over $\mathcal{O}$.

Lemma 10.6. Let M be a finitely generated projective $\mathcal{O}$-module of rank n and N a submodule of M of the same rank. Assume that $((\mathfrak{a}_i), (v_i))$ is a pseudo-basis of M and for each $1 \leq i \leq n$ the family $(\omega_i^j)_{1 \leq j \leq d}$ is a $\mathbf{Z}$-basis of $\mathfrak{a}_i$. Then for each $1 \leq i \leq n$ there exists $\alpha_i \in \mathfrak{a}_i$ such that $(\alpha_1, \dots, \alpha_n) \neq 0$, $\sum_{i=1}^{n} \alpha_i v_i \in N$ and

$$|\alpha_i|_k \leq d \cdot \max_{1 \leq j \leq d} |\omega_i^j|_k \cdot |M : N|^{\frac{1}{dn}} \text{ for } 1 \leq i \leq n,\ 1 \leq k \leq d.$$

Proof. Since $\mathcal{O}$ is a free $\mathbf{Z}$-module of rank d, we can consider M and N as free $\mathbf{Z}$-modules of rank nd. As

$$M = \bigoplus_{i=1}^{n} \mathfrak{a}_i v_i = \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{d} \mathbf{Z}\omega_i^j v_i,$$

the elements $(\omega_i^j v_i)_{i,j}$ form a $\mathbf{Z}$-basis of M. Now Lemma 10.5 asserts the existence of $a_j^i \in \mathbf{Z}$ not all equal zero with $|a_j^i| \leq |M : N|^{\frac{1}{dn}}$ and

$$\sum_{i=1}^{n} \sum_{j=1}^{d} a_j^i \omega_i^j v_i \in N.$$

Thus the elements $\alpha_i = \sum_{j=1}^{d} a_j^i \omega_i^j \in \mathfrak{a}_i$, $1 \leq i \leq n$, satisfy $\sum_{i=1}^{n} \alpha_i v_i \in N$. The claim about the absolute values follows immediately. □

Remark 10.7. In Lemma 10.6 the dependency on the absolute values of the ideal bases instead of the ideals themselves should been seen as the price we have to pay for choosing an explicit isomorphism $M \to \mathbf{Z}^{dn}$ and relying on the analogous result for $\mathbf{Z}$-modules.

Theorem 10.8 (Jordan–Zassenhaus for number fields). Let V be an irreducible KG-module and $M \subseteq V$ an $\mathcal{O}G$-lattice with pseudo-basis $((\mathfrak{a}_i), (v_i))$ with the property that all coefficient ideals $\mathfrak{a}_i$ are integral. For each $1 \leq i \leq n$ let $(\omega_i^j)_{1 \leq j \leq d}$ be a $\mathbf{Z}$-basis of $\mathfrak{a}_i$. Denote by $\rho \colon G \to \mathrm{GL}_n(K), g \mapsto \rho_{ij}(g)$ the representation corresponding to V with respect to the K-basis $(v_1, \ldots, v_n)$ of V. Then Jordan–Zassenhaus holds for M with constant

$$c = (\#G \cdot n^2 d \cdot \max_{i,j,k,g} |\rho_{ij}(g)|_k^2 \cdot \max_{i,j,k} |\omega_j^i|_k)^{dn} \leq (\#G \cdot n^2 d \cdot \max_g \|\rho(g)\|^2 \cdot \max_{i,j} \|\omega_j^i\|')^{dn},$$

where for $\alpha \in K$ we put $\|\alpha\|' = \max_k |\alpha|_k$ and $\|\rho(g)\| = \max_{i,j} \|\rho_{ij}(g)\|'$.

Proof. Note that since M is invariant under the action of G, we have $\rho_{ij}(g) \in \mathfrak{a}_i^{-1}\mathfrak{a}_j$ ([Coh00, Proposition 1.4.4]) and $v_i g = \sum_{j=1}^n \rho_{ij}(g) v_j$. Now let N be an $\mathcal{O}G$-lattice of V. After replacing N with a suitable multiple αN, $\alpha \in K$, we can assume that N is contained in M. As V is an irreducible KG-module, the $\mathcal{O}G$-lattice N has the same rank as M and we can apply Lemma 10.6. Thus there exist $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$ not all equal to zero with $\sum_{i=1}^n \alpha_i v_i \subseteq N$, and $|\alpha_i|_k \leq d \cdot \max_{1 \leq j \leq d} |\omega_j^i|_k |M : N|^{\frac{1}{dn}}$ for $1 \leq i \leq n$, $1 \leq k \leq d$. Let $1 \leq m \leq n$ be an index such that $\alpha_m \neq 0$. Consider now the K-linear map

$$\sigma \colon V \longmapsto V, \sum_{i=1}^n \beta_i v_i \longmapsto \beta_m \Big(\sum_{i=1}^n \alpha_i v_i \Big).$$

We claim that σ maps M to N. Let $v = \sum_{i=1}^n \beta_i v_i$ be an element of M, that is, $\beta_i \in \mathfrak{a}_i \subseteq \mathcal{O}$ for $1 \leq i \leq n$. Then $v\sigma = \beta_m \sum_{i=1}^n \alpha_i v_i \in \beta_m N \subseteq \mathcal{O}N \subseteq N$ and we conclude that $M\sigma \subseteq N$.

With respect to the K-basis $(v_i)_i$ of V the map σ is represented by the matrix obtained by replacing the mth row of the zero matrix with $(\alpha_1, \ldots, \alpha_n)$. In particular σ satisfies $\mathrm{Tr}(\sigma) = \alpha_m \neq 0$. Therefore we can apply Lemma 10.3 which shows that the morphism $\tau = \sum_{g \in G} g\sigma g^{-1}$ is a G-equivariant, K-linear morphism $V \to V$ with $M\tau \subseteq N$ and $\tau \neq 0$. Since V is irreducible, according to Schur's Lemma all nonzero elements of $\mathrm{Hom}_{KG}(V, V)$ are invertible and in particular $\tau^{-1} \in \mathrm{Hom}_{KG}(V, V)$ exists. We now want to bound $|M : M\tau| = \mathbf{N}(\det(\tau))$ in terms of $|M : N|$. To this end we consider the matrix $(\tau_{ij})_{ij} \in \mathrm{GL}_n(K)$ corresponding to τ with respect to the K-basis $(v_1, \ldots, v_n)$ of V. Exploiting the fact that only the mth row of the matrix corresponding to σ is nonzero, we obtain that with respect to the K-basis $(v_i)_i$ of V, the map $g\sigma g^{-1}$ is represented by the matrix

$$\left(\rho_{i,m}(g) \sum_{l=1}^n \alpha_l \cdot \rho_{lj}(g^{-1}) \right)_{i,j} \quad \text{which yields } \tau_{ij} = \left(\sum_{g \in G} \rho_{i,m}(g) \sum_{l=1}^n \alpha_l \cdot \rho_{lj}(g^{-1}) \right)$$

when summing over all $g \in G$. Therefore

$$|\tau_{ij}|_k \leq \#G \cdot n \cdot \max_{u,v,g} |\rho_{uv}(g)|_k \cdot \max_{u,v,g} |\rho_{uv}(g^{-1})|_k \cdot \max_{1 \leq u \leq n} |\alpha_u|_k \leq \#G \cdot n \cdot \max_{u,v,g} |\rho_{uv}(g)|_k^2 \cdot \max_{1 \leq u \leq n} |\alpha_u|_k \quad \text{for } 1 \leq k \leq d.$$

Using Leibniz's formula for the determinant we get $|\det(\tau)|_k \leq n^n \max_{i,j} |\tau_{ij}|_k^n$ and combining this with our estimates for the matrix entries and α_i we finally obtain

$$|\det(\tau)|_k \leq (\#G)^n \cdot n^{2n} \cdot d^n \cdot \max_{i,j,g} |\rho_{ij}(g)|_k^{2n} \cdot \max_{i,j} |\omega_j^i|_k^n \cdot |M : N|^{\frac{1}{d}} \quad \text{for } 1 \leq k \leq d.$$

Thus for the norm we have

$$\begin{aligned} \mathbf{N}(\det(\tau)) = |\mathrm{N}_{\mathbf{Q}}^K(\det(\tau))| &= |\det(\tau)|_1 \cdot |\det(\tau)|_2 \cdots |\det(\tau)|_d \\ &\leq (\#G)^{dn} \cdot n^{2dn} \cdot d^{dn} \cdot \max_{i,j,k,g} |\rho_{ij}(g)|_k^{2dn} \cdot \max_{i,j,k} |\omega_j^i|^{dn} \cdot |M : N| = c \cdot |M : N|, \end{aligned}$$

where c is as in the statement. Now the module $L = N\tau^{-1}$ is isomorphic to N as $\mathcal{O}G$-modules with $L \supseteq M$ and

$$|L : M| = |N\tau^{-1} : M| = |N : M\tau| = \frac{|M : M\tau|}{|M : N|} = \frac{\mathbf{N}(\det(\tau))}{|M : N|} \leq c,$$

proving the theorem. □

§10B. Global function fields

We now turn to the proof of Jordan–Zassenhaus in positive characteristic.

Assumption 10.9. Let K be a finite separable extension of $\mathbf{F}_q(X)$, q a prime power, and $\mathcal{O}$ the integral closure of $\mathbf{F}_q[X]$ in K.

By $|\ |_\infty\colon \mathbf{F}_q(X) \to \mathbf{R}_{>0}$, $f \longmapsto q^{\deg(f)}$ we denote the unique representative for the non-Archimedean place at infinity with $|X|_\infty = q$ and by $\mathbf{F}_q(X)_\infty$ the completion of $\mathbf{F}_q(X)$ at $|\ |_\infty$. Now let $|\ |_1, \dots, |\ |_s$ be the non-Archimedean absolute values of K lying above $|\ |_\infty$ and K_i, $1 \le i \le s$, the corresponding completions. Note that since $|\ |_i$ extends $|\ |_\infty$ we necessarily have $|f|_i = |\mathrm{N}_K^{K_i}(f)|_\infty^{1/[K_i:\mathbf{F}_q(X)_\infty]}$ for $f \in K_i$. For convenience let us denote the local degree $[K_i : \mathbf{F}_q(X)_\infty]$ by d_i.

Lemma 10.10. For $f \in K^\times$ we have $\mathbf{N}((f)) = \prod_{i=1}^s |f|_i^{d_i}$.

Proof. Since both sides are multiplicative in f it is sufficient to prove it for $f \in \mathcal{O}$. Denote by μ_f the K-linear map $K \to K$, $g \mapsto fg$. Then

$$\mathbf{N}((f)) = |\det(\mu_f)|_\infty = |\mathrm{N}^K_{\mathbf{F}_q(X)}(f)|_\infty = \prod_{i=1}^s |\mathrm{N}^{K_i}_{\mathbf{F}_q(X)_\infty}(f)|_\infty = \prod_{i=1}^s |f|_i^{d_i}.$$ □

In order to carry over the ideas of the characteristic 0 case, we need to invoke the following theorem of Tornheim [Tor41], which is an analogue of Minkowski's theorem on linear forms for polynomial rings.

Theorem 10.11 ([Tor41, Theorem 1]). Let k be a field, $C = (c_{ij})_{i,j} \in \mathrm{Mat}_n(k[X])$ and $u_1, \dots, u_n \in \mathbf{Z}_{>0}$ integers with $\deg(\det(C)) < \sum_{i=1}^n (u_i + 1)$. Then there exist $a_1, \dots, a_n \in k[X]$ such that

$$\deg\Bigl(\sum_{j=1}^n a_j c_{ij}\Bigr) < u_i \quad \text{for } 1 \le i \le n.$$

We can now derive the analogous results of Lemmata 10.5 and 10.6.

Lemma 10.12. Let M be a free $\mathbf{F}_q[X]$-module with basis $(v_i)_{1 \le i \le n}$ and N a submodule of the same rank. Then there exist $a_1, \dots, a_n \in \mathbf{F}_q[X]$ not all equal to zero with $\deg(a_i) \le \log_q(|M:N|)/n$ (that is, $|a_i|_\infty \le |M:N|^{1/n}$) and $\sum_{i=1}^n a_i v_i \in N$.

Proof. We set $n_i = \lfloor \log_q(|M:N|)/n \rfloor$ for $1 \le i \le n$ and denote by $C \in \mathbf{F}_q[X]$ a basis matrix of N with respect to $(v_i)_i$. Then

$$\deg(\det(C)) = \log_q(|M:N|) < \sum_{i=1}^n (n_i + 1)$$

and by Theorem 10.11 there exist $b_i \in \mathbf{F}_q[X]$, $1 \le i \le n$, with $\deg(\sum_{j=1}^n c_{ij} b_j) \le \lfloor \log_q(|M:N|)/n \rfloor \le \log_q(|M:N|)/n$. Now the elements $a_i = \sum_{j=1}^n b_j c_{ij}$, $1 \le i \le n$, satisfy the condition. □

Lemma 10.13. Let M be a finitely generated torsion-free $\mathcal{O}$-module of rank n and N a submodule of M of the same rank. Assume that $((\mathfrak{a}_i), (v_i))$ is a pseudo-basis of M and $(\omega_i^j)_{1 \le j \le d}$, $1 \le i \le n$ are $\mathbf{F}_q[X]$-bases of $\mathfrak{a}_i$ for $1 \le i \le n$. Then there exist $f_1, \dots, f_n \in K$ not all equal to zero with $\sum_{i=1}^n f_i v_i \in N$ and

$$|f_i|_k \le \max_{1 \le j \le d} |\omega_i^j|_k \cdot |M:N|^{\frac{1}{dn}} \quad \text{for } 1 \le i \le n,\ 1 \le k \le s.$$

Proof. The proof is similar to the proof of Lemma 10.6. We have

$$M = \bigoplus_i^n \mathfrak{a}_i v_i = \bigoplus_{i=1}^n \bigoplus_{j=1}^d \mathbf{F}_q[X] \omega_j^i \alpha_i$$

and consider M as a free $\mathbf{F}_q[X]$-module of rank dn. Due to Theorem 10.12 there exist elements $a_j^i \in \mathbf{F}_q[X]$, $1 \le i \le n$, $1 \le j \le d$, such that $|a_j^i|_\infty \le |M/N|^{\frac{1}{dn}}$. For $1 \le i \le n$ we now define $f_i = \sum_{j=1}^n a_j^i \omega_j^i$. Then we obtain $\sum_{i=1}^n f_i v_i \in N$ as well as

$$|f_i|_k \le \max_j |\omega_j^i a_j^i|_k \le \max_{u,v} |\omega_v^u|_k \cdot \max_{u,v}(q^{\deg(a_v^u)}) \le \max_{u,v} |\omega_v^u|_k \cdot |M:N|^{\frac{1}{dn}} \quad \text{for } 1 \le k \le s.$$ □

Theorem 10.14 (Jordan–Zassenhaus for global function fields). Let V be an irreducible KG-module and $M \subseteq V$ an $\mathcal{O}G$-lattice with pseudo-basis $((\mathfrak{a}_i), (v_i))$ such that $\mathfrak{a}_i$ is integral for $1 \leq i \leq n$. For each $1 \leq i \leq n$ let $(\omega_i^j)_{1 \leq j \leq d}$ be a $\mathbf{F}_q[X]$-basis of $\mathfrak{a}_i$. Denote by $\rho \colon G \to \mathrm{GL}_n(K)$, $g \mapsto \rho_{ij}(g)$ the representation corresponding to V with respect to the K-basis $(v_1, \ldots, v_n)$ of V. Then Jordan–Zassenhaus holds for M with constant

$$c = (\max_{i,j,k,g} |\rho_{ij}(g)|_k^2 \cdot \max_{i,j,k} |\omega_j^i|_k)^{dn} = (\max_g \|\rho(g)\| \cdot \max_{i,j} \|\omega_j^i\|)^{dn}.$$

Proof. We proceed as in the proof of Theorem 10.8 up to the point where we have to determine $\mathbf{N}(\det(\tau))$. Note that a big difference is the fact that all valuations are non-Archimedean, that is, the strong triangle inequality holds. For $1 \leq k \leq s$ we have

$$|\tau_{ij}|_k \leq (\max_{u,v,k,g} |\rho_{uv}(g)|_k)^2 \max_u |f_u|_k$$

and therefore

$$|\det(\tau)|_k \leq (\max_{i,j,u,g} |\rho_{ij}(g)|_u)^{2n} \max_i |f_i|_u^n.$$

Now raising these inequalities to the power d_k and multiplying them up gives us by Lemma 10.10:

$$\mathbf{N}(\det(\tau)) \leq (\max_{i,j,k,g} |\rho_{ij}(g)|_k)^{2dn} (\max_{i,j,k} |\omega_j^i|_k)^{dn} |M : N|.$$

□

Defining $L = N\tau^{-1}$ and $c = (\max_{i,j,k,g} |\rho_{ij}(g)|_k)^{2dn} \cdot (\max_{i,j,k} |\omega_j^i|_k)^{dn}$ we obtain $L \cong N$ as $\mathcal{O}G$-modules and $|L : M| < c$.

§10C. The general case

We come now back to the general case, whose proof will involve a known reduction trick due to Swan.

Lemma 10.15. Let $\mathcal{O}$ be a Dedekind domain with field of fractions K being a global field and S a multiplicatively closed subset of $\mathcal{O}$ with $0 \notin S$. Assume that V is an irreducible KG-module and M an $(S^{-1}\mathcal{O})G$-lattice of V, generated by $m_1, \ldots, m_l$ as an $S^{-1}\mathcal{O}G$-module. If Jordan–Zassenhaus holds for the $\mathcal{O}G$-lattice $M_{\mathcal{O}} = \mathcal{O}Gm_1 + \cdots + \mathcal{O}Gm_l$ with constant c, then Jordan–Zassenhaus holds for M with constant c.

Proof. This is [Swa70, Lemma 3.7]. As we want to keep track of the constant c, we will reproduce it here. First note that $S^{-1}(\mathcal{O}G) = (S^{-1}\mathcal{O})G$ and $M_{\mathcal{O}}$ determines M as $S^{-1}M_{\mathcal{O}} = M$. Now let N be another $(S^{-1}\mathcal{O})G$-lattice of V to which we associate an $\mathcal{O}G$-lattice $N_{\mathcal{O}}$ in the same way. As Jordan–Zassenhaus holds for $M_{\mathcal{O}}$ with constant c, there exists an $\mathcal{O}G$-lattice L of V such that $M_{\mathcal{O}} \subseteq L$, $N_{\mathcal{O}} \cong L$ as $\mathcal{O}G$-lattices and $|L : M_{\mathcal{O}}| < c$. But then $S^{-1}L$ is an $(S^{-1}\mathcal{O})G$-lattice with $M = S^{-1}M_{\mathcal{O}} \subseteq S^{-1}L$, $N = S^{-1}N_{\mathcal{O}} \cong S^{-1}L$ as $(S^{-1}\mathcal{O})G$-lattices and

$$|S^{-1}L : S^{-1}M_{\mathcal{O}}| = \mathbf{N}((S^{-1}L : S^{-1}M_{\mathcal{O}})) = \mathbf{N}(S^{-1}(L : M_{\mathcal{O}})) \leq \mathbf{N}((L : M_{\mathcal{O}})) = |L : M_{\mathcal{O}}| < c.$$

□

Lemma 10.16. Let R be a Dedekind domain with field of fractions K being a global field.

(i) If $\mathrm{char}(K) = 0$, then $R = S^{-1}\mathcal{O}$ where $\mathcal{O}$ is the ring of integers of the number field K and S is a multiplicatively closed subset.

(ii) If $\mathrm{char}(K) = p > 0$, then there exists an element $X \in K$ and a power q of p such that $K|\mathbf{F}_q(X)$ is a finite separable extension and $R = S^{-1}\mathcal{O}$, where $\mathcal{O}$ is the integral closure of $\mathbf{F}_p[X]$ in K and S is a multiplicatively closed subset of $\mathcal{O}$.

Proof. This is [Swa70, Proposition A21 and A23]. □

Theorem 10.17. Let G be a finite group and $\mathcal{O}$ a Dedekind domain such that the field of fractions K is a global field and KG is semisimple. Let V be an irreducible KG-module and $M \subseteq V$ an $\mathcal{O}G$-lattice. Then there exists an explicitly computable constant $c \in \mathbf{R}_{>0}$, such that Jordan–Zassenhaus holds for M with constant c.

Proof. This now follows from Lemma 10.15 applied to Theorem 10.8 and 10.14. □

For completeness let us reformulate Jordan–Zassenhaus using sublattices instead of superlattices.

Corollary 10.18. Let G be a finite group and $\mathcal{O}$ a Dedekind domain such that the field of fractions K is a global field an KG is semisimple. Let V be an irreducible KG-module and $M \subseteq V$ an $\mathcal{O}G$-lattice. Then there exists an explicitly computable constant $c \in \mathbf{R}_{>0}$ such that for all $\mathcal{O}G$-lattices L of V there exists an $\mathcal{O}G$-lattice $N \subseteq M$ such that $L \cong N$ and $|M : N| \leq c$.

Proof. Let c' be the constant obtained by applying Theorem 10.17 to M, and L an $\mathcal{O}G$-lattice of V. Then there exists $N' \supseteq M$ such that $N' \cong L$ and $|N' : M| \leq c'$. Now set $N = |N' : M| \cdot N'$. Then $N \cong N' \cong L$ and $N \subseteq M \subseteq N'$. Moreover we have $|M : N| \leq |N' : N| = |N' : M|^{dn} \leq (c')^{dn}$. Thus $c = (c')^{dn}$ is a valid choice. □

§10D. On the number of lattices

Assumption 10.19. Let G be a finite group and $\mathcal{O}$ a Dedekind domain such that the field of fractions K is a global field of characteristic 0.

As an application of the previous section, we want to derive bounds on the number of isomorphism classes of lattices rationally equivalent to V. Let us denote by $h(V)$ the number of isomorphism classes of $\mathcal{O}G$-lattices of a KG-module V. We first start with the irreducible case and deal then with the general case using extensions of lattices.

The irreducible case.

Lemma 10.20. Let M be a finitely-generated torsion-free $\mathcal{O}$-module of rank n and $B \in \mathbf{Z}_{>0}$. Then

(i) M has at most B^{dn^2} many submodules N with $|M : N| = B$,

(ii) M has at most B^{dn^2+1} many submodules N with $|M : N| \leq B$.

Proof. (i): The number of submodules N of M with $|M : N| = B$ is bounded by the number of submodules of M/BM. Now the latter module is isomorphic to the $\mathcal{O}/B\mathcal{O}$-module $(\mathcal{O}/B\mathcal{O})^n$. As $\mathcal{O}/B\mathcal{O}$ is a finite euclidean ring with cardinality $\mathbf{N}((B))$, the Howell normal form shows that $(\mathcal{O}/B\mathcal{O})^n$ has at most $\mathbf{N}((B))^{n^2}$ many submodules. Since $\mathbf{N}((B)) \leq B^d$, the claim follows. For (ii) we just sum over B terms. □

Given an irreducible KG-module V and an $\mathcal{O}G$-lattice M of V, using Corollary 10.18 and the previous lemma we can now bound $h(V)$ in terms of data attached to M. Since the formulae won't get prettier, we just mention a special case which often occurs in applications.

Corollary 10.21. Let V be an irreducible $\mathbf{Q}G$-module with associated representation $\rho\colon G \to \mathrm{GL}_n(\mathbf{Z})$ and $B \in \mathbf{R}_{>0}$ such that $|\rho(g)|_\infty \leq B$ for all $g \in G$. Then

$$h(V) \leq (\#G \cdot n^2 B^2)^{n^4+n^2}.$$

Remark 10.22. To see that bounds on $h(V)$ we obtain in this way are in general way too large we consider the symmetric group $G = \mathfrak{S}_{n+1}$ on $n+1$ letters. Attached to the partition $(2, 1^{n-1})$ of $n+1$ we have the corresponding Specht module $V = S^{(2,1^{n-1})}$, which is an irreducible $\mathbf{Q}G$-module of dimension n. We want to bound $h(V)$ using Corollary 10.21 and compare the result with the actual value $h(V) = \sigma_0(n+1)$, where σ_0 is the divisor counting function, obtained by Craig in [Cra76] and Plesken in [Ple74]. To this end we want to show that there exists a representation $\rho\colon \mathfrak{S}_{n+1} \to \mathrm{GL}_n(\mathbf{Z})$ associated to $S^{(2,1^{n-1})}$ such that $|\rho(\sigma)|_\infty = 1$ for all $\sigma \in \mathfrak{S}_{n+1}$. Since $S^{(2,1^{n-1})} \cong S^{(n,1)} \otimes_{\mathbf{Q}G} \mathrm{sgn}$, where sgn is the 1-dimensional signum representation, it is sufficient to show that $S^{(n,1)}$ admits a representation where all matrix entries are in $\{0, \pm 1\}$. Denote by $M^{(n,1)}$ the natural permutation module of dimension $n+1$ with basis $\omega_1, \dots, \omega_{n+1}$, on which $\mathfrak{S}_{n+1}$ acts via $\sigma(\omega_i) = \omega_{\sigma(i)}$ ($\sigma \in G$, $1 \leq i \leq n+1$). Then $S^{(n,1)}$ can be identified with the kernel of the augmentation morphism, that is,

$$S^{(n,1)} = \Big\{ \sum_{i=1}^{n+1} a_i \omega_i \,\Big|\, \sum_{i=1}^{n+1} a_i = 0 \Big\} = \bigoplus_{i=2}^{n+1} \mathbf{Q}(\omega_1 - \omega_i).$$

For we have $\sigma(\omega_1 - \omega_i) = (\omega_1 - \omega_{\sigma(i)}) - (\omega_1 - \omega_{\sigma(1)})$, with respect to the $\mathbf{Q}$-basis $(\omega_1 - \omega_i)_i$, the entries of the representation matrices are in $\{0, \pm 1\}$. Thus Corollary 10.21 implies that $h(V)$ is bounded by

$$((n+1)! \cdot n^2)^{n^4+n^2},$$

which is of magnitudes larger than $h(V) = \sigma_0(n+1) < n+1$.

The general case. Now let V be an arbitrary KG-module. Using the irreducible case we want to derive bounds on the number $h(V)$ of isomorphism classes of $\mathcal{O}G$-lattices in V. Assume that $W \subseteq V$ is a non-trivial KG-module. We then have an exact sequence

$$0 \longrightarrow W \longrightarrow V \longrightarrow V/W \longrightarrow 0$$

of KG-modules. Any $\mathcal{O}G$-lattice M of V induces an exact sequence

$$0 \longrightarrow W \cap M \longrightarrow M \longrightarrow M/(W \cap M) \longrightarrow 0$$

of $\mathcal{O}G$-modules. Moreover $W \cap M$ and $W/(W \cap M)$ respectively are $\mathcal{O}G$-lattices of W and V/W respectively. Thus any $\mathcal{O}G$-lattice M gives rise to two $\mathcal{O}G$-lattices of smaller rank. To what extent M is determined by these pieces is exactly the well-understood theory of extensions.

We start with arbitrary $\mathcal{O}G$-lattices M and N. Recall that an extension of M by N is an $\mathcal{O}G$-exact sequence

$$0 \longrightarrow M \longrightarrow X \longrightarrow N \longrightarrow 0.$$

(The $\mathcal{O}G$-module X is then also an $\mathcal{O}G$-lattice since the sequence is $\mathcal{O}$-split). We call X the $\mathcal{O}G$-lattice corresponding to this extension. Two extensions

$$0 \longrightarrow M \longrightarrow X_i \longrightarrow N \longrightarrow 0 \quad (1 \leq i \leq 2)$$

are called equivalent, if there exists a morphism $\varphi \colon X_1 \to X_2$ such that

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r] \arrow[d, equal] & X_1 \arrow[r] \arrow[d, "\varphi"'] & N \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & M \arrow[r] & X_2 \arrow[r] & N \arrow[r] & 0
\end{tikzcd}$$

commutes. Note that φ is necessarily an $\mathcal{O}G$-isomorphism. The set of extensions of M by N modulo this equivalence relation is naturally an $\mathcal{O}$-module, denoted by $\operatorname{Ext}_{\mathcal{O}G}(M, N)$.

Lemma 10.23. Let

$$\begin{tikzcd}
0 \arrow[r] & U \arrow[r, "\iota"] & V \arrow[r, "\pi"] & W \arrow[r] & 0
\end{tikzcd}$$

be an exact sequence of KG-modules, $\{X_i\}_{i \in I}$ and $\{Y_j\}_{j \in J}$ representatives of the isomorphism classes of $\mathcal{O}G$-lattices of U and W respectively. Then the following hold:

(i) For every $\mathcal{O}G$-lattice M of V there exist $i \in I$, $j \in J$ and an extension

$$0 \longrightarrow X_i \longrightarrow M \longrightarrow Y_j \longrightarrow 0$$

of X_i by Y_j.

(ii) If I, J and $\operatorname{Ext}_{\mathcal{O}G}(X_i, Y_j)$ $(i \in I, j \in J)$ are finite, then

$$h(V) \leq \prod_{i \in I} \prod_{j \in J} \# \operatorname{Ext}_{\mathcal{O}G}(X_i, Y_j).$$

In particular if $\# \operatorname{Ext}_{\mathcal{O}G}(X_i, Y_j) \leq B$ for all $i \in I$, $j \in J$ for some $B \in \mathbf{R}_{>0}$, then

$$h(V) \leq B^{h(U)h(W)}.$$

Proof. (1): The $\mathcal{O}G$-modules $\iota^{-1}(M) \subseteq U$ and $\pi(M) \subseteq W$ are $\mathcal{O}G$-lattices of U and W respectively. Thus we can find $i \in I$ and $j \in J$ such that $\iota^{-1}(M) \cong X_i$ and $\pi(M) \cong Y_j$ as $\mathcal{O}G$-lattices. Now the claim follows as the sequence

$$\begin{tikzcd}
0 \arrow[r] & \iota^{-1}(M) \arrow[r, "\iota"] & M \arrow[r, "\pi"] & \pi(M) \arrow[r] & 0
\end{tikzcd}$$

is $\mathcal{O}G$-exact.

(2): This follows from the fact that equivalent extensions have isomorphic corresponding $\mathcal{O}G$-lattices. □

Thus once we know that $\operatorname{Ext}_{\mathcal{O}G}(M, N)$ is finite for all $\mathcal{O}G$-lattices M and N we can inductively conclude that V contains only finitely many $\mathcal{O}G$-lattices up to $\mathcal{O}G$-isomorphism. Moreover any bound on $\operatorname{Ext}_{\mathcal{O}G}(M, N)$ will give us bounds on $h(V)$.

Lemma 10.24. Let M and N be $\mathcal{O}G$-lattices. Then the following hold:

(i) The $\mathcal{O}$-module $\mathrm{Ext}_{\mathcal{O}G}(M,N)$ is finitely generated and $\#G \cdot \mathrm{Ext}_{\mathcal{O}G}(M,N) = 0$.

(ii) We have
$$\#\,\mathrm{Ext}_{\mathcal{O}G}(M,N) \leq \mathbf{N}(\#G\mathcal{O})^{\#G \dim_K(KM)\dim_K(KN)}.$$

Proof. (1): This is (25.12) Theorem in [CR81].

(2): Assume that the $\mathcal{O}$-module $\mathrm{Ext}_{\mathcal{O}G}(M,N)$ can be generated by s elements $a_1,\dots,a_s$. Then (1) implies that the kernel of the surjection $\pi\colon \mathcal{O}^s \to \mathrm{Ext}_{\mathcal{O}G}(M,N)$, $e_i \mapsto a_i$ contains $(\#G \cdot \mathcal{O})^s \subseteq \mathcal{O}^s$ (here $e_1,\dots,e_s$ is an $\mathcal{O}$-basis of $\mathcal{O}^s$). Thus the canonical map

$$(\mathcal{O}/\#G\mathcal{O})^s \longrightarrow \mathcal{O}/\ker(\pi) \longrightarrow \mathrm{Ext}_{\mathcal{O}G}(M,N)$$

is surjective yielding $\#\,\mathrm{Ext}_{\mathcal{O}G}(M,N) \leq \mathbf{N}(\#G\cdot\mathcal{O})^s$. Therefore it remains to show that $\mathrm{Ext}_{\mathcal{O}G}(M,N)$ can be generated by at most $\#G \dim_K(KM)\dim_K(KN)$ elements. But this can be seen by appealing to the description of $\mathrm{Ext}_{\mathcal{O}G}(M,N)$ in terms of derivations: In [CR81, (25.10) Proposition] it is shown that $\mathrm{Ext}_{\mathcal{O}G}(M,N)$ is $\mathcal{O}$-isomorphic to a quotient of

$$\mathrm{Der}(\mathcal{O}G, \mathrm{Hom}_{\mathcal{O}}(M,N)) \subseteq \mathrm{Hom}_{\mathcal{O}}(\mathcal{O}G, \mathrm{Hom}_{\mathcal{O}}(M,N)),$$

where Der denotes the $\mathcal{O}$-module of derivations. As the rank of $\mathrm{Hom}_{\mathcal{O}}(\mathcal{O}G, \mathrm{Hom}_{\mathcal{O}}(M,N))$ is

$$s = \#G \dim_K(KM)\dim_K(KN),$$

the rank of $\mathrm{Der}(\mathcal{O}G, \mathrm{Hom}_{\mathcal{O}}(M,N))$ is bounded by s. The elementary divisor theorem for Dedekind domains implies that every quotient of $\mathrm{Der}(\mathcal{O}G, \mathrm{Hom}_{\mathcal{O}}(M,N))$, which is torsion, can be generated by s elements. □

Theorem 10.25. Let V be a KG-module with composition series

$$0 = W_1 \subseteq W_2 \subseteq \cdots \subseteq W_{r+1} = V$$

and $V_1,\dots,V_r$ irreducible KG-submodules of V with $V_i \cong W_{i+1}/W_i$ for $1 \leq i \leq r$. Then the numbers $h(W_i)$ of isomorphism classes of $\mathcal{O}G$-lattices satisfy $h(W_1) = h(V_1)$ and

$$h(W_{i+1}) \leq \mathbf{N}(\#G\mathcal{O})^{\dim_K(W_i)\dim_K(V_i)\#Gh(W_i)h(V_i)} \quad \text{for } 2 \leq i \leq r.$$

Proof. This follows from Lemma 10.23 and 10.24. □

CHAPTER 4

Algorithmic aspects of lattices over orders

Let K be an algebraic number field with ring of integers $\mathcal{O}$ and Λ an $\mathcal{O}$-order in a semisimple K-algebra A. In this chapter we will provide algorithms for the following problems:

(i) Given Λ-lattices M and N compute (pseudo-)bases of $\operatorname{Hom}_\Lambda(M,N)$, $\operatorname{Hom}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p},N_\mathfrak{p})/\mathfrak{p}^l \operatorname{Hom}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p},N_\mathfrak{p})$ and $\operatorname{Hom}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p},N_\mathfrak{p})$, where $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}$ and $l \in \mathbf{Z}_{>0}$. (Recall that $M_\mathfrak{p}$ denotes $\mathfrak{p}$-adic completion.)

(ii) Given Λ-lattices M and N, $\mathfrak{p}$ a nonzero prime ideal of $\mathcal{O}$ and $\sim \in \{\sim_\mathfrak{p}, \vee\}$ decide whether $M \sim N$.

(iii) Given a finite-dimensional A-module V, $\mathfrak{p}$ a nonzero prime ideal of $\mathcal{O}$ and $\sim \in \{\sim_\mathfrak{p}, \vee\}$, compute a set of representatives of $\mathcal{L}(V)/\sim$.

(iv) Given a Λ-lattice M, compute the local factors of the Solomon zeta function of M.

While for special cases algorithms and results can be found in the literature, in this generality the above questions have not been dealt with before. Most notably is—in the context of crystallographic groups—the case $A = \mathbf{Q}G$, $\Lambda = \mathbf{Z}G$, G a finite group, where one can compute isomorphism classes of $\mathbf{Z}G$-lattices using an algorithm of Plesken [Ple74] (see also [OPS98]).

Assumption. Let K be an algebraic number field with ring of integers $\mathcal{O}$ and Λ an $\mathcal{O}$-order in a semisimple finite dimensional K-algebra A. Let M and N be Λ-lattices of A-modules V and W respectively with dimension n and m respectively. We make the following assumptions:

(i) If $\mathscr{M}$ and $\mathscr{N}$ are K-bases of V and W respectively, we can compute a K-basis of $\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\operatorname{Hom}_A(V,W)) \subseteq \operatorname{Mat}_{n\times m}(K)$. (The task of computing $\operatorname{Hom}_A(V,W)$ is a common problem in algorithmic representation theory. While Plesken and Souvignier [PS96] handled the case $A = \mathbf{Q}G$ using the averaging operator technique (see also [Sch02, 2.2]), Steel gave in [Ste12] an algorithm in case A is an arbitrary finite dimensional semisimple algebra over a number field.)

(ii) We know a set of prime ideals $S \subseteq \operatorname{Spec}(\mathcal{O})$ such that $\Lambda_\mathfrak{p}$ is maximal for all nonzero prime ideals $\mathfrak{p} \notin S$. (This can be reduced to the computation of a maximal overorder, which is described in [Fri00]: If Λ_0 is a maximal overorder of Λ, then S can be chosen to be any finite set of prime ideals containing the prime ideal divisors of the index ideal $(\Lambda_0 : \Lambda)$. See Remark 6.15 and also Example 6.16 for the case of group rings and group algebras, where no computation of maximal orders is necessary.)

(iii) We know an ideal $\mathfrak{h}$ of $\mathcal{O}$, such that $\mathfrak{h} \cdot \operatorname{Ext}^1_\Lambda(M',N') = 0$ for all Λ-lattices M', N'. (Similar to (ii), such an ideal $\mathfrak{h}$ can be deduced once a maximal overorder Λ_0 is known. For in this case $\mathfrak{h}$ can be chosen to be any integral multiple of $(\Lambda_0 : \Lambda)$. See the comment following Remark 7.5 and also Example 7.6 for the case of group rings and group algebras, where again no computation of maximal orders is necessary.)

§11. Computations with Homomorphisms

The key ingredient for computing the homomorphism ring is Lemma 7.2 (ii), which allows us to reduce the problem to a saturation of $\mathcal{O}$-modules. Recall that for a function $f\colon X \to Y$ and subsets $X' \subseteq X$, $Y' \subseteq Y$ with $f(X') \subseteq Y'$ we denote by $f|_{Y'}^{X'}$ the function $X' \to Y'$ induced by f.

Lemma 11.1. Assume that $\mathcal{O}$ is a principal ideal domain and that $\mathscr{M}$ and $\mathscr{N}$ are $\mathcal{O}$-bases of M and N respectively. Then the following hold:

(i) For $\varphi \in \mathrm{Hom}_K(V, W)$ we have $\varphi(M) \subseteq N$ if and only if $\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\varphi) \in \mathrm{Mat}_{n\times m}(\mathcal{O})$. Moreover in this case we have $\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\varphi) = \mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\varphi|_N^M)$.

(ii) We have $\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_\Lambda(M, N)) = \mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_A(V, W)) \cap \mathrm{Mat}_{n\times m}(\mathcal{O})$.

(iii) Let $(X_i)_{1\le i\le l}$ be a K-basis of $\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_A(V, W))$. Then

$$\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_\Lambda(M, N)) = \langle X_i \mid 1 \le i \le l\rangle_K \cap \mathrm{Mat}_{n\times m}(\mathcal{O}).$$

(iv) Let $(X_i)_{1\le i\le l}$ be a K-basis of $\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_A(V, W))$ such that $X_i \in \mathrm{Mat}_{n\times m}(\mathcal{O})$ for all $1 \le i \le l$. Then $\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_\Lambda(M, N))$ is the saturation of $\langle X_i \mid 1 \le i \le l\rangle_{\mathcal{O}}$ in $\mathrm{Mat}_{n\times m}(\mathcal{O})$, that is,

$$\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_\Lambda(M, N)) = (K\langle X_i \mid 1 \le i \le l\rangle_{\mathcal{O}}) \cap \mathrm{Mat}_{n\times m}(\mathcal{O}).$$

Proof. (i): This is clear. (ii): By Lemma 7.2 we know that $\mathrm{Hom}_\Lambda(M, N) = \{\varphi|_N^M \mid \varphi \in \mathrm{Hom}_A(V, W),\ \varphi(M) \subseteq N\}$. Thus using (i) we get

$$\begin{aligned}\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_\Lambda(M, N)) &= \{\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\varphi|_N^M) \mid \varphi \in \mathrm{Hom}_A(V, W),\ \mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\varphi) \in \mathrm{Mat}_{n\times m}(\mathcal{O})\}\\ &= \mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_A(V, W)) \cap \mathrm{Mat}_{n\times m}(\mathcal{O}).\end{aligned}$$

(iii) and (iv): Follow from (ii). □

As expected, due to the presence of pseudo-bases, the general case is more involved.

Lemma 11.2. Assume that $((\mathfrak{a}_i), \mathscr{M})$ and $((\mathfrak{b}_i), \mathscr{N})$ are pseudo-bases of M and N respectively. We set $\mathrm{E} = \bigoplus_{1\le i\le n, 1\le j\le m} \mathfrak{a}_i^{-1}\mathfrak{b}_j \mathrm{e}_{ij}$. Then the following hold:

(i) For $\varphi \in \mathrm{Hom}_K(V, W)$ we have $\varphi(M) \subseteq N$ if and only if $\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\varphi) \in \mathrm{E}$. Moreover in this case we have $\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\varphi) = \mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\varphi|_N^M)$.

(ii) We have $\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_\Lambda(M, N)) = \mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_A(V, W)) \cap \mathrm{E}$.

(iii) Let $(X_i)_{1\le i\le l}$ be a K-basis of $\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_A(V, W))$. Then

$$\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_\Lambda(M, N)) = \langle X_i \mid 1 \le i \le l\rangle_K \cap \mathrm{E}.$$

(iv) Let $(X_i)_{1\le i\le l}$ be a K-basis of $\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_A(V, W))$ such that $X_i \in \mathrm{E}$ for all $1 \le i \le l$. Then the module $\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_\Lambda(M, N))$ is the saturation of $\langle X_i \mid 1 \le i \le l\rangle_{\mathcal{O}}$ in E, that is,

$$\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_\Lambda(M, N)) = (K\langle X_i \mid 1 \le i \le l\rangle_{\mathcal{O}}) \cap \mathrm{E}.$$

Proof. (i): This follows from the defining properties of a pseudo-basis. (ii), (iii) and (iv): Analogously to Lemma 11.1. □

The lemma translates immediately into an algorithm for computing homomorphism rings.

Algorithm 11.3. Given Λ-lattices M and N with pseudo-bases $((\mathfrak{a}_i), \mathscr{M})$ and $((\mathfrak{b}_i), \mathscr{N})$ respectively, the following procedure returns a pseudo-basis of $\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_\Lambda(M, N))$. Set $\mathrm{E} = \bigoplus_{1\le i\le n, 1\le j\le m} \mathfrak{a}_i\mathfrak{b}_j^{-1}\mathrm{e}_{ij}$.

(1) Compute a K-basis $(X_i)_{1\le i\le l}$ of $\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_A(V, W))$. Scale X_i such that $X_i \in \mathrm{E}$ for all $1 \le i \le l$.

(2) Return a pseudo-basis of the saturation of $\langle X_i \mid 1 \le i \le l\rangle_{\mathcal{O}}$ in E, which can be computed using the pseudo-Smith normal form (see Lemma 1.35).

Example 11.4. We consider the dicyclic group G of order 12, given by the presentation $G = \langle a, b, c \mid a^2b^{-1} = b^2 = c^3 = c^ac^{-2} = 1\rangle$. The group G admits a unique rational character of degree 2 with Schur index 2. Over the quadratic field $K = \mathbf{Q}(\alpha)$, $\alpha^2 + 10 = 0$, this character can be realized via the representation

$$G \longrightarrow \mathrm{GL}_2(K),\ a \longmapsto \begin{pmatrix} -\alpha+1 & \alpha/5 \\ -\alpha+5 & \alpha-1 \end{pmatrix},\ b \longmapsto \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},\ c \longmapsto \begin{pmatrix} -3 & (5-\alpha)/5 \\ -\alpha-5 & 2 \end{pmatrix}.$$

We denote by $V = K^2$ the associated KG-module with canonical basis $\mathscr{M} = (e_1, e_2)$. Furthermore we denote by $\mathcal{O}$ the maximal order $\mathbf{Z}[\alpha]$ of K and by $\mathfrak{p}_2$ and $\mathfrak{p}_5$ the unique prime ideals of $\mathcal{O}$ lying above 2 and 5 respectively. Let us now consider the two $\mathcal{O}G$-lattices M and N of V, spanned by the pseudo-matrices

$$\begin{array}{c} \mathcal{O} \\ \mathfrak{p}_5^{-1} \end{array} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{array}{c} \mathfrak{p}_2 \\ \mathfrak{p}_2\mathfrak{p}_5^{-1} \end{array} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

respectively. Thus M has pseudo-basis $((\mathcal{O}, \mathfrak{p}_5^{-1}), \mathscr{M})$ and N has pseudo-basis $((\mathfrak{p}_2, \mathfrak{p}_2\mathfrak{p}_5^{-1}), \mathscr{M})$. As

$$\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_{\mathcal{O}}(M,N)) = \begin{pmatrix} \mathfrak{p}_2 & \mathfrak{p}_2\mathfrak{p}_5 \\ \mathfrak{p}_2\mathfrak{p}_5^{-1} & \mathfrak{p}_2 \end{pmatrix} \quad \text{and} \quad \mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_{KG}(V,V)) = \langle \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \rangle_K,$$

we conclude that

$$\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_{\mathcal{O}G}(M,N)) = \mathfrak{p}_2 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Note that due to the simple structure of the involved homomorphism modules we could easily read off the saturation and there was no need to involve the pseudo-Smith normal form.

Using Remark 7.5 we also obtain an algorithm to compute $\mathrm{Hom}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p})$ for some nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$.

Algorithm 11.5. Assume that $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}$. Let $((\mathfrak{a}_i), \mathscr{M})$ and $((\mathfrak{b}_i), \mathscr{N})$ be $\mathfrak{p}$-free pseudo-bases of M and N respectively. The following steps return an $\mathcal{O}_\mathfrak{p}$-basis $\mathscr{H} = (h_i)_{1 \le i \le r}$ of $\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}))$ with $h_i \in \mathrm{Mat}_{n \times m}(K)$.

(1) Use Algorithm 11.3 to compute a $\mathfrak{p}$-free pseudo-basis $((\mathfrak{c}_i), \mathscr{H})$ of $\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_\Lambda(M,N))$
(2) Return $\mathscr{H}$.

Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}$ and $l > 0$. We now discuss the computation of

$$\mathrm{Hom}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}) / \mathfrak{p}^l \,\mathrm{Hom}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}),$$

which will be important in the next section. One possibility is to first compute generators for $\mathrm{Hom}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p})$ via saturation and reduction afterwards. We will see that we can change the order of these operations: The reduced homomorphism ring can be obtained by first reducing and then saturating.

Algorithm 11.6 (Computing reductions of $\mathfrak{p}$-adic homomorphism rings). Assume that $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}$ and $l \in \mathbf{Z}_{>0}$. Let $((\mathfrak{a}_i), \mathscr{M})$ and $((\mathfrak{b}_i), \mathscr{N})$ be $\mathfrak{p}$-free pseudo-bases of M and N respectively. The following steps return an $\mathcal{O}/\mathfrak{p}^l$-generating set $\mathscr{H} = (h_i)_{1 \le i \le r}$ with $h_i \in \mathrm{Mat}_{n \times m}(\mathcal{O}/\mathfrak{p}^l)$ of $\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}))/\mathfrak{p}^l\, \mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}))$.

(1) Set $\mathrm{E} = \bigoplus_{1 \le i \le n, 1 \le j \le m} \mathfrak{a}_i^{-1}\mathfrak{b}_j \mathrm{e}_{ij}$.
(2) Compute a K-basis $(X_i)_{1 \le i \le r}$ of $\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_A(V,W))$ such that $X_i \in \mathrm{E}$ $(\subseteq \mathrm{Mat}_{n \times m}(\mathcal{O}_\mathfrak{p}))$ for all $1 \le i \le l$ and set

$$H = \langle X_i \mid 1 \le i \le r \rangle_{\mathcal{O}_\mathfrak{p}} \subseteq \mathrm{Mat}_{n \times m}(\mathcal{O}_\mathfrak{p}).$$

(3) Denote by L the saturation of H in $\mathrm{Mat}_{n \times m}(\mathcal{O}_\mathfrak{p})$. Compute an $\mathcal{O}/\mathfrak{p}^l$-generating set $\mathscr{H}$ of $L/\mathfrak{p}^l L$ using Lemma 1.36.
(4) Return $\mathscr{H}$.

Lemma 11.7. Algorithm 11.6 is correct.

Proof. We apply Lemma 1.36 to the $\mathcal{O}_\mathfrak{p}$-module $H = \langle X_i \mid 1 \le i \le l \rangle_{\mathcal{O}_\mathfrak{p}}$ with basis matrix corresponding to the basis $(X_i)_{1 \le i \le l}$. The saturation L is just $\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}))$ and the reduction can be obtained by a Smith normal form computation over $\mathcal{O}_\mathfrak{p}/\mathfrak{p}^l\mathcal{O}_\mathfrak{p} \cong \mathcal{O}/\mathfrak{p}^l$. □

Example 11.8. Consider the finite group $G = \mathrm{SL}_2(\mathbf{F}_3)$ of order 24, which is generated by $a = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $b = \left(\begin{smallmatrix} 0 & 1 \\ 2 & 1 \end{smallmatrix}\right)$. Let $\zeta \in \mathbf{C}$ be a primitive 3rd root of unity and $K = \mathbf{Q}(\zeta)$ the 3rd cyclotomic field with ring of integers $\mathcal{O} = \mathbf{Z}[\zeta]$. There exists an irreducible 2-dimensional KG-module $V_2 = K^2$, where the action of G is given by

$$a \longmapsto \begin{pmatrix} \zeta & -\zeta - 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad b \longmapsto \begin{pmatrix} \zeta & \zeta + 1 \\ \zeta + 1 & \zeta \end{pmatrix}.$$

Denote by $V_1 = K$ the non-trivial 1-dimensional KG-module with action

$$a \longmapsto \zeta \quad \text{and} \quad b \longmapsto 1.$$

We now consider the reducible KG-module $V = V_1 \oplus V_2$ and the $\mathcal{O}G$-lattices

$$M = \mathcal{O}e_1 \oplus \mathcal{O}e_2 \oplus \mathcal{O}e_3, \quad N = \mathcal{O}e_1 \oplus \mathcal{O}e_2 \oplus \mathcal{O}(1 - \zeta)e_3,$$

where $\mathscr{M} = (e_1, e_2, e_3)$ is the canonical basis of V. Let us set $\alpha = 1 - \zeta$, $e_3' = \alpha e_3$ and $\mathscr{N} = (e_1, e_2, e_3')$. Then the $\mathcal{O}G$-modules M and N are $\mathcal{O}$-free with bases $\mathscr{M}$ and $\mathscr{N}$. The endomorphism ring $\mathrm{End}_{KG}(V)$ is of K-dimension 2 and a basis of $\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{End}_{KG}(V))$ is given for example by the matrices

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \; B = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \alpha \end{pmatrix} \in \mathrm{Mat}_{3\times 3}(K).$$

We now consider the prime ideal $\mathfrak{p} = (3, 1-\zeta)$ of norm 3 and for $l \in \mathbf{Z}_{\geq 2}$ we want to compute

$$\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_{\mathcal{O}_\mathfrak{p} G}(M_\mathfrak{p}, N_\mathfrak{p}))/\mathfrak{p}^l \,\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_{\mathcal{O}_\mathfrak{p} G}(M_\mathfrak{p}, N_\mathfrak{p}))$$

using only A and B. To compute this reduced homomorphism ring we have to compute the Smith normal form of the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha \end{pmatrix}$$

modulo $\mathfrak{p}^l \mathcal{O}_\mathfrak{p} = (\alpha^l)$. As

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\equiv \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \bmod (\alpha^l)$$

we conclude that the rows of

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

form a generating set of the saturation modulo (α^l) and therefore

$$\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_{\mathcal{O}_\mathfrak{p} G}(M_\mathfrak{p}, N_\mathfrak{p}))/\mathfrak{p}^l \,\mathrm{M}_{\mathscr{N}}^{\mathscr{M}}(\mathrm{Hom}_{\mathcal{O}_\mathfrak{p} G}(M_\mathfrak{p}, N_\mathfrak{p})) = \langle \overline{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}}, \overline{\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}} \rangle_{\mathcal{O}/\mathfrak{p}^l}.$$

We now turn to the final problem related to the computation of homomorphism rings. More precisely for a nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$ and an integer $l \in \mathbf{Z}_{>0}$ we want to describe the computation of (a generating set of)

$$\mathrm{Hom}_{\Lambda/\mathfrak{p}^l\Lambda}(M/\mathfrak{p}^l M, N/\mathfrak{p}^l N) \cong \mathrm{Hom}_{\Lambda_\mathfrak{p}/\mathfrak{p}^l\Lambda_\mathfrak{p}}(M_\mathfrak{p}/\mathfrak{p}^l M_\mathfrak{p}, N_\mathfrak{p}/\mathfrak{p}^l N_\mathfrak{p}).$$

After fixing $(\mathcal{O}/\mathfrak{p}^k)$-bases of $M_k = M/\mathfrak{p}^k M$ and $N_k = N/\mathfrak{p}^k N$, the action of Λ is given by

$$\rho_M \colon \Lambda \longrightarrow \mathrm{Aut}_{\mathcal{O}/\mathfrak{p}^k}(M_k) \cong \mathrm{GL}_n(\mathcal{O}/\mathfrak{p}^k) \quad \text{and} \quad \rho_N \colon \Lambda \longrightarrow \mathrm{Aut}_{\mathcal{O}/\mathfrak{p}^k}(N_k) \cong \mathrm{GL}_n(\mathcal{O}/\mathfrak{p}^k)$$

respectively. Moreover the homomorphism space $\mathrm{Hom}_{\Lambda/\mathfrak{p}^k\Lambda}(M/\mathfrak{p}^k M, N/\mathfrak{p}^k N)$ is isomorphic to

$$\{X \in \mathrm{Mat}_{n\times n}(\mathcal{O}/\mathfrak{p}^k) \mid \text{for all } g \in \mathcal{G} \text{ we have } \rho_M(g)X = X\rho_N(g)\},$$

as Λ_k-modules, where $\mathcal{G} \subseteq \Lambda$ is an $\mathcal{O}$-generating set of Λ. By introducing n^2 many indeterminates, it is easy to see that there exists a matrix $\mathbf{M} \in \mathrm{Mat}_{n^2 \times \#\mathcal{G}}(\mathcal{O}/\mathfrak{p}^k)$ such that

$$\ker(\mathbf{M}) \cong \mathrm{Hom}_{\Lambda/\mathfrak{p}^k\Lambda}(M/\mathfrak{p}^k M, N/\mathfrak{p}^k N).$$

Thus the problem of finding an $(\mathcal{O}/\mathfrak{p}^k)$-generating set of $\mathrm{Hom}_{\Lambda/\mathfrak{p}^k\Lambda}(M/\mathfrak{p}^k M, N/\mathfrak{p}^k N)$ is reduced to computing the kernel of a matrix over $(\mathcal{O}/\mathfrak{p}^k)$. As $(\mathcal{O}/\mathfrak{p}^k)$ is an Euclidean ring, this can be done using the Howell normal form.

Example 11.9. We consider the quaternion group $G = Q_8$ of order 8 with presentation $\langle x, y, z \mid x^2 = z, y^2 = z, x^{-1}yx = yz \rangle$ and the absolutely irreducible representation

$$\rho\colon G \longrightarrow \mathrm{GL}_2(\mathbf{Q}(i)), \quad x \longmapsto \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \quad z \longmapsto \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix},$$

over the imaginary quadratic field $K = \mathbf{Q}(i)$, where $i^2 + 1 = 0$. In the ring of integers $\mathcal{O} = \mathbf{Z}[i]$ of $\mathbf{Q}(i)$ we have the decomposition $(2) = \mathfrak{p}^2$ with $\mathfrak{p} = (1 - i)$ the prime ideal of norm 2. We denote by $e_1, e_2 \in \mathbf{Q}(i)^2$ the canonical basis and consider the two $\mathcal{O}G$-lattices $M = \mathcal{O}e_1 \oplus \mathcal{O}e_2$ and $N = \mathcal{O}e_1 \oplus \mathfrak{p}(e_1 + e_2)$. Our aim is to determine $\mathrm{Hom}_{(\mathcal{O}/\mathfrak{p}^7\mathcal{O})G}(M/\mathfrak{p}^7M, N/\mathfrak{p}^7N)$. For the sake of readability, in the following discussion we will omit $\bar{}$ when denoting elements of $\mathcal{O}/\mathfrak{p}^7$. Since $\mathcal{O}/\mathfrak{p}^7$ is the only ring we are dealing with, no confusion will arise. Reducing M and N modulo $\mathfrak{p}^7$, we obtain the two representations

$$\begin{aligned} \rho_M\colon G &\longrightarrow \mathrm{GL}_2(\mathcal{O}/\mathfrak{p}^7), x \longmapsto \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, z \longmapsto \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, \\ \rho_N\colon G &\longrightarrow \mathrm{GL}_2(\mathcal{O}/\mathfrak{p}^7), x \longmapsto \begin{pmatrix} -i & 0 \\ -1-i & i \end{pmatrix}, z \longmapsto \begin{pmatrix} i & 1-i \\ 0 & -i \end{pmatrix}. \end{aligned}$$

Since

$$\mathrm{Hom}_{(\mathcal{O}/\mathfrak{p}^7\mathcal{O})G}(M/\mathfrak{p}^7M, N/\mathfrak{p}^7N) = \{X \in \mathrm{Mat}_{2\times 2}(\mathcal{O}/\mathfrak{p}^7) \mid \rho_M(x)X = X\rho_N(x) \text{ and } \rho_M(z)X = X\rho_N(z)\},$$

we see that $X = \left(\begin{smallmatrix} X_1 & X_2 \\ X_3 & X_4 \end{smallmatrix}\right) \in \mathrm{Mat}_{2\times 2}(\mathcal{O}/\mathfrak{p}^7)$ is an $(\mathcal{O}/\mathfrak{p}^7)G$-morphism if and only if

$$\begin{pmatrix} -iX_1 & -iX_2 \\ iX_3 & iX_4 \end{pmatrix} = \begin{pmatrix} -iX_3{-}1 - iX_2 & iX_2 \\ -iX_3{-}1 - iX_4 & iX_4 \end{pmatrix} \text{ and } \begin{pmatrix} -iX_3 & -iX_4 \\ -iX_1 & -iX_2 \end{pmatrix} = \begin{pmatrix} iX_1 & 1 - iX_1{-}iX_2 \\ iX_3 & 1 - iX_3{-}iX_4 \end{pmatrix},$$

which is equivalent to $(X_1\, X_2\, X_3\, X_4) \in \ker(A)$, where $A \in \mathrm{Mat}_{4\times 8}(\mathcal{O}/\mathfrak{p}^7)$ is given by

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & -i & -1+i & -i & 0 \\ 1+i & -2i & 0 & 0 & 0 & i & 0 & -i \\ 0 & 0 & 2i & 0 & -i & 0 & -i & -1+i \\ 0 & 0 & 1+i & 0 & 0 & -i & 0 & i \end{pmatrix}.$$

Using the normal form techniques, we can find the following generating set for $\ker(A)$:

$$\langle (1\ 0\ {-1}\ 1+i), (0\ 8\ 0\ 8) \rangle_{\mathcal{O}/\mathfrak{p}^7} = \ker(A)$$

which in turn implies

$$\mathrm{Hom}_{(\mathcal{O}/\mathfrak{p}^7)G}(M/\mathfrak{p}^7M, N/\mathfrak{p}^7N) = \langle \begin{pmatrix} 1 & 0 \\ -1 & 1+i \end{pmatrix}, \begin{pmatrix} 0 & 8 \\ 0 & 8 \end{pmatrix} \rangle_{\mathcal{O}/\mathfrak{p}^7}.$$

§12. Testing for $\mathfrak{p}$-equivalence

Assumption. For the rest of this section, let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}$.

Recall that M and N are $\mathfrak{p}$-equivalent (written $M \sim_{\mathfrak{p}} N$) if and only if $M_{\mathfrak{p}}$ and $N_{\mathfrak{p}}$ are isomorphic $\Lambda_{\mathfrak{p}}$-lattices. In terms of the homomorphism rings this is equivalent to $\mathrm{Hom}_{\Lambda_{\mathfrak{p}}}(M_{\mathfrak{p}}, N_{\mathfrak{p}})$ containing an invertible element. While this theoretically sounds easy, testing whether this free $\mathcal{O}_{\mathfrak{p}}$-module contains an invertible element in practice is not obvious at all. Fortunately we are in the local case, where we have full control over the unit group $\mathcal{O}_{\mathfrak{p}}^{\times}$. In addition, $M_{\mathfrak{p}}$ and $N_{\mathfrak{p}}$ are—$\mathcal{O}_{\mathfrak{p}}$ being a principal ideal domain—$\mathcal{O}_{\mathfrak{p}}$-free, allowing us to involve the determinant $\det\colon \mathrm{Hom}_{\mathcal{O}_{\mathfrak{p}}}(M_{\mathfrak{p}}, N_{\mathfrak{p}}) \longrightarrow \mathcal{O}_{\mathfrak{p}}$. Both facts will allow us to formulate $\mathfrak{p}$-equivalence tests.

Lemma 12.1. The following hold:

(i) The lattices M and N are $\mathfrak{p}$-equivalent if and only if there exists $\varphi \in \mathrm{Hom}_{\Lambda_{\mathfrak{p}}}(M_{\mathfrak{p}}, N_{\mathfrak{p}})$ such that $\det(\varphi) \not\equiv 0 \bmod \mathfrak{p}\mathcal{O}_{\mathfrak{p}}$.

(ii) Let $\varphi_1, \dots, \varphi_s \in \mathrm{Hom}_{\Lambda/\mathfrak{p}\Lambda}(M/\mathfrak{p}M, N/\mathfrak{p}N)$ be morphisms such that $(\varphi_1, \dots, \varphi_s)$ is a $k_{\mathfrak{p}}$-generating set of $\mathrm{Hom}_{\Lambda_{\mathfrak{p}}}(M_{\mathfrak{p}}, N_{\mathfrak{p}})/\mathfrak{p}\,\mathrm{Hom}_{\Lambda_{\mathfrak{p}}}(M_{\mathfrak{p}}, N_{\mathfrak{p}})$. Then M and N are $\mathfrak{p}$-equivalent if and only if there exists $(a_1, \dots, a_s) \in k_{\mathfrak{p}}^s$ such that $\det(a_1\varphi_1 + \dots + a_s\varphi_s) \neq 0$.

Proof. (i): An element φ of $\operatorname{Hom}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p})$ is invertible if and only if $\det(\varphi) \in \mathcal{O}_\mathfrak{p}^\times$. The claim follows from $\mathcal{O}_\mathfrak{p}^\times = \mathcal{O} \backslash \mathfrak{p}\mathcal{O}_\mathfrak{p}$. (ii): As

$$\begin{tikzcd}
\operatorname{Hom}_{\mathcal{O}_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}) \arrow[r, "\det"] \arrow[d, "\otimes \mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p}"] & \mathcal{O}_\mathfrak{p} \arrow[d] \\
\operatorname{Hom}_{k_\mathfrak{p}}(M/\mathfrak{p}M, N/\mathfrak{p}N) \arrow[r, "\det"] & k_\mathfrak{p}
\end{tikzcd}$$

commutes, the result follows from (i). □

§12A. Deterministic $\mathfrak{p}$-equivalence test

Algorithm 12.2 (Deterministic $\mathfrak{p}$-equivalence test I). Given two Λ-lattices M and N in $\mathcal{L}(V)$ the following procedure decides whether M and N are $\mathfrak{p}$-equivalent.

(1) Use Algorithm 11.6 with $l = 1$ to obtain $\varphi_1, \ldots, \varphi_s \in \operatorname{Hom}_{k_\mathfrak{p}}(M/\mathfrak{p}M, N/\mathfrak{p}N)$ such that $\varphi_1, \ldots, \varphi_s$ is a $k_\mathfrak{p}$-generating system of $\operatorname{Hom}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p})/\mathfrak{p} \operatorname{Hom}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p})$.
(2) For all tuples $(a_1, \ldots, a_s) \in k_\mathfrak{p}^s$ test whether $\det(a_1\varphi_1 + \cdots + a_s\varphi_s) = 0$. If this is the case, return false. Else return true.

Example 12.3. We pick up on Example 11.8. We now want to test whether M and N are $\mathfrak{p}$-equivalent. We have already seen that the matrices

$$X_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad X_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \operatorname{Mat}_{3\times 3}(k_\mathfrak{p})$$

form a $k_\mathfrak{p}$-generating set of $\operatorname{Hom}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p})/\mathfrak{p} \operatorname{Hom}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p})$. (We proved this result for $\operatorname{Hom}_\Lambda(M_\mathfrak{p}, N_\mathfrak{p})$ modulo $\mathfrak{p}^l \operatorname{Hom}_\lambda(M_\mathfrak{p}, N_\mathfrak{p})$ for $l > 1$. But then the same holds for $l = 1$ by projecting down). As $\det(X_1 + X_2) = 1 \neq 0$ we conclude that M and N are $\mathfrak{p}$-equivalent.

A second deterministic $\mathfrak{p}$-equivalence test can be read off from the following theorem. This statement is originally due to Maranda [Mar53], was independently discovered by Takahashi [Tak59] and generalized by Higman in [Hig60]. Recall that $\mathfrak{h}$ denotes an integral ideal of $\mathcal{O}$ such that $\mathfrak{h} \cdot \operatorname{Ext}^1_\Lambda(M', N') = 0$ for all Λ-lattices M' and N'.

Theorem 12.4. The following hold:

(i) Let $l \geq v_\mathfrak{p}(\mathfrak{h}) + 1$ and assume that $\varphi\colon M/\mathfrak{p}^l M \to N/\mathfrak{p}^l N$ is an isomorphism of $\Lambda/\mathfrak{p}^l\Lambda$-modules. Then there exists an $\Lambda_\mathfrak{p}$-isomorphism $\psi\colon M_\mathfrak{p} \to N_\mathfrak{p}$ such that $\overline{\varphi} = \overline{\psi}$. Here by abuse of notation $\overline{}$ denotes the canonical map $\operatorname{Hom}_{\Lambda/\mathfrak{p}^l\Lambda}(M/\mathfrak{p}^l M, N/\mathfrak{p}^l N) \to \operatorname{Hom}_{\Lambda/\mathfrak{p}\Lambda}(M/\mathfrak{p}M, N/\mathfrak{p}N)$ as well as the canonical map $\operatorname{Hom}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}) \to \operatorname{Hom}_{\Lambda/\mathfrak{p}\Lambda}(M/\mathfrak{p}M, N/\mathfrak{p}N)$.
(ii) The modules $M_\mathfrak{p}$ and $N_\mathfrak{p}$ are isomorphic $\Lambda_\mathfrak{p}$-lattices if and only if $M/\mathfrak{p}^k M$ and $N/\mathfrak{p}^k N$ are isomorphic $\Lambda/\mathfrak{p}^k\Lambda$-modules for some $k \geq v_\mathfrak{p}(\mathfrak{h}) + 1$.

Proof. This is [Hig60, Theorem 3], see also [CR81, (30.14) Theorem] for a more modern treatment. □

Algorithm 12.5 (Deterministic $\mathfrak{p}$-equivalence test II). Given two Λ-lattices M and N in $\mathcal{L}(V)$ the following procedure decides whether M and N are $\mathfrak{p}$-equivalent.

(1) Set $k = v_\mathfrak{p}(\mathfrak{h}) + 1$.
(2) Compute morphisms $\varphi_1, \ldots, \varphi_s \in \operatorname{Hom}_{\mathcal{O}/\mathfrak{p}^k}(M/\mathfrak{p}^k M, N/\mathfrak{p}^k N)$ such that $\varphi_1, \ldots, \varphi_s$ is an $\mathcal{O}/\mathfrak{p}^k$ generating set of $\operatorname{Hom}_{\Lambda/\mathfrak{p}^k\Lambda}(M/\mathfrak{p}^k M, N/\mathfrak{p}^k N)$.
(3) Reduce each φ_i to a $k_\mathfrak{p}$-morphism $\psi_i \in \operatorname{Hom}_{k_\mathfrak{p}}(M/\mathfrak{p}M, N/\mathfrak{p}N)$.
(4) For all tuples $(a_1, \ldots, a_s) \in k_\mathfrak{p}^s$ test whether $\det(a_1\psi_1 + \cdots + a_s\psi_s) = 0$. If this is the case, return false. Else return true.

Example 12.6. We consider again the two $\mathcal{O}G$-modules of Example 11.9. Since $\mathfrak{p} = (1 - i)$ is ramified and $\mathfrak{h} = \#G = (2^3)$ we take $k = 6 + 1 = 7$. We fortunately know already that

$$\operatorname{Hom}_{(\mathcal{O}/\mathfrak{p}^7)G}(M/\mathfrak{p}^7 M, N/\mathfrak{p}^7 N) = \langle \begin{pmatrix} 1 & 0 \\ -1 & 1+i \end{pmatrix}, \begin{pmatrix} 0 & 8 \\ 0 & 8 \end{pmatrix} \rangle_{\mathcal{O}/\mathfrak{p}^7}.$$

Reducing both matrices modulo $\mathfrak{p}$ we get $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in \operatorname{Mat}_{2\times 2}(\mathbf{F}_2)$. Since no $\mathbf{F}_2$-linear combination of these matrices results in an invertible matrix, we conclude that M and N are not $\mathfrak{p}$-equivalent.

Remark 12.7. In Examples 12.3 and 12.6 we were really lucky since eventually we could just read off whether or not there exists some invertible linear combination. If M and N are not $\mathfrak{p}$-equivalent, that is, if $M_\mathfrak{p}$ and $N_\mathfrak{p}$ are not isomorphic as $\Lambda_\mathfrak{p}$-modules, and the number s of nonzero generators in Algorithm 12.2 and Algorithm 12.5 respectively is greater than 1, then Step 2 and 4 respectively require $\mathbf{N}(\mathfrak{p})^s$ many determinant computations over the residue field $k_\mathfrak{p}$. Thus an increasing field degree or an increasing number of generators will tremendously slow down the algorithm. On the other hand, if $\mathrm{Hom}_A(V, W)$ has dimension 1, then one needs only one determinant computation.

§12B. Probabilistic $\mathfrak{p}$-equivalence test

As already remarked in the last section, if the number s of generators of the reduced homomorphism ring (or of the homomorphism ring of the reduced modules) or the cardinality of the residue field gets large, the number of determinant computations will get very large. By introducing probabilistic techniques we will see how Algorithms 12.2, 12.5 can be modified to allow much larger parameters.

Assume that the morphisms $\varphi_1, \dots, \varphi_s \in \mathrm{Hom}_{k_\mathfrak{p}}(M/\mathfrak{p}M, N/\mathfrak{p}N)$ have the property that M and N are $\mathfrak{p}$-equivalent if and only if there exists $(a_1, \dots, a_s) \in k_\mathfrak{p}^s$ such that $\det(a_1\varphi_1 + \cdots + a_s\varphi_s) \neq 0$. Instead of computing all determinants we consider the polynomial

$$f = \det(X_1\varphi_1 + \cdots + X_s\varphi_s) \in k_\mathfrak{p}[X_1, \dots, X_s],$$

which is of total degree at most n. Then we know that M and N are $\mathfrak{p}$-equivalent if and only if f is not identitcally zero on $k_\mathfrak{p}^s$. Thus we have condensed all the information we have into a single polynomial f whose structure—being zero or not—answers whether the two lattices are $\mathfrak{p}$-equivalent. It is tempting to just compute this polynomial using classical methods. The following example shows that this is not a good idea.

Example 12.8. We consider the K-space $V = K^n$, which is viewed as an A-module with trivial action. For all Λ-lattices M and N of V the $\Lambda_\mathfrak{p}$-module $\mathrm{Hom}_{\Lambda_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p})$ is isomorphic to the full matrix algebra $\mathrm{Mat}_{n\times n}(\mathcal{O}_\mathfrak{p})$ and therefore

$$f = \det((X_{ij})_{1\leq i,j\leq n}) \in k_\mathfrak{p}[X_{ij} | 1 \leq i, j \leq n].$$

Using the Leibniz formula for determinants we conclude that f is the sum of $n! \sim n^n$ distinct monomials, which is an object we cannot compute efficiently for large n.

While we cannot compute the coefficients of f directly, it is no problem for us to evaluate f at points in $k_\mathfrak{p}^s$ (this is just one determinant computation of a matrix over a finite field). The natural question is therefor: Can we decide whether f is the zero-polynomial by just evaluating it at some (small number of) points? Fortunately this is exactly the topic of polynomial identity testing in complexity theory (see [Sax09]) and as a matter of fact there exist efficient probabilistic algorithms based on the following theorem (see [Sch80, Zip79]). In the following we use the notation pr to denote the probability measure of the appropriate (finite) probability space.

Theorem 12.9 (Schwartz–Zippel–Lemma). Let $\mathbf{F}$ be a finite field and $g \in \mathbf{F}[X_1, \dots, X_s]$ a nonzero polynomial of total degree $d < \#\mathbf{F}$. Then

$$\mathrm{pr}(\{(a_1, \dots, a_s) \in \mathbf{F}^s \mid g(a_1, \dots, a_s) = 0\}) \leq \frac{d}{\#\mathbf{F}}.$$

In particular if $f \in \mathbf{F}[X_1, \dots, X_s]$ is a polynomial of total degree $d < \#\mathbf{F}$, then the following hold: If $\mathbf{v}_1, \dots, \mathbf{v}_l \in \mathbf{F}^s$ are chosen random independently and uniformly and $f(\mathbf{v}_i) = 0$ for $1 \leq i \leq l$, then the probability that f is nonzero is at most $(d/\#\mathbf{F})^l$.

Since $f = 0$ over $\mathbf{F}$ is equivalent to $f = 0$ over $\mathbf{F}'$ for every extension $\mathbf{F}'$ of $\mathbf{F}$, the condition on the total degree is not really a restriction. If necessary we just have to extend scalars. We can now formulate a Monte Carlo version of Algorithm 12.2.

Algorithm 12.10. Let M and N be Λ-lattices of $\mathcal{L}(V)$, $\mathfrak{p}$ a prime ideal of $\mathcal{O}$ and $\varepsilon \in]0, 1[$. The following procedure is a true-biased Monte Carlo algorithm for deciding whether M and N are $\mathfrak{p}$-equivalent and if it terminates with false, then the probability that the output is false is less than ε.

(1) Use one of the techniques from Section 11 to find morphisms $\varphi_1, \dots, \varphi_s \in \mathrm{Hom}_{k_\mathfrak{p}}(M/\mathfrak{p}M, N/\mathfrak{p}N)$ such that $M \sim_\mathfrak{p} N$ if and only if there exists $(a_1, \dots, a_s) \in k_\mathfrak{p}^s$ such that $\det(a_1\varphi_1 + \cdots + a_s\varphi_s) \neq 0$. Define $f = \det(X_1\varphi_1 + \cdots + X_s\varphi_s) \in k_\mathfrak{p}[X_1, \dots, X_s]$.

(2) Choose $l, m \in \mathbf{Z}_{>0}$ such that $\mathbf{N}(\mathfrak{p})^l > n$ and $(n/\mathbf{N}(\mathfrak{p})^l)^m < \varepsilon$.
(3) Let $\mathbf{F}$ be the degree l extension of $k_{\mathfrak{p}}$. Choose $\mathbf{v}_1, \dots, \mathbf{v}_m \in \mathbf{F}^s$ uniformly distributed.
(4) If $f(\mathbf{v}_i) \neq 0$ for some $1 \leq i \leq m$, then return true. If this is not the case return false.

Proposition 12.11. Algorithm 12.10 is correct.

Proof. This is evident from the preceding discussion. Note that the Schwartz–Zippel–Lemma can be applied since $\#\mathbf{F} = \mathbf{N}(\mathfrak{p})^l > n \geq \deg(f)$. □

§13. Genera computation

While the $\mathfrak{p}$-equivalence tests are interesting in their own right, we now turn to the main application: computing the different genera of Λ-lattices in a given finite dimensional A-module V. This will be done for each relevant prime ideal $\mathfrak{p}$ separately and then put together. Before describing the technique, we make a general remark on the location of representatives of equivalence classes for equivalence relations on $\mathcal{L}(V)$. For a Λ-lattice M of $\mathcal{L}(V)$ let us denote by $\mathcal{L}(M)$ the Λ-sublattices of M contained in $\mathcal{L}(V)$.

Lemma 13.1. Let $\sim$ be an equivalence relation on $\mathcal{L}(V)$ which is weaker than Λ-isomorphism, that is, for isomorphic Λ-lattices $M, N \in \mathcal{L}(V)$ we have $M \sim N$. Then

$$(\mathcal{L}(M)/{\sim}) \longrightarrow (\mathcal{L}(V)/{\sim}),\ [M] \longmapsto [M]$$

is a bijection. In particular for $\sim \in \{\sim_{\mathfrak{p}}, \vee\}$ any set of representatives of $\mathcal{L}(M)/{\sim}$ is a set of representatives for $\mathcal{L}(V)/{\sim}$.

Proof. Given a Λ-lattice N we can find $\alpha \in K$ such that $\alpha N \subseteq M$. Since αN and N are isomorphic Λ-lattices, the result follows. □

This lemma justifies that in the following we can restrict our search for the different genera or $\mathfrak{p}$-equivalence classes to the sublattices of a fixed Λ-lattice M of $\mathcal{L}(V)$.

Computing $\mathfrak{p}$-maximal sublattices. Using Lemma 8.4 it is easy to describe an algorithm for computing the $\mathfrak{p}$-maximal sublattices of M.

Algorithm 13.2 ($\mathfrak{p}$-maximal sublattice computation). Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}$. The following steps return the set of $\mathfrak{p}$-maximal sublattices of M.
(1) Compute a set $\mathcal{C}$ of composition factors of the $\Lambda/\mathfrak{p}\Lambda$-module $M/\mathfrak{p}M$.
(2) Return the preimages of all kernels of nonzero elements of $\operatorname{Hom}_{\Lambda/\mathfrak{p}\Lambda}(M/\mathfrak{p}M, C)$ under the projection $M \to M/\mathfrak{p}M$, where C runs through the elements of $\mathcal{C}$.

Remark 13.3. The computation of the composition factors and the homomorphism rings can both be done using the Meataxe algorithm. The Meataxe was initially described and used by Parker in [Par84] as a tool for modular representation theory of finite groups. It was later improved by Holt and Rees in [HR94], see also [HEO05, Chapter 7] and [Ste12].

For a fixed nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$ we now turn to the computation of the $\mathcal{L}(M)/{\sim_{\mathfrak{p}}}$. By this we mean the computation of a subset $\mathcal{S} = \{M_1, \dots, M_r\}$ of $\mathcal{L}(M)$ such that no two elements of $\mathcal{S}$ are $\mathfrak{p}$-equivalent and every element of $\mathcal{L}(M)$ is $\mathfrak{p}$-equivalent to an element of $\mathcal{S}$. The basic idea is that given a $\mathfrak{p}$-equivalence class in $\mathcal{L}(V)$ there exists a representative N in this class such that the composition series of M/N is of special type. One important tool will be the transition

$$\mathcal{L}(V) \longrightarrow \mathcal{L}(V_{\mathfrak{p}}),\ M \longmapsto M_{\mathfrak{p}},$$

between Λ-lattices of V and $\Lambda_{\mathfrak{p}}$-lattices of $V_{\mathfrak{p}}$.

Lemma 13.4. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}$. The map

$$\begin{aligned}\{N \in \mathcal{L}(M) \mid N\ \mathfrak{p}\text{-maximal}\}/{\sim_{\mathfrak{p}}} &\longrightarrow \{\hat{N} \in \mathcal{L}(M_{\mathfrak{p}}) \mid \hat{N} \text{ maximal }\}/{\cong}\\ [N] &\longmapsto [N_{\mathfrak{p}}]\end{aligned}$$

is a bijection.

Proof. First note that this map is well-defined. For if $N \subsetneq M$ is a $\mathfrak{p}$-maximal Λ-lattice, then M/N is a simple $\Lambda/\mathfrak{p}\Lambda$-module. Since M/N is isomorphic to $M_\mathfrak{p}/N_\mathfrak{p}$, the $\Lambda_\mathfrak{p}$-lattice $N_\mathfrak{p}$ is a maximal sublattice of $M_\mathfrak{p}$.

By definition of $\sim_\mathfrak{p}$ the map is injective. Thus it remains to show surjectivity. Let $\hat{N} \subsetneq M_\mathfrak{p}$ be a maximal sublattice. Now apply Corollary 6.12 to construct a Λ-lattice $N \subseteq M$ with $N_\mathfrak{p} = \hat{N}$ and $N_\mathfrak{q} = M_\mathfrak{q}$ for all primes $\mathfrak{q} \neq \mathfrak{p}$. Since the index $(M : N)$ is a $\mathfrak{p}$-power, it remains to show that N is a maximal sublattice of M. Let L be Λ-lattice of V with $N \subseteq L \subseteq M$. Then $L_\mathfrak{q} = N_\mathfrak{q} = M_\mathfrak{q}$ for all prime ideals $\mathfrak{q} \neq \mathfrak{p}$ and by the maximality of $N_\mathfrak{p}$ in $M_\mathfrak{p}$ we either have $L_\mathfrak{p} = N_\mathfrak{p}$ or $L_\mathfrak{p} = M_\mathfrak{p}$. As

$$L' = \bigcap_{\mathfrak{p}} (V \cap L'_\mathfrak{p})$$

for any $\mathcal{O}$-module L' of V it follows that $L = N$ or $L = M$. □

Lemma 13.5. Let M and N be Λ-lattices of V. If M and N are $\mathfrak{p}$-equivalent, then the $\mathfrak{p}$-equivalence classes of the $\mathfrak{p}$-maximal sublattices of M and N coincide.

Proof. This follows immediately from Lemma 13.4 □

Proposition 13.6. Let N be a lattice in $\mathcal{L}(M)$. Then there exist $N_1, \dots, N_j \in \mathcal{L}(M)$ such that N is $\mathfrak{p}$-equivalent to N_j, $N_1 = M$ and $N_i \subseteq N_{i-1}$ is $\mathfrak{p}$-maximal for $i = 2, \dots, j$.

Proof. Consider the situation $N_\mathfrak{p} \subseteq M_\mathfrak{p}$ over $\Lambda_\mathfrak{p}$. By lifting a composition series of $M_\mathfrak{p}/N_\mathfrak{p}$ we obtain $\Lambda_\mathfrak{p}$-modules $N_1^{(\mathfrak{p})}, \dots, N_j^{(\mathfrak{p})}$ with $M_\mathfrak{p} = N_1^{(\mathfrak{p})}$, $N_\mathfrak{p} = N_j^{(\mathfrak{p})}$ such that $N_i^{(\mathfrak{p})} \subseteq N_{i-1}^{(\mathfrak{p})}$ is maximal for $i = 2, \dots, j$. For each $i = 1, \dots, j$ we apply Corollary 6.12 to the module M and the $\Lambda_\mathfrak{p}$-lattice $N_i^{(\mathfrak{p})}$ to obtain a Λ-lattice N_i of V satisfying $(N_i)_\mathfrak{p} = N_i^{(\mathfrak{p})}$ and $(N_i)_\mathfrak{q} = M_\mathfrak{q}$ for all prime ideals $\mathfrak{q} \neq \mathfrak{p}$. The $\mathfrak{p}$-maximality follows as in the proof of Lemma 13.4. □

We can now formulate the algorithm for computing $\mathcal{L}(M)/{\sim_\mathfrak{p}}$. The basic idea of repeatedly adding sublattices until no new class is found, is due to Plesken [Ple74].

Algorithm 13.7 (Computation of $\mathfrak{p}$-equivalence classes). Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}$. The following algorithm returns a set $\mathcal{M}$ of representatives for the $\mathfrak{p}$-equivalence classes in $\mathcal{L}(M)$.

```
(1) Set $\mathcal{M} = \mathcal{N} = \{M\}$.
(2) While $\mathcal{N} \neq \emptyset$ repeat the following steps:
    (3) Use Algorithm 13.2 to compute $\mathcal{T} = \bigcup_{N \in \mathcal{N}} \{L \mid L \subseteq N$ a $\mathfrak{p}$-maximal $\Lambda$-sublattice of $N\}$.
    (4) Use Algorithm 12.5 to remove elements of $\mathcal{T}$ in such a way that no two elements of $\mathcal{T}$ are $\mathfrak{p}$-equivalent
        and no element of $\mathcal{T}$ is $\mathfrak{p}$-equivalent to some lattice in $\mathcal{M}$.
    (5) Set $\mathcal{N} = \mathcal{T}$ and $\mathcal{M} = \mathcal{M} \cup \mathcal{T}$.
(6) Return $\mathcal{M}$.
```

Theorem 13.8. Algorithm 13.7 terminates and is correct. Moreover the output $\mathcal{M}$ satisfies the following property. For each lattice $N \in \mathcal{M}$ and every prime ideal $\mathfrak{q} \neq \mathfrak{p}$ we have $M \sim_\mathfrak{q} N$.

Proof. The termination is a consequence of the theorem of Jordan–Zassenhaus (see [Rei03, (26.4) Theorem]). Let us turn to the correctness. We temporarily say that a Λ-lattice $N \in \mathcal{L}(M)$ appears in the j-th layer of M, if there exists modules $N_1, \dots, N_j \in \mathcal{L}(M)$ such that $N_1 = M$, $N_j = N$ and $N_i \subseteq N_{i-1}$ is $\mathfrak{p}$-maximal for $i = 2, \dots, j$. Note that by Proposition 13.6 any element of $\mathcal{L}(M)$ appears in the j-th layer of M for some j. For $j \in \mathbf{Z}_{>0}$ let $\mathcal{M}_j$ be $\mathcal{M}$ of Algorithm 13.7 before the j-th execution of the while loop (e.g. $\mathcal{M} = \mathcal{M}_1$). We will show, by induction on j, that any N appearing in the j-th layer of M is $\mathfrak{p}$-equivalent to an element in $\mathcal{M}_j$. The case $j = 1$ being trivial, we now assume that the statement holds for j. Let N occur in the $(j+1)$-th layer of M, say $N \sim_\mathfrak{p} N_{j+1} \subseteq \cdots \subseteq N_1 = M$. Thus N_j appears in the j-th layer of M and there exists $L \in \mathcal{M}_j$ such that $N_j \sim_\mathfrak{p} L$. By Lemma 13.5 we conclude that N_{j+1}—and therefore also N—is $\mathfrak{p}$-equivalent to a $\mathfrak{p}$-maximal sublattice L' of L. Now by construction a Λ-lattice which is $\mathfrak{p}$-equivalent to L' is contained in $\mathcal{M}_{j+1}$, finishing the proof. □

Remark 13.9. In Step 2 of Algorithm 13.7 we use the deterministic $\mathfrak{p}$-equivalence test developed in the previous section. One might ask what happens if we instead use the probabilistic version Algorithm 12.10 for all $\mathfrak{p}$-equivalence tests, which is of magnitudes faster then the deterministic one. It may happen that then

Algorithm 13.7 will not terminate, due to the fact that it always finds new lattices in each execution of the while loop. By choosing the initial value for ε small enough, in practice such an infinite loop can be avoided. So assume that Algorithm 13.7—using the probabilistic $\mathfrak{p}$-equivalence test—finishes and returns a set $\mathcal{M}$. Then $\mathcal{M}$ will always contain a set of representatives for the $\mathfrak{p}$-equivalence class of elements of $\mathcal{L}(V)$ but by the nature of the probabilistic test it may happen that the result is not correct in the sense that two elements of $\mathcal{M}$ are $\mathfrak{p}$-equivalent and we did not notice. At this point we don't know that probability such that our result is not correct. To get the correct result with a bounded error probability we can proceed as follows.

Algorithm 13.10. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}$ and $\varepsilon \in]0, 1[$. The following steps return a set $\mathcal{M}$ containing a set of representatives for the $\mathfrak{p}$-equivalence classes in $\mathcal{L}(M)$. The probability that the two lattices in $\mathcal{M}$ are $\mathfrak{p}$-equivalent is less then ε:

(1) Run Algorithm 13.7 with probabilistic $\mathfrak{p}$-equivalence test and parameter ε, and denote the result by $\mathcal{M}$.
(2) For all $q = \#\mathcal{M}(\#\mathcal{M} + 1)/2$ unordered pairs (L, N) of elements of $\mathcal{M}$ we apply Algorithm 12.10 with error $\varepsilon^{1/q}$ to test $M \sim_{\mathfrak{p}} N$. In case we find two $\mathfrak{p}$-equivalent lattices L and N, we remove N from $\mathcal{M}$.
(3) Return $\mathcal{M}$.

Computation of genera. Using the algorithm for computing $\mathcal{L}(M)/{\sim_{\mathfrak{p}}}$, we can now derive a method for computing the different genera in $\mathcal{L}(M)$. Recall that by S we denote a finite set of prime ideals such that $\Lambda_{\mathfrak{p}}$ is maximal for all prime ideals $\mathfrak{p}$ not in S. In particular we know that two Λ-lattices $M, N \in \mathcal{L}(V)$ lie in the same genus if and only if M and N are $\mathfrak{p}$-equivalent for all $\mathfrak{p} \in S$.

Definition 13.11. For a nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$ we denote by $h_{\mathfrak{p}}(V)$ the number of $\mathfrak{p}$-equivalence classes of Λ-lattices in $\mathcal{L}(V)$. By $h(V)$ we denote the number of different genera of Λ-lattices in $\mathcal{L}(V)$, that is $h(V) = \#\,\mathcal{L}(V)/\vee$.

Lemma 13.12. We have
$$h(V) = \prod_{\mathfrak{p} \in S} h_{\mathfrak{p}}(V).$$

Proof. This follows from the definition of lying in the same genus, the defining property of S and Corollary 6.12. □

Using the discussion about $\mathfrak{p}$-equivalence classes, we can turn this result into an algorithm for computing $h(V)$.

Algorithm 13.13. Given a finite-dimensional A-module V, the following steps return $h(V)$.

(1) Find a Λ-lattice $M \in \mathcal{L}(V)$.
(2) For each $\mathfrak{p} \in S$ use Algorithm 13.7 to compute a set $\mathcal{M}_{\mathfrak{p}}$ of representatives for the $\mathfrak{p}$-equivalence classes in $\mathcal{L}(M)$.
(3) Return $\prod_{\mathfrak{p} \in S} \#\mathcal{M}_{\mathfrak{p}}$.

We can use the same idea to compute a set of representatives for the different genera in $\mathcal{L}(V)$.

Algorithm 13.14. Given a finite-dimensional A-module V, the following steps return a set of representatives of $\mathcal{L}(V)/\vee$.

(1) Find a Λ-lattice $M \in \mathcal{L}(V)$.
(2) For each $\mathfrak{p} \in S$ use Algorithm 13.7 to compute a set $\mathcal{M}_{\mathfrak{p}}$ of representatives for the $\mathfrak{p}$-equivalence classes in $\mathcal{L}(M)$.
(3) Return
$$\mathcal{M} = \Big\{ \bigcap_{\mathfrak{p} \in S} N^{(\mathfrak{p})} \,\Big|\, (N^{(\mathfrak{p})})_{\mathfrak{p} \in S} \in \prod_{\mathfrak{p} \in S} \mathcal{M}_{\mathfrak{p}} \Big\}.$$

Theorem 13.15. Algorithm 13.14 is correct.

Proof. Obviously the output $\mathcal{M}$ of Algorithm 13.14 satisfies $\#\mathcal{M} = \prod_{\mathfrak{p} \in S} h_{\mathfrak{p}}(V)$, which is exactly the number of different genera in $\mathcal{L}(V)$ by Lemma 13.12. As no two elements of $\mathcal{M}$ lie in the same genus we conclude that $\mathcal{M}$ is indeed a complete set of representatives. □

Remark 13.16.

(i) Note that all the lattices involved in Algorithm 13.14 are finitely generated $\mathcal{O}$-modules, which are represented using pseudo-bases and pseudo-matrices. Using the pseudo-Hermite normal form we can compute intersections, see [Coh00, Algorithm 1.5.1].

(ii) Note that concerning the use probabilistic algorithms for the $\mathfrak{p}$-equivalence, the discussion of Remark 13.9 also applies here. Using the randomized algorithms we can find a set containing a complete set of representatives of the different genera in $\mathcal{L}(V)$. Moreover, given any $\varepsilon \in \,]0,1[$ we can modify this set such that the probability that it is not a complete set of representatives is at most ε.

§14. Computing Solomon Zeta Functions of Lattices

In this section show how the algorithms introduced in the previous sections can be applied to the computation of Solomon zeta functions.

§14A. Solomon's original algorithm

Interestingly enough, Solomon's proof of the rationality of local factors of the zeta function of lattices applies not only to groups rings but in a much more general setting and is at the same time constructive. Since this is also the basis for our approach, we outline the arguments without proofs. We refer the reader to [Sol77].

Assumption. Throughout the section Λ denotes a unitary ring, M a left Λ-module and

$$\Delta(M) = \{N \subseteq M \ \Lambda\text{-submodule} \mid |M : N| \text{ finite}\}$$

the set of all submodules of M with finite index. Furthermore we assume that M satisfies the following conditions:

(i) There are only finitely many Λ-submodules of M of any given finite index $n \in \mathbf{Z}_{\geq 1}$, that is,

$$\{N \in \Delta(M) \mid |M : N| = n\}$$

is finite.

(ii) The set $\Delta(M)$ contains only finitely many isomorphism classes of Λ-modules.

(iii) There exists an integer $q \in \mathbf{Z}_{\geq 1}$, such that $|M : N|$ is a power of q for all $N \in \Delta(M)$.

(iv) Every element of $\Delta(M)$ has only finitely many maximal Λ-submodules, which are all contained in $\Delta(M)$.

Property (i) ensures that the formal Dirichlet series

$$\zeta_\Lambda(M, s) = \sum_{N \in \Delta(M)} |M : N|^{-s}, \ s \in \mathbf{C}$$

is well-defined. We call $\zeta_\Lambda(M, s)$ the *zeta function of* M. Denoting by a_n the number of elements N of $\Delta(M)$ with $|M : N| = q^n$, $n \in \mathbf{Z}_{\geq 0}$, using (iii) the zeta function of M can be rewritten as

$$\zeta_\Lambda(M, s) = \sum_{n \in \mathbf{Z}_{\geq 0}} a_n q^{-sn}.$$

It is now evident how to transform this into the setting of formal power series: Introducing

$$Z(M) = \sum_{n \in \mathbf{Z}_{\geq 0}} a_n X^n \in \mathbf{Z}[[X]],$$

we now have $Z(M)(q^{-s}) = \zeta_\Lambda(M, s)$. For convenience it is useful to introduce $[M : N] = X^{\log_q(|M:N|)} \in \mathbf{Z}[[X]]$, so that $Z(M)$ can be rewritten as

$$Z(M) = \sum_{N \in \Delta(M)} [M : N].$$

Solomon's first idea was to split $Z(M)$ according to isomorphism classes of Λ-modules in $\Delta(M)$. Let $\{M = M_1, \ldots, M_h\}$ be a set of representatives for the isomorphism classes of Λ-lattices in $\Delta(M)$ (this is finite by (ii)). For each $1 \leq i \leq h$ define the *partial zeta function* $Z(M, M_i) \in \mathbf{Z}[[X]]$ as

$$Z(M, M_i) = \sum_{\substack{N \in \Delta(M) \\ N \cong M_i}} [M : N],$$

so that we have the decomposition $Z(M) = \sum_{i=1}^h Z(M, M_i)$. Determining $Z(M)$ is therefore "reduced" to computing $Z(M, M_i)$ for all $1 \le i \le h$. Instead of looking only at $(Z(M_1, M_i))_{1 \le i \le h}$ Solomon had the ingenious idea of working with the whole matrix

$$\mathbf{B} = (Z(M_i, M_j))_{1 \le i,j \le h} \in \mathrm{Mat}_{h \times h}(\mathbf{Z}[[X]])$$

and explicitly computing the inverse of this matrix using combinatorial methods.

We need a little more notation. Denote by $\max(M)$ the—according to (iv)—finite set of maximal Λ-submodules of M and by $\mathrm{rad}(M) = \bigcap_{N \in \max(M)} N \in \Delta(M)$ the *radical of* M. Let

$$\Phi(M) = \{N \in \Delta(M) \mid \mathrm{rad}(M) \subseteq N \subseteq M\}$$

and for $N \in \Delta(M)$ define

$$\Phi(M, N) = \{L \in \Phi(M) \mid L \cong N\}.$$

For $\mathcal{N} \subseteq \max(M)$ define

$$M_{\mathcal{N}} = \bigcap_{N \in \mathcal{N}} N.$$

Finally for $N \in \Delta(M)$ define

$$\mu(N, M) = \sum_{\substack{\mathcal{N} \subseteq \max(M) \\ M_{\mathcal{N}} = N}} (-1)^{\#\mathcal{N}}.$$

Lemma 14.1. For $N \in \Delta(M)$ we have

$$\sum_{N \in \Phi(M)} \mu(N, M)(M : N)Z(N, M) = \begin{cases} 1, & \text{if } M \cong N \\ 0, & \text{else} \end{cases}$$

Proof. This is proven in [Sol77, Lemma 2]. □

Let us now define the matrix $\mathbf{A} = (\mathbf{A}_{ij})_{1 \le i,j \le h} \in \mathrm{Mat}_{h \times h}(\mathbf{Z}[X])$ via

$$\mathbf{A}_{ij} = \sum_{N \in \Phi(M_i, M_j)} \mu(N, M_i)[M_i : N].$$

Lemma 14.2. The matrix $\mathbf{A}$ is the inverse of $\mathbf{B}$. In particular $Z(M_i, M_j)$ as well as $Z(M_i)$ are rational functions, that is, they are elements of $\mathbf{Q}(X)$.

Proof. This is proven in [Sol77, Lemma 3]. □

Remark 14.3. While the definition of the involved objects, for example μ, look ad hoc, they arise naturally when looking at this as a combinatorial problem. The pair $(\Delta(L), \subseteq)$ is by assumption a locally finite poset and therefore gives rise to a Möbius function which turns out to be equal to μ. This combinatorial point of view is picked up by Solomon in [Sol79], where the above situation is generalized in the context of "posets with colors". In this thesis we do not include a presentation of the more general combinatorial setting, since we will only deal with modules over rings and the related counting-problem, for which the abstract setting does not yield new insight.

§14B. A variation of Solomon's algorithm

We now come back to zeta functions of lattices, as described in Section §9.

Assumption 14.4. Let K be a number field with ring of integers $\mathcal{O}$, A a semisimple K-algebra, Λ an $\mathcal{O}$-order of A and M a Λ-lattice. Moreover we set $V = KM$. We assume that the following data is given:

(i) The set B (or a finite superset thereof) of prime ideals $\mathfrak{p}$ of $\mathcal{O}$ which either divide $\mathrm{disc}(A)$ or for which Λ is not a full matrix algebra over a field.

(ii) The zeta function ζ_V in terms of zeta functions of number fields.

As seen in 9.10, to compute $\zeta_\Lambda(M, s)$ it is sufficient to determine $\zeta(M_{\mathfrak{p}}, s)$ for all prime ideals $\mathfrak{p} \in B$. Let $p \in \mathbf{Z}_{>0}$ be the prime lying under $\mathfrak{p}$ and consider the set $\mathcal{L}(M_{\mathfrak{p}})$ of $\Lambda_{\mathfrak{p}}$-sublattices of $M_{\mathfrak{p}}$ (note that $\Delta(M_{\mathfrak{p}}) = \mathcal{L}(M_{\mathfrak{p}})$, where $\Delta(M_{\mathfrak{p}})$ denotes the set of $\Lambda_{\mathfrak{p}}$-sublattices of $M_{\mathfrak{p}}$ with finite index):

(i) Let $n \in \mathbf{Z}_{\geq 1}$ and $N \in \mathcal{L}(M_\mathfrak{p})$ with $|M_\mathfrak{p} : N| = n$. Then $nM_\mathfrak{p} \subseteq N \subseteq M_\mathfrak{p}$ and therefore N is the preimage of a submodule of $M_\mathfrak{p}/nM_\mathfrak{p}$ under the natural projection $M_\mathfrak{p} \to M_\mathfrak{p}/nM_\mathfrak{p}$. Since $M_\mathfrak{p}/nM_\mathfrak{p}$ is finite, we conclude that there are only finitely many elements of $\mathcal{L}(M_\mathfrak{p})$ with index n.

(ii) By the theorem of Jordan–Zassenhaus, $\Delta(M_\mathfrak{p})$ contains only finitely many isomorphism classes of $\Lambda_\mathfrak{p}$-lattices.

(iii) For $N \in \Delta(M_\mathfrak{p})$ the $\mathcal{O}_\mathfrak{p}$-module $M_\mathfrak{p}/N$ is torsion. In particular, by the theorem on elementary divisors, it is isomorphic to a sum of modules of the form $\mathcal{O}_\mathfrak{p}/\mathfrak{p}^i\mathcal{O}_\mathfrak{p}$, whose cardinality is a power of $\mathbf{N}(\mathfrak{p})$. Since $\mathbf{N}(\mathfrak{p})$ itself is a power of p, we see that for all $N \in \Delta(M_\mathfrak{p})$, the index $|M_\mathfrak{p} : N|$ is a power of p.

(iv) The module $M_\mathfrak{p}$ has only finitely many maximal sublattices.

Thus all assumptions of §14A are satisfied and in principle we know how to compute the rational function $Z(M_\mathfrak{p}) \in \mathbf{Q}(X)$ such that $\zeta(M_\mathfrak{p}, s) = Z(M_\mathfrak{p})(p^{-s})$. Of course applying Solomon's original algorithm directly has the major drawback, that we need to compute with objects defined over p-adic fields and their valuation rings respectively. One possibility to overcome this obstacle is to work with localizations instead of completions: Solomon successfully used this approach to compute the zeta function of $M = \Lambda = \mathbf{Z}G$ and $A = \mathbf{Q}G$, where G is a finite cyclic group of prime order (see [Sol77, Section 5]). The aim of this section is to show that even localizations are not necessary to compute the Euler factors of the global Solomon zeta function. Our main ingredient will be the lattice isomorphism from Lemma 8.8, which relates the poset of sublattices in the complete setting with the lattice of sublattices with index a prime ideal power. Recall that

$$\mathcal{L}_\mathfrak{p}(M) = \{N \in \mathcal{L}(M) \mid (M : N) \text{ is a } \mathfrak{p}\text{-power}\} \quad \text{and} \quad \mathcal{L}_\mathfrak{p}^{\max}(M) = \mathcal{L}_\mathfrak{p}(M) \cap \mathcal{L}^{\max}(M).$$

Now let $\{M = M_1, \ldots, M_h\}$ be a set of representatives for $\mathcal{L}_\mathfrak{p}(M)/{\sim_\mathfrak{p}}$. Then the set $\{(M_1)_\mathfrak{p}, \ldots, (M_h)_\mathfrak{p}\}$ is a set of representatives for the isomorphism classes of $\Lambda_\mathfrak{p}$-lattices in $\mathcal{L}(M_\mathfrak{p})$. Let

$$\mathbf{B} = (Z((M_i)_\mathfrak{p}), Z((M_j)_\mathfrak{p}))_{1 \leq i,j \leq h} \in \mathrm{Mat}_{h\times h}(\mathbf{Z}[[X]])$$

be the matrix encoding all the partial zeta functions of these $\Lambda_\mathfrak{p}$-lattices. Note that by Lemma 14.2 we know that the inverse matrix $\mathbf{A} = (\mathbf{A}_{ij})_{1\leq i,j \leq h}$ of $\mathbf{B}$ is an element of $\mathrm{Mat}_{h\times h}(\mathbf{Z}[X])$ and is explicitly given by

$$\mathbf{A}_{ij} = \sum_{N \in \Phi((M_i)_\mathfrak{p}, (N_j)_\mathfrak{p})} \mu(N, (M_i)_\mathfrak{p})[(M_i)_\mathfrak{p} : N].$$

The reward of our careful investigation of the poset of $\mathfrak{p}$-sublattices—and its connection to the local setting at $\mathfrak{p}$—is the following theorem. It basically tells us that when M is a Λ-lattice, then the zeta function of the $\Lambda_\mathfrak{p}$-lattice $M_\mathfrak{p}$ can be derived from information about the sublattices of M itself. For a $\mathfrak{p}$-sublattice N of M let us set $[M : N] = X^{v_\mathfrak{p}((M:N))}$.

Theorem 14.5. Let $\{M = M_1, M_2, \ldots, M_h\}$ be a set of representatives for $\mathcal{L}_\mathfrak{p}(M)/{\sim_\mathfrak{p}}$ and $\mathbf{A}$ the inverse of $\mathbf{B} = (Z((M_i)_\mathfrak{p}), Z((M_j)_\mathfrak{p}))_{1\leq i,j\leq h} \in \mathrm{Mat}_{h\times h}(\mathbf{Z}[[X]])$. Then

$$\mathbf{A}_{ij} = \sum_{N \in \Phi_\mathfrak{p}(M_i, M_j)} \mu_\mathfrak{p}(N, M_i)[M_i : N] \in \mathbf{Z}[X]$$

Proof. By Lemma 14.2 we have

$$\mathbf{A}_{ij} = \sum_{N \in \Phi((M_i)_\mathfrak{p}, (M_j)_\mathfrak{p})} \mu(N, (M_i)_\mathfrak{p})[(M_i)_\mathfrak{p} : N].$$

Since $\Phi((M_i)_\mathfrak{p}, (M_j)_\mathfrak{p}) = \Phi_\mathfrak{p}(M_i, M_j)$ by Lemma 8.9 (iii) and for all $N \in \Phi_\mathfrak{p}(M_i, M_j)$ we have

$$\mu(N_\mathfrak{p}, (M_i)_\mathfrak{p}) \cdot [(M_i)_\mathfrak{p} : N_\mathfrak{p}] = \mu_\mathfrak{p}(N, M_i) \cdot [M_i : N]$$

by Lemma 8.9 (iv), the claim follows. □

Algorithm 14.6 (Euler factor of zeta functions). Given a Λ-lattice M and a prime ideal $\mathfrak{p}$ of $\mathcal{O}$, the following steps return $Z(M_\mathfrak{p}) \in \mathbf{Q}(X)$, such that

$$\zeta_{\Lambda_\mathfrak{p}}(M_\mathfrak{p}, s) = Z(M_\mathfrak{p})(p^{-s}).$$

(1) Compute a set of representatives $\{M = M_1, \ldots, M_h\}$ for $\mathcal{L}_\mathfrak{p}(M)/{\sim_\mathfrak{p}}$ using Algorithm 13.7.

(2) For each $1 \leq i \leq h$ use Algorithm 13.2 to compute the set $\mathcal{L}_{\mathfrak{p}}^{\max}(M_i)$ of $\mathfrak{p}$-maximal sublattices of M_i. Finally compute the $\mathfrak{p}$-radical $\operatorname{rad}_{\mathfrak{p}}(M_i)$ of M_i, as well as $\Phi(M_i, M_j)$ for all $1 \leq j \leq h$.

(3) For each $1 \leq i, j \leq h$ compute

$$\mathbf{A}_{ij} = \sum_{N \in \Phi_{\mathfrak{p}}(M_i, M_j)} \mu_{\mathfrak{p}}(N, M_i)[M_i : N] \in \mathbf{Z}[X].$$

(4) Compute $\mathbf{B} = \mathbf{A}^{-1}$ and return $\sum_{i=1}^{h} \mathbf{B}_{1i}$.

Theorem 14.7. Algorithm 14.6 is correct.

Proof. This follows from Theorem 14.5. □

Remark 14.8. While this algorithm is easy to state, in practice it has only a limited range of applicability due to the following reasons:

(i) For the computation of $\mu_{\mathfrak{p}}$ in Step 3 we need to loop through all 2^r subsets of $\{1, \ldots, r\}$, where r is the number of maximal sublattices. Clearly this is unfeasible as soon as r gets large.

(ii) Through the determination of $\Phi_{\mathfrak{p}}(-,-)$, there is a large amount of isomorphism tests contained in this algorithm. We have seen in Section §12 that this leads to a tremendous slowdown as soon as $\dim_K(\operatorname{End}_A(V))$ or the size of $k_{\mathfrak{p}}$ gets large, where $V = KM$. By employing probabilistic isomorphism tests this can be overcome. Of course we then have a result which is only correct with some probability < 1.

(iii) The algorithm is also sensitive to the number h of $\mathfrak{p}$-isomorphism classes of Λ-lattices in $\mathcal{L}(M)$, since in step 14.6 we have to invert an $h \times h$ matrix with entries in $\mathbf{Z}[X]$.

Algorithm 14.9 (Computation of Solomon zeta function). The following steps return $\varphi_{\mathfrak{p}} \in \mathbf{Z}[X]$, $\mathfrak{p} \in B$, such that

$$\zeta_\Lambda(M, s) = \zeta_V(s) \prod_{\mathfrak{p} \in B} \varphi_{\mathfrak{p}}(p^{-s}),$$

where $p \in \mathbf{Z}$ is the prime lying under $\mathfrak{p}$:

(1) For each $\mathfrak{p} \in B$ do the following:

  (2) Compute $Z(M_{\mathfrak{p}}) \in \mathbf{Q}(X)$ using Algorithm 14.6.

  (3) Compute $f_{\mathfrak{p}} \in \mathbf{Q}(X)$ such that $\zeta_{V,\mathfrak{p}} = f_{\mathfrak{p}}(p^{-s})$, where $p \in \mathbf{Z}$ is the prime lying under $\mathfrak{p}$.

  (4) Set

$$\varphi_{\mathfrak{p}} = \frac{Z(M_{\mathfrak{p}})}{f_{\mathfrak{p}}}.$$

(5) Return $(\varphi_{\mathfrak{p}})_{\mathfrak{p} \in B}$.

§14C. Computational results

Known results. The case where $\Lambda = \mathbf{Z}G$ for some finite group G (which was the motivation for Solomon in the first place) is—due to its connection to the representation theory of finite groups—of particular interest. While the machinery of J. Bushnell and Reiner reveal the beauty and rich structure of the associated zeta functions, the actual computation for non-trivial groups G and $\mathbf{Z}G$-lattices M seems like a hard task. In the past the case $M = \Lambda = \mathbf{Z}G$ has gained the most attention, resulting in the computation of $\zeta_{\mathbf{Z}G}(\mathbf{Z}G, s)$ for

- G cyclic of prime order ([Sol77, Rei80, BR80b]),
- G cyclic of order p^2 for p a prime ([Rei80]),
- G cyclic of order p^3 for p a prime ([Wit04]),
- $G \in \{C_2 \times C_2, C_3 \times C_3\}$ ([Tak87]),
- G dihedral of order $2p$ for p an odd prime ([BR81]),
- G metacyclic ([Hir81, Hir85]).

In addition, in [VH09, VH12], Villa-Hernandez determines the Solomon zeta functions of Burnside rings $B(G)$, for $G \in \{C_p, C_{p^2}\}$ with $p \in \mathbf{Z}_{>0}$ a prime, and $G \in \{\mathfrak{S}_3, \mathfrak{A}_4, \mathfrak{A}_5\}$.

The natural lattice of a Specht module. In this section, we present the results obtained by applying Algorithm 14.6 to a (finite) family of lattices associated to symmetric groups.

More precisely let $n \in \mathbf{Z}_{\geq 2}$ be a fixed integer and $G = \mathfrak{S}_{n+1}$ the symmetric group of degree $n+1$. Corresponding to the hook partition $\lambda = (2, 1^{n-1})$ of $n+1$ there exists the Specht module $V = S^\lambda$, an absolutely irreducible $\mathbf{Q}G$-module of dimension n. The Specht module V has a distinguished basis $(e_T)_T$, the Specht basis, labeled by the standard Young tableaux of shape λ. It is well known that with respect to this basis, the representation matrices have only integral entries, turning the $\mathbf{Z}$-module

$$L^\lambda = \bigoplus_T \mathbf{Z} e_T$$

into a $\mathbf{Z}G$-module, which we refer to as the *Specht lattice* corresponding to λ.

It is well known that the number of isomorphism classes of $\mathbf{Z}G$-lattices in $\mathcal{L}(V)$ is $\sigma(n+1)$, where σ denotes the divisor counting function. This was worked out independently by Wilhelm Plesken in [Ple74], Maurice Graig in [Cra76], and was later reproven using entirely different techniques by Walter Feit in [Fei98]. As V is absolutely irreducible, we have $\zeta_V(s) = \zeta_{\mathbf{Q}}(sn)$ and $\zeta_{V,p}(s) = (1-p^{-sn})^{-1}$. We have used Algorithm 14.6 to compute $\varphi_p \in \mathbf{Z}[X]$ such that $\varphi_p(p^{-s}) = \zeta(L_p^\lambda, s)/\zeta_{V,p}(s)$ for all rational primes p dividing $\#G = (n+1)!$ (these are exactly the rational primes less or equal then $n+1$). The results are presented in Table 4.1.

n	$\varphi_p \neq 1$	n	$\varphi_p \neq 1$
3	$\varphi_3 = 1+X$	28	$\varphi_2 = 1+X+X^2$, $\varphi_7 = 1+X$
4	$\varphi_2 = 1+X+X^2$	29	$\varphi_{29} = 1+X$
5	$\varphi_5 = 1+X$	30	$\varphi_2 = \varphi_3 = \varphi_5 = 1+X$
6	$\varphi_2 = \varphi_3 = 1+X$	31	$\varphi_{31} = 1+X$
7	$\varphi_7 = 1+X$	32	$\varphi_2 = 1+X+X^2+X^3+X^4+X^5$
8	$\varphi_2 = 1+X+X^2+X^3$	33	$\varphi_3 = \varphi_{11} = 1+X$
9	$\varphi_3 = 1+X+X^2$	34	$\varphi_2 = 1+X$, $\varphi_{17} = 1+X$
10	$\varphi_2 = \varphi_5 = 1+X$	35	$\varphi_5 = \varphi_7 = 1+X$
11	$\varphi_{11} = 1+X$	36	$\varphi_2 = \varphi_3 = 1+X+X^2$
12	$\varphi_2 = 1+X+X^2$, $\varphi_3 = 1+X$	37	$\varphi_{37} = 1+X$
13	$\varphi_{13} = 1+X$	38	$\varphi_2 = \varphi_{19} = 1+X$
14	$\varphi_2 = 1+X$, $\varphi_7 = 1+X$	39	$\varphi_3 = \varphi_{13} = 1+X$
15	$\varphi_3 = 1+X$, $\varphi_5 = 1+X$	40	$\varphi_2 = 1+X+X^2+X^3$, $\varphi_5 = 1+X$
16	$\varphi_2 = 1+X+X^2+X^3+X^4$	41	$\varphi_{41} = 1+X$
17	$\varphi_{17} = 1+X$	42	$\varphi_2 = \varphi_3 = \varphi_7 = 1+X$
18	$\varphi_2 = 1+X$, $\varphi_3 = 1+X+X^2$	43	$\varphi_{43} = 1+X$
19	$\varphi_{19} = 1+X$	44	$\varphi_2 = 1+X+X^2$, $\varphi_{11} = 1+X$
20	$\varphi_2 = 1+X+X^2$, $\varphi_5 = 1+X$	45	$\varphi_3 = 1+X+X^2$, $\varphi_5 = 1+X$
21	$\varphi_3 = \varphi_7 = 1+X$	46	$\varphi_2 = \varphi_{23} = 1+X$
22	$\varphi_2 = \varphi_{11} = 1+X$	47	$\varphi_{47} = 1+X$
23	$\varphi_{23} = 1+X$	48	$\varphi_2 = 1+X+X^2+X^3+X^4$, $\varphi_3 = 1+X$
24	$\varphi_2 = 1+X+X^2+X^3$, $\varphi_3 = 1+X$	49	$\varphi_7 = 1+X+X^2$
25	$\varphi_5 = 1+X+X^2$	50	$\varphi_2 = 1+X$, $\varphi_5 = 1+X+X^2$
26	$\varphi_2 = \varphi_{13} = 1+X$	51	$\varphi_3 = \varphi_{17} = 1+X$
27	$\varphi_3 = \varphi_7 = 1+X$	52	$\varphi_2 = 1+X+X^2$, $\varphi_{13} = 1+X$

Table 4.1.: Result of Algorithm 14.6 applied to the Specht lattice $L^{(2,1^{n-1})}$ for $3 \leq n \leq 53$ and all primes p dividing n.

The result of the computation can be summarized in the following lemma.

Lemma 14.10. Let $3 \leq n \leq 100$ and p a rational prime. Then

$$\varphi_p = \sum_{i=0}^{v_p(n)} X^i \in \mathbf{Z}[X].$$

In particular, if p does not divide n, then $\varphi_p = 1$.

§14D. A family of Solomon zeta functions

We now want to show that the algorithm given in the previous section can also be applied for computing Solomon zeta functions for families of lattices. We will need a considerable amount of representation theory of the symmetric group. The result of this section appeared as [Hof16]. The reference for all unexplained material is [Jam78].

Assumption 14.11. Let $n \geq 3$, $G = \mathfrak{S}_{n+1}$ and V the Specht module corresponding to the partition $\lambda = (2, 1^{n-1})$.

In this section we will determine the Solomon zeta functions of all $\mathbf{Z}G$-lattices rationally equivalent to V. In particular, we will show that Lemma 14.10 holds for all $n \geq 3$. As already mentioned in §14C, the $\mathbf{Z}G$-lattices rationally equivalent to V have been determined by Plesken, Craig and Feit. Here we will use the lattices as constructed by Craig. Due to [Cra76] we know that we can choose a $\mathbf{Q}$-basis $(e_1, \ldots, e_n)$ of V such that for $1 \leq k \leq n$ the action of the adjacent transposition $(k\ k+1)$ is given by multiplication with the matrix $E^{k,k-1} + 2E^{k,k} + E^{k,k+1} - I_k$. Here for $1 \leq i, j \leq n$ we denote by $E^{i,j}$ the matrix $(\delta_{ik}\delta_{jl})_{1 \leq k,l, \leq n}$ and set $E^{i,j} = 0$ whenever i or j are not in $\{1, \ldots, n\}$.

With respect to this chosen representation, in [Cra76] representatives for the isomorphism classes of $\mathbf{Z}G$-lattices rationally equivalent to V are explicitly constructed.

Definition 14.12. Denote by v the element $e_n + \sum_{i=1}^{n-1} (-1)^{n+1-i} i e_i \in V$. For every integer $d \in \mathbf{Z}_{>0}$ define the $\mathbf{Z}$-module $L(d)$ via

$$L(d) = \Big(\bigoplus_{i=1}^{n-1} \mathbf{Z} d e_i\Big) \oplus \mathbf{Z} v,$$

that is, with respect to $(e_1, \ldots, e_n)$ the basis matrix of $L(d)$ is

$$\begin{pmatrix} d & 0 & 0 & \ldots & (-1)^n \cdot 1 \\ 0 & d & 0 & \ldots & (-1)^{n-1} \cdot 2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots & 0 & d & n-1 \\ 0 & \ldots & 0 & 0 & 1 \end{pmatrix} \in \mathrm{Mat}_{n \times n}(\mathbf{Z}).$$

The main result of [Cra76] is the following classification.

Theorem 14.13 (Craig). *If d is a divisor of $n+1$, then the $\mathbf{Z}$-module $L(d)$ is a $\mathbf{Z}G$-lattice of V. Moreover $\{L(d) \mid d \text{ divides } n+1\}$ is a set of representatives for the isomorphism classes of $\mathbf{Z}G$-lattices rationally equivalent to V.*

The lattice of p-sublattices and Euler factors. In order to apply the techniques introduced in §14C, for each prime divisor p of $\#G$ and each $\mathbf{Z}G$-lattice L rationally equivalent to V, we need to determine the sublattice structure of the p-sublattices of L.

Assumption. Let us fix a rational prime $p \in \mathbf{Z}_{>0}$. For $X \in \{\Phi, \mathcal{L}, \mathcal{L}^{\max}, \mathrm{rad}, \mu\}$ we write X_p instead of $X_{p\mathbf{Z}}$.

Lemma 14.14. *Let $L \subseteq L(1)$ be a $\mathbf{Z}G$-sublattice and assume there exists an exponent $c \in \mathbf{Z}_{\geq 1}$ such that $p^c L(1) \subseteq L$. Then there exist $a, b \in \mathbf{Z}_{\geq 0}$ with $a + b \leq c$, $p^b \mid n+1$ (i.e. $b \leq v_p(n+1)$) and $L = p^a L(p^b)$.*

Proof. Choose some basis matrix $B \in \mathrm{Mat}_{n \times n}(\mathbf{Z})$ of L with respect to $(e_1, \ldots, e_n)$ and denote by t the GCD of the entries of B. We write $B = tB'$ with $B' = (b'_{ij})_{ij}$ an element of $\mathrm{M}_n(\mathbf{Z})$ satisfying $\gcd(b'_{ij} \mid i, j) = 1$. Denote by L' the lattice spanned by the columns of B'. By assumption the index $|L(1) : L| = \det(B)$ is a p-power. Thus the same is true for t and there exists $a \in \mathbf{Z}_{\geq 0}$ such that $t = p^a$ implying $p^{c-a} L(1) \subseteq L'$. Now [Cra76, Lemma 9], applied to L' with basis matrix B', shows that there exists an integer $b \in \mathbf{Z}_{\geq 0}$ with $b \leq c - a$, $p^b \mid n+1$ and $L' = L(p^b)$. □

Lemma 14.15. *Let $a, b, a', b' \in \mathbf{Z}_{\geq 0}$ be integers. Then the following hold:*

(i) *We have $p^a L(p^b) \cap p^{a'} L(p^{b'}) = p^{\max(a,a')} L(p^{\max(a+b,a'+b')-\max(a,a')})$.*

(ii) *The inclusion $p^a L(p^b) \subseteq p^{a'} L(p^{b'})$ holds if and only if $a \geq a'$ and $a + b \geq a' + b'$. In this case we have $|p^{a'} L(p^{b'}) : p^a L(p^b| = p^{(a-a')n+(b-b')(n-1)}$.*

Proof. We have

$$p^a L(p^b) = \Big(\bigoplus_{i=1}^{n-1} \mathbf{Z}p^{a+b}e_i\Big) \oplus \mathbf{Z}p^a v \text{ and } p^{a'} L(p^{b'}) = \Big(\bigoplus_{i=1}^{n-1} \mathbf{Z}p^{a'+b'}e_i\Big) \oplus \mathbf{Z}p^{a'} v.$$

By comparing the coefficients in front of v and the e_i, the claims follow. □

Lemma 14.16. Let $0 \le i \le v_p(n+1)$ and assume that L is a proper $\mathbf{Z}G$-sublattice of $L(p^i)$ with index a p-power. Then the following hold:

(i) If $i = 0$, then L is contained in $L(p)$.
(ii) If $0 < i < v_p(n+1)$, then L is contained in $L(p^{i+1})$ or $pL(p^{i-1})$.
(iii) If $i = v_p(n+1)$, then L is contained in $pL(p^{v_p(n+1)-1})$.

Proof. Write $L = p^a L(p^b)$ with $a, b \in \mathbf{Z}_{\geq 0}$ and $b \le v_p(n+1)$.
(i): Assume that L is a proper $\mathbf{Z}G$-sublattice of $L(1)$. Then $(a,b) \neq (0,0)$ and therefore $a + b \geq 1$. By Lemma 14.15 we have $L \subseteq L(p)$.
(ii): Assume that L is a proper $\mathbf{Z}G$-sublattice of $L(p^i)$. Then $(a,b) \neq (0,i)$. If $a \neq 0$, then $a \geq 1$ and $a + b \geq i = 1 + (i-1)$. Thus by Lemma 14.15 we have $L \subseteq pL(p^{i-1})$. If $a = 0$, then we necessarily have $b > i$ and therefore $L = L(p^b) \subseteq L(p^{i+1})$.
(iii): Assume that L is a proper $\mathbf{Z}G$-sublattice of $L(p^{v_p(n+1)})$. Then $(a,b) \neq (0, v_p(n+1))$. Since we also have $b \le v_p(n+1)$, we conclude that $a \geq 1$. Thus by Lemma 14.15 we obtain $L \subseteq pL(p^{v_p(n+1)-1})$. □

As a consequence we obtain:

Lemma 14.17. For $0 \le i \le v_p(n+1)$ we have

$$\mathcal{L}_p^{\max}(L(p^i)) = \begin{cases} \{L(p)\}, & \text{if } i = 0, \\ \{L(p^{i+1}), pL(p^{i-1})\}, & \text{if } 0 < i < v_p(n+1), \\ \{pL(p^{i-1})\}, & \text{if } i = v_p(n+1). \end{cases}$$

Remark 14.18. Let M and N be sublattices of $L(1)$ with index a p-power and $L \in \Phi_p(M,N)$. Then the condition $L_p \cong N_p$ as $\mathbf{Z}_pG$-lattices is equivalent to $L \cong N$ as $\mathbf{Z}G$-lattices. This can be seen as follows. Assume that $L_p \cong N_p$ as $\mathbf{Z}_pG$-lattices. If $q \neq p$ is a rational prime, we have—the indices $|L(1) : M|$, $|L(1) : N|$ and $|L(1) : L|$ being p-powers—$L(1)_q = M_q = N_q = L_q$. Thus L and N lie in the same genus. As V is absolutely irreducible this implies $L \cong N$ as $\mathbf{Z}G$-lattices (see [CR81, 31.26 Theorem]). Thus

$$\Phi_p(M,N) = \{L \in \Phi_p(M) \mid N \cong L \text{ as } \mathbf{Z}G\text{-lattices } \}.$$

Lemma 14.19. For $0 \le i \le v_p(n+1)$ we have

$$\mathrm{rad}_p(L) = \begin{cases} L(p), & \text{if } i = 0, \\ pL(p^i), & \text{if } 0 < i < v_p(n+1), \\ pL(p^{i-1}), & \text{if } i = v_p(n+1). \end{cases}$$

Proof. This follows from Lemma 14.15 and 14.17. □

Lemma 14.20. For $0 \le i \le v_p(n+1)$ the following hold:

$$\Phi_p(L(p^i)) = \begin{cases} \{L(1), L(p)\}, & \text{if } i = 0, \\ \{pL(p^{i-1}), L(p^i), pL(p^i), L(p^{i+1})\}, & \text{if } 0 < i < v_p(n+1), \\ \{pL(p^{i-1}), L(p^i)\}, & \text{if } i = v_p(n+1) \end{cases}$$

Proof. By Lemma 14.19 we know the p-radical of $L(p^i)$. The result follows by applying Lemma 14.15. □

We can now determine $\Phi_p(L(p^i), L(p^j))$ for all $0 \le i,\ j \le v_p(n+1)$.

Lemma 14.21. The following hold:

(i) We have

$$\Phi_p(L(1), L(p^j)) = \begin{cases} \{L(1)\}, & \text{if } j = 0, \\ \{L(p)\}, & \text{if } j = 1, \\ \emptyset, & \text{otherwise.} \end{cases}$$

(ii) For $0 < i < v_p(n+1)$ we have

$$\Phi_p(L(p^i), L(p^j)) = \begin{cases} \{pL(p^{i-1})\}, & \text{if } j = i-1, \\ \{L(p^i), pL(p^i)\}, & \text{if } j = i, \\ \{L(p^{i+1})\}, & \text{if } j = i+1, \\ \emptyset, & \text{otherwise.} \end{cases}$$

(iii) We have

$$\Phi_p(L(p^{v_p(n+1)}), L(p^j)) = \begin{cases} \{pL(p^{v_p(n+1)-1})\}, & \text{if } j = v_p(n+1)-1, \\ \{L(p^{v_p(n+1)})\}, & \text{if } j = v_p(n+1), \\ \emptyset, & \text{otherwise.} \end{cases}$$

Proof. Note that by the classification of Craig we know that for $0 \leq i, j \leq v_p(n+1)$ the $\mathbf{Z}G$-lattices $L(p^i)$ and $L(p^j)$ are isomorphic if and only if $i = j$. Since for any $\mathbf{Z}G$-lattice M and integer $m \in \mathbf{Z}\backslash\{0\}$ the $\mathbf{Z}G$-lattices M and mM are isomorphic, it follows, by Remark 14.18, that $(p^a L(p^i))_p \cong (p^b L(p^j))_p$ as $\mathbf{Z}_pG$-lattices if and only if $i = j$. □

We have now gathered enough information to compute the Euler factor of the lattices $L(p^i)$ at p. First of all note that $\{L(p^i)_p \mid 0 \leq i \leq v_p(n+1)\}$ is a complete set of representatives for isomorphism classes of $\mathbf{Z}_pG$-lattices in $L(1)_p$. Let $\mathbf{B} = (Z(L(p^i)_p), Z(L(p^j)_p))_{0\leq i,j\leq v_p(n+1)} \in \mathrm{Mat}_{(v_p(n+1)+1)\times(v_p(n+1)+1)}(\mathbf{Z}[[X]])$ and denote by $\mathbf{A}$ its inverse.

Proposition 14.22. The matrix $\mathbf{A} = (\mathbf{A}_{ij})_{0\leq i,j\leq v_p(n+1)}$ is a tridiagonal matrix with $\mathbf{A}_{ij} = 0$ if $|i-j| > 1$ and

$$\mathbf{A}_{ij} = \begin{cases} 1, & \text{if } i = j = 0 \text{ or } i = j = v_p(n+1), \\ 1 + X^n, & \text{if } 0 < i = j < v_p(n+1), \\ -X, & \text{if } j = i-1, \\ -X^{n-1}, & \text{if } j = i+1, \end{cases}$$

that is,

$$\mathbf{A} = \begin{pmatrix} 1 & -X^{n-1} & 0 & 0 & 0 & \dots & 0 \\ -X & 1+X^n & -X^{n-1} & 0 & 0 & \cdots & 0 \\ 0 & -X & 1+X^n & -X^{n-1} & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & -X & 1+X^n & -X^{n-1} & 0 \\ 0 & \dots & 0 & 0 & -X & 1+X^n & -X^{n-1} \\ 0 & \dots & 0 & 0 & 0 & -X & 1 \end{pmatrix}.$$

Proof. By Theorem 14.5 we have

$$\mathbf{A}_{ij} = \sum_{M\in\Phi_p(L(p^i),L(p^j))} \mu_p(M, L(p^i))[L(p^i) : M].$$

Now apply Lemma 14.21. □

Proposition 14.23. The matrix $\mathbf{B} = (\mathbf{B}_{ij})_{0\leq i,j\leq v_p(n+1)} \in \mathrm{Mat}_{(v_p(n+1)+1)\times(v_p(n+1)+1)}(\mathbf{Q}[X])$ with $\mathbf{B}_{ij} = Z(L(p^i)_p, L(p^j)_p)$ is given by

$$\mathbf{B}_{ij} = \frac{1}{1-X^n} \begin{cases} 1, & \text{if } i = j, \\ X^{(i-j)(n-1)}, & \text{if } i < j, \\ X^{j-i}, & \text{if } i > j, \end{cases}$$

that is,

$$\mathbf{B} = \frac{1}{1-X^n}\begin{pmatrix} 1 & X^{n-1} & X^{2(n-1)} & X^{3(n-1)} & X^{4(n-1)} & \cdots & X^{(v_p(n+1))(n-1)} \\ X & 1 & X^{n-1} & X^{2(n-1)} & X^{3(n-1)} & \cdots & X^{(v_p(n+1)-1)(n-1)} \\ X^2 & X & 1 & X^{n-1} & X^{2(n-1)} & \cdots & X^{(v_p(n+1)-2)(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ X^{v_p(n+1)-2} & X^{v_p(n+1)-3} & \cdots & X & 1 & X^{n-1} & X^{2(n-1)} \\ X^{v_p(n+1)-1} & X^{v_p(n+1)-2} & X^{v_p(n+1)-3} & \cdots & X & 1 & X^{n-1} \\ X^{v_p(n+1)} & X^{v_p(n+1)-1} & X^{v_p(n+1)-2} & \cdots & X^2 & X & 1 \end{pmatrix}.$$

Proof. This is a straightforward calculation. For $0 \le i \le v_p(n+1)$ denote by A_i the ith row of A and by B_i the ith column of B. We need to show that $A_iB_j = \delta_{ij}$ for $0 \le i, j \le v_p(n+1)$. As an example let us verify the case $1 \le i, j \le v_p(n+1) - 1$, for which we have $A_iB_j = \mathbf{A}_{i,i-1}\mathbf{B}_{j,i-1} + \mathbf{A}_{i,i}\mathbf{B}_{j,i} + \mathbf{A}_{i,i+1}\mathbf{B}_{j,i+1} = -X\mathbf{B}_{j,i-1} + (1+X^n)\mathbf{B}_{j,i} - X^{n-1}\mathbf{B}_{j,i+1}$. Now

$$(\mathbf{B}_{j,i-1}, \mathbf{B}_{j,i}, \mathbf{B}_{j,i+1}) = \begin{cases} (X^{(j-i+1)(n-1)}, X^{(j-i)(n-1)}, X^{(j-i-1)(n-1)}), & \text{if } i < j \\ (X^{n-1}, 1, X), & \text{if } i = j \\ (X^{i-j-1}, X^{i-j}, X^{i-j+1}), & \text{if } i > j. \end{cases}$$

and we easily conclude that $A_iB_j = \delta_{ij}$. □

Corollary 14.24. For $0 \le i \le v_p(n+1)$ we have $\zeta_{\mathbf{Z}_pG}(L(p^i)_p, s) = \varphi_{p,i}(p^{-s})$, where

$$\varphi_{p,i} = \frac{1}{1-X^n}\left(\sum_{j=0}^{i} X^j + \sum_{j=i+1}^{v_p(n+1)} X^{(j-i)(n-1)}\right).$$

Proof. The claim follows from $Z(L(p^i)_p, X) = \sum_{j=0}^{v_p(n+1)} B_{ij}$ and $\zeta_{\mathbf{Z}_pG}(L(p^i)_p, s) = Z(L(p^i)_p, p^{-s})$. □

Computation of the Solomon zeta function. We now return to the global Solomon zeta function. Since V is absolutely irreducible of dimension n, we have

$$\zeta_V(s) = \zeta_{\mathbf{Q}}(ns)$$

and for every prime ideal $\mathfrak{p} = p\mathbf{Z}$ the Euler factor $\zeta_{V,\mathfrak{p}}$ is given by

$$\zeta_{V,p}(s) = \frac{1}{1+p^{-ns}}.$$

Now if M is a $\mathbf{Z}G$-lattice of V, by Theorem 9.14 we have

$$\zeta_{\mathbf{Z}G}(M, s) = \zeta_V(s) \prod_{p \mid \#G} \frac{\zeta_{\mathbf{Z}_pG}(M_p, s)}{\zeta_{V,p}(s)}.$$

As $\#G = (n+1)!$ we have

$$\zeta_{\mathbf{Z}G}(M, s) = \zeta_V(s) \prod_{\substack{p \text{ prime} \\ p \le n+1}} \frac{\zeta_{\mathbf{Z}_pG}(M_p, s)}{\zeta_{V,p}(s)}$$

and it remains to determine the local factors for all rational primes $p \le n+1$.

Proposition 14.25. Let M be a $\mathbf{Z}G$-lattice of V. Then for all rational primes $p \in \mathbf{Z}$ not dividing $n+1$ we have

$$\frac{\zeta_{\mathbf{Z}_pG}(M_p, s)}{\zeta_{V,p}(s)} = 1.$$

Proof. If p does not divide $n+1$, then by [Jam78, 23.7 Theorem] the quotient M/pM is an irreducible $\mathbf{F}_pG$-module. In particular $M/pM \cong M_p/pM_p$ is irreducible. This implies that pM_p is the only maximal $\mathbf{Z}_pG$-sublattice of M_p and therefore $\{p^iM_p \mid i \in \mathbf{Z}_{\ge 0}\}$ is the set of all $\mathbf{Z}_pG$-sublattices of M_p. Hence

$$\zeta_{\mathbf{Z}_pG}(M_p, s) = \sum_{i=0}^{\infty} (p^{in})^{-s} = \frac{1}{1+p^{-ns}} = \zeta_{V,p}(s).$$

□

Theorem 14.26. For a divisor d of $n+1$ the Solomon zeta function of the $\mathbf{Z}G$-lattice $L(d)$ is given by

$$\zeta_{\mathbf{Z}G}(L(d),s) = \zeta_{\mathbf{Q}}(ns) \prod_{p \mid n+1} \varphi_{p,d}(p^{-s}),$$

where p runs over all prime divisors of $n+1$, $\zeta_{\mathbf{Q}}$ denotes the classical Riemann zeta function and

$$\varphi_{p,d} = \sum_{j=0}^{v_p(d)} X^j + \sum_{j=v_p(d)+1}^{v_p(n+1)} X^{(j-v_p(d))(n-1)}.$$

Proof. Let $m = (n+1)!/n$. The proof of [Cra76, Lemma 10] and its corollary show that

$$L(d) = \sum_{p \mid n+1} m_p L(p^{v_p(d)}),$$

where $m_p = m/p^{v_p(m)}$. While $(m_p L(p^{v_p(d)}))_p = L(p^{v_p(d)})_p$, for a prime $q \neq p$ we have $(m_q L(q^{v_q(d)}))_p = p^{v_p(m)} L(1)_p$. Since $p^{v_p(m)} L(1) \subseteq p^{v_p(d)} L(1) \subseteq L(p^{v_p(d)})$ we conclude that

$$L(d)_p = L(p^{v_p(d)})_p.$$

Together with Proposition 14.25 we obtain

$$\zeta_{\mathbf{Z}G}(L(d),s) = \zeta_{\mathbf{Q}}(ns) \prod_{p \mid n+1} \frac{\zeta_{\mathbf{Z}_pG}(L(d)_p,s)}{\zeta_{V,p}(s)} = \zeta_{\mathbf{Q}}(ns) \prod_{p \mid n+1} \frac{\zeta_{\mathbf{Z}_pG}(L(p^{v_p(d)})_p,s)}{\zeta_{V,p}(s)}.$$

Since $\zeta_{V,p}(s)^{-1} = g(p^{-s})$, where $g = 1 - X^n$, the claim follows from Corollary 14.24. □

To compute the Solomon zeta function of the Specht lattice L^λ, it is sufficient to locate it in the classification of Craig.

Lemma 14.27. If the rational prime p is a divisor of $n+1$, the module L^λ has a unique p-maximal sublattice. This sublattice has index p in L^λ.

Proof. It is sufficient to prove that the $\mathbf{F}_pG$-module L^λ/pL^λ has a unique maximal submodule and that this submodule has index p. Let S^λ be the Specht module over $\mathbf{F}_p$ corresponding to λ. Then L^λ/pL^λ is isomorphic to S^λ and we can use the rich theory of Specht modules. Let μ be the conjugate partition of λ, that is, $\mu = (n,1)$. Then by [Jam78, Theorem 8.15] we have

$$(S^\lambda)^* \cong S^\mu \otimes S^{(1^{n+1})},$$

where $(S^\lambda)^* = \operatorname{Hom}_{\mathbf{F}_p}(S^\lambda, \mathbf{F}_p)$ is the dual of S^λ. As $n \geq 2$ the partition μ is p-regular and by [Jam78, Corollary 12.2] the module S^μ has the unique composition series

$$S^\mu \supsetneq S \supsetneq \{0\}.$$

where S is isomorphic to the trivial $\mathbf{F}_pG$-module. Thus S^μ has a unique 1-dimensional minimal submodule. As $S^{(1^{n+1})}$ is 1-dimensional, also the tensor product $S^\mu \otimes S^{(1^{n+1})}$ has a unique 1-dimensional minimal submodule. Since

$$N \longmapsto N^\perp = \{f \in (S^\lambda)^* \mid f(n) = 0 \text{ for all } n \in N\}$$

is an anti-isomorphism between the lattice of submodules of S^λ and the lattice of submodules of $(S^\lambda)^*$ with $\dim_{\mathbf{F}_p}(N^\perp) = \dim_{\mathbf{F}_p}(S^\lambda) - \dim_{\mathbf{F}_p}(N)$ (see [HGK07, Proposition 4.1.1]), the module S^λ has a unique maximal submodule of dimension $n-1$. □

Proposition 14.28. We have $L^\lambda \cong L(n+1)$ as $\mathbf{Z}G$-modules.

Proof. Assume that they are not isomorphic. Then there exists a prime divisor p of $n+1$ such that $(L^\lambda)_p$ and $(L(n+1))_p$ are not isomorphic as $\mathbf{Z}_pG$-modules. Since $(L(n+1))_p = (L^{v_p(n+1)})_p$ there exists $0 \leq i < v_p(n+1)$ such that $(L^\lambda)_p \cong L(p^i)_p$. By Lemma 14.17 this implies that L^λ has a p-maximal submodule of index $> p$, contradicting Lemma 14.27. □

This proves the following corollary.

Corollary 14.29. The Solomon zeta function of the Specht lattice $L^{(2,1^{n-1})}$ is given by

$$\zeta_{\mathbf{Z}G}(L^{(2,1^{n-1})}) = \zeta_{\mathbf{Q}}(ns) \prod_{p \mid n+1} \varphi_p(p^{-s}), \qquad \text{where} \quad \varphi_p = \frac{X^{v_p(n+1)} - 1}{X - 1},$$

and p runs over all prime divisors of $n+1$.

CHAPTER 5

Integrality of representations of finite groups

In this chapter we come to the problem to which all the theory and algorithms in the previous chapters were built toward to: Integrality of representations of finite groups. We begin by introducing the problem and by linking it to the theory of lattices developed in the previous chapter. To give an algorithm for deciding integrality, we have to investigate the reduction of lattices modulo (infinitely many) prime ideals. We finish this topic by generalizing a theoretical result of Serre on the existence and non-existence of integral representations realizing a given character. Combined with extensive numerical results this leads to various conjectures.

§15. The question of integrality

Assumption. Let G be a finite group, K a number field with ring of integers $\mathcal{O}$ and $\rho\colon G \to \mathrm{GL}_n(K)$ an irreducible representation of G. We denote by V the associated irreducible KG-module.

Definition 15.1. The representation $\rho\colon G \to \mathrm{GL}_n(K)$ is called *integral*, if and only if $\rho(g) \in \mathrm{GL}_n(\mathcal{O})$ for all $g \in G$. We say that ρ *can be made integral*, if and only if there exists an integral representation $G \to \mathrm{GL}_n(\mathcal{O})$ which is equivalent to ρ. We call V *integral* if ρ can be made integral.

In other words, ρ can be made integral if and only if we can apply a base change such that all matrices have integral entries. Recall that Burnside [Bur08] asked the question whether every representation over a number field can be made integral. To investigate this question, let us translate integrality into the setting of lattices. We have the following well-known result.

Lemma 15.2. The following are equivalent:

(i) The representation ρ can be made integral.
(ii) There exists a G-invariant finitely generated $\mathcal{O}$-free $\mathcal{O}$-module $M \subseteq V$.
(iii) There exists $M \in \mathcal{L}(V)$ such that M is $\mathcal{O}$-free.
(iv) For all $M \in \mathcal{L}(V)$ we have $1 \in \mathrm{cl}(\mathcal{L}(M))$.
(v) There exists $M \in \mathcal{L}(V)$ such that $1 \in \mathrm{cl}(\mathcal{L}(M))$.
(vi) We have $\mathrm{cl}(\mathcal{L}(V)) \cap \mathrm{im}(f_n) \neq \emptyset$, where $f_n\colon \mathrm{Cl}_K \to \mathrm{Cl}_K, [\mathfrak{a}] \mapsto [\mathfrak{a}]^n$ is the nth power map.

Proof. (i)⇒(ii): Let $\rho'\colon G \to \mathrm{GL}_n(K)$ be integral and equivalent to ρ. Then $\mathcal{O}^n$ is a free $\mathcal{O}$-module, invariant under $\rho'(G)$. Let $A \in \mathrm{GL}_n(K)$ be such that $\rho(g)A = A\rho'(g)$ for all $g \in G$. Then if M denotes the image of $\mathcal{O}^n$ under $A\colon K^n \to K^n$, M is G-invariant and $\mathcal{O}$-free.
(ii)⇒(iii)⇒(iv)⇒(v)⇒(vi): Clear.
(vi)⇒(i): Let $M \in \mathcal{L}(V)$ such that $\mathrm{cl}(M)$—and therefor also $\mathrm{cl}(M)^{-1}$—is an nth power. Thus we can find an integral ideal $\mathfrak{a}$ of K such that $[\mathfrak{a}]^n = \mathrm{cl}(M)^{-1}$. Then $\mathfrak{a}M \in \mathcal{L}(V)$ and $\mathrm{cl}(\mathfrak{a}M) = [\mathfrak{a}]^n \,\mathrm{cl}(M) = 1$. Thus $\mathfrak{a}M$ is $\mathcal{O}$-free and the representation obtained by choosing any $\mathcal{O}$-basis of $\mathfrak{a}M$ is integral and equivalent to ρ. □

Using this characterization it is easy to derive sufficient criteria for integrality. Note that they were obtained already by Schur in [Sch11]:

Corollary 15.3. Assume that one of the conditions hold:

(i) We have $K = \mathbf{Q}$.

(ii) We have $h_K = 1$.

(iii) We have $\gcd(h_K, n) = 1$.

Then the representation ρ can be made integral.

Proof. (iii): If the class number is coprime to n, then the nth power map $f_n\colon \mathrm{Cl}_K \to \mathrm{Cl}_K$ from the previous lemma is a bijection. Thus the result follows from Lemma 15.2. Since (i) or (ii) imply (iii), we are done. □

Note that Corollary 15.3 provides us with a large amount of representations which can be made integral. In sharp contrast, we are rather ignorant when it comes to representations which cannot be made integral. Since Burnside raised the question in 1908, we only know of the following examples.

Example 15.4.

(i) Let Q_8 be the quaternion group and $\rho\colon Q_8 \to \mathrm{GL}_n(\mathbf{Q}(\sqrt{-35}))$ an absolutely irreducible representation affording the unique irreducible $\mathbf{C}$-character of Q_8 of degree 2. Then in 1974, in a letter to Serre (see [Ser08]), Feit showed that ρ cannot be made integral. The same example was independently discovered by Cliff–Ritter–Weiss in [CRW92].

(ii) In [CRW92], it is shown that the metacyclic group $G = \langle x, y \mid x^9 = y^{19} = 1, y^x = y^7 \rangle$ admits an absolutely irreducible representation $G \to \mathrm{GL}_3(K)$ which cannot be made integral, where K is the unique subfield of $\mathbf{Q}(\zeta_{57})$ of degree 12.

(iii) In response to Feit, in 1997 Serre extended (i) in the following way (see [Ser08]). Let $\mathbf{Q}(\sqrt{-n})$ be a imaginary quadratic field such that the irreducible $\mathbf{C}$-character of the quaternion group Q_8 of degree 2 can be realized by a representation $\rho_n\colon Q_8 \to \mathrm{GL}_2(\mathbf{Q}(\sqrt{-n}))$. Serre showed that ρ can be made integral if and only if n can be written as $x^2 + 2y^2$ with $x, y \in \mathbf{Z}$. In particular for infinitely many values of n, the representation ρ_n cannot be made integral.

Now let M be an $\mathcal{O}G$-lattice of V and assume that we know the Steinitz class $\mathrm{cl}(M)$ of M. In Lemma 15.2 we have seen that the integrality of ρ is intimately linked to the set $\mathrm{cl}(\mathcal{L}(M))$ of Steinitz classes of all sublattices of M. Since for a sublattice $N \subseteq M$ we have $\mathrm{cl}(N) = [(M : N)] \cdot \mathrm{cl}(M)$, it is therefore sufficient to study $[(M : N)]$, as N ranges through all sublattices of M. As a first step in this direction, we will now describe all occurring index ideals $(M : N)$, as $N \in \mathcal{L}^{\max}(M)$ ranges through the maximal sublattices of M. By Lemma 8.4 it is sufficient to understand the dimension of the composition factors of (the head of) $M/\mathfrak{p}M$ for all nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}$.

§16. Reduction theory

Assumption. Let G be a finite group, K a number field with ring of integers $\mathcal{O}$ and $\rho\colon G \to \mathrm{GL}_n(K)$ a representation of G. We denote by V the associated KG-module.

The study of the reduced lattices $M/\mathfrak{p}M$ in case K is a splitting field of G (and therefore V absolutely irreducible) is a very old topic in representation theory and can be found in many textbooks, for example [CR81]. The more general situation we will now discuss has not been studied before. Nevertheless we will use the same language: Grothendieck groups and decomposition maps.

Definition 16.1. Let A be a ring and W an A-module of finite length, that is, W has a composition series. An A-module S is called a *composition factor* of W, if S is isomorphic to a composition factor of W.

Lemma 16.2. Let M and N be $\mathcal{O}G$-lattices of V and $\mathfrak{p}$ a nonzero prime ideal of $\mathcal{O}$. Then $M/\mathfrak{p}M$ and $N/\mathfrak{p}N$ have the same composition factors as $k_{\mathfrak{p}}G$-modules (up to isomorphism and counted with multiplicities).

Proof. This is proven in [CR81, (16.16) Proposition] in the setting of p-modular systems. It is easy to see that it also holds in the present situation. □

Definition 16.3. Let A be a ring. We define the *Grothendieck group* $\mathrm{G}_0(A)$ to be the group generated by the isomorphism classes $[X]$ of finitely generated A-modules X, with relations of the form

$$[X] = [Y] + [Z],$$

for every exact sequence

$$0 \longrightarrow Y \longrightarrow X \longrightarrow Z \longrightarrow 0$$

of finitely generated A-modules.

Remark 16.4. The definition of G_0 actually boils down to the following important fact: Two finitely generated A-modules U and W of finite length satisfy $[U] = [W]$ in $\mathrm{G}_0(A)$ if and only if U and W have the same composition factors counted with multiplicities. In particular, if A is semisimple, then $[U] = [W]$ if and only if U and W are isomorphic as A-modules.

Definition 16.5. Let A be a ring and $[X] \in \mathrm{G}_0(A)$, where X has finite length. We define the *composition factors* of $[X]$ to be the composition factors of X. In case A is a finite-dimensional K-module, we also define $\dim_K([X]) = \dim_K(X)$. We call $[X]$ *irreducible* if $[X]$ has only one composition factor. (These notions are well-defined by the previous remark.)

Definition 16.6. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}$. We define

$$\mathrm{d}_{\mathfrak{p}} \colon \mathrm{G}_0(KG) \longrightarrow \mathrm{G}_0(k_{\mathfrak{p}}G),\ [W] \longmapsto [N/\mathfrak{p}N],$$

where N is an $\mathcal{O}G$-lattice of W, to be the *decomposition map at* $\mathfrak{p}$ (this map is well-defined by Lemma 16.2). We call $\mathrm{d}_{\mathfrak{p}}([W])$ the *reduction of* W *at* $\mathfrak{p}$. Moreover we set

$$\mathrm{D}_W(\mathfrak{p}) = \{\dim_{k_{\mathfrak{p}}}(S) \mid S \text{ is a composition factor of } \mathrm{d}_{\mathfrak{p}}([W])\}.$$

Our aim will now be an explicit description of $\bigcup_{\mathfrak{p}} \mathrm{D}_V(\mathfrak{p})$, where $\mathfrak{p}$ runs through all nonzero prime ideals of $\mathcal{O}$. While a single set $\mathrm{D}_V(\mathfrak{p})$ can be computed in finite time, it is not clear that the same holds for $\bigcup_{\mathfrak{p}} \mathrm{D}_V(\mathfrak{p})$. Actually we only need a description of $\bigcup_{\mathfrak{p}\notin S} \mathrm{D}_V(\mathfrak{p})$, for some finite set S, since we can compute $\bigcup_{\mathfrak{p}\in S} \mathrm{D}_V(\mathfrak{p})$ in finite time.

Remark 16.7. In case V is absolutely irreducible, for every nonzero prime ideal $\mathfrak{p}$ not dividing the group order we know by a theorem of Brauer and Nesbitt ([BN41, Theorem 1]) that $\mathrm{d}_{\mathfrak{p}}([V])$ is irreducible and therefore $\mathrm{D}_V(\mathfrak{p}) = \{n\}$. Thus in this case we have

$$\mathrm{D}_V(\mathfrak{p}) = \{n\} \cup \bigcup_{\mathfrak{p} \mid \#G} \mathrm{D}_V(\mathfrak{p}).$$

If V is merely irreducible, the situation gets much more involved as the reduction $\mathrm{d}_{\mathfrak{p}}([V])$ will not be irreducible in general, even if the prime ideal $\mathfrak{p}$ does not divide the group order. We illustrate this with a simple but highly instructive example.

Example 16.8. Consider the cyclic group $G = C_\ell$ of prime order ℓ with rational group algebra isomorphic to $\mathbf{Q}[X]/(X^\ell - 1) \cong \mathbf{Q}[X]/(\Phi_\ell) \times \mathbf{Q}[X]/(X-1)$, where $\Phi_\ell \in \mathbf{Z}[X]$ denotes the ℓ-th cyclotomic polynomial. Let V be $\mathbf{Q}[X]/(\Phi_\ell)$, which is an irreducible (but not absolutely irreducible) $\mathbf{Q}G$-module with $\mathbf{Z}G$-lattice $M = \mathbf{Z}[X]/(\Phi_\ell)$. We wish to determine $\mathrm{d}_{p\mathbf{Z}}([V])$ and $\mathrm{D}_V(p\mathbf{Z})$ for all primes $p \neq \ell$. (Here $S = \{\ell\}$ is the set of primes which need special treatment). This is done by reducing the $\mathbf{Z}G$-lattice M modulo $p\mathbf{Z}$ yielding

$$M/pM \cong \mathbf{F}_p[X]/(\overline{\Phi_\ell}) \cong \prod_{i=1}^{g} \mathbf{F}_p[X]/(\overline{f_i}^{n_i}),$$

where $\overline{\Phi_\ell} = \prod_{i=1}^{g} \overline{f_i}^{n_i}$ is the decomposition into irreducible pairwise non-associated polynomials $\overline{f_i} \in \mathbf{F}_p[X]$. In particular $\mathrm{d}_{(p)}([V])$ depends only on the factorization of Φ_ℓ modulo p. But we know that $\overline{\Phi_\ell}$ is equal to the product of $(\ell-1)/f$ distinct irreducible polynomials of $\mathbf{F}_p[X]$ of degree f, where f denotes the order of p modulo ℓ. (This is just the decomposition law of primes in the cyclotomic extension $\mathbf{Q}(\zeta_\ell)|\mathbf{Q}$.) In particular we obtain

$$\mathrm{D}_V(p\mathbf{Z}) = \{\text{order of } p \text{ modulo } \ell\} = \{f_{\mathbf{Q}(\zeta_\ell)|\mathbf{Q}}(p)\},$$

where $f_{\mathbf{Q}(\zeta_\ell)|\mathbf{Q}}(p)$ is the inertia degree of p in the abelian extension $\mathbf{Q}(\zeta_\ell)|\mathbf{Q}$. For example, if $\ell = 7$, then

$$\mathrm{D}_V(p\mathbf{Z}) = \begin{cases} \{1\}, & p \equiv 1 \bmod 7, \\ \{3\}, & p \equiv 2, 4 \bmod 7, \\ \{6\}, & p \equiv 3, 5 \bmod 7, \\ \{2\}, & p \equiv 6 \bmod 7. \end{cases}$$

(By appealing to Chebotarev's density theorem, we could even quantify for how many primes which type of decomposition occurs asymptotically.)

We see that for this particular representation, the decomposition modulo $\mathfrak{p}$ can be characterized purely by congruence conditions. In this situation the corresponding simple component of the group algebra is an abelian extension of $\mathbf{Q}$ and therefore decomposition modulo $\mathfrak{p}$ is closely related to decomposition of prime ideals in this abelian extension. In general the simple component is neither an abelian extension nor a field extension of the ground field, but merely some matrix algebra over a division ring. Yet we will see that there exists a closed formula for $\mathrm{D}_V(\mathfrak{p})$ in terms of basic invariants of V and $\mathfrak{p}$ for almost all $\mathfrak{p}$. To obtain this formula, we need more representation theory. In particular we need the theory of splitting fields and Schur indices as described for example in [Isa06].

Definition 16.9.

(i) If k is a field and W a kG-module, we denote by $\chi_W\colon G \to k$ the k-character of G associated to W and by $m_k(\chi)$ the Schur index of χ over k. We denote by $\mathrm{Irr}_k(G)$ the set of all irreducible k-characters of G. If $\mathrm{char}(k) = 0$, $L|k$ is a field extension and $\theta \in \mathrm{Irr}_L(G)$ an irreducible character of G over L, we call θ a *constituent* of χ, if θ is a constituent of χ considered as a character of G over L.

(ii) If $L|k$ is a field extension and $f\colon X \to L$ a map, we define

$$k(f) = k(f(x) \,|\, x \in X) \subseteq L.$$

(In case $\chi\colon G \to L$ is a character, the field $k(\chi)$ is the usual character field.)

(iii) If $R \subseteq \tilde{R}$ is an extension of commutative rings, A an R-algebra and W an A-module, we denote by $W^{\tilde{R}}$ the $\tilde{R} \otimes_R A$-module $\tilde{R} \otimes_R W$. Thus, in our setting, if $L|K$ is a field extension, then V^L is the LG-module obtained by extending scalars from K to L.

A key ingredient for computing D_V will be the extension of scalars to a splitting field and the following lemma, which will allow us to pass down again and to get information in our original situation. This statement can be found in [Isa06, Corollary 9.23]. We formulate it in the language of modules.

Lemma 16.10. Let k be a field of prime characteristic and $L|k$ a field extension. Let U be an irreducible LG-module. Let W be an irreducible kG-module, such that U is a constituent of W^L. Then

$$\dim_k(W) = [k(\chi_U) : k] \cdot \dim_L(U).$$

Hence in prime characteristic, as soon as we know the dimension of an irreducible constituent in a larger field and the character (field) thereof, we can compute the dimension. We begin with a general statement on $\mathrm{D}_V(\mathfrak{p})$, which will be refined step by step.

Theorem 16.11. Let $\chi \in \mathrm{Irr}_{\mathbf{C}}(G)$ be an irreducible constituent of $\chi_V\colon G \to \mathbf{C}$. Then the following hold:

(i) If $m_K(\chi) > 1$, then for all nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}$ the following hold: For all $x \in \mathrm{D}_V(\mathfrak{p})$ we have $x < \dim_K(V)$.

(ii) If $m_K(\chi) = 1$, then for all nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}$ the following hold: For all $x \in \mathrm{D}_V(\mathfrak{p})$ we have

$$x \leq \frac{f_{K(\chi)|K}(\mathfrak{p})}{[K(\chi) : K]} \dim_K(V),$$

where $K(\chi)$ is the character field of χ and $f_{K(\chi)|K}(\mathfrak{p})$ the inertia degree of $\mathfrak{p}$ in the abelian extension $K(\chi)|K$.

Proof. Let $L \supseteq K$ be a splitting field of χ with $[L : K(\chi)] = m_K(\chi)$. We set $m = m_K(\chi)$. By the theory of the Schur index, we know that $\chi_V = m(\chi_1 + \cdots + \chi_l)$, where $\chi = \chi_1, \chi_2, \ldots, \chi_l$ are the distinct Galois conjugates of χ over K so that $l = [K(\chi) : K]$. On the module side this implies $V^L \cong \bigoplus_{i=1}^l V_i^{\oplus m}$, for (absolutely) irreducible LG-modules $V_1, \ldots, V_l$. We order the modules such that $\chi_{V_i} = \chi_i$ for all $i = 1, \ldots, l$. Now let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$ lying above $\mathfrak{p}$ with associated residue field $k_{\mathfrak{P}} = \mathcal{O}_L/\mathfrak{P}$ and canonical surjection

$$\pi_{\mathfrak{P}}\colon \mathcal{O}_L \longrightarrow k_{\mathfrak{P}}.$$

We have a residue field extension $k_{\mathfrak{p}} \subseteq k_{\mathfrak{P}}$ of degree $f_{L|K}(\mathfrak{P}|\mathfrak{p})$ and the following commutative diagram:

$$\begin{tikzcd}
\mathrm{G}_0(LG) \arrow[r, "\mathrm{d}_{\mathfrak{P}}"] & \mathrm{G}_0(k_{\mathfrak{P}}G) \\
\mathrm{G}_0(KG) \arrow[r, "\mathrm{d}_{\mathfrak{p}}"] \arrow[u, "(-)^L"] & \mathrm{G}_0(k_{\mathfrak{p}}G) \arrow[u, "(-)^{k_{\mathfrak{P}}}"']
\end{tikzcd}$$

Let $\mathrm{d}_{\mathfrak{p}}([V]) = \sum_{i=1}^{r}[S_i]$ with irreducible $k_{\mathfrak{p}}G$-modules S_i and $\mathrm{d}_{\mathfrak{P}}([V^L]) = \sum_{j=1}^{t}[T_j]$ with irreducible $k_{\mathfrak{P}}G$-modules T_j. Then in $\mathrm{G}_0(k_{\mathfrak{P}}G)$ we have the following equality:

$$\sum_{i=1}^{r}[S_i^{k_{\mathfrak{P}}}] = \mathrm{d}_{\mathfrak{p}}([V])^{k_{\mathfrak{P}}} = \mathrm{d}_{\mathfrak{P}}([V^L]) = \sum_{j=1}^{t}[T_j] = m\sum_{i=1}^{l}\mathrm{d}_{\mathfrak{P}}([V_i]).$$

We want to use Lemma 16.10 to compute the dimensions of the S_i. To do this, let us fix a composition factor S_i of $\mathrm{d}_{\mathfrak{p}}([V])$. Then by the above consideration, we know that there exists V_j such that $\mathrm{d}_{\mathfrak{P}}([V_j])$ and $[S_i^{k_{\mathfrak{P}}}]$ have a common composition factor. (Since $\mathfrak{P}$ is an arbitrary nonzero prime ideal, the reductions of the absolutely irreducible LG-modules V_j need not be irreducible.)
(i): Assume that $\mathrm{d}_{\mathfrak{P}}([V_j])$ is not irreducible and let T_k be a common composition factor of $\mathrm{d}_{\mathfrak{p}}([V_j])$ and $S_i^{k_{\mathfrak{P}}}$. Then using Lemma 16.10 we have

$$\begin{aligned}\dim_{k_{\mathfrak{p}}}(S_i) &= [k_{\mathfrak{p}}(\chi_{T_k}) : k_{\mathfrak{p}}] \cdot \dim_{k_{\mathfrak{P}}}(T_k)\\ &\leq [k_{\mathfrak{P}} : k_{\mathfrak{p}}] \cdot \dim_{k_{\mathfrak{P}}}(T_k)\\ &< f_{L|K}(\mathfrak{P}|\mathfrak{p}) \cdot \dim_{k_{\mathfrak{P}}}(\mathrm{d}_{\mathfrak{P}}([V_j]))\\ &= f_{L|K}(\mathfrak{P}|\mathfrak{p}) \cdot \dim_L(V_j)\\ &\leq [L : K] \cdot \frac{\dim_K(V)}{[K(\chi) : K] \cdot [L : K(\chi)]}\\ &= \dim_K(V).\end{aligned}$$

Now assume that $\mathrm{d}_{\mathfrak{P}}([V_j])$ is irreducible and let $\mathfrak{q} = \mathfrak{P} \cap K(\chi)$ be the prime ideal of $\mathcal{O}_{K(\chi)}$ lying below $\mathfrak{P}$ and above $\mathfrak{p}$. Then the character of $\mathrm{d}_{\mathfrak{P}}([V_j])$ is just the composition

$$G \xrightarrow{\chi_j} \mathcal{O}_{K(\chi)} \xrightarrow{\pi_{\mathfrak{q}}} k_{\mathfrak{q}},$$

with $\pi_{\mathfrak{q}}$ the canonical projection $\pi_{\mathfrak{q}} \colon \mathcal{O}_{K(\chi)} \to k_{\mathfrak{q}}$. In particular $k_{\mathfrak{p}}(\chi_{\mathrm{d}_{\mathfrak{P}}([V_j])}) \subseteq k_{\mathfrak{q}}$. As $\mathrm{d}_{\mathfrak{P}}([V_j])$ is a composition factor of $S_i^{k_{\mathfrak{P}}}$, by using Lemma 16.10 we obtain

$$\begin{aligned}\dim_{k_{\mathfrak{p}}}(S_i) &= [k_{\mathfrak{p}}(\chi_{\mathrm{d}_{\mathfrak{P}}([V_j])}) : k_{\mathfrak{p}}] \cdot \dim_{k_{\mathfrak{P}}}(\mathrm{d}_{\mathfrak{P}}([V_i]))\\ &\leq [k_{\mathfrak{q}} : k_{\mathfrak{p}}] \cdot \dim_L(V_i)\\ &= f_{K(\chi)|K)}(\mathfrak{p}) \cdot \frac{\dim_K(V)}{m \cdot [K(\chi) : K]}\\ &\leq \frac{\dim_K(V)}{m}\\ &< \dim_K(V).\end{aligned}$$

(ii): Assume that the $k_{\mathfrak{p}}G$-module T_k is a composition factor of $\mathrm{d}_{\mathfrak{P}}([V_j])$ and $S_i^{k_{\mathfrak{P}}}$. Then by Lemma 16.10 we obtain

$$\begin{aligned}\dim_{k_{\mathfrak{p}}}(S_i) &= [k_{\mathfrak{p}}(\chi_{T_k}) : k_{\mathfrak{p}}] \cdot \dim_{k_{\mathfrak{P}}}(T_k)\\ &\leq [k_{\mathfrak{P}} : k_{\mathfrak{p}}] \cdot \dim_{k_{\mathfrak{P}}}(\mathrm{d}_{\mathfrak{P}}([V_j])\\ &= f_{L|K}(\mathfrak{P}|\mathfrak{p}) \cdot \frac{\dim_K(V)}{[L : K]}.\end{aligned}$$

Since $m_K(\chi) = 1$ we have $L = K(\chi)$ and the claim follows. □

Lemma 16.12. Let $\chi \in \mathrm{Irr}_{\mathbf{C}}(G)$ be an irreducible constituent of χ_V. For each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$ with $\#G \notin \mathfrak{p}$ and every prime ideal $\mathfrak{q}$ of $\mathcal{O}_{K(\chi)}$ lying above $\mathfrak{p}$ we have

$$\mathrm{D}_V(\mathfrak{p}) = \left\{ \frac{[k_{\mathfrak{p}}(\pi_{\mathfrak{q}} \circ \chi^{\sigma}) : k_{\mathfrak{p}}]}{[K(\chi) : K] \cdot m_K(\chi)} \cdot \dim_K(V) \;\middle|\; \sigma \in \mathrm{Gal}(K(\chi)|K) \right\},$$

where for $\sigma \in \mathrm{Gal}(K(\chi)|K)$ we denote by χ^{σ} the associated Galois conjugate of χ.

Proof. We use the same notation as in the previous proof. In particular $\mathfrak{q}$ is the prime ideal of $\mathcal{O}_{K(\chi)}$ lying between $\mathfrak{p}$ and $\mathfrak{P}$. Since $\#G \notin \mathfrak{P}$, we know that $\mathrm{d}_{\mathfrak{P}}([V_i])$ is irreducible for $i = 1, \dots, l$. Thus if the $k_{\mathfrak{p}}G$-module S is a composition factor of $\mathrm{d}_{\mathfrak{p}}([V])$, we know that there exists V_i such that $\mathrm{d}_{\mathfrak{P}}([V_i])$ is a composition factor of $S^{k_{\mathfrak{P}}}$. Vice versa for every V_i there exists a composition factor S of $\mathrm{d}_{\mathfrak{p}}([V])$ such that $\mathrm{d}_{\mathfrak{P}}([V_i])$ is a composition factor of $S^{k_{\mathfrak{P}}}$. Since in this case we have (as in the proof of Theorem 16.11)

$$\dim_{k_{\mathfrak{p}}}(S) = [k_{\mathfrak{p}}(\pi_{\mathfrak{q}} \circ \chi_i) : k_{\mathfrak{p}}] \cdot \dim_{k_{\mathfrak{P}}}(\mathrm{d}_{\mathfrak{P}}([V_i])) = \frac{[k_{\mathfrak{p}}(\pi_{\mathfrak{q}} \circ \chi_i) : k_{\mathfrak{p}}]}{[K(\chi) : K] \cdot m_K(\chi)} \cdot \dim_K(V),$$

the claim follows by noting that $\{\chi_1, \dots, \chi_l\} = \{\chi^\sigma \mid \sigma \in \mathrm{Gal}(K(\chi)|K)\}$. □

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$ and $\mathfrak{q}$ a prime ideal of $\mathcal{O}_{K(\chi)}$ lying above $\mathfrak{p}$. Recall that for each $\sigma \in \mathrm{Gal}(K(\chi)|K)$ the ideal $\sigma(\mathfrak{q})$ is also a prime ideal of $\mathcal{O}_{K(\chi)}$ lying above $\mathfrak{p}$ and we have an induced isomorphism of $k_{\mathfrak{p}}$-algebras

$$\overline{\sigma}_{\mathfrak{q}} : k_{\mathfrak{q}} \longrightarrow k_{\sigma(\mathfrak{q})},$$

making the diagram

$$\begin{tikzcd}
\mathcal{O}_{K(\chi)} \arrow[r, "\pi_{\mathfrak{q}}"] \arrow[d, "\sigma"] & k_{\mathfrak{q}} \arrow[d, "\overline{\sigma}_{\mathfrak{q}}"] \\
\mathcal{O}_{K(\chi)} \arrow[r, "\pi_{\sigma(\mathfrak{q})}"] & k_{\sigma(\mathfrak{q})}
\end{tikzcd}$$

commute.

Lemma 16.13. Let $\chi \in \mathrm{Irr}_{\mathbf{C}}(G)$ be an irreducible constituent of χ_V. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}$ with $\#G \notin \mathfrak{p}$ and $\mathfrak{q}$ a prime ideal of $\mathcal{O}_{K(\chi)}$ lying above $\mathfrak{p}$. Then the following hold:

(i) For all $\tau, \sigma \in \mathrm{Gal}(K(\chi)|K)$ we have

$$[k_{\mathfrak{p}}(\pi_{\mathfrak{q}} \circ \chi^\sigma) : k_{\mathfrak{p}}] = [k_{\mathfrak{p}}(\pi_{\tau(\mathfrak{q})} \circ \chi^{\tau\sigma}) : k_{\mathfrak{p}}].$$

(ii) We have

$$\mathrm{D}_V(\mathfrak{p}) = \left\{ \frac{[k_{\mathfrak{p}}(\pi_{\sigma(\mathfrak{q})} \circ \chi) : k_{\mathfrak{p}}]}{[K(\chi) : K] \cdot m_K(\chi)} \cdot \dim_K(V) \,\middle|\, \sigma \in \mathrm{Gal}(K(\chi)|K) \right\}.$$

Proof. (i): We have

$$\overline{\tau}_{\mathfrak{q}}(k_{\mathfrak{p}}(\pi_{\mathfrak{q}} \circ \chi^\sigma)) = k_{\mathfrak{p}}(\overline{\tau}_{\mathfrak{q}} \circ \pi_{\mathfrak{q}} \circ \chi^\sigma) = k_{\mathfrak{p}}(\pi_{\tau(\mathfrak{q})} \circ \tau \circ \chi^\sigma) = k_{\mathfrak{p}}(\pi_{\tau(\mathfrak{q})} \circ \chi^{\tau\sigma}).$$

Since $\overline{\tau}_{\mathfrak{q}}$ is an isomorphism of $k_{\mathfrak{p}}$-algebras, the claim follows.
(ii): By (i) we have

$$[k_{\mathfrak{p}}(\pi_{\sigma(\mathfrak{q})} \circ \chi) : k_{\mathfrak{p}}] = [k_{\mathfrak{p}}(\pi_{\mathfrak{q}} \circ \chi^{\sigma^{-1}}) : k_{\mathfrak{p}}]$$

and therefore

$$\begin{aligned}
\{[k_{\mathfrak{p}}(\pi_{\sigma(\mathfrak{q})} \circ \chi) : k_{\mathfrak{p}}] \mid \sigma \in \mathrm{Gal}(K(\chi)|K)\} &= \{[k_{\mathfrak{p}}(\pi_{\mathfrak{q}} \circ \chi^{\sigma^{-1}}) : k_{\mathfrak{p}}] \mid \sigma \in \mathrm{Gal}(K(\chi)|K)\} \\
&= \{[k_{\mathfrak{p}}(\pi_{\mathfrak{q}} \circ \chi^{\sigma}) : k_{\mathfrak{p}}] \mid \sigma \in \mathrm{Gal}(K(\chi)|K)\}.
\end{aligned}$$

Now the claim follows from Lemma 16.12 □

The next lemma will help us to simplify the terms $[k_{\mathfrak{p}}(\pi_{\sigma(\mathfrak{q})} \circ \chi) : k_{\mathfrak{p}}]$.

Lemma 16.14. Let $E|K$ be a finite abelian extension and $\alpha_1, \dots, \alpha_r \in \mathcal{O}_E$ integral elements such that $E = K(\alpha_1, \dots, \alpha_r)$. Then there exists an explicitly computable set $S \subseteq \mathrm{Spec}(\mathcal{O})$ such that for all nonzero prime ideals $\mathfrak{p} \notin S$ the following hold: For all prime ideals $\mathfrak{q}$ of $\mathcal{O}_E$ lying above $\mathfrak{p}$ we have

$$[k_{\mathfrak{p}}(\pi_{\mathfrak{q}}(\alpha_1), \dots, \pi_{\mathfrak{q}}(\alpha_r)) : k_{\mathfrak{p}}] = f_{E|K}(\mathfrak{p}).$$

Proof. The theorem of Sonn–Zassenhaus ([SZ67]) shows that there exist $\mu_1, \ldots, \mu_r \in \{0,1\}$ such that the element $\beta = \mu_1\alpha_1 + \cdots + \mu_r\alpha_r \in E$ is a primitive element of the extension $E|K$. In particular we may assume that $\mu_i \in \mathcal{O}_E$ for all $1 \leq i \leq r$, implying that

$$\mathcal{O}[\beta] \subseteq \mathcal{O}[\alpha_1, \ldots, \alpha_r] \subseteq \mathcal{O}_E.$$

Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}$ not dividing the index $m = |\mathcal{O}_E : \mathcal{O}[\beta]|$, and $\mathfrak{q}$ a prime ideal of $\mathcal{O}_E$ lying above $\mathfrak{p}$. According to the theorem of Kummer–Dedekind, we know that

$$[k_{\mathfrak{p}}(\pi_{\mathfrak{q}}(\beta)) : k_{\mathfrak{p}}] = f_{E|K}(\mathfrak{p}).$$

Thus it is sufficient to show that $k_{\mathfrak{p}}(\pi_{\mathfrak{q}}(\beta)) = k_{\mathfrak{p}}(\pi_{\mathfrak{q}}(\alpha_1), \ldots, \pi_{\mathfrak{q}}(\alpha_r))$. One of the inclusions being trivial, we have to show that $\pi_{\mathfrak{q}}(\alpha_i) \in k_{\mathfrak{p}}(\pi_{\mathfrak{q}}(\beta))$ for all $1 \leq i \leq r$. But this follows from $m\mathcal{O}[\alpha_1, \ldots, \alpha_r] \subseteq m\mathcal{O}_E \subseteq \mathcal{O}[\beta]$ and the fact that $\pi_{\mathfrak{q}}(m) \in k_{\mathfrak{p}}^{\times}$. □

Theorem 16.15. There exists an explicitly computable finite set S of prime ideals of $\mathfrak{p}$ of $\mathcal{O}$, such that for all prime ideals $\mathfrak{p} \notin S$ we have $\#G \notin \mathfrak{p}$ and

$$\mathrm{D}_V(\mathfrak{p}) = \left\{ \frac{f_{K(\chi)|K}(\mathfrak{p})}{[K(\chi) : K] \cdot m_K(\chi)} \cdot \dim_K(V) \right\},$$

Proof. By applying Lemma 16.14 to $E = K(\chi) = K(\chi(g) \mid g \in G)$ (with $\{\alpha_1, \ldots, \alpha_r\} = \{\chi(g) \mid g \in G\}$) we obtain a finite set S_0 of nonzero prime ideals such that $[k_{\mathfrak{p}}(\pi_{\mathfrak{q}} \circ \chi) : k_{\mathfrak{p}}] = [k_{\mathfrak{p}}(\pi_{\mathfrak{q}}(\chi(g)) \mid g \in G) : k_{\mathfrak{p}}] = f_{K(\chi)|K}(\mathfrak{p})$ for $\mathfrak{p} \notin S_0$ and all nonzero prime ideals $\mathfrak{q}$ of $\mathcal{O}_{K(\chi)}$ lying above $\mathfrak{p}$. Setting $S = S_0 \cup \{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}) \mid \#G \notin \mathfrak{p}\}$, the theorem now follows from Lemma 16.13. □

We end this section by answering the following basic question: Given an irreducible KG-module V, does there exist a prime ideal $\mathfrak{p}$ such that $\mathrm{d}_{\mathfrak{p}}([V])$ is irreducible? And if this is the case, how many prime ideals are there with this property?

Corollary 16.16. Let V be an absolutely irreducible KG-module. Then for almost all prime ideals $\mathfrak{p}$ of $\mathcal{O}$ the reduction $\mathrm{d}_{\mathfrak{p}}([V])$ is irreducible.

Proof. This is a well known consequence of the theorem of Brauer–Nesbitt. □

Corollary 16.17. Let V be an irreducible KG-module which is not absolutely irreducible. Assume that $\chi \in \mathrm{Irr}_{\mathbf{C}}(G)$ is an irreducible constituent of χ_V. If $m_K(\chi) > 1$, then $\mathrm{d}_{\mathfrak{p}}(V)$ is reducible for all nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}$.

Proof. This is Theorem 16.11 (i). □

Corollary 16.18. Let V be an irreducible KG-module which is not absolutely irreducible. Assume that $\chi \in \mathrm{Irr}_{\mathbf{C}}(G)$ is an irreducible constituent of χ_V. If $m_K(\chi) = 1$, then the following are equivalent:

(i) There exists a prime ideal $\mathfrak{p}$ of $\mathcal{O}$ such that $\mathrm{d}_{\mathfrak{p}}([V])$ is irreducible.
(ii) There are infinitely many prime ideals $\mathfrak{p}$ of $\mathcal{O}$ such that $\mathrm{d}_{\mathfrak{p}}([V])$ is irreducible.
(iii) The abelian extension $K(\chi)|K$ is cyclic.

Proof. (i)⇒(iii): Assume that $\mathrm{d}_{\mathfrak{p}}([V])$ is irreducible at $\mathfrak{p}$. Then by Theorem 16.11 (ii) we know that $f_{K(\chi)|K}(\mathfrak{p}) = [K(\chi) : K]$, that is, $\mathfrak{p}$ is inert in $K(\chi)$. This implies that the Frobenius automorphism corresponding to $\mathfrak{p}$—which is an element of $\mathrm{Gal}(K(\chi)|K)$—has order $f_{K(\chi)|K}(\mathfrak{p}) = [K(\chi) : K] = |\mathrm{Gal}(K(\chi)|K)|$.
(iii)⇒(ii): Let S be a set as in Theorem 16.15. Since $K(\chi)|K$ is cyclic, the Galois group contains an element of order $[K(\chi) : K]$. By the Chebotarev density theorem this implies, that there are infinitely many prime ideals $\mathfrak{p}$ of $\mathcal{O}$ with $\mathfrak{p} \notin S$ and $f_{K(\chi)|K}(\mathfrak{p}) = [K(\chi) : K]$ (since S is finite). Now (ii) follows from Theorem 16.15.
(ii)⇒(i): Trivial. □

Corollary 16.19. Let χ be an irreducible constituent of χ_V. Then there exists an explicitly computable finite set $S \subseteq \mathrm{Spec}(\mathcal{O})$ such that

$$\mathrm{D}_V(\mathrm{Spec}(\mathcal{O})\backslash S) = \{\mathrm{ord}(\sigma) \cdot \deg(\chi) \mid \sigma \in \mathrm{Gal}(K(\chi)|K)\}.$$

Moreover, for each $\sigma \in \mathrm{Gal}(K(\chi)|K)$, the fiber $\mathrm{D}_V^{-1}(\{\mathrm{ord}(\sigma) \cdot \deg(\chi)\})$ is infinite.

Proof. Let S be as in Theorem 16.15, enlarged to contain the zero ideal and the prime ideals of $\mathcal{O}$ which ramify in $K(\chi)|K$. For all $\mathfrak{p} \notin S$ we have $\mathrm{ord}(\mathrm{Frob}_{K(\chi)|K}(\mathfrak{p})) = f_{K(\chi)|K}(\mathfrak{p})$ and for a given $\sigma \in \mathrm{Gal}(K(\chi)|K)$ there are infinitely many $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O})$ with $\mathrm{Frob}_{K(\chi)|K}(\mathfrak{p}) = \sigma$. As $\deg(\chi) = \dim_K(V)/([K(\chi) : K] \cdot m_K(\chi))$ the claim follows. □

Reduction at prime ideals in ideal classes. In the previous section we have seen that there exists an explicitly computable finite set of prime ideals S, such that $\mathrm{D}_V(\mathrm{Spec}(\mathcal{O})\backslash S)$ can be described purely in terms of the invariants of an irreducible constituent $\chi \in \mathrm{Irr}_{\mathbf{C}}(G)$ of χ_V and the local behavior of the abelian extension $K(\chi)|K$. In particular this allows us to algorithmically determine $\mathrm{D}_V(\mathrm{Spec}(\mathcal{O})) = \mathrm{D}_V(\mathrm{Spec}(\mathcal{O})\backslash S) \cup \mathrm{D}_V(S)$.

For our application to the question of integrality, this is not enough. Although we now know in principle

$$\mathrm{D}_V(\mathrm{Spec}(\mathcal{O})) = \{n \in \mathbf{Z} \mid (M : N) = \mathfrak{p}^n \text{ for some } N \in \mathcal{L}^{\max}(M) \text{ and } \mathfrak{p} \in \mathrm{Spec}(\mathcal{O})\,\},$$

that is, we know the exponents of the index ideals with respect to the particular $\mathfrak{p}$, this is not sufficient. We need to understand the Steinitz classes of the index ideals $[(M : N)]$ as N ranges through $\mathcal{L}^{\max}(M)$, the set of all maximal sublattices of M. What we really need are the exponents of the index ideals of $\mathfrak{p}$-maximal sublattices, where $\mathfrak{p}$ is restricted to lie in an fixed ideal class of $\mathcal{O}$. Thus we want to describe $\mathrm{D}_V(\mathfrak{C} \cap \mathrm{Spec}(\mathcal{O}))$, where $\mathfrak{C}$ is an ideal class of $\mathcal{O}$. Using this and Lemma 8.4 we then have

$$\{\mathfrak{C}^n \mid n \in \mathrm{D}_V(\mathfrak{C} \cap \mathrm{Spec}(\mathcal{O}))\} = \{\, [(M : N)] \mid N \in \mathcal{L}_{\mathfrak{p}}^{\max}(M) \text{ for some } \mathfrak{p} \in \mathfrak{C}\,\}$$

and consequently using Lemma 8.3 we obtain

$$\begin{aligned} \mathrm{cl}(\mathcal{L}^{\max}(M)) &= \mathrm{cl}(M) \cdot \bigcup\nolimits_{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O})} \{\, [(M : N)] \mid N \in \mathcal{L}_{\mathfrak{p}}^{\max}(M)\} \\ &= \mathrm{cl}(M) \cdot \bigcup\nolimits_{\mathfrak{C} \in \mathrm{Cl}_K} \{\, [(M : N)] \mid N \in \mathcal{L}_{\mathfrak{p}}^{\max}(M) \text{ for some } \mathfrak{p} \in \mathfrak{C}\,\} \\ &= \mathrm{cl}(M) \cdot \bigcup\nolimits_{\mathfrak{C} \in \mathrm{Cl}_K} \{\mathfrak{C}^n \mid n \in \mathrm{D}_V(\mathfrak{C} \cap \mathrm{Spec}(\mathcal{O}))\,\}. \end{aligned}$$

To get the refined information $\mathrm{D}_V(\mathfrak{C} \cap \mathrm{Spec}(\mathcal{O}))$, we make the following observation: Apart from a contribution from an irreducible complex constituent of χ_V, for almost all prime ideals $\mathfrak{p}$ the value of $\mathrm{D}_V(\mathfrak{p})$ depends only on $f_{K(\chi)|K}(\mathfrak{p}) = \mathrm{ord}(\mathrm{Frob}_{K(\chi)|K}(\mathfrak{p}))$, where $\mathrm{Frob}_{K(\chi)|K}(\mathfrak{p})$ is the Frobenius automorphism of $K(\chi)|K$ at $\mathfrak{p}$. Fortunately, a similar result holds for the condition $\mathfrak{p} \in \mathfrak{C}$: Denote by H the Hilbert class field of K and by $\tau \in \mathrm{Gal}(H|K)$ the element $\mathrm{Frob}_{H|K}(\mathfrak{q})$ for some $\mathfrak{q} \in \mathfrak{C}$. Then $\mathfrak{p} \in \mathfrak{C}$ if and only if $\mathrm{Frob}_{H|K}(\mathfrak{p}) = \tau$. Thus $\mathrm{D}_V(\mathfrak{C} \cap \mathrm{Spec}(\mathcal{O}))$ can be obtained from the set

$$\{(\mathrm{Frob}_{H|K}(\mathfrak{p}), \mathrm{Frob}_{K(\chi)|K}(\mathfrak{p})) \mid \mathfrak{p} \in \mathrm{Spec}(\mathcal{O})\backslash S\} \subseteq \mathrm{Gal}(H|K) \times \mathrm{Gal}(K(\chi)|K),$$

by intersecting with $\{\tau\} \times \mathrm{Gal}(K(\chi)|K)$, where S is a finite set of prime ideals. To ease the notation we now treat this problem for two arbitrary finite abelian extensions.

Assumption 16.20. For the rest of this section assume that $L_1|K$, $L_2|K$, are abelian extensions of K in a fixed algebraic closure of K with associated Frobenius automorphism $\mathrm{Frob}_{L_i|K}$. For $i = 1, 2$ we denote by $S_i \subseteq \mathrm{Spec}(\mathcal{O})$ the set of ramified prime ideals of $L_i|K$ and set $S_0 = S_1 \cup S_2$.

We now want to describe the "diagonal" Δ of the Frobenius automorphisms defined as

$$\Delta = \{(\mathrm{Frob}_{L_1|K}(\mathfrak{p}), \mathrm{Frob}_{L_2|K}(\mathfrak{p})) \mid \mathfrak{p} \in \mathrm{Spec}(\mathcal{O})\backslash S_0\} \subseteq \mathrm{Gal}(L_1|K) \times \mathrm{Gal}(L_2|K).$$

Lemma 16.21. Let $E = L_1 L_2$ be the compositum, $F = L_1 \cap L_2$ the intersection and

$$\iota\colon \mathrm{Gal}(E|K) \longrightarrow \mathrm{Gal}(L_1|K) \times \mathrm{Gal}(L_2|K),\ \sigma \longmapsto (\sigma|_{L_1}, \sigma|_{L_2})$$

the canonical inclusion. Then the following hold:

(i) We have $\Delta = \mathrm{im}(\iota)$.

(ii) We have

$$\Delta = \{(\sigma_1, \sigma_2) \in \mathrm{Gal}(L_1|K) \times \mathrm{Gal}(L_2|K)) \mid \sigma_1|_F = \sigma_2|_F\}.$$

(iii) We have

$$\Delta = \{(\mathrm{Frob}_{E|K}(\mathfrak{p})|_{L_1}, \mathrm{Frob}_{E|K}(\mathfrak{p})|_{L_2}) \mid \mathfrak{p} \in \mathrm{Spec}(\mathcal{O})\backslash S_0\}.$$

Proof. First note that since E is the compositum of the fields L_1, L_2 the set S_0 is the set of ramified primes of $E|K$. (i), (iii): Using Chebotarev's density theorem we have

$$\mathrm{im}(\iota) = \iota(\mathrm{Gal}(E|K)) = \iota(\{\mathrm{Frob}_{E|K}(\mathfrak{p}) \mid \mathfrak{p} \in \mathrm{Spec}(\mathcal{O})\backslash S_0\}).$$

As $\mathrm{Frob}_{E|K}(\mathfrak{p})|_{L_i} = \mathrm{Frob}_{L_i|K}(\mathfrak{p})$, both claims follow.
(ii): Follows from (i) and Galois theory. □

Lemma 16.22. Let $E = L_1L_2$ be the compositum. Assume that $B \in \mathbf{R}_{>0}$ has the following property: For each $\sigma \in \mathrm{Gal}(E|K)$ there exists $\mathfrak{p}$ with $\mathbf{N}(\mathfrak{p}) \leq B$ and $\mathrm{Frob}_{E|K}(\mathfrak{p}) = \sigma$. Then

$$\Delta = \{(\mathrm{Frob}_{L_1|K}(\mathfrak{p}), \mathrm{Frob}_{L_2|K}(\mathfrak{p})) \mid \mathfrak{p} \in \mathrm{Spec}(\mathcal{O})\backslash S_0,\, \mathbf{N}(\mathfrak{p}) \leq B\}.$$

Proof. This follows from Lemma 16.21 (iii). □

Remark 16.23. Let $E|K$ be any abelian extension. While the Chebotarev density theorem (and the finiteness of $\mathrm{Gal}(E|K)$) guarantees the existence of a number $B_E \in \mathbf{R}_{>0}$ such that

$$\mathrm{Gal}(E|K) = \{\mathrm{Frob}_{E|K}(\mathfrak{p}) \mid \mathfrak{p} \in \mathrm{Spec}(\mathcal{O})\backslash S_0,\, \mathbf{N}(\mathfrak{p}) \leq B_E\},$$

this does not give us any clue on how to find such a B_E given E. A solution to the problem of finding a suitable B_E is usually referred to as the "effective Chebotarev density theorem" and was given by Lagarias, Montgomery and Odlyzko in [LMO79]. They show that there exist explicitly computable constants $A_1, b \in \mathbf{R}_{>0}$ such that we can take

$$B_E = \begin{cases} b(\log(|d_E|))^2, & \text{if GRH is true,} \\ 2|d_E|^{A_1}, & \text{else,} \end{cases}$$

where d_E is the absolute discriminant of E and GRH is the generalized Riemann hypothesis. Note that in [LMO79] a more general statement is proven with $E|K$ any normal extension and elements of $\mathrm{Gal}(E|K)$ being replaced by conjugacy classes.

This easily turns into an algorithm for computing Δ.

Algorithm 16.24. The following steps return Δ.

(i) Compute a bound for d_E, the absolute discriminant of E, and B_E as in Remark 16.23. Denote by S_0 the set of ramified primes of $E|K$.

(ii) Return
$$\{(\mathrm{Frob}_{L_1|K}(\mathfrak{p}), \mathrm{Frob}_{L_2|K}(\mathfrak{p})) \mid \mathfrak{p} \in \mathrm{Spec}(\mathcal{O})\backslash S_0,\, \mathbf{N}(\mathfrak{p}) \leq B_E\}.$$

We now want to describe a second method for computing Δ, which is based on Lemma 16.21 (iii) and (constructive) class field theory. Let us recall some basic facts about class field theory using the classical pre-second world war formulation with moduli and congruence subgroups. We refer the reader to [Jan96] for a complete treatment of this subject.

Recall that $\Sigma_{\mathbf{R}}$ is the set of real infinite places of K. A modulus of K is a pair $(\mathfrak{m}_0, \mathfrak{m}_\infty)$ where $\mathfrak{m}_0$ is an integral ideal of K and $\mathfrak{m}_\infty \subseteq \Sigma_{\mathbf{R}}$ is a set of real places. For an element $\alpha \in K$ we set

$$\alpha \equiv^* 1 \bmod \mathfrak{m} \quad \text{if and only if} \quad v_{\mathfrak{p}}(x-1) \geq v_{\mathfrak{p}}(\mathfrak{m}_0) \text{ for all } \mathfrak{p} \mid \mathfrak{m}_0 \text{ and } i(\alpha) > 0 \text{ for all } i \in \mathfrak{m}_\infty.$$

The ray modulo $\mathfrak{m}$ is defined to be $K_{\mathfrak{m}} = \{\alpha \in K \mid \alpha \equiv^* 1 \bmod \mathfrak{m}\}$ and the ray class group modulo $\mathfrak{m}$ is defined to be $\mathrm{Cl}_{\mathfrak{m}} = I^{\mathfrak{m}}/\iota(K_{\mathfrak{m}})$, where $I^{\mathfrak{m}}$ is the set of fractional ideals with trivial valuations at all prime ideals dividing $\mathfrak{m}_0$ and $\iota(x)$ is the principal ideal generated by $x \in K$. A congruence subgroup modulo $\mathfrak{m}$ is a subgroup U of $\mathrm{Cl}_{\mathfrak{m}}$. The main theorem of class field theory asserts that—among other things—the abelian extensions of K can be parametrized by pairs $(\mathfrak{m}, U)$ consisting of a modulus $\mathfrak{m}$ and a congruence subgroup U modulo $\mathfrak{m}$, modulo an equivalence relation we will not describe here. Moreover, if $L|K$ corresponds to $(\mathfrak{m}, U)$, then there exists an isomorphism

$$\varphi_{L|K,\mathfrak{m}} \colon \mathrm{Cl}_{\mathfrak{m}}/U \longrightarrow \mathrm{Gal}(L|K),$$

(the Artin map), such that for all prime ideals $\mathfrak{p}$ not dividing $\mathfrak{m}$, the element $\varphi_{L|K}([\mathfrak{p}])$ is equal to $\mathrm{Frob}_{L|K}(\mathfrak{p})$.

Lemma 16.25. Assume that for L_1, L_2 we are given moduli $\mathfrak{m}_1$, $\mathfrak{m}_2$ and congruence subgroups $U_i \subseteq \mathrm{Cl}_{\mathfrak{m}_i}$, $i = 1, 2$, and the Artin maps $\varphi_{L_i|K,\mathfrak{m}_i} \colon \mathrm{Cl}_{\mathfrak{m}_i}/U \to \mathrm{Gal}(L_i|K)$. Let $\mathfrak{m} = \mathrm{lcm}(\mathfrak{m}_1, \mathfrak{m}_2)$ and for $i = 1, 2$ denote by φ_i the natural map $\varphi_i \colon \mathrm{Cl}_{\mathfrak{m}} \to \mathrm{Cl}_{\mathfrak{m}_i}/U_i$. Denote by F the intersection $L_1 \cap L_2$. Then the following hold:

(i) For $i = 1, 2$ the diagram

$$\begin{tikzcd}
\mathrm{Cl}_{\mathfrak{m}}/\ker(\varphi_i) \arrow[r] \arrow[rr, bend left, "\varphi_{L_i|K,\mathfrak{m}}"] \arrow[d, "\pi_i"] & \mathrm{Cl}_{\mathfrak{m}_i}/U_i \arrow[r] & \mathrm{Gal}(L_i|K) \arrow[d, "(-)|_F"] \\
\mathrm{Cl}_{\mathfrak{m}}/\langle \ker(\varphi_1), \ker(\varphi_2)\rangle \arrow[rr, "\varphi_{F|K,\mathfrak{m}}"] & & \mathrm{Gal}(F|K)
\end{tikzcd}$$

commutes.

(ii) We have

$$\Delta = \left\{(\varphi_{L_1|K,\mathfrak{m}}(\mathfrak{C}_1), \varphi_{L_2|K,\mathfrak{m}}(\mathfrak{C}_2)) \,\middle|\, (\mathfrak{C}_1, \mathfrak{C}_2) \in (\mathrm{Cl}_\mathfrak{m}/\ker(\varphi_1)) \times (\mathrm{Cl}_\mathfrak{m}/\ker(\varphi_2)),\ \pi_1(\mathfrak{C}_1) = \pi_2(\mathfrak{C}_2)\right\}.$$

Proof. (i): The upper part of the diagram uses the well known fact, that we can always increase the modulus while adjusting the congruence subgroup. Proceeding in this way, for $i = 1, 2$ the abelian extension $L_i|K$ is parametrized by $(\mathfrak{m}, \ker(\varphi_i))$. But then class field theory tells us that $F = L_1 \cap L_2$ is parametrized by $(\mathfrak{m}, \ker(\varphi_1) \cap \ker(\varphi_2))$. By class field theory, the restriction on the Galois group side corresponds to projection on the ray class group side, thus $(-)|_F \circ \varphi_{L_i|K,\mathfrak{m}} = \varphi_{F|K,\mathfrak{m}} \circ \pi_i$.
(ii): Follows immediately from (i) and Lemma 16.21 (ii). □

Remark 16.26. While class field theory itself dates back to the end of the 19th century, computational class field theory is a rather young topic, which emerged in the 1990s. We won't give any details here, but refer the reader to the survey articles [Coh99, CS08] as well as [Coh00]. Note that class field theory is fully under control from an algorithmic point of view. For example, [Fie06] describes how class field theory can be used within the computer algebra system MAGMA.

Let us now come back to the computation of $\mathrm{D}_V(\mathfrak{C} \cap \mathrm{Spec}(\mathcal{O}))$, where $\mathfrak{C} \in \mathrm{Cl}_K$ is a fixed ideal class of K. We view $\mathfrak{C}$ as a subset of I_K, the set of fractional ideals of K.

Algorithm 16.27. Let $\mathfrak{C} \in \mathrm{Cl}_K$ be an ideal class and $\chi \in \mathrm{Irr}_\mathbf{C}(G)$ an irreducible constituent of χ_V. The following steps return a finite set $S \subseteq \mathrm{Spec}(\mathcal{O})$ and $\mathrm{D}_V(\mathfrak{C} \cap (\mathrm{Spec}(\mathcal{O})\backslash S))$.

(i) Let $S \subseteq \mathrm{Spec}(\mathcal{O})$ be as in Theorem 16.15.
(ii) Determine a modulus $\mathfrak{m}$ of K and a congruence subgroup $U \subseteq \mathrm{Cl}_\mathfrak{m}$ such that $K(\chi)|K$ is parametrized by $(\mathfrak{m}, U)$ and compute the Artin map $\varphi_{K(\chi)|K,\mathfrak{m}} \colon \mathrm{Cl}_\mathfrak{m}/U \longrightarrow \mathrm{Gal}(K(\chi)|K)$.
(iii) Let $\mathfrak{n}$ be the trivial modulus of K and H the Hilbert class field (which is parametrized by $(\mathfrak{n}, 1)$). Determine the Artin map $\varphi_{H|K,\mathfrak{n}} \colon \mathrm{Cl}_K \longrightarrow \mathrm{Gal}(H|K)$ and $\tau = \varphi_{H|K,\mathfrak{n}}(\mathfrak{C})$.
(iv) Use Lemma 16.25 to determine

$$\Delta = \{(\mathrm{Frob}_{K(\chi)|K}(\mathfrak{p}), \mathrm{Frob}_{H|K}(\mathfrak{p})) \mid \mathfrak{p} \in \mathrm{Spec}(\mathcal{O})\backslash S\}.$$

(v) Compute

$$T = \{\, \sigma_1 \mid (\sigma_1, \sigma_2) \in \Delta,\ \sigma_2 = \tau\} = \Delta \cap (\mathrm{Gal}(K(\chi)|K) \times \{\tau\}).$$

(vi) Return S and

$$\left\{ \frac{\mathrm{ord}(\sigma)}{[K(\chi):K] \cdot m_K(\chi)} \dim_K(V) \,\middle|\, \sigma \in T \right\}.$$

Theorem 16.28. Algorithm 16.27 is correct.

Proof. First note that $\mathrm{Frob}_{H|K}(\mathfrak{p}) = \tau$ if and only if $\mathfrak{p} \in \mathfrak{C}$. Together with Theorem 16.15 it follows that

$$\begin{aligned} \mathrm{D}_V(\mathfrak{C} \cap (\mathrm{Spec}(\mathcal{O})\backslash S)) &= \left\{ \frac{f_{K(\chi)|K}(\mathfrak{p})}{[K(\chi):K] \cdot m_K(\chi)} \cdot \dim_K(V) \,\middle|\, \mathfrak{p} \in \mathfrak{C} \cap (\mathrm{Spec}(\mathcal{O})\backslash S) \right\} \\ &= \left\{ \frac{\mathrm{ord}(\mathrm{Frob}_{K(\chi)|K}(\mathfrak{p}))}{[K(\chi):K] \cdot m_K(\chi)} \cdot \dim_K(V) \,\middle|\, \mathfrak{p} \in (\mathrm{Spec}(\mathcal{O})\backslash S),\ \mathrm{Frob}_{H|K}(\mathfrak{p}) = \tau \right\} \\ &= \left\{ \frac{\mathrm{ord}(\sigma)}{[K(\chi):K] \cdot m_K(\chi)} \cdot \dim_K(V) \,\middle|\, \sigma \in T \right\}. \end{aligned}$$
□

Remark 16.29. To compute a parametrization of $K(\chi)|K$ one can proceed as follows. One first computes a parametrization $(\mathfrak{m}', U')$ of the abelian extension $\mathbf{Q}(\chi)|\mathbf{Q}$. Note that using the fact that $\mathbf{Q}(\chi) \subseteq \mathbf{Q}(\zeta_{\exp(G)})$ this essentially boils down to finding $\mathrm{Gal}(\mathbf{Q}(\zeta_{\exp(G)})|\mathbf{Q}(\chi))$, for which there exist algorithms. By extending the modulus $\mathfrak{m}'$ of $\mathbf{Q}$ to a modulus $\mathfrak{m}$ of K, we get the following diagram

$$\begin{tikzcd} \mathrm{Cl}_\mathfrak{m} \arrow[r] \arrow[d, "N"] & \mathrm{Gal}(K(\chi)|K) \arrow[d, "(-)|_{\mathbf{Q}(\chi)}"] \\ \mathrm{Cl}_{\mathfrak{m}'}/U' \arrow[r, "\varphi_{\mathbf{Q}(\chi)|\mathbf{Q},\mathfrak{m}'}"] & \mathrm{Gal}(\mathbf{Q}(\chi)|\mathbf{Q}) \end{tikzcd}$$

where N is the map induced by the ideal norm from K to $\mathbf{Q}$. Now the translation theorem tells us that $(\mathfrak{m}, \ker(N))$ is the parametrization of $K(\chi)|K$.

§17. Testing integrality

We will now put everything together and present algorithms for testing integrality.

Using the Eichler condition. When studying the theory of algebras over number fields, one encounters a dichotomy which penetrates large parts of the theory: Algebras which satisfy the Eichler condition and algebras which do not satisfy this condition. The same applies in our case. Under the Eichler condition we are able to provide much better algorithms for testing integrality.

Definition 17.1. A central simple K-algebra A is called a *totally definite quaternion algebra* if

(i) $\dim_K(A) = 4$,
(ii) every infinite place of K is real, that is, K is totally real,
(iii) we have $A_v \cong \mathbf{H}$ for every infinite place v of K, where $\mathbf{H}$ are the Hamilton quaternions (the unique real division algebra of dimension 4).

A central simple K-algebra A satisfies the *Eichler condition*, if and only if A is not a totally definite quaternion algebra. Now let A be a semisimple K-algebra with simple components A_i. Denote by K_i the center of A_i. We say that A satisfies the *Eichler condition*, if and only if the central simple K_i-algebra A_i satisfy the Eichler condition for all i. Finally, if V is an A-module we say that V satisfies the *Eichler condition*, if and only if all A_i with $A_iV \neq \{0\}$ satisfy the Eichler condition (which is equivalent to $\operatorname{End}_A(V)$ satisfying the Eichler condition).

Remark 17.2. There are well known instances when the Eichler condition is satisfied.

(i) Assume that V is an absolutely irreducible A-module. Then V satisfies the Eichler condition.
(ii) Assume that KG is does not satisfy the Eichler condition. Then one of the following groups is a homomorphic image of G (see [Rei03, (38.1)]):
   (a) Generalized quaternion group of order $4n$, $n \geq 2$,
   (b) binary tetrahedral group $|2,3,3|$ of order 24,
   (c) binary octahedral group $|2,3,4|$ or order 48,
   (d) binary icosahedral group $|2,3,5|$ of order 120.

For us the most important property of algebras satisfying the Eichler condition is the following embedding theorem, which is due to Jacobinski [Jac70].

Theorem 17.3. Assume that V is irreducible, satisfies the Eichler condition and M is an $\mathcal{O}G$-lattice of V. Fix a finite set of prime ideals $S \subseteq \operatorname{Spec}(\mathcal{O})$. Then every $\mathcal{O}G$-lattice in the genus of M is isomorphic to an $\mathcal{O}G$-lattice $N \subseteq M$ such that $N \in \mathcal{L}_{\mathfrak{p}}^{\max}(M)$ for some prime ideal $\mathfrak{p} \notin S$. That is, every $\mathcal{O}G$-lattice in the genus of M is isomorphic to a maximal sublattice N of M such that $(M : N)$ is not divisible by a prime ideal in S.

Using this theorem, it is now easy to describe the classes of all lattices in a fixed genus. Recall that $g(M) = \{N \in \mathcal{L}(M) \mid N \vee M\}$ is the set of sublattices which lie in the same genus as M.

Lemma 17.4. Assume that V satisfies the Eichler condition. Let S be a finite set of prime ideals of $\mathcal{O}$ containing the prime ideal divisors of $\#G$. Then the following hold:

(i) We have
$$\operatorname{cl}(g(M)) = \bigcup\nolimits_{\mathfrak{p} \in \operatorname{Spec}(\mathcal{O}) \setminus S} \operatorname{cl}(\mathcal{L}_{\mathfrak{p}}^{\max}(M)).$$
(ii) For $\mathfrak{p} \notin S$ we have
$$\operatorname{cl}(\mathcal{L}_{\mathfrak{p}}^{\max}(M)) = \operatorname{cl}(M) \cdot \{[\mathfrak{p}]^l \mid l \in \mathrm{D}_V(\mathfrak{p})\}.$$

Proof. (i): One of the inclusions is Theorem 17.3. Now assume that $N \in \mathcal{L}_{\mathfrak{p}}^{\max}(M)$ for some $\mathfrak{p} \notin S$. Then $N_{\mathfrak{q}} = M_{\mathfrak{q}}$ for all $\mathfrak{q} \neq \mathfrak{p}$. In particular $N_{\mathfrak{q}} = M_{\mathfrak{q}}$ for all $\mathfrak{q} \in S$ by Theorem 6.19. Thus $N \vee M$.

(ii): By Lemma 8.4 and Remark 8.5 we know that
$$\{(M : N) \mid N \in \mathcal{L}_{\mathfrak{p}}^{\max}(M)\} = \{\mathfrak{p}^{\dim_{k_{\mathfrak{p}}}(C)} \mid C \text{ is a composition factor of } (M/\mathfrak{p}M)/\operatorname{rad}(M/\mathfrak{p}M)\}.$$

As $\#G \notin \mathfrak{p}$, the $k_{\mathfrak{p}}G$-module $M/\mathfrak{p}M$ is semisimple and therefor the radical satisfies $\operatorname{rad}(M/\mathfrak{p}M) = 0$. Hence using Theorem 1.21 (vii) we obtain
$$\operatorname{cl}(\mathcal{L}_{\mathfrak{p}}^{\max}(M)) = \operatorname{cl}(M) \cdot \{[(M : N)] \mid N \in \mathcal{L}_{\mathfrak{p}}^{\max}(M)\} = \operatorname{cl}(M) \cdot \{[\mathfrak{p}]^l \mid l \in \mathrm{D}_V(\mathfrak{p})\}. \qquad \square$$

Lemma 17.5. Assume that V satisfies the Eichler condition. Let $S \subseteq \operatorname{Spec}(\mathcal{O})$ be as in Lemma 17.4. Then the following hold:

(i) We have

$$\operatorname{cl}(g(M)) = \operatorname{cl}(M) \cdot \bigcup\nolimits_{\mathfrak{C} \in \operatorname{Cl}_K} \{\mathfrak{C}^l \mid l \in \mathrm{D}_V(\mathfrak{C} \cap (\operatorname{Spec}(\mathcal{O}) \backslash S))\}.$$

(ii) Let $M_1, \dots, M_r \in \mathcal{L}(M)$ be sublattices of M such that any element of $\mathcal{L}(M)$ lies in the same genus as one of the M_i. Then

$$\operatorname{cl}(\mathcal{L}(M)) = \bigcup\nolimits_{i=1}^{r} \operatorname{cl}(M_i) \cdot \bigcup\nolimits_{\mathfrak{C} \in \operatorname{Cl}_K} \{\mathfrak{C}^l \mid l \in \mathrm{D}_V(\mathfrak{C} \cap (\operatorname{Spec}(\mathcal{O}) \backslash S))\}.$$

Proof. (i): We use Lemma 17.4. The claim follows by decomposing $\operatorname{Spec}(\mathcal{O}) \backslash S = \bigcup_{\mathfrak{C} \in \operatorname{Cl}_K} \mathfrak{C} \cap (\operatorname{Spec}(\mathcal{O}) \backslash S)$. (ii): Clear. □

Corollary 17.6. Assume that V is absolutely irreducible. Then we have

$$\operatorname{cl}(g(M)) = \operatorname{cl}(M) \cdot \operatorname{Cl}_K^n.$$

Proof. Since V is absolutely irreducible, it satisfies the Eichler condition. We now use Lemma 17.5 (i). Since for $\mathfrak{C} \in \operatorname{Cl}_K$ no prime ideal in $\mathfrak{C} \cap (\operatorname{Spec}(\mathcal{O}) \backslash S)$ is a prime ideal divisor of $\#G$, we have $\mathrm{D}_V(\mathfrak{C} \cap (\operatorname{Spec}(\mathcal{O}) \backslash S)) = \{n\}$. □

As a consequence we have the following algorithms for testing integrality:

Algorithm 17.7 (Integrality test for irreducible representations). Assume that V satisfies the Eichler condition. The following steps decide whether V is integral:

(i) Compute a Λ-lattice $M \in \mathcal{L}(V)$.

(ii) Compute a set containing representatives $M_1, \dots, M_r$ for the different genera in $\mathcal{L}(M)$ using Algorithm 13.14 or a Monte-Carlo version thereof.

(iii) Use Algorithm 16.27 to compute a finite set $S \subseteq \operatorname{Spec}(\mathcal{O})$ and $\mathrm{D}_V(\mathfrak{C} \cap (\operatorname{Spec}(\mathcal{O}) \backslash S))$ for all $\mathfrak{C} \in \operatorname{Cl}_K$.

(iv) Compute

$$C = \bigcup\nolimits_{i=1}^{r} \operatorname{cl}(M_i) \cdot \bigcup\nolimits_{\mathfrak{C} \in \operatorname{Cl}_K} \{\mathfrak{C}^d \mid d \in \mathrm{D}_V(\mathfrak{C} \cap (\operatorname{Spec}(\mathcal{O}) \backslash S))\}.$$

(v) If $1 \in C$ return true, else return false.

Since in the absolutely irreducible case, Step (iv) has a very simple form, we formulate it as a separate algorithm.

Algorithm 17.8 (Integrality test for absolutely irreducible representations). Assume that V is absolutely irreducible. The following steps decide whether V is integral or not:

(i) Compute a Λ-lattice $M \in \mathcal{L}(V)$.

(ii) Compute a set containing representatives $M_1, \dots, M_r$ for the different genera in $\mathcal{L}(V)$ using Algorithm 13.14 or a Monte-Carlo version thereof.

(iii) Compute

$$C = \bigcup\nolimits_{i=1}^{r} \operatorname{cl}(M_i) \cdot \operatorname{Cl}_K^n.$$

(iv) If $1 \in C$ return true, else return false.

Without Eichler condition. Let us now assume that V is a KG-module not necessarily satisfying the Eichler condition. By appealing to the constructive version of Jordan–Zassenhaus, we can still show that testing whether V is integral or not can be done in finite time.

Algorithm 17.9. The following steps determine whether V is integral or not.

(i) Compute an $\mathcal{O}G$-lattice $M \in \mathcal{L}(V)$.

(ii) Let c be a an explicit constant of the theorem of Jordan–Zassenhaus, as in Corollary 10.18.

(iii) By iteratively constructing maximal submodules, compute the set

$$\mathcal{M} = \{N \in \mathcal{L}(M) \mid \mathbf{N}((M : N)) < c\}.$$

(iv) Check if one of the $\mathcal{O}G$-modules in $\mathcal{M}$ is $\mathcal{O}$-free. If so, return true, else return false.

Theorem 17.10. Algorithm 17.9 is correct.

Proof. This follows from the fact that $\mathcal{M}$ contains—by the choice of c—a set of representatives for the isomorphism classes of $\mathcal{O}G$-lattices in V. □

§18. Existence of integral and nonintegral representations

As already mentioned in §15, it is very easy to come up with integral representations. For example, any representation over $\mathbf{Q}$ will do. On the other hand, our knowledge of representations which cannot be made integral is very limited, see Example 15.4. In this section, we will deal with the existence problem of non-integral and integral representations realizing a given character of a finite group. Building on the work of Serre, we will show that for characters of degree 2, rational character field and Schur index 2, there exist non-integral representations realizing this character. This theoretical result is followed by experimental data obtained by applying the techniques of §17 to a large set of characters. Eventually we formulate various conjectures explaining the experimental and generalizing the theoretical result.

§18A. Theoretical results

We will need a considerable amount of the theory of Schur indices, in particular its connection to the theory of algebras. Moreover we will have to investigate quaternion algebras in more detail. We refer the reader to [Vig80, Lor08] for all unexplained material.

Splitting fields of characters.

Definition 18.1. Let G be a finite group and $\chi \in \mathrm{Irr}_{\mathbf{C}}(G)$ an irreducible character. A number field $K|\mathbf{Q}$ is called a *splitting field of* χ, if there exists a representation of G over K affording χ. A splitting field K is called *(degree-)minimal*, if there is no splitting field of χ with degree smaller than K.

A splitting field K of χ is called *integral*, if a(ny) representation of G over K affording χ can be made integral. Otherwise, the splitting field K is called *nonintegral*.

Let χ be an irreducible complex character of a finite group. Recall that the theory of minimal splitting fields is closely connected to the theory of Schur indices. Since χ is just the trace of a representation affording χ, all splitting fields of χ contain the character field $\mathbf{Q}(\chi)$. All minimal splitting fields of χ have the same relative degree over $\mathbf{Q}(\chi)$, which is called the Schur index χ over $\mathbf{Q}$ and is denoted by $m_{\mathbf{Q}(\chi)}(\chi)$. For each place v of $\mathbf{Q}(\chi)$, there is an associated *local Schur index of* χ *at* v, denoted by $m_{\mathbf{Q}(\chi)_v}(\chi)$. We have

$$m_{\mathbf{Q}(\chi)}(\chi) = \operatorname*{lcm}_{v \in \Sigma_{\mathbf{Q}(\chi)}} m_{\mathbf{Q}(\chi)_v}(\chi)$$

and a field $\mathbf{Q}(\chi) \subseteq K$ is a splitting field of χ, if and only if $m_{\mathbf{Q}(\chi)_v}(\chi)$ divides $[K_w : \mathbf{Q}(\chi)_v]$ for all places v of $\mathbf{Q}(\chi)$ and all places w of K lying above v.

A consequence of the previous discussion (and class field theory) is the fact that if $m_{\mathbf{Q}}(\chi) = 1$, then $\mathbf{Q}(\chi)$ is the unique minimal splitting field of χ, and if $m_{\mathbf{Q}}(\chi) > 1$, then there are infinitely many minimal splitting fields of χ. In connection with integrality we now ask: Do there exist integral and nonintegral minimal splitting fields of a given character? If so, how many are there?

Remark 18.2. Let us consider the case of trivial Schur index. In this case $\mathbf{Q}(\chi)$ is the only minimal splitting field of χ. Example 15.4 (ii) (see also [CRW92, Proposition 2.1]) shows that it can be nonintegral. On the other hand, for a character χ with $\mathbf{Q}(\chi) = \mathbf{Q}$ the minimal splitting field of χ is integral. Thus in general both cases will occur.

We will now concentrate on the case $m_{\mathbf{Q}}(\chi) > 1$, more precisely on the case $m_{\mathbf{Q}}(\chi) = 2$, $\mathbf{Q}(\chi) = \mathbf{Q}$ and $\deg(\chi) = 2$. Before doing so, let us recall the interpretation of the theory of splitting fields of characters in terms of splittings of simple algebras. For a field K, a central simple K-algebra A is said to be *split by* L, where L is an extension of K, if $A \otimes L$ is isomorphic to a full matrix algebra over L. By the theory of central simple algebras, in case K is a number field this happens if and only if L_w splits $A_v = A \otimes K_v$ for all places v of K and all places w of L lying above v. The connection to the splitting field of characters is given by specializing K to be $\mathbf{Q}(\chi)$ and A to be the simple component of the semisimple algebra $\mathbf{Q}(\chi)G$ corresponding to χ. Then $L|K$ is a splitting field of χ if and only if L splits A.

A special situation. We will now concentrate on a special situation, originally treated by Serre in [Ser08], for which the existence of integral and nonintegral minimal splitting fields is closely connected to the theory of quaternion algebras and Hilbert symbols.

Assumption. Let G be a finite group and $\chi \in \mathrm{Irr}_{\mathbf{C}}(G)$ an irreducible character with $\mathbf{Q}(\chi) = \mathbf{Q}$, $m_{\mathbf{Q}}(\chi) = 2$ and $\deg(\chi) = 2$.

Thus, the simple component of $\mathbf{Q}G$ corresponding to χ is a non-split quaternion algebra over $\mathbf{Q}$, which we denote by D. Recall that a quaternion algebra is just a 4-dimensional $\mathbf{Q}$-algebra with center $\mathbf{Q}$. We have the following equivalence:

(i) A quadratic field K is a splitting field of χ,

(ii) all places v of $\mathbf{Q}$ with $m_{\mathbf{Q}_v}(\chi) = 2$ do not split in $K|\mathbf{Q}$,

(iii) the field K can be embedded as a maximal subfield of D.

(iv) For all places v of $\mathbf{Q}$ at which D is ramified, the field K_w splits D_v for all places w of K lying above v.

(The algebra D is called ramified at a place v of $\mathbf{Q}$, if and only if $D_v = \mathbf{Q}_v \otimes D$ is a division algebra). Denote by d_D the product of all ramified primes of D including the factor -1, if D is ramified at ∞. For $a, b \in \mathbf{Q}$ we denote by (a, b) the quaternion algebra over $\mathbf{Q}$ constructed as follows: On the 4-dimensional $\mathbf{Q}$-vector space with basis $\{1, i, j, k\}$ we define multiplication using the rules $i^2 = a$, $j^2 = b$, $ij = k$ and $ji = -k$. Note that by abuse of notation we will view (a, b) also as the Hilbert symbol (a, b) over $\mathbf{Q}$ and for a place v of $\mathbf{Q}$ denote by $(a, b)_v$ the corresponding local Hilbert symbol over $\mathbf{Q}_v$. By $\mathrm{Br}_2(\mathbf{Q})$ we denote the subgroup of the Brauer group of $\mathbf{Q}$ generated by quaternion algebras.

Definition 18.3. Let K be an imaginary quadratic number field with discriminant $-d$, $d > 0$. We define the map

$$e_K \colon \mathrm{Cl}_K/\mathrm{Cl}_K^2 \longrightarrow \mathrm{Br}_2(\mathbf{Q}),\ [\mathfrak{a}] \longmapsto (\mathbf{N}(\mathfrak{a}), -d).$$

Remark 18.4. Since we will interpret elements of $\mathrm{Br}_2(\mathbf{Q})$ very often as Hilbert symbols, we will use *multiplicative* notation for the group operation in $\mathrm{Br}_2(\mathbf{Q})$. Note that this is in contrast to the additive notation of [Ser08].

Proposition 18.5. Let K be an imaginary quadratic number field with discriminant $-d$, which splits D and which we consequently view as a subfield of D. Then the following hold:

(i) The map e_K is well-defined and injective.

(ii) Let R be a maximal order of D containing $\mathcal{O}$. Then the $\mathcal{O}$-module R is G-invariant. In particular R is an $\mathcal{O}G$-lattice.

(iii) If R and R' are two maximal orders of D containing $\mathcal{O}$, then $\mathrm{cl}(R) = \mathrm{cl}(R')$ in $\mathrm{Cl}_K/\mathrm{Cl}_K^2$.

(iv) Let R be a maximal order of D containing $\mathcal{O}$. Then we have $e_K(\mathrm{cl}(R)) = (D) \cdot (d_D, -d)$, where (D) is the class of D in $\mathrm{Br}_2(\mathbf{Q})$.

Proof. This is all contained in [Ser08]. □

At this point, Serre turns to the special case $D = (-1, -1)$ arising from the irreducible character of degree 2 of the quaternion group. In this special case, he is able to derive a simple characterization of all integral minimal splitting fields.

Let K be an imaginary quadratic field which splits D. Then we can view D as a KG-module, which we denote by V_K, and we have seen that a maximal order R of D is an $\mathcal{O}G$-lattice of V_K. To determine integrality, it is now sufficient to consider the set $\mathrm{cl}(\mathcal{L}(R))$ of classes of sublattices of R or—as e_K is injective—the set $e_K(\mathrm{cl}(\mathcal{L}(R)))$. As the possible classes of sublattices are closely connected to the decomposition of V_K at prime ideals $\mathfrak{p}$ of K, we need to understand how the decomposition behaves for different splitting fields.

Definition 18.6. For a minimal splitting field K of χ we define $S_K = \{\mathfrak{p} \subseteq \mathcal{O} \text{ prime} \mid \mathrm{d}_\mathfrak{p}([V_K]) \text{ is reducible}\}$ and $S_{K,\mathbf{Q}} = \{p \in \mathbf{Z} \mid (p) = \mathbf{Z} \cap \mathfrak{p} \text{ for some } \mathfrak{p} \in S_K\}$.

Remark 18.7. In general, $S_{K_1} \neq S_{K_2}$ for different splitting fields K_1 and K_2 of χ. Consider for example $G = C_7 \ltimes C_4$, where the generator of C_7 acts on the generator of C_4 by inversion. This group has a character $\chi \in \mathrm{Irr}_\mathbf{C}(G)$ with $\deg(\chi) = 2$, $m_\mathbf{Q}(\chi) = 2$ and $\mathbf{Q}(\chi) = \mathbf{Q}(\alpha)$, where $\alpha^3 - 2\alpha - \alpha + 1 = 0$. The only prime with non-trivial Schur index is 7. Consider the two splitting fields $K_1 = \mathbf{Q}(\chi, \sqrt{-46})$ and $K_2 = \mathbf{Q}(\chi, \sqrt{-7})$ of χ and K_iG-modules V_i realizing χ. For $i = 1, 2$ let $\mathfrak{p}_i$ be a prime ideal of K_i lying above 7. Then $k_{\mathfrak{p}_1} \cong \mathbf{F}_{7^2}$ and $k_{\mathfrak{p}_2} \cong \mathbf{F}_7$. By computing the decomposition maps $\mathrm{d}_{\mathfrak{p}_i}([V_i])$, we find that for $\mathfrak{p}_1$ the reduction of V_1 decomposes into two one-dimensional representations, while for $\mathfrak{p}_2$ the reduction of V_2 stays irreducible. Thus $7 \in S_{K_1,\mathbf{Q}}$ while $7 \notin S_{K_2,\mathbf{Q}}$.

Lemma 18.8. Let R be a maximal order of D containing $\mathcal{O}$. Then

$$\mathrm{cl}(\mathcal{L}(V_K)) = \mathrm{cl}(R) \cdot \left\{\prod\nolimits_{\mathfrak{p} \in S} [\mathfrak{p}] \mid S \subseteq S_K\right\} \text{ in } \mathrm{Cl}_K/\mathrm{Cl}_K^2.$$

Proof. This is an easy application of Lemma 8.4. The class of a sublattice of R can only change by a square or $[\mathfrak{p}]$, where $\mathfrak{p}$ is a prime ideal for which $\mathrm{d}_{\mathfrak{p}}([V_K])$ is reducible. □

Now define $S_\chi = \bigcap_K S_{K,\mathbf{Q}}$, where the intersection is over all minimal splitting fields K of D. In addition we set $e(D,K) = e_K(\mathrm{cl}(R))$, where R is any maximal order of D containing $\mathcal{O}$.

Proposition 18.9. We have

$$e_K(\mathrm{cl}(\mathcal{L}(V_K))) = e(D,K) \cdot \left\{\prod\nolimits_{p\in S}(p^{f_{K|\mathbf{Q}}(p)}, -d) \mid S \subseteq S_\chi\right\}.$$

Proof. By applying the map e_K to the equation obtained in the previous lemma, we obtain

$$e_K(\mathrm{cl}(\mathcal{L}(V_K))) = e(D,K) \cdot \left\{\prod\nolimits_{p\in S}(p^{f_{K|\mathbf{Q}}(p)}, -d) \mid S \subseteq S_{K,\mathbf{Q}}\right\}.$$

Assume that $p \in S_{K,\mathbf{Q}} \backslash S_\chi$ and $\mathfrak{p}$ is a prime ideal of K above p. Then there exists a minimal splitting field L and a prime ideal $\mathfrak{q}$ of L lying above p such that $\mathrm{d}_{\mathfrak{p}}([V_K])$ is reducible, while $\mathrm{d}_{\mathfrak{q}}([V_L])$ is irreducible. This is only possible if $k_{\mathfrak{p}}$ is strictly larger then $k_{\mathfrak{q}}$. Thus $\mathbf{N}(\mathfrak{p}) = p^{f_{K|\mathbf{Q}}(p)} = p^2$ and therefore $(p^{f_{K|\mathbf{Q}}(p)}, -d) = 1$. □

Proposition 18.10. We have

$$e_K(\mathrm{cl}(\mathcal{L}(V_K))) \subseteq e(D,K) \cdot \left\{\prod\nolimits_{p\in S}(p, -d) \mid S \subseteq S_\chi\right\}.$$

Proof. This is clear. □

To construct nonintegral splitting fields we proceed as follows. The right hand side of Proposition 18.10 is just a set of quaternion algebras over $\mathbf{Q}$, which depends on the field K (remember that $-d$ is the discriminant of K). If we can show that for some splitting field K of χ, none of the quaternion algebras split, then we are done. Since being a splitting field of an algebra is a local condition, we will carefully choose K such that each quaternion algebra on the right hand side will be non-split at some place. At the same time we have to ensure that K is a splitting field of χ, which is also a local condition but should not interfere with the splitting of the quaternion algebras on the right hand side. Eventually everything boils down to finding integers with prescribed Hilbert symbol (which is well understood).

In the following, for an odd integer n we will set $\varepsilon(n) = (n-1)/2$ and $\omega(n) = (n^2-1)/8$. Now let p be a prime and $a, b \in \mathbf{Z}$. We write $a = p^{v_p(a)}a'$, $b = p^{v_p(b)}b'$ with $a', b' \in \mathbf{Z}$. If p is odd, the Hilbert symbol at p can be rewritten as

$$(a,b)_p = (-1)^{v_p(a)v_p(b)\varepsilon(q)} \left(\frac{a'}{p}\right)^{v_p(b)} \left(\frac{b'}{p}\right)^{v_p(a)}.$$

For the case $p = 2$ we have

$$(a,b)_2 = (-1)^{\varepsilon(a')\varepsilon(b') + v_p(a)\omega(b') + v_p(b)\omega(a')}.$$

Lemma 18.11. Let $d \in \mathbf{Z}$ be a square-free integer and q a prime.

(i) If q is odd, then $(q,d)_q = (-1)^{1+\varepsilon(q)}$ implies $(\frac{-d}{q}) = -1$ or $q \mid d$, that is, q is not split in $\mathbf{Q}(\sqrt{-d})$.

(ii) If q is 2, then $(2,d)_2 = -1$ implies that 2 is not split in $\mathbf{Q}(\sqrt{-d})$.

Proof. (i): If $\varepsilon(q) \equiv 1 \bmod 2$ and $(q,d)_q = 1$, then $1 = (q,d)_q = (-1)^{v_q(d)}(d'/q)$, where $d = q^{v_q(d)}d'$. Thus $v_q(d) \geq 1$ (and d' satisfies some condition), that is $q \mid d$, or $v_q(d) = 0$ and $1 = (d'/q) = (d/q)$. As $(d/q) = 1$ is equivalent to $(-d/q) = -1$, that is, q is inert in $\mathbf{Q}(\sqrt{-d})$, the claim follows. Now if $\varepsilon(q) \equiv 0 \bmod 2$ and $(q,d)_q = -1$, then $-1 = (q,d)_q = (d/q)$. Thus $q \mid d$ or $(d/q) = -1$. As the latter is equivalent to $(-d/q) = -1$, the claim follows.
(ii): If $-1 = (2,d)_2 = (-1)^{\omega(d')}$, then either $2 \mid d$ or $\omega(d) \equiv 1 \bmod 4$. As the later implies $d \equiv 5 \bmod 8$ (2 is inert in $\mathbf{Q}(\sqrt{-d})$) or $d \equiv 3 \bmod 4$ (2 is ramified in $\mathbf{Q}(\sqrt{-d})$), the claim follows. □

The following theorem shows that integers with prescribed local Hilbert symbols exist in case all the obvious necessary conditions are satisfied. We will use only the following rational version which can be found in [Ser73, Chapter III, Theorem 4]. Note that the theorem holds in more general settings, see [Gra03, 7.3.2 Exercise] and [Par13].

Theorem 18.12. Let $(a_i)_{i\in I}$ be a finite family of elements of $\mathbf{Q}^\times$, $\Sigma \subseteq \Sigma_{\mathbf{Q}}$ a finite set of places of $\mathbf{Q}$ and let $(\varepsilon_{i,v})_{i\in I, v\in\Sigma}$ be a family with $\varepsilon_{i,v} \in \{\pm 1\}$. Assume that for all $v \in \Sigma$ there exists $x_v \in \mathbf{Q}_v^\times$ such that $(a_i, x_v)_v = \varepsilon_{i,v}$ for all $i \in I$. Then there are infinitely many $\overline{x} \in \mathbf{Q}^\times/(\mathbf{Q}^\times)^2$ such that $(a_i, x)_v = \varepsilon_{i,v}$ for all $i \in I$ and $v \in \Sigma$.

Proof. This is one of the directions of [Ser73, Chapter III, Theorem 4]. While Serre states the existence of only one solution, the statement about the infinitely many follows readily (the proof involves Dirichlet's result on primes in arithmetic progression). □

To get the necessary existence in the assumption of the previous theorem, we will make use of the following proposition.

Proposition 18.13. Let $(p_i)_{i\in I}$ be a finite family of pairwise different elements of $\mathbf{P} \cup \{-1\}$ and $(\varepsilon_i)_{i\in I}$ a family with $\varepsilon \in \{\pm 1\}$. Then there exist infinitely many primes q and integers $x \in \mathbf{Z}$ such that $(p_i, x)_q = \varepsilon_i$ for all $i \in I$.

Proof. Let q be an odd prime different from p_i, $i \in I$ and $x \in \mathbf{Z}$ with $v_q(x) = 1$ (e.g. $x = q$). If $p = -1$, then

$$(p, x)_q = \left(\frac{-1}{q}\right) = (-1)^{\varepsilon(q)},$$

where $\varepsilon(q) = (q-1)/2$. If $p = 2$, then

$$(p, x)_q = \left(\frac{2}{q}\right) = (-1)^{\omega(q)},$$

where $\omega(q) = (q^2-1)/8$. Note that

$$\begin{aligned}
&\text{if } q \equiv 1 \bmod 8, \text{ then } (2,x)_q = 1 \text{ and } (-1,x)_q = 1,\\
&\text{if } q \equiv 3 \bmod 8, \text{ then } (2,x)_q = -1 \text{ and } (-1,x)_q = -1,\\
&\text{if } q \equiv 5 \bmod 8, \text{ then } (2,x)_q = -1 \text{ and } (-1,x)_q = 1,\\
&\text{if } q \equiv 7 \bmod 8, \text{ then } (2,x)_q = 1 \text{ and } (-1,x)_q = -1.
\end{aligned}$$

Thus by choosing the residue class of q modulo 8 appropriately, we can obtain q and x with suitable behavior of $(p_i, x)_q$ in case $p_i \in \{-1, 2\}$. Moreover, the value $\varepsilon(q)$ is fixed. If p_i is different from 2 and -1, then any odd prime q with $(\frac{q}{p_i}) = (-1)^{\varepsilon(p_i)\varepsilon(q)}\varepsilon_i$ will satisfy

$$(p_i, x)_q = \left(\frac{p_i}{q}\right) = (-1)^{\varepsilon(p_i)\varepsilon(q)}\left(\frac{q}{p_i}\right) = \varepsilon_i.$$

We see that for q and x to satisfy the condition of the statement, it is sufficient that q satisfies certain congruence conditions modulo the numbers 8 and all odd primes among the p_i. Thus the claim follows from Dirichlet's theorem on primes in arithmetic progression. □

We now come back to the existence of integral and nonintegral minimal splitting fields.

Theorem 18.14. Let χ be an irreducible character of a finite group with $\deg(\chi) = 2$, $\mathbf{Q}(\chi) = \mathbf{Q}$ and $m_{\mathbf{Q}}(\chi) = 2$. Then there exist infinitely many nonintegral minimal splitting fields of χ.

Proof. By Proposition 18.10 it is sufficient to show that there are infinitely many splitting fields $K = \mathbf{Q}(\sqrt{-d})$, $d < 0$, of D such that

$$1 \notin e(D, K) \cdot \left\{\prod\nolimits_{p\in S} (p, -d) \mid S \subseteq S_\chi\right\}.$$

Let $\mathrm{Ram}_0(D)$ be the set of finite primes p at which D is ramified. Moreover define

$$\mathrm{Ram}(D) = \begin{cases} \mathrm{Ram}_0(D) \cup \{-1\}, & D \text{ is ramified at } \infty,\\ \mathrm{Ram}_0(D), & \text{else.}\end{cases}$$

By Lemma 18.11 for $K = \mathbf{Q}(\sqrt{-d})$, $d < 0$, to be a splitting field of D it is sufficient that for all $q \in \mathrm{Ram}_0(D)$ we have $(q,d)_q = (-1)^{1+\varepsilon(q)}$ or $(q,d)_q = 1$ for $q = 2$ respectively (the possible condition at the infinite place is automatically satisfied as K is imaginary). For each $S \subseteq S_\chi$ we can write

$$e(D,K) \cdot \prod\nolimits_{p\in S}(p,-d) = (D)\cdot(d_D,-d)\cdot \prod_{p\in S}(p,-d) = (D)\cdot \prod_{p\in \mathrm{Ram}(D)}(p,-d)\cdot\prod_{p\in S}(p,-d) = (D)\cdot\prod_{p\in T_S}(p,-d)$$

for a suitable set $T_S \subseteq S_\chi \cup \mathrm{Ram}(D)$. Thus it remains to show that there are infinitely many d such that

$$1 \notin \left\{(D)\cdot \prod\nolimits_{p\in T_S}(p,-d) \mid S \subseteq S_\chi\right\}.$$

As $1 \neq (D)$ (D is a non-split algebra), we will from now on assume that all T_S are non-empty.

For each $S \subseteq S_\chi$ choose a family of elements $(\varepsilon_{p,S})_{p\in\mathrm{Ram}_0(D)\cup S_\chi}$ of $\{\pm 1\}$ with $\prod_{p\in T_S}\varepsilon_{p,S} = -1$. For fixed S, by Proposition 18.13 there exists a prime $q_S \notin S_\chi \cup \mathrm{Ram}(D)$ and $x \in \mathbf{Z}$ such that $(D_S)_{q_S} = 1$ (the quaternion algebra D_S is non-split only at finitely many places) and $(p,x)_{q_S} = \varepsilon_{S,p}$ for all $p \in \mathrm{Ram}_0(D)\cup S_\chi$. Thus we have

$$\left((D)\cdot\prod_{p\in T_S}(p,-x)\right)_{q_S} = (D)_{q_S}\cdot\prod_{p\in T_S}(p,-x)_{q_S} = \prod_{p\in T_S}(p,x)_{q_S} = -1.$$

(As $q_S \notin T_S$ we have $(p,-1)_{q_S} = 1$.) We can also assume that $q_S \neq q_{S'}$ for $S \neq S'$. We are now in the situation of Theorem 18.12 with $I = S_\chi \cup \mathrm{Ram}(D)$, $(a_i)_{i\in I} = (p)_{p\in S_\chi\cup\mathrm{Ram}(D)}$, $\Sigma = (q_S)_{S\subseteq S_\chi}$ and $\varepsilon_{i,v} = \varepsilon_{p,S}$. After taking into account the condition for $\mathbf{Q}(\sqrt{-d})$ to be a splitting field, Theorem 18.12 is still applicable as the additional conditions only affect the places $\mathrm{Ram}(D)$ and $\mathrm{Ram}(D)\cap\Sigma = \emptyset$. The claim now follows from Theorem 18.12 with $(a_i)_{i\in I} = (p)_{p\in\mathrm{Ram}_0(D)\cup S_\chi}$ and ε appropriately. □

We will now show that there are also infinitely many integral minimal splitting fields. Note that this is much easier, since it is sufficient to show that $\mathrm{Cl}_K/\mathrm{Cl}_K^2$ vanishes for infinitely many minimal splitting fields K of χ.

Proposition 18.15. Let $p_1,\dots,p_l$ be distinct rational primes. Then there exist infinitely many imaginary quadratic number fields $K|\mathbf{Q}$ such that p_i is inert in K for $1 \le i \le l$ and $\mathrm{Cl}_K/\mathrm{Cl}_K^2 = 1$.

Proof. From genus theory we know that $\mathrm{Cl}_K/\mathrm{Cl}_K^2 = 1$ for all fields $K = \mathbf{Q}(\sqrt{-p})$ where p is a prime with $p \equiv -1 \pmod 4$ ([FT93, V.1, Corollary 2]). Hence we are done if we can show that among the primes p with $p \equiv -1 \pmod 4$ there are infinitely many primes such that $p_1,\dots,p_l$ are inert in $\mathbf{Q}(\sqrt{-p})$. Let now be p a prime with $p \equiv -1 \pmod 4$. Since there are infinitely many primes p with $p \equiv -1 \pmod 4$ we can assume that $p \notin \{p_1,\dots,p_l\}$. Note that in particular we have $d_K = -p$ for the discriminant of K.

Consider first the case $p_i = 2$ for some $1 \le i \le l$. Then p_i is inert in K if and only if $d_K \equiv 1 \pmod 8$ which is equivalent to $p \equiv -1 \pmod 8$. Thus we have the congruence condition $p \equiv -1 \pmod 8$ at 8 which also implies $p \equiv -1 \pmod 4$.

Now let $p_i \neq 2$. Then p_i is inert in K if and only if the Legendre symbol (d_K/p_i) is equal to -1. Since $d_K = -p$ this is equivalent to

$$\left(\frac{p}{p_i}\right) = (-1)(-1)^{\frac{p_i-1}{2}} = (-1)^{\frac{p_i+1}{2}}.$$

Using Dirichlet's theorem on primes in arithmetic progression we conclude that there are infinitely many p satisfying the above congruence conditions for all p_i. □

Theorem 18.16. Let χ be an irreducible character of a finite group with $\deg(\chi) = 2$, $\mathbf{Q}(\chi) = \mathbf{Q}$ and $m_{\mathbf{Q}}(\chi) = 2$. Then there exist infinitely integral minimal splitting fields of χ.

Proof. Let $(s_p)_{p\in S}$, S a finite set of places of $\mathbf{Q}$, be the collection of local Schur indices with $s_p > 1$, i.e., $s_p = 2$ since $m_{\mathbf{Q}}(\chi) = 2$. Then an extension K of the character field $\mathbf{Q}$ is a splitting field of χ if all places of K above the $p \in S$ have inertia degree divisible by 2. If K is quadratic this just means that all $p \in S$ are inert. We now apply Proposition 18.15 to the set of finite places of S. Note that since Proposition 18.15 yields imaginary quadratic fields the possible condition at the infinite place is also satisfied. □

Corollary 18.17. Let χ be an irreducible character of a finite group with $\deg(\chi) = 2$, $\mathbf{Q}(\chi) = \mathbf{Q}$ and $m_{\mathbf{Q}}(\chi) = 2$. Then there exist infinitely many integral and nonintegral minimal splitting fields of χ.

§18B. Computational results

To test whether Corollary 18.17 holds in a more general setting, we have tried to find minimal integral and nonintegral splitting fields for a large number of characters of various groups. Assume that χ is an irreducible character of G with $m_{\mathbf{Q}}(\chi) > 1$. To find these minimal splitting fields we proceeded as follows.

(i) Find some representation $\rho\colon G \to \mathrm{GL}_n(L)$ affording χ over some minimal splitting field L of χ. We refer the reader to the PhD thesis of Steel [Ste12] for details on this highly nontrivial problem.
(ii) Find an extension K of $\mathbf{Q}(\chi)$ such that χ can be afforded by a representation over K and K is minimal. Note that this can easily be checked using the local Schur indices of χ and the prime decomposition of the corresponding prime ideals in K.
(iii) Extend ρ to a representation $G \to \mathrm{GL}_n(KL)$ of the compositum KL.
(iv) Using the descent algorithm of Fieker [Fie09], it is now possible to find a representation $\rho_K : G \to \mathrm{GL}_n(K)$ affording χ. This is the costly step, since it involves a Galois cohomology computation in the extension $KL|\mathbf{Q}$.
(v) Check if ρ_K can be made integral using Algorithm 17.8.
(vi) Repeat steps (ii)-(v) until we have found an integral and a nonintegral minimal splitting field of χ.

Note that most of the time is spent during the construction of the representation in (i) and the descent in (iv). Once this is done, the integrality test takes only a fraction of the overall time. Consequently, the limiting factor of this approach is the degree of KL over $\mathbf{Q}$. As K and L have degree $m_{\mathbf{Q}}(\chi)$ over $\mathbf{Q}(\chi)$, the compositum KL can have degree $m_{\mathbf{Q}}(\chi)^2$ over $\mathbf{Q}(\chi)$. As $\mathbf{Q}(\chi)$ always contains the $m_{\mathbf{Q}}(\chi)$-th roots of unity, we have $[\mathbf{Q}(\chi) : \mathbf{Q}] \geq \varphi(m_{\mathbf{Q}}(\chi))$, where φ is Euler's totient function. Thus it can (and will) happen that KL has degree $m_{\mathbf{Q}}(\chi)^2 \cdot \varphi(m_{\mathbf{Q}}(\chi))$ over $\mathbf{Q}$. Consequently, we cannot hope to get results for $m_{\mathbf{Q}}(\chi) \geq 5$. In our computations, we have therefore only considered the case $m_{\mathbf{Q}}(\chi) \in \{2, 3\}$.

To find these characters, we relied on the table of small groups up to order 2000 by Besche, Eick and O'Brien ([BEO02]). For each of the groups with order bounded by 127 we have computed the character table, the Schur indices, the degrees of the character fields and singled out the characters with reasonable parameters. While the quantitative results are captured by Table A.1, the qualitative results are summarized in the following theorem.

Theorem 18.18. Let G be a finite group with $\#G \leq 127$ and χ a character with $m_{\mathbf{Q}}(\chi) \in \{2, 3\}$ and $m_{\mathbf{Q}}(\chi) \cdot [\mathbf{Q}(\chi) : \mathbf{Q}] \leq 8$. Then χ has an integral minimal splitting field. Assuming that the generalized Riemann hypothesis holds, every χ also has a nonintegral minimal splitting field.

§18C. Two conjectures

The previous results of this section indicate that in case the Schur index is non-trivial, there should exist integral and nonintegral minimal splitting fields.

Conjecture 18.19. Let χ be an irreducible character of a finite group with Schur index $m_{\mathbf{Q}}(\chi) > 1$. Then the following hold:

(i) There exists an integral minimal splitting field of χ.
(ii) There exists a nonintegral minimal splitting field of χ.

Corollary 18.17 gives evidence that also a stronger conjecture could hold.

Conjecture 18.20. Let χ be an irreducible character of a finite group with Schur index $m_{\mathbf{Q}}(\chi) > 1$. Then the following hold:

(i) There exist infinitely many integral minimal splitting fields of χ.
(ii) There exist infinitely many nonintegral minimal splitting fields of χ.

APPENDIX A

Numerical results

Description of the table. The data in Table A.1 is to be read as follows. Each row corresponds to an isomorphism class of a finite group G. The column headed "(k, l)" contains the ID of the group in the table of Besche, Eick and O'Brien, which is isomorphic to G. Here $k = \#G$. The column headed "$\#\{\chi\}$" denotes the number of irreducible complex characters χ of G with $m_{\mathbf{Q}}(\chi) \in \{2, 3\}$ and $m_{\mathbf{Q}}(\chi) \cdot [\mathbf{Q}(\chi) : \mathbf{Q}] \leq 8$. The third column contains a set of number fields or defining equations for number fields respectively, such that every character χ of G with $m_{\mathbf{Q}}(\chi) \in \{2, 3\}$ and $m_{\mathbf{Q}}(\chi) \cdot [\mathbf{Q}(\chi) : \mathbf{Q}] \leq 8$ has a minimal integral splitting field contained in this set. Finally, the last column contains a set of number fields or defining equations for number fields respectively, such that every character χ with $m_{\mathbf{Q}}(\chi) \in \{2, 3\}$ and $m_{\mathbf{Q}}(\chi) \cdot [\mathbf{Q}(\chi) : \mathbf{Q}] \leq 8$ has a minimal nonintegral splitting field contained in this set. If for a group G there is no corresponding row in Table A.1, then G does not have a character χ with $m_{\mathbf{Q}}(\chi) \in \{2, 3\}$ and $m_{\mathbf{Q}}(\chi) \cdot [\mathbf{Q}(\chi) : \mathbf{Q}] \leq 8$.

Reliability of the data. The correctness of the results given by the fourth column depends on the generalized Riemann hypothesis (GRH): To test whether the classes of lattices are not principal, we computed the class group of the number field assuming GRH and then used this class group to prove that something is not principal. On the other hand, the results given by the third column are unconditional. Once a generator of a class of a sublattice is found, this proves that the ideal is a principal ideal and the representation can be made integral.

Table A.1.: Groups G with $\#G \leq 127$ and characters χ with $m_{\mathbf{Q}}(\chi) \in \{2, 3\}$ and $m_{\mathbf{Q}}(\chi) \cdot [\mathbf{Q}(\chi) : \mathbf{Q}] \leq 8$

		Defining equations for minimal	
(k, l)	$\#\{\chi\}$	integral splitting fields	nonintegral splitting fields
$(8, 4)$	1	$X^2 - X + 1$	$X^2 - X + 9$
$(12, 1)$	1	$X^2 + 1$	$X^2 + 10$
$(16, 4)$	1	$X^2 - X + 1$	$X^2 - X + 9$
$(16, 9)$	2	$X^4 + 1$	$X^4 + 20X^2 + 121$
$(16, 12)$	2	$X^2 - X + 1$	$X^2 - X + 9$
$(20, 1)$	2	$X^4 + 6X^2 + 4$	$X^4 + 7X^2 + 36$
$(24, 1)$	1	$X^2 + 1$	$X^2 + 10$
$(24, 3)$	1	$X^2 - X + 1$	$X^2 - X + 9$
$(24, 4)$	3	$X^2 - X + 1$ $X^4 + 2X^3 + 5X^2 + 4X + 1$	$X^2 - X + 9$ $X^4 - 2X^3 + 7X^2 - 6X + 78$
$(24, 7)$	2	$X^2 + 1$	$X^2 + 10$
$(24, 11)$	1	$X^2 - X + 1$	$X^2 - X + 9$
$(28, 1)$	3	$X^6 + 10X^4 + 24X^2 + 8$	$X^6 + X^5 + 7X^4 + 5X^3 + 49X^2 + 9X + 139$
$(32, 2)$	1	$X^2 - X + 1$	$X^2 - X + 9$
$(32, 8)$	1	$X^2 - X + 1$	$X^2 - X + 39$
$(32, 10)$	2	$X^4 + 1$	$X^4 + 20X^2 + 121$
$(32, 12)$	1	$X^2 - X + 1$	$X^2 - X + 9$

Continued

		Defining equations for minimal	
(k,l)	$\#\{\chi\}$	integral splitting fields	nonintegral splitting fields
$(32,13)$	1	X^2-X+1	X^2-X+9
$(32,14)$	3	X^2-X+1 X^4+1	X^2-X+9 X^4+20X^2+121
$(32,15)$	1	X^2-X+1	X^2-X+9
$(32,20)$	4	X^8+1	$X^8+60X^6+1218X^4+7680X^2+16384$
$(32,23)$	2	X^2-X+1	X^2-X+9
$(32,26)$	2	X^2-X+1	X^2-X+9
$(32,29)$	2	X^2-X+1	X^2-X+9
$(32,32)$	2	X^2-X+1	X^2-X+9
$(32,35)$	4	X^2-X+1	X^2-X+9
$(32,41)$	4	X^4+1	X^4+20X^2+121
$(32,44)$	1	X^2-X+1	X^2-X+39
$(32,47)$	4	X^2-X+1	X^2-X+9
$(32,50)$	1	X^2-X+1	X^2-X+39
$(36,1)$	4	X^2+1 $X^6+6X^4+9X^2+1$	X^2+10 $X^6-6X^5+39X^4-118X^3+474X^2-660X+1961$
$(36,6)$	1	X^2+1	X^2+10
$(36,7)$	4	X^2+1	X^2+10
$(40,1)$	6	X^4+6X^2+4 X^8+7X^4+1	X^4+7X^2+36 $X^8+4X^7-24X^6-86X^5+357X^4+862X^3-3054X^2-3500X+12164$
$(40,3)$	1	X^2+2	X^2+17
$(40,4)$	5	X^2-X+1 $X^8-X^6+X^4-X^2+1$	X^2-X+9 $X^8+195X^6+13605X^4+390000X^2+4000000$
$(40,7)$	4	X^4+6X^2+4	X^4+7X^2+36
$(40,11)$	1	X^2-X+1	X^2-X+9
$(44,1)$	5	$X^{10}-X^9+5X^8-2X^7+16X^6-7X^5+20X^4+X^3+12X^2-3X+1$	$X^{10}-8X^9+90X^8-454X^7+2928X^6-10186X^5+46169X^4-106648X^3+359878X^2-441108X+1116809$
$(48,1)$	5	X^2+1 X^8+1	X^2+10 $X^8-192X^6+272X^5+14800X^4-22328X^3-439416X^2+1040240X+8797729$ $X^8+4X^7-148X^6-320X^5+8906X^4+12688X^3-236588X^2-440160X+4654850$ $X^8+4X^7-18X^6-112X^5-97X^4+552X^3+1882X^2+3332X+4337$
$(48,8)$	6	X^4+1 X^8-X^4+1	X^4+20X^2+121 $X^8+4X^7+46X^6+124X^5+903X^4+1604X^3+8986X^2+8204X+36622$
$(48,9)$	2	X^2+1	X^2+10
$(48,10)$	2	X^2+1	X^2+10
$(48,11)$	2	X^2+1	X^2+10
$(48,12)$	3	X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2-X+9 $X^4-2X^3+7X^2-6X+78$
$(48,13)$	5	X^2+1 X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2+10 X^2-X+9 $X^4-2X^3+7X^2-6X+78$
$(48,15)$	1	X^2-X-1	$X^2-X-4423$
$(48,16)$	1	X^2-X+1	X^2-X+75
$(48,18)$	3	X^2+1 X^4+1	X^2+514 X^4+20X^2+121
$(48,19)$	2	X^2+1	X^2+10
$(48,22)$	1	X^2-X+1	X^2-X+9
$(48,27)$	2	X^4+1	X^4+20X^2+121
$(48,28)$	3	X^2+1 X^4+1	X^2+514 X^4+6X^2+16
$(48,30)$	1	X^2+1	X^2+10
$(48,32)$	2	X^2-X+1	X^2-X+9
$(48,34)$	6	X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2-X+9 $X^4-2X^3+7X^2-6X+78$
$(48,39)$	1	X^2+1	X^2+274

Continued

		Defining equations for minimal	
(k,l)	$\#\{\chi\}$	integral splitting fields	nonintegral splitting fields
$(48,40)$	3	X^2-X+1	X^2-X+75 X^2-X+9
$(48,41)$	1	X^2-X-1	$X^2-X-4423$
$(48,42)$	4	X^2+1	X^2+10
$(48,46)$	2	X^2-X+1	X^2-X+9
$(56,1)$	3	$X^6+10X^4+24X^2+8$	$X^6+X^5+7X^4+5X^3+49X^2+9X+139$
$(56,3)$	1	X^2-X+1	X^2-X+9
$(56,6)$	6	$X^6+10X^4+24X^2+8$	$X^6+X^5+7X^4+5X^3+49X^2+9X+139$
$(56,10)$	1	X^2-X+1	X^2-X+9
$(60,1)$	1	X^2+1	X^2+10
$(60,2)$	2	X^4+6X^2+4	X^4+7X^2+36
$(60,3)$	7	X^2+1 X^4+6X^2+4 $X^8-X^7+X^5-X^4+X^3-X+1$	X^2+10 X^4+7X^2+36 $X^8-6X^7+2603X^6-11670X^5+2543416X^4-7581630X^3+1105646142X^2-1645203312X+180426088701$
$(60,7)$	1	X^2+1	X^2+10
$(64,5)$	1	X^2-X+1	X^2-X+39
$(64,7)$	2	X^4+1	X^4+20X^2+121
$(64,9)$	2	X^4+1	X^4+20X^2+121
$(64,11)$	1	X^2-X+1	X^2-X+39
$(64,13)$	3	X^2-X+1 X^4+1	X^2-X+39 X^4+20X^2+121
$(64,14)$	4	X^4+1	X^4+20X^2+121
$(64,15)$	1	X^2-X+1	X^2-X+9
$(64,16)$	3	X^2-X+1 X^4+1	X^2-X+9 X^4+20X^2+121
$(64,17)$	1	X^2-X+1	X^2-X+9
$(64,18)$	1	X^2-X+1	X^2-X+9
$(64,19)$	1	X^2-X+1	X^2-X+9
$(64,20)$	1	X^2-X+1	X^2-X+9
$(64,21)$	3	X^2-X+1 X^4+1	X^2-X+9 X^4+20X^2+121
$(64,22)$	1	X^2-X+1	X^2-X+9
$(64,23)$	1	X^2-X+1	X^2-X+9
$(64,24)$	2	X^2-X+1	X^2-X+39 X^2-X+9
$(64,25)$	1	X^2-X+1	X^2-X+9
$(64,37)$	2	X^2-X+1	X^2-X+39
$(64,39)$	4	X^8+1	$X^8+60X^6+1218X^4+7680X^2+16384$
$(64,43)$	2	X^4+1	X^4+68X^2+1225
$(64,44)$	1	X^2-X+1	X^2-X+9
$(64,45)$	1	X^2-X+1	X^2-X+9
$(64,46)$	1	X^2-X+1	X^2-X+9
$(64,47)$	7	X^2-X+1 X^4+1 X^8+1	X^2-X+9 X^4+20X^2+121 $X^8+60X^6+1218X^4+7680X^2+16384$
$(64,48)$	3	X^2-X+1 X^4+1	X^2-X+9 X^4+20X^2+121
$(64,49)$	3	X^2-X+1 X^4+1	X^2-X+9 X^4+20X^2+121
$(64,56)$	2	X^2-X+1	X^2-X+9
$(64,59)$	2	X^2-X+1	X^2-X+9
$(64,61)$	2	X^2-X+1	X^2-X+9
$(64,63)$	2	X^2-X+1	X^2-X+9
$(64,65)$	6	X^2-X+1	X^2-X+9
$(64,66)$	2	X^2-X+1	X^2-X+9
$(64,68)$	2	X^2-X+1	X^2-X+9

Continued

		Defining equations for minimal	
(k,l)	$\#\{\chi\}$	integral splitting fields	nonintegral splitting fields
$(64,70)$	4	X^2-X+1	X^2-X+9
$(64,72)$	4	X^2-X+1	X^2-X+9
$(64,74)$	2	X^2-X+1	X^2-X+9
$(64,76)$	6	X^2-X+1	X^2-X+9
$(64,77)$	2	X^2-X+1	X^2-X+9
$(64,79)$	4	X^2-X+1	X^2-X+9
$(64,80)$	2	X^2-X+1	X^2-X+9
$(64,81)$	2	X^2-X+1	X^2-X+9
$(64,93)$	2	X^2-X+1	X^2-X+39
$(64,96)$	4	X^4+1	X^4+20X^2+121
$(64,98)$	1	X^2-X+1	X^2-X+39
$(64,100)$	2	X^2-X+1	X^2-X+39
$(64,103)$	2	X^2-X+1	X^2-X+9
$(64,104)$	2	X^2-X+1	X^2-X+9
$(64,105)$	2	X^2-X+1	X^2-X+9
$(64,106)$	2	X^2-X+1	X^2-X+9
$(64,107)$	6	X^2-X+1 X^4+1	X^2-X+9 X^4+20X^2+121
$(64,108)$	2	X^2-X+1	X^2-X+9
$(64,109)$	3	X^2-X+1	X^2-X+39 X^2-X+9
$(64,110)$	2	X^2-X+1	X^2-X+9
$(64,111)$	2	X^2-X+1	X^2-X+9
$(64,120)$	4	X^4+1	X^4+20X^2+121
$(64,121)$	1	X^2-X+1	X^2-X+39
$(64,122)$	2	X^2-X+1	X^2-X+39
$(64,126)$	2	X^2-X+1	X^2-X+9
$(64,127)$	2	X^2-X+1	X^2-X+9
$(64,129)$	1	X^2-X+1	X^2-X+39
$(64,132)$	5	X^2-X+1 X^4+1	X^2-X+39 X^4+20X^2+121
$(64,133)$	1	X^2-X+1	X^2-X+39
$(64,137)$	2	X^2-X+1	X^2-X+39
$(64,142)$	1	X^2-X+1	X^2-X+39
$(64,143)$	5	X^2-X+1 X^4+1	X^2-X+39 X^4+20X^2+121
$(64,145)$	1	X^2-X+1	X^2-X+39
$(64,148)$	4	X^4+1	X^4+20X^2+121
$(64,149)$	1	X^2-X+1	X^2-X+39
$(64,151)$	2	X^2-X+1	X^2-X+39
$(64,154)$	2	X^4+1	X^4+68X^2+1225
$(64,155)$	3	X^2-X+1	X^2-X+39 X^2-X+9
$(64,156)$	3	X^2-X+1	X^2-X+39 X^2-X+9
$(64,157)$	2	X^2-X+1	X^2-X+9
$(64,158)$	6	X^2-X+1 X^4+1	X^2-X+9 X^4+20X^2+121
$(64,159)$	2	X^2-X+1	X^2-X+9
$(64,160)$	3	X^2-X+1	X^2-X+39 X^2-X+9
$(64,161)$	1	X^2-X+1	X^2-X+39
$(64,164)$	1	X^2-X+1	X^2-X+39
$(64,165)$	4	X^4+1	X^4+20X^2+121
$(64,166)$	1	X^2-X+1	X^2-X+39
$(64,168)$	4	X^4+1	X^4+20X^2+121
$(64,170)$	1	X^2-X+1	X^2-X+39

Continued

		Defining equations for minimal	
(k, l)	$\#\{\chi\}$	integral splitting fields	nonintegral splitting fields
$(64, 172)$	2	$X^2 - X + 1$	$X^2 - X + 39$
$(64, 175)$	8	$X^4 + 1$	$X^4 + 20X^2 + 121$
$(64, 178)$	2	$X^2 - X + 1$	$X^2 - X + 39$
$(64, 179)$	4	$X^2 - X + 1$	$X^2 - X + 9$
$(64, 180)$	4	$X^2 - X + 1$	$X^2 - X + 9$
$(64, 181)$	8	$X^2 - X + 1$ $X^4 + 1$	$X^2 - X + 9$ $X^4 + 20X^2 + 121$
$(64, 182)$	5	$X^2 - X + 1$	$X^2 - X + 39$ $X^2 - X + 9$
$(64, 188)$	8	$X^8 + 1$	$X^8 + 60X^6 + 1218X^4 + 7680X^2 + 16384$
$(64, 191)$	2	$X^4 + 1$	$X^4 + 68X^2 + 1225$
$(64, 194)$	4	$X^2 - X + 1$	$X^2 - X + 9$
$(64, 197)$	4	$X^2 - X + 1$	$X^2 - X + 9$
$(64, 200)$	2	$X^2 - X + 1$	$X^2 - X + 39$
$(64, 201)$	1	$X^2 - X + 1$	$X^2 - X + 39$
$(64, 204)$	4	$X^2 - X + 1$	$X^2 - X + 9$
$(64, 208)$	4	$X^2 - X + 1$	$X^2 - X + 9$
$(64, 212)$	8	$X^2 - X + 1$	$X^2 - X + 9$
$(64, 214)$	4	$X^2 - X + 1$	$X^2 - X + 9$
$(64, 217)$	2	$X^2 - X + 1$	$X^2 - X + 39$
$(64, 218)$	1	$X^2 - X + 1$	$X^2 - X + 39$
$(64, 220)$	1	$X^2 - X + 1$	$X^2 - X + 39$
$(64, 222)$	2	$X^2 - X + 1$	$X^2 - X + 39$
$(64, 223)$	1	$X^2 - X + 1$	$X^2 - X + 39$
$(64, 224)$	4	$X^2 - X + 1$	$X^2 - X + 9$
$(64, 225)$	5	$X^2 - X + 1$	$X^2 - X + 39$ $X^2 - X + 9$
$(64, 228)$	1	$X^2 - X + 1$	$X^2 - X + 39$
$(64, 229)$	1	$X^2 - X + 1$	$X^2 - X + 39$
$(64, 230)$	5	$X^2 - X + 1$	$X^2 - X + 39$ $X^2 - X + 9$
$(64, 233)$	1	$X^2 - X + 1$	$X^2 - X + 39$
$(64, 235)$	4	$X^2 - X + 1$	$X^2 - X + 9$
$(64, 237)$	1	$X^2 - X + 1$	$X^2 - X + 39$
$(64, 238)$	5	$X^2 - X + 1$	$X^2 - X + 39$ $X^2 - X + 9$
$(64, 239)$	8	$X^2 - X + 1$	$X^2 - X + 9$
$(64, 243)$	1	$X^2 - X + 1$	$X^2 - X + 39$
$(64, 244)$	2	$X^2 - X + 1$	$X^2 - X + 39$
$(64, 245)$	3	$X^2 - X + 1$	$X^2 - X + 39$
$(64, 252)$	8	$X^4 + 1$	$X^4 + 20X^2 + 121$
$(64, 255)$	2	$X^2 - X + 1$	$X^2 - X + 39$
$(64, 259)$	2	$X^4 + 1$	$X^4 + 68X^2 + 1225$
$(64, 262)$	8	$X^2 - X + 1$	$X^2 - X + 9$
$(64, 265)$	2	$X^2 - X + 1$	$X^2 - X + 39$
$(72, 1)$	4	$X^2 + 1$ $X^6 + 6X^4 + 9X^2 + 1$	$X^2 + 10$ $X^6 - 6X^5 + 39X^4 - 118X^3 + 474X^2 - 660X + 1961$
$(72, 3)$	1	$X^2 - X + 1$	$X^2 - X + 9$
$(72, 4)$	3	$X^2 - X + 1$ $X^4 + 2X^3 + 5X^2 + 4X + 1$	$X^2 - X + 9$ $X^4 - 2X^3 + 7X^2 - 6X + 78$
$(72, 7)$	8	$X^2 + 1$ $X^6 + 6X^4 + 9X^2 + 1$	$X^2 + 10$ $X^6 - 6X^5 + 39X^4 - 118X^3 + 474X^2 - 660X + 1961$
$(72, 11)$	1	$X^2 - X + 1$	$X^2 - X + 9$
$(72, 12)$	1	$X^2 + 1$	$X^2 + 10$
$(72, 13)$	4	$X^2 + 1$	$X^2 + 10$
$(72, 19)$	2	$X^2 + 1$	$X^2 + 34$

Continued

		Defining equations for minimal	
(k,l)	$\#\{\chi\}$	integral splitting fields	nonintegral splitting fields
$(72,20)$	3	X^2+1	X^2+10 X^2+34
$(72,22)$	1	X^2+1	X^2+94
$(72,24)$	6	X^2+1 X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2+94 X^2-X+9 $X^4-2X^3+7X^2-6X+78$
$(72,25)$	1	X^2-X+1	X^2-X+9
$(72,26)$	3	X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2-X+9 $X^4-2X^3+7X^2-6X+78$
$(72,29)$	2	X^2+1	X^2+10
$(72,31)$	9	X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2-X+9 $X^4-2X^3+7X^2-6X+78$
$(72,34)$	8	X^2+1	X^2+10
$(72,38)$	1	X^2-X+1	X^2-X+9
$(72,41)$	1	X^2-X+1	X^2-X+9
$(80,1)$	6	X^4+6X^2+4 X^8+7X^4+1	X^4+7X^2+36 $X^8+4X^7-24X^6-86X^5+357X^4+862X^3-$ $3054X^2-3500X+12164$
$(80,3)$	1	X^2+2	X^2+17
$(80,8)$	2	X^4+1	X^4+20X^2+121
$(80,9)$	12	X^4+6X^2+4 X^8+7X^4+1	X^4+7X^2+36 $X^8+4X^7-24X^6-86X^5+357X^4+862X^3-$ $3054X^2-3500X+12164$
$(80,10)$	4	X^4+6X^2+4	X^4+7X^2+36
$(80,11)$	4	X^4+6X^2+4	X^4+7X^2+36
$(80,12)$	5	X^2-X+1 $X^8-X^6+X^4-X^2+1$	X^2-X+9 $X^8+195X^6+13605X^4+390000X^2+4000000$
$(80,13)$	9	X^2-X+1 X^4+6X^2+4 $X^8-X^6+X^4-X^2+1$	X^2-X+9 X^4+7X^2+36 $X^8+195X^6+13605X^4+390000X^2+4000000$
$(80,15)$	2	$X^4-2X^3-2X^2+3X+1$ X^4-6X^2+49	$X^4-2X^3+270X^2-269X+15559$ $X^4-X^3+245X^2-113X+15109$
$(80,16)$	2	$X^4+X^3+X^2+X+1$	$X^4-X^3+245X^2-113X+15109$
$(80,17)$	2	X^4-2X^3+X-1 X^4-6X^2+49	$X^4-2X^3+270X^2-269X+15559$
$(80,18)$	4	X^4+1 X^4-6X^2+49	X^4+20X^2+121 $X^4-2X^3+270X^2-269X+15559$
$(80,19)$	4	X^4+6X^2+4	X^4+7X^2+36
$(80,22)$	1	X^2-X+1	X^2-X+9
$(80,27)$	2	X^4+1	X^4+20X^2+121
$(80,28)$	2	X^4+1	X^4+57X^2+784
$(80,31)$	1	X^2-X+1	X^2-X+9
$(80,32)$	2	X^2+2	X^2+17
$(80,33)$	2	X^4+6X^2+4	$X^4-4X^3+13X^2-18X+44$
$(80,35)$	10	X^2-X+1 $X^8-X^6+X^4-X^2+1$	X^2-X+9 $X^8+195X^6+13605X^4+390000X^2+4000000$
$(80,40)$	2	X^4+6X^2+4	X^4+117X^2+3721
$(80,41)$	4	X^2-X+1 X^4+6X^2+4	X^2-X+9 X^4+117X^2+3721
$(80,43)$	8	X^4+6X^2+4	X^4+7X^2+36
$(80,47)$	2	X^2-X+1	X^2-X+9
$(84,1)$	1	X^2+2	X^2-X+4
$(84,3)$	1	X^2+1	X^2+10
$(84,4)$	3	$X^6+10X^4+24X^2+8$	$X^6+X^5+7X^4+5X^3+49X^2+9X+139$
$(84,5)$	4	X^2+1 $X^6+10X^4+24X^2+8$	X^2+10 $X^6+X^5+7X^4+5X^3+49X^2+9X+139$
$(88,1)$	5	$X^{10}-X^9+5X^8-2X^7+16X^6-7X^5+20X^4+$ X^3+12X^2-3X+1	$X^{10}-8X^9+90X^8-454X^7+2928X^6-$ $10186X^5+46169X^4-106648X^3+359878X^2-$ $441108X+1116809$
$(88,3)$	1	X^2-X+1	X^2-X+39
$(88,6)$	10	$X^{10}-X^9+5X^8-2X^7+16X^6-7X^5+20X^4+$ X^3+12X^2-3X+1	$X^{10}-8X^9+90X^8-454X^7+2928X^6-$ $10186X^5+46169X^4-106648X^3+359878X^2-$ $441108X+1116809$

Continued

		Defining equations for minimal	
(k,l)	$\#\{\chi\}$	integral splitting fields	nonintegral splitting fields
$(88,10)$	1	X^2-X+1	X^2-X+39
$(96,1)$	5	X^2+1 $X^8+12X^6+56X^4+72X^2+100$	X^2+10 $X^8-1660X^6+1510448X^4-694691220X^2+117434419425$
$(96,3)$	1	X^2-X+1	X^2-X+9
$(96,8)$	4	X^8+1	$X^8+60X^6+1218X^4+7680X^2+16384$
$(96,9)$	2	X^2+1	X^2+10
$(96,10)$	2	X^2+1	X^2+10
$(96,11)$	5	X^2+1 X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2+10 X^2-X+9 $X^4-2X^3+7X^2-6X+78$
$(96,14)$	7	X^2+1 X^2-X-1 X^2-X+1 X^4+1 $X^4+2X^3+5X^2+4X+1$	X^2+514 $X^2-X-4423$ X^2-X+9 X^4+20X^2+121 $X^4-2X^3+7X^2-6X+78$
$(96,15)$	4	X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2-X+75 X^2-X+9 $X^4-2X^3+7X^2-6X+78$
$(96,16)$	1	X^2-X-1	$X^2-X-4423$
$(96,17)$	4	X^2+1 X^2-X+1 X^4+1	X^2+514 X^2-X+75 X^4+20X^2+121
$(96,18)$	10	X^2+1 $X^8+12X^6+56X^4+72X^2+100$	X^2+10 $X^8+1604X^6+3504X^5+1231696X^4+2510928X^3+577854404X^2+581218680X+149508673825$
$(96,19)$	2	X^2+1	X^2+10
$(96,20)$	2	X^2+1	X^2+10
$(96,21)$	3	X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2-X+9 $X^4-2X^3+7X^2-6X+78$
$(96,22)$	2	X^2+1	X^2+10
$(96,23)$	6	X^4+1 X^8-X^4+1	X^4+20X^2+121 $X^8+4X^7+46X^6+124X^5+903X^4+1604X^3+8986X^2+8204X+36622$
$(96,24)$	5	X^2+1 X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2+10 X^2-X+9 $X^4-2X^3+7X^2-6X+78$
$(96,25)$	11	X^2+1 X^2-X+1 X^4+1 $X^4+2X^3+5X^2+4X+1$ X^8-X^4+1	X^2+10 X^2-X+9 X^4+20X^2+121 $X^4-2X^3+7X^2-6X+78$ $X^8+4X^7+46X^6+124X^5+903X^4+1604X^3+8986X^2+8204X+36622$
$(96,26)$	5	X^2+1 X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2+10 X^2-X+9 $X^4-2X^3+7X^2-6X+78$
$(96,29)$	3	X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2-X+9 $X^4-2X^3+7X^2-6X+78$
$(96,31)$	3	X^2-X+1 X^4-X^2+1	X^2-X+39 $X^4-2X^3+79X^2-78X+2022$
$(96,33)$	3	X^2-X-1 $X^4-4X^3+8X^2-8X+28$	$X^2-X-4423$ $X^4-2X^3+227X^2-226X+6719$
$(96,34)$	3	X^2-X-1 $X^4-4X^3+8X^2-8X+28$	$X^2-X-4423$ $X^4-2X^3+227X^2-226X+6719$
$(96,35)$	3	X^2+1 $X^4-4X^3+8X^2-8X+28$	$X^2-17693$ $X^4-2X^3+227X^2-226X+6719$
$(96,36)$	7	X^2-X-1 $X^4-4X^3+8X^2-8X+28$ X^8+1	$X^2-X-4423$ $X^4-2X^3+227X^2-226X+6719$ $X^8+60X^6+1218X^4+7680X^2+16384$
$(96,37)$	2	X^2+1	X^2+10
$(96,38)$	5	X^2+1 X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2+10 X^2-X+9 $X^4-2X^3+7X^2-6X+78$
$(96,39)$	4	X^2+1 X^2-X-1 X^2-X+1	X^2+10 $X^2-X-4423$ X^2-X+75

Continued

		Defining equations for minimal	
(k,l)	$\#\{\chi\}$	integral splitting fields	nonintegral splitting fields
$(96,40)$	2	X^2+1	X^2+10
$(96,41)$	2	X^2+1	X^2+10
$(96,42)$	5	X^2+1 X^4+1	X^2+10 X^2+274 X^4+20X^2+121
$(96,43)$	3	X^2+1 X^2-X+1	X^2+10 X^2-X+39
$(96,44)$	2	X^2+1	X^2+10
$(96,45)$	1	X^2-X+1	X^2-X+9
$(96,51)$	1	X^2-X+1	X^2-X+39
$(96,53)$	2	X^4+1	X^4+20X^2+121
$(96,55)$	1	X^2-X+1	X^2-X+9
$(96,56)$	1	X^2-X+1	X^2-X+9
$(96,57)$	3	X^2-X+1 X^4+1	X^2-X+9 X^4+20X^2+121
$(96,58)$	1	X^2-X+1	X^2-X+9
$(96,63)$	4	X^8+1	$X^8+60X^6+1218X^4+7680X^2+16384$
$(96,65)$	1	X^2+1	X^2+10
$(96,66)$	4	X^2+1 X^4+1	X^2+10 X^2+514 X^4+6X^2+16
$(96,67)$	1	X^2+1	X^2+10
$(96,69)$	2	X^2-X+1	X^2-X+9
$(96,75)$	6	X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2-X+9 $X^4-2X^3+7X^2-6X+78$
$(96,76)$	12	X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2-X+9 $X^4-2X^3+7X^2-6X+78$
$(96,77)$	6	X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2-X+9 $X^4-2X^3+7X^2-6X+78$
$(96,84)$	2	X^2+1	X^2+514
$(96,85)$	7	X^2+1 X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2+514 X^2-X+9 $X^4-2X^3+7X^2-6X+78$
$(96,86)$	2	X^2+1	X^2+274 X^2+514
$(96,88)$	1	X^2+1	X^2+514
$(96,90)$	1	X^2+1	X^2+514
$(96,92)$	1	X^2+1	X^2+334
$(96,93)$	2	X^2+1	X^2+274 X^2+514
$(96,94)$	4	X^2+1 X^2-X+1	X^2+274 X^2-X+75 X^2-X+9
$(96,95)$	9	X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2-X+75 X^2-X+9 $X^4-2X^3+7X^2-6X+78$
$(96,96)$	4	X^2+1 X^2-X+1	X^2+514 X^2-X+75 X^2-X+9
$(96,97)$	8	X^2+1 X^2-X-1 X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2+514 $X^2-X-4423$ X^2-X+9 $X^4-2X^3+7X^2-6X+78$
$(96,98)$	3	X^2-X+1	X^2-X+75 X^2-X+9
$(96,99)$	2	X^2+1 X^2-X-1	X^2+274 $X^2-X-4423$
$(96,100)$	1	X^2-X-1	$X^2-X-4423$
$(96,101)$	1	X^2-X-1	$X^2-X-4423$
$(96,102)$	1	X^2-X-1	$X^2-X-4423$
$(96,103)$	3	X^2-X+1	X^2-X+75 X^2-X+9

Continued

		Defining equations for minimal	
(k,l)	$\#\{\chi\}$	integral splitting fields	nonintegral splitting fields
$(96,104)$	4	X^2+1 X^2-X+1	X^2+334 X^2-X+75 X^2-X+9
$(96,105)$	2	X^2+1 X^2-X-1	X^2+514 $X^2-X-4423$
$(96,112)$	12	X^4+1 X^8-X^4+1	X^4+20X^2+121 $X^8+4X^7+46X^6+124X^5+903X^4+1604X^3+$ $8986X^2+8204X+36622$
$(96,116)$	3	X^2-X+1 X^4-X^2+1	X^2-X+39 $X^4-2X^3+79X^2-78X+2022$
$(96,119)$	2	X^4+1	X^4+68X^2+1225
$(96,122)$	3	X^2-X+1 $X^4-2X^3+X^2+6X+3$	X^2-X+39 $X^4-2X^3+73X^2-72X+2298$
$(96,123)$	2	X^4+1	$X^4+1098X^2+300304$
$(96,124)$	6	X^4+1	X^4+20X^2+121 X^4+68X^2+1225
$(96,125)$	1	X^2-X+1	X^2-X+39
$(96,127)$	4	X^2+1	X^2+10
$(96,128)$	4	X^2+1	X^2+10
$(96,129)$	4	X^2+1	X^2+10
$(96,130)$	6	X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2-X+9 $X^4-2X^3+7X^2-6X+78$
$(96,131)$	6	X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2-X+9 $X^4-2X^3+7X^2-6X+78$
$(96,132)$	10	X^2+1 X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2+10 X^2-X+9 $X^4-2X^3+7X^2-6X+78$
$(96,133)$	4	X^2+1	X^2+10
$(96,138)$	2	X^2-X-1	$X^2-X-4423$
$(96,140)$	2	X^2-X+1	X^2-X+75
$(96,141)$	5	X^2+1	X^2+10 X^2+274
$(96,142)$	2	X^2+1	X^2+274 X^2+514
$(96,143)$	2	X^2+1	X^2+514
$(96,145)$	1	X^2+1	X^2+514
$(96,146)$	1	X^2+1	X^2+334
$(96,149)$	1	X^2-X+1	X^2-X+39
$(96,150)$	6	X^2+1 X^4+1	X^2+514 X^4+20X^2+121
$(96,151)$	6	X^2-X+1	X^2-X+75 X^2-X+9
$(96,152)$	8	X^2+1 X^2-X-1 X^2-X+1	X^2+10 $X^2-X-4423$ X^2-X+75 X^2-X+9
$(96,153)$	4	X^2-X-1 X^2-X+1	$X^2-X-4423$ X^2-X+75 X^2-X+9
$(96,154)$	2	X^2-X-1	$X^2-X-4423$
$(96,155)$	4	X^2+1	X^2+10
$(96,158)$	3	X^2-X+1 X^4-X^2+1	X^2-X+39 $X^4-2X^3+79X^2-78X+2022$
$(96,159)$	4	X^2+1	X^2+10
$(96,163)$	2	X^2-X+1	X^2-X+9
$(96,166)$	2	X^2-X+1	X^2-X+9
$(96,169)$	2	X^2-X+1	X^2-X+9
$(96,172)$	2	X^2-X+1	X^2-X+9
$(96,175)$	4	X^2-X+1	X^2-X+9
$(96,181)$	4	X^4+1	X^4+20X^2+121
$(96,184)$	1	X^2-X+1	X^2-X+39

Continued

(k,l)	$\#\{\chi\}$	Defining equations for minimal	
		integral splitting fields	nonintegral splitting fields
$(96,185)$	4	X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2-X+39 X^2-X+9 $X^4-2X^3+7X^2-6X+78$
$(96,188)$	6	X^2+1 X^4+1	X^2+94 X^4+6X^2+16
$(96,190)$	1	X^2-X+1	X^2-X+75
$(96,191)$	3	X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2-X+75 $X^4-2X^3+79X^2-78X+2022$
$(96,194)$	2	X^2+1	X^2+10
$(96,198)$	4	X^2-X+1	X^2-X+9
$(96,199)$	2	X^2-X+1	X^2-X+9
$(96,202)$	1	X^2-X+1	X^2-X+39
$(96,203)$	2	X^2-X+1	X^2-X+9
$(96,205)$	12	X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2-X+9 $X^4-2X^3+7X^2-6X+78$
$(96,210)$	2	X^2+1	X^2+334
$(96,212)$	6	X^2-X+1	X^2-X+75 X^2-X+9
$(96,213)$	2	X^2-X-1	$X^2-X-4423$
$(96,214)$	1	X^2-X+1	X^2-X+39
$(96,217)$	3	X^2-X+1 X^4-X^2+1	X^2-X+39 $X^4-2X^3+79X^2-78X+2022$
$(96,218)$	8	X^2+1	X^2+10
$(96,222)$	4	X^2-X+1	X^2-X+9
$(96,225)$	1	X^2-X+1	X^2-X+39
$(100,1)$	2	X^4+6X^2+4	X^4+7X^2+36
$(100,6)$	2	X^4+6X^2+4	X^4+7X^2+36
$(100,7)$	12	X^4+6X^2+4	X^4+7X^2+36
$(100,10)$	2	X^4+6X^2+4	X^4+7X^2+36
$(104,3)$	3	$X^6+20X^4+116X^2+200$	$X^6-4X^5+121X^4-306X^3+5360X^2-$ $7492X+86945$
$(104,4)$	1	X^2-X+1	X^2-X+9
$(104,11)$	1	X^2-X+1	X^2-X+9
$(108,1)$	4	X^2+1 $X^6+6X^4+9X^2+1$	X^2+10 $X^6-6X^5+39X^4-118X^3+474X^2-660X+1961$
$(108,6)$	4	X^2+1 $X^6+6X^4+9X^2+1$	X^2+10 $X^6-6X^5+39X^4-118X^3+474X^2-660X+1961$
$(108,7)$	1	X^2+1	X^2+10
$(108,8)$	2	X^2+1	X^2+10
$(108,9)$	2	X^2+1	X^2+10
$(108,10)$	13	X^2+1 $X^6+6X^4+9X^2+1$	X^2+10 $X^6-6X^5+39X^4-118X^3+474X^2-660X+1961$
$(108,11)$	4	X^2+1	X^2+10
$(108,32)$	1	X^2+1	X^2+10
$(108,33)$	4	X^2+1	X^2+10
$(108,34)$	13	X^2+1	X^2+10
$(108,37)$	1	X^2+1	X^2+10
$(112,1)$	3	$X^6+10X^4+24X^2+8$	$X^6+X^5+7X^4+5X^3+49X^2+9X+139$
$(112,7)$	2	X^4+1	X^4+20X^2+121
$(112,8)$	6	$X^6+10X^4+24X^2+8$	$X^6+X^5+7X^4+5X^3+49X^2+9X+139$
$(112,9)$	6	$X^6+10X^4+24X^2+8$	$X^6+X^5+7X^4+5X^3+49X^2+9X+139$
$(112,10)$	6	$X^6+10X^4+24X^2+8$	$X^6+X^5+7X^4+5X^3+49X^2+9X+139$
$(112,11)$	1	X^2-X+1	X^2-X+9
$(112,12)$	7	X^2-X+1 $X^6+10X^4+24X^2+8$	X^2-X+9 $X^6+X^5+7X^4+5X^3+49X^2+9X+139$
$(112,15)$	3	$X^6+10X^4+24X^2+8$	$X^6-2X^5+420X^4-558X^3+59927X^2-$ $40048X+2903473$
$(112,16)$	3	$X^6-X^5-7X^4+2X^3+7X^2-2X-1$	$X^6+3X^5-20720X^4-41459X^3+$ $142933525X^2+142664420X-328270991399$

Continued

		Defining equations for minimal	
(k,l)	$\#\{\chi\}$	integral splitting fields	nonintegral splitting fields
$(112,17)$	5	X^4+1 $X^6-X^5+3X^4+5X^2-2X+1$	X^4+20X^2+121 $X^6-X^5+190X^4-190X^3+10396X^2-10396X+148177$ $X^6-X^5+64X^4-64X^3+1198X^2-1198X+6301$
$(112,18)$	6	$X^6+10X^4+24X^2+8$	$X^6+X^5+7X^4+5X^3+49X^2+9X+139$
$(112,21)$	1	X^2-X+1	X^2-X+9
$(112,26)$	2	X^4+1	X^4+20X^2+121
$(112,27)$	2	X^2-X+1	X^2-X+9
$(112,32)$	3	$X^6+10X^4+24X^2+8$	$X^6-2X^5+420X^4-558X^3+59927X^2-40048X+2903473$
$(112,33)$	5	X^2-X+1 $X^6-X^5+3X^4+5X^2-2X+1$	X^2-X+9 $X^6-X^5+64X^4-64X^3+1198X^2-1198X+6301$
$(112,34)$	3	$X^6-X^5-7X^4+2X^3+7X^2-2X-1$	$X^6+5X^5-17206X^4-57377X^3+98676389X^2+164531422X-188625400223$
$(112,35)$	12	$X^6+10X^4+24X^2+8$	$X^6+X^5+7X^4+5X^3+49X^2+9X+139$
$(112,39)$	2	X^2-X+1	X^2-X+9
$(120,1)$	1	X^2+1	X^2+10
$(120,2)$	6	X^4+6X^2+4 X^8+7X^4+1	X^4+7X^2+36 $X^8+4X^7-24X^6-86X^5+357X^4+862X^3-3054X^2-3500X+12164$
$(120,3)$	11	X^2+1 X^4+6X^2+4 X^8+7X^4+1 $X^8-X^7+X^5-X^4+X^3-X+1$	X^2+10 X^4+7X^2+36 $X^8+4X^7-24X^6-86X^5+357X^4+862X^3-3054X^2-3500X+12164$ $X^8-6X^7+2603X^6-11670X^5+2543416X^4-7581630X^3+1105646142X^2-1645203312X+180426088701$ $X^8-6X^7+3311X^6-14856X^5+4114291X^4-12280980X^3+2274017655X^2-3389537250X+471714036795$
$(120,5)$	4	X^2+1 X^2-X+1 X^4+6X^2+4	X^2+94 X^2-X+39 $X^4-2X^3+113X^2-112X+3421$ $X^4-2X^3+75X^2-74X+1559$
$(120,6)$	1	X^2+2	X^2+17
$(120,7)$	2	X^2+1 X^2+2	X^2+10 X^2+17
$(120,8)$	4	X^2+1 X^4+6X^2+4	X^2+10 $X^4-4X^3+183X^2-358X+8459$
$(120,9)$	6	X^4+6X^2+4	$X^4-2X^3+851X^2-850X+182755$ X^4+7X^2+36
$(120,11)$	2	$X^4-2X^3+5X^2-4X+19$	$X^4+659X^2+107039$
$(120,12)$	2	$X^4-2X^3+5X^2-4X+19$	$X^4+296X^2+19484$
$(120,13)$	2	$X^4-2X^3+5X^2-4X+19$	$X^4+296X^2+19484$ $X^4-2X^3-57X^2-1962X-202309$
$(120,14)$	9	X^2-X+1 $X^4+2X^3+5X^2+4X+1$ $X^4-2X^3+5X^2-4X+19$ $X^8-X^6+X^4-X^2+1$	X^2-X+9 $X^4-2X^3+7X^2-6X+78$ $X^4+659X^2+107039$ $X^8+195X^6+13605X^4+390000X^2+4000000$
$(120,15)$	1	X^2-X+1	X^2-X+9
$(120,16)$	5	X^2-X+1 $X^8-X^6+X^4-X^2+1$	X^2-X+9 $X^8+195X^6+13605X^4+390000X^2+4000000$
$(120,19)$	4	X^4+6X^2+4	X^4+7X^2+36
$(120,21)$	3	X^2-X+1 $X^4+2X^3+5X^2+4X+1$	X^2-X+9 $X^4-2X^3+7X^2-6X+78$
$(120,24)$	2	X^2+1	X^2+10
$(120,26)$	7	X^2-X+1 $X^4+2X^3+5X^2+4X+1$ $X^8-X^6+X^4-X^2+1$	X^2-X+9 $X^4-2X^3+7X^2-6X+78$ $X^8+195X^6+13605X^4+390000X^2+4000000$
$(120,29)$	14	X^2+1 X^4+6X^2+4 $X^8-X^7+X^5-X^4+X^3-X+1$	X^2+10 X^4+7X^2+36 $X^8-6X^7+2603X^6-11670X^5+2543416X^4-7581630X^3+1105646142X^2-1645203312X+180426088701$
$(120,33)$	1	X^2-X+1	X^2-X+9

Continued

		Defining equations for minimal	
(k,l)	$\#\{\chi\}$	integral splitting fields	nonintegral splitting fields
$(120,41)$	2	X^2+1	X^2+10
$(126,1)$	2	$X^6-3X^5+5X^3-3X+1$	$X^6+5X^5+56X^4+125X^3+572X^2+65X+403$

Bibliography

[AF95] A. Göksel Ağargün and Colin R. Fletcher, *Euclidean rings*, Turkish J. Math. **19** (1995), no. 3, 291–299.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.

[Bel04] Karim Belabas, *Topics in computational algebraic number theory*, J. Théor. Nombres Bordeaux **16** (2004), no. 1, 19–63.

[BEO02] Hans Ulrich Besche, Bettina Eick, and Eamonn A. O'Brien, *A millennium project: constructing small groups*, Internat. J. Algebra Comput. **12** (2002), no. 5, 623–644.

[Ber08] Daniel J. Bernstein, *Fast multiplication and its applications*, Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ., vol. 44, Cambridge University Press, Cambridge, 2008, pp. 325–384.

[BFH14] Jean-François Biasse, Claus Fieker, and Tommy Hofmann, *On the computation of the HNF of a module over the ring of integers of a number field*, submitted (2014).

[Bie12] Ludwig Bieberbach, *Über die Minkowskische Reduktion der positiven quadratischen Formen und die endlichen Gruppen linearer ganzzahliger Substitutionen*, Nachr. Ges. Wiss. Göttingen, Math.-Phys. Kl. **1912** (1912), 207–216.

[BN41] Richard Brauer and Cecil J. Nesbitt, *On the modular characters of groups*, Ann. of Math. **42** (1941), 556–590.

[Bou03] Nicolas Bourbaki, *Algebra II. Chapters 4–7*, Elements of Mathematics, Springer, Berlin, 2003.

[BP91] Wieb Bosma and Michael Pohst, *Computations with finitely generated modules over Dedekind rings.*, Proceedings of the 1991 international symposium on symbolic and algebraic computation (New York), ISSAC '91, ACM, 1991, pp. 151–156.

[BQ12] Jean-François Biasse and Guillaume Quintin, *An algorithm for list decoding number field codes*, Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on, 2012, pp. 91–95.

[BR80a] Colin J. Bushnell and Irving Reiner, *Solomon's conjectures and the local functional equation for zeta functions of orders*, Bull. Amer. Math. Soc. **2** (1980), no. 2, 306–310.

[BR80b] ———, *Zeta functions of arithmetic orders and Solomon's conjectures*, Math. Z. **173** (1980), no. 2, 135–161.

[BR81] ———, *Zeta functions of hereditary orders and integral group rings*, Texas Tech. Univ. Math. Series **14** (1981), 71–94.

[BR84] ———, *Analytic continuation of partial zeta functions of arithmetic orders*, J. Reine Angew. Math. **349** (1984), 160–178.

[BR86] ———, *Functional equations for Hurwitz series and partial zeta functions of orders*, J. Reine Angew. Math. **364** (1986), 130–148.

[BR87] ______, *Zeta functions and composition factors for arithmetic orders*, Math. Z. **194** (1987), no. 3, 415–428.

[Bra51] Richard Brauer, *Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers*, Math. Nachr. **4** (1951), 158–174.

[Bur08] William Burnside, *On the arithmetical nature of the coefficients in a group of linear substitutions*, Proc. Lond. Math. Soc. **7** (1908), 8–13.

[Coh93] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer, Berlin, 1993.

[Coh96] ______, *Hermite and Smith normal form algorithms over Dedekind domains*, Math. Comp. **65** (1996), no. 216, 1681–1699.

[Coh99] ______, *A survey of computational class field theory*, J. Théor. Nombres Bordeaux **11** (1999), no. 1, 1–13.

[Coh00] ______, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer, New York, 2000.

[CR62] Charles W. Curtis and Irving Reiner, *Representation theory of finite groups and associative algebras*, Interscience Publishers, New York-London, 1962.

[CR81] ______, *Methods of representation theory. Vol. I*, John Wiley & Sons Inc., New York, 1981.

[Cra76] Maurice Craig, *A characterization of certain extreme forms*, Illinois J. Math. **20** (1976), no. 4, 706–717.

[CRW92] Gerald Cliff, Jürgen Ritter, and Alfred Weiss, *Group representations and integrality*, J. Reine Angew. Math. **426** (1992), 193–202.

[CS08] Henri Cohen and Peter Stevenhagen, *Computational class field theory*, Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ., vol. 44, Cambridge University Press, Cambridge, 2008, pp. 497–534.

[CSV12] Xiao-Wen Chang, Damien Stehlé, and Gilles Villard, *Perturbation analysis of the QR factor R in the context of LLL lattice basis reduction*, Math. Comp. **81** (2012), no. 279, 1487–1511.

[DFK$^+$97] Mario Daberkow, Claus Fieker, Jürgen Klüners, Michael Pohst, Katherine Roegner, Martin Schörnig, and Klaus Wildanger, *KANT V4*, J. Symbolic Comput. **24** (1997), no. 3-4, 267–283.

[Dix82] John D. Dixon, *Exact solution of linear equations using p-adic expansions*, Numer. Math. **40** (1982), no. 1, 137–141.

[DKT87] Paul D. Domich, Ravindran Kannan, and Leslie E. Trotter, Jr., *Hermite normal form computation using modulo determinant arithmetic*, Math. Oper. Res. **12** (1987), no. 1, 50–59.

[Fei98] Walter Feit, *Integral representations of Weyl groups rationally equivalent to the reflection representation*, J. Group Theory **1** (1998), no. 3, 213–218.

[Fie06] Claus Fieker, *Applications of the class field theory of global fields*, Discovering mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 31–62.

[Fie09] ______, *Minimizing representations over number fields. II. Computations in the Brauer group*, J. Algebra **322** (2009), no. 3, 752–765.

[FH14] Claus Fieker and Tommy Hofmann, *Computing in quotients of rings of integers*, LMS J. Comput. Math. **17** (2014), no. suppl. A, 349–365.

[FS10] Claus Fieker and Damien Stehlé, *Short bases of lattices over number fields*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 6197, Springer, Berlin, 2010, pp. 157–173.

[Fle71] Colin R. Fletcher, *Euclidean rings*, J. London Math. Soc. (2) **4** (1971), 79–82.

[Fri00] Carsten Friedrichs, *Berechnung von Maximalordnungen über Dedekindringen*, Ph.D. thesis, Fachbereich 3 Mathematik, Technische Universtität Berlin, 2000.

[FT93] Albert Fröhlich and Martin J. Taylor, *Algebraic number theory*, Cambridge Studies in Advanced Mathematics, vol. 27, Cambridge University Press, Cambridge, 1993.

[Für07] Martin Fürer, *Faster integer multiplication*, STOC'07—Proceedings of the 39th Annual ACM Symposium on Theory of Computing, ACM, New York, 2007, pp. 57–66.

[Gas06] Wolfgang Gaschütz, *Zum Hauptsatz von C. Jordan über ganzzahlige Darstellungen endlicher Gruppen*, J. Reine Angew. Math. **596** (2006), 153–154.

[GP00] Meinolf Geck and Götz Pfeiffer, *Characters of finite Coxeter groups and Iwahori-Hecke algebras*, London Mathematical Society Monographs. New Series, vol. 21, The Clarendon Press Oxford University Press, New York, 2000.

[Gra03] Georges Gras, *Class field theory*, Springer Monographs in Mathematics, Springer, Berlin, 2003.

[HEO05] Derek F. Holt, Bettina Eick, and Eamonn A. O'Brien, *Handbook of computational group theory*, Discrete Mathematics and its Applications, Chapman & Hall/CRC, Boca Raton, FL, 2005.

[HGK07] Michiel Hazewinkel, Nadiya Gubareni, and Vladimir V. Kirichenko, *Algebras, rings and modules. Vol. 2*, Mathematics and Its Applications, vol. 586, Springer, Dordrecht, 2007.

[Hig60] Donald G. Higman, *On representations of orders over Dedekind domains*, Canad. J. Math. **12** (1960), 107–125.

[Hir81] Yumiko Hironaka, *Zeta functions of integral group rings of metacyclic groups*, Tsukuba J. Math. **5** (1981), no. 2, 267–283.

[Hir85] ______, *Corrections to my paper: "Zeta functions of integral group rings of metacyclic groups"*, Tsukuba J. Math. **9** (1985), no. 2, 373–374.

[HM91] James L. Hafner and Kevin S. McCurley, *Asymptotically fast triangularization of matrices over rings*, SIAM J. Comput. **20** (1991), no. 6, 1068–1083.

[Hof16] Tommy Hofmann, *Zeta Functions of Lattices of the Symmetric Group*, Comm. Algebra **44** (2016), no. 5, 2243–2255.

[Hop98] Andreas Hoppe, *Normal forms over Dedekind domains, efficient implementations in the computer algebra system KANT*, Ph.D. thesis, Technische Universität Berlin, 1998.

[How86] John A. Howell, *Spans in the module $(Z_m)^s$*, Linear Multilinear Algebra **19** (1986), no. 1, 67–77.

[HR94] Derek F. Holt and Sarah Rees, *Testing modules for irreducibility*, J. Austral. Math. Soc. Ser. A **57** (1994), no. 1, 1–16.

[Ili89] Costas S. Iliopoulos, *Worst-case complexity bounds on algorithms for computing the canonical structure of finite abelian groups and the Hermite and Smith normal forms of an integer matrix*, SIAM J. Comput. **18** (1989), no. 4, 658–669.

[Isa06] I. Martin Isaacs, *Character theory of finite groups*, American Mathematical Society, Providence, RI, 2006.

[Iya03] Osamu Iyama, *A proof of Solomon's second conjecture on local zeta functions of orders*, J. Algebra **259** (2003), no. 1, 119–126.

[Jac70] Heinz Jacobinski, *On embedding of lattices belonging to the same genus*, Proc. Amer. Math. Soc. **24** (1970), 134–136.

[Jam78] Gordon D. James, *The Representation Theory of the Symmetric Groups*, Lecture Notes in Mathematics, vol. 682, Springer, Berlin, 1978.

[Jan96] Gerald J. Janusz, *Algebraic number fields*, second ed., Graduate Studies in Mathematics, vol. 7, American Mathematical Society, Providence, RI, 1996.

[Jor80] Camille Jordan, *Mémoire sur l'équivalence des formes*, J. Éc. Polyt. **48** (1880), 111–150.

[Kap49] Irving Kaplansky, *Elementary divisors and modules*, Trans. Amer. Math. Soc. **66** (1949), 464–491.

[KV04] Erich Kaltofen and Gilles Villard, *Computing the sign or the value of the determinant of an integer matrix, a complexity survey*, Proceedings of the International Conference on Linear Algebra and Arithmetic, vol. 162, 2004, pp. 133–146.

[Lan94] Serge Lang, *Algebraic number theory*, second ed., Graduate Texts in Mathematics, vol. 110, Springer, New York, 1994.

[LMO79] Jeffrey C. Lagarias, Hugh L. Montgomery, and Andrew M. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem*, Invent. Math. **54** (1979), no. 3, 271–296.

[Lor08] Falko Lorenz, *Algebra. Vol. II*, Universitext, Springer, New York, 2008.

[Mar53] Jean-Marie Maranda, *On $\mathfrak{B}$-adic integral representations of finite groups*, Canadian J. Math. **5** (1953), 344–355.

[Min06] Hermann Minkowski, *Diskontinuitätsbereich für arithmetische Äquivalenz*, J. Reine Angew. Math. **129** (1906), 220–274.

[Neu99] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften, vol. 322, Springer, Berlin, 1999.

[NS09] Phong Q. Nguyen and Damien Stehlé, *An LLL algorithm with quadratic complexity*, SIAM J. Comput. **39** (2009), no. 3, 874–903.

[NSV11] Andrew Novocin, Damien Stehlé, and Gilles Villard, *An LLL-reduction algorithm with quasi-linear time complexity*, STOC'11—Proceedings of the 43rd ACM Symposium on Theory of Computing, ACM, New York, 2011, pp. 403–412.

[NT89] Hirosi Nagao and Yukio Tsushima, *Representations of finite groups*, Academic Press Inc., Boston, MA, 1989.

[O'M63] O. Timothy O'Meara, *Introduction to quadratic forms*, Die Grundlehren der mathematischen Wissenschaften, vol. 117, Springer, Berlin, 1963.

[OPS98] Jürgen Opgenorth, Wilhelm G. Plesken, and Tilman Schulz, *Crystallographic algorithms and tables*, Acta Cryst. Sect. A **54** (1998), no. 5, 517–531.

[PARI] The PARI Group, Bordeaux, *PARI/GP version* `2.7.0`, 2014, available from `http://pari.math.u-bordeaux.fr/`.

[Par84] Richard A. Parker, *The computer calculation of modular characters (the meat-axe)*, Computational group theory, Academic Press, London, 1984, pp. 267–274.

[Par13] Jennifer Park, *A universal first-order formula defining the ring of integers in a number field*, Math. Res. Lett. **20** (2013), no. 5, 961–980.

[Ple74] Wilhelm G. Plesken, *Beiträge zur Bestimmung der endlichen irreduziblen Untergruppen von GL(n,Z) und ihrer ganzzahligen Darstellungen*, Ph.D. thesis, RWTH Aachen, 1974.

[PP77] Wilhelm G. Plesken and Michael Pohst, *On maximal finite irreducible subgroups of* $\mathrm{GL}(n, \mathbf{Z})$*. I. The five and seven dimensional cases*, Math. Comp. **31** (1977), no. 138, 536–551.

[PS96] Wilhelm G. Plesken and Bernd Souvignier, *Constructing rational representations of finite groups*, Experiment. Math. **5** (1996), no. 1, 39–47.

[PZ89] Michael Pohst and Hans Zassenhaus, *Algorithmic algebraic number theory*, Encyclopedia of Mathematics and its Applications, vol. 30, Cambridge University Press, Cambridge, 1989.

[Rei80] Irving Reiner, *Zeta functions of integral representations*, Comm. Algebra **8** (1980), no. 10, 911–925.

[Rei03] ______, *Maximal orders*, London Mathematical Society Monographs, vol. 28, The Clarendon Press Oxford University Press, Oxford, 2003.

[RHD70] Klaus W. Roggenkamp and Verena Huber-Dyson, *Lattices over orders. I*, Lecture Notes in Mathematics, vol. 115, Springer, Berlin, 1970.

[RS62] J. Barkley Rosser and Lowell Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.

[Sax09] Nitin Saxena, *Progress on polynomial identity testing*, Bull. Eur. Assoc. Theor. Comput. Sci. EATCS (2009), no. 99, 49–79.

[Sch11] Issai Schur, *Über Gruppen linearer Substitutionen mit Koeffizienten aus einem algebraischen Zahlkörper*, Math. Ann. **71** (1911), no. 3, 355–367.

[Sch80] Jacob T. Schwartz, *Fast probabilistic algorithms for verification of polynomial identities*, J. Assoc. Comput. Mach. **27** (1980), no. 4, 701–717.

[Sch02] Tilman Schulz, *Konstruktion rationaler darstellungen endlicher gruppen.*, Ph.D. thesis, RWTH Aachen, 2002.

[Ser73] Jean-Pierre Serre, *A course in arithmetic*, Graduate Texts in Mathematics, vol. 7, Springer, New York, 1973.

[Ser08] ______, *Three letters to Walter Feit on group representations and quaternions*, J. Algebra **319** (2008), no. 2, 549–557.

[Sho90] Victor Shoup, *On the deterministic complexity of factoring polynomials over finite fields*, Inform. Process. Lett. **33** (1990), no. 5, 261–267.

[Sol77] Louis Solomon, *Zeta functions and integral representation theory*, Advances in Math. **26** (1977), no. 3, 306–326.

[Sol79] ______, *Partially ordered sets with colors*, Relations between combinatorics and other parts of mathematics (Proc. Sympos. Pure Math., Ohio State Univ., Columbus, Ohio, 1978), American Mathematical Society, Providence, R.I., 1979, pp. 309–329.

[Spe23] Andreas Speiser, *Die Theorie der Gruppen von endlicher Ordnung. mit anwendungen auf algebraische zahlen und gleichungen sowie auf die kristallographie*, Die Grundlehren der mathematischen Wissenschaften, vol. 5, Springer, Berlin, 1923.

[SS71] Arnold Schönhage and Volker Strassen, *Schnelle Multiplikation grosser Zahlen*, Computing **7** (1971), 281–292.

[Ste11] Ernst Steinitz, *Rechteckige Systeme und Moduln in algebraischen Zahlköppern. I*, Math. Ann. **71** (1911), no. 3, 328–354.

[Ste12] ______, *Rechteckige Systeme und Moduln in algebraischen Zahlkörpern. II*, Math. Ann. **72** (1912), no. 3, 297–345.

[Ste12] Allan K. Steel, *Construction of Ordinary Irreducible Representations of Finite Groups*, Ph.D. thesis, Pure Mathematics, University of Sydney, 2012.

[Sto00] Arne Storjohann, *Algorithms for matrix canonical forms*, Ph.D. thesis, Department of Computer Science, Swiss Federal Institute of Technology – ETH, 2000.

[SM98] Arne Storjohann and Thom Mulders, *Fast algorithms for linear algebra modulo N*, Algorithms—ESA '98 (Venice), Lecture Notes in Comput. Sci., vol. 1461, Springer, Berlin, 1998, pp. 139–150.

[Swa70] Richard G. Swan, *K-theory of finite groups and orders*, Lecture Notes in Mathematics, vol. 149, Springer, Berlin-New York, 1970.

[SZ67] Jack Sonn and Hans Zassenhaus, *On the theorem on the primitive element*, Amer. Math. Monthly **74** (1967), 407–410.

[Tak59] Shuichi Takahashi, *Arithmetic of group representations*, Tôhoku Math. J. **11** (1959), 216–246.

[Tak87] Yugen Takegahara, *Zeta functions of integral group rings of abelian (p, p)-groups*, Comm. Algebra **15** (1987), no. 12, 2565–2615.

[Tor41] Leonard Tornheim, *Linear forms in function fields*, Bull. Amer. Math. Soc. **47** (1941), 126–127.

[VH09] David Villa-Hernández, *Zeta functions of Burnside rings of groups of order p and p^2*, Comm. Algebra **37** (2009), no. 5, 1758–1786.

[VH12] ______, *Zeta functions of Burnside rings for symmetric and alternating groups*, Int. J. Algebra **6** (2012), no. 25-28, 1207–1220.

[Vig80] Marie-France Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, vol. 800, Springer, Berlin, 1980.

[vzGG03] Joachim von zur Gathen and Jürgen Gerhard, *Modern computer algebra*, second ed., Cambridge University Press, Cambridge, 2003.

[Wit04] Christian Wittmann, *Zeta functions of integral representations of cyclic p-groups*, J. Algebra **274** (2004), no. 1, 271–308.

[Zas37] Hans Zassenhaus, *Neuer Beweis der Endlichkeit der Klassenzahl bei unimodularer Äquivalenz endlicher ganzzahliger Substitutionsgruppen*, Abh. Math. Sem. Univ. Hamburg **12** (1937), no. 1, 276–288.

[Zip79] Richard Zippel, *Probabilistic algorithms for sparse polynomials*, Symbolic and algebraic computation (EUROSAM '79, Internat. Sympos., Marseille, 1979), Lecture Notes in Comput. Sci., vol. 72, Springer, Berlin, 1979, pp. 216–226.

[ZS75] Oscar Zariski and Pierre Samuel, *Commutative algebra. Vol. 1*, Springer, New York, 1975.

Wissenschaftlicher Werdegang

06/2006	Abitur am Gymnasium Alexander von Humboldt, Werdau
10/2007 – 09/2011	Studium der Mathematik an der TU Kaiserslautern
09/2011	Diplom in Mathematik, TU Kaiserslautern
seit 09/2011	Wissenschaftlicher Mitarbeiter am Fachbereich Mathematik der TU Kaiserslautern

Curriculum Vitae

06/2006	Abitur at the Gymnasium Alexander von Humboldt, Werdau
10/2007 – 09/2011	Study of mathematics at the TU Kaiserslautern
09/2011	Diploma in mathematics, TU Kaiserslautern
since 09/2011	Scientific assistant at the department of mathematics at the TU Kaiserslautern