Master Thesis

On a Theorem of Eichler

Über einen Satz von Eichler

Johannes Schmitt

23rd October 2019

Supervisor
Dr. Tommy Hofmann

Technische Universität Kaiserslautern
Fachbereich Mathematik
AG Algebra, Geometrie und Computeralgebra

Contents

Symbols and notation

K	algebraic number field
R	Dedekind ring with quotient field K and $R \neq K$
$\mathbb{P}(R)$	set of non-zero prime ideals of R
A	simple central algebra over K
n	square root of the dimension of A: $n^2 = \dim_K A$
$\mathrm{IntCls}_S(R)$	integral closure of the ring R in the ring S, that is, all elements of S which are integral over R
$S_\mathfrak{p}$	localization of the ring S at the prime ideal $\mathfrak{p}$
$\hat{S}_\mathfrak{p}$	completion of the ring S at the place $\mathfrak{p}$
$v_\mathfrak{p}$	valuation corresponding to the place $\mathfrak{p}$
$\sigma_\mathfrak{p}$	embedding corresponding to the infinite place $\mathfrak{p}$
$m_\mathfrak{p}$	local index of A at the place $\mathfrak{p}$
$\kappa_\mathfrak{p}$	local capacity of A at the place $\mathfrak{p}$
S_∞^A	set of infinite places of K ramified in A
K_A^+	elements of $K^\times$ which are positive at all places in S_∞^A

Introduction

Starting point and theoretical foundation of the thesis is the eponymous Theorem of Eichler [Eic37]. In a nutshell, this states that a normal ideal I in a simple central algebra A over a number field K is under certain conditions, which we will state in Theorem 2.10, principal if and only if its reduced norm $\operatorname{nr} I$ is principal. So far, this could in practice only be used to check whether an ideal is principal, by testing if the reduced norm (an ideal in a number field) has this property. In this thesis we give an algorithm which actually computes a principal generator for I.

One application of this is the computation of isomorphisms between modules of a maximal order in A. Accordingly, Bley and Johnston [BJ11] and Hofmann and Johnston [HJ18] require the hypothesis, that one is able to solve the principal ideal problem in a maximal order of a skew field, to give algorithms for modules respectively lattices of maximal orders in algebras.

Algorithms to solve the principal ideal problem in quaternion algebras have been published by Kirschmer and Voight [KV10]. These make heavy use of the fact that the reduced norm map is for those algebras a quadratic form. Page gives another algorithm for this problem in indefinite quaternion algebras [Pag14a] and discusses an algorithm for skew fields over $\mathbb{Q}$ [Pag14b].

We are going to present a very general algorithm for algebras fulfilling the Eichler condition relative to a Dedekind ring $R \neq K$ with quotient field K (see Definition 2.1). This is a requirement of the theory lying underneath and notably excludes totally positive quaternion algebras. The algorithm presented in this thesis is fit for use in practice in the sense that it has been implemented in the programming language Julia [Bez+17] as part of the software package Hecke [Fie+17]. Although the complete algorithm works for general Dedekind rings, we implemented it only for the case where R is the integral closure of $\mathbb{Z}$ in K. Accordingly, if we give references for algorithms which take R as input, then these usually only cover this special case.

Structure of this thesis

The thesis is structured as follows. In Chapter 1 we fix some notation and collect basic theory needed for the coming chapters. Particularly important results in this chapter are the Theorem of Hasse-Schilling-Maass (Theorem 1.1), the finiteness of the type number (Theorem 1.4), and the factorization of integral ideals into maximal ideals (Theorem 1.8). Also the definition of what exactly we mean by the word "ideal" is of great importance here, as it differs from the usual ring-theoretical meaning.

Chapter 2 is then dedicated to actually two Theorems of Eichler, the second one being the already mentioned one. To avoid confusion, we call the first Theorem of Eichler (Theorem 2.3) "Eichler's Norm-Theorem" in what follows and when we say "Theorem of Eichler" we mean the second one (Theorem 2.10). It should be pointed out, that from Chapter 2 onwards we assume that the algebra A fulfils the Eichler condition relative to R. At the end of this chapter we already state the algorithm making the Theorem of Eichler constructive by following its proof. We make of course use of algorithms there which we present in the following chapters.

We start with this in Chapter 3, where we state an algorithm which computes an integral and coprime representative of an ideal (Section 3.1). Further, we present an algorithm to compute representatives of the conjugacy classes of maximal orders (Section 3.3) which is an application of the computation of maximal ideals (Section 3.2). This is also needed for the factorization of ideals (Section 3.4).

The following Chapter 4 gives an algorithm for Eichler's Norm-Theorem, that is an algorithm which solves integral norm equations, where "integral" is meant with respect to R. We first consider integral norm equations in finite extensions of number fields where we try to find solutions in maximal as well as non-maximal orders (Section 4.1). We then make use of these results in the situation of algebras (Sections 4.2 and 4.3).

The last Chapter 5 is concerned with making a major part of the proof of the Theorem of Eichler constructive. We describe how this problem can be reduced to a completely group-theoretical question (Section 5.1) and then discuss this question in more detail (Section 5.2). In Section 5.3 we state a different approach to the initial problem of Chapter 5 which appears to be a promising starting point for future optimizations of the algorithm.

In the appendices we give some algorithms for ideals in matrix algebras (Appendix A) and explain the computation of quotients of modules over Dedekind rings (Appendix B). The results stated there are needed in Chapter 3, and although we think they are mostly well-known, we could not find a reference in the literature. We conclude with a short discussion of S-units and unit groups of Dedekind rings in algebraic number fields (Appendix C), which is needed in Chapter 4.

One final remark: We occasionally give exercises in [Rei06] as reference, but only if these exercises have a very detailed "hint", which is actually the proof.

Acknowledgements

I owe thanks to Dr. Tommy Hofmann for often enough nudging me in the right direction and helping me getting the right ideas. I thank PD Dr. Andreas Paffenholz for his helpful advice regarding the installation of polymake and Dr. Oliver Braun and his co-authors for providing examples of algebras as part of their "Database of unit groups"[1] with which I could test my implementation. I finally thank Dr. Stefano Marseglia as I discovered a way to optimize Algorithm 4.8 in source code written by him albeit in a completely different context.

[1] Available at `http://www.math.rwth-aachen.de/~Oliver.Braun/unitgroups/`.

1. Definitions and basic theory

We start with fixing some notation and stating basic facts needed in the coming chapters. Our main references are [Rei06] and [CR81].

Throughout the thesis let K be an algebraic number field, $R \neq K$ a Dedekind ring with quotient field K, and A a central simple algebra over K. Let $\dim_K A = n^2$ for an $n \in \mathbb{N}$, where $\dim_K A$ is indeed a square by [CR81, Theorem 3.28] and [Rei06, Theorem 7.15].

For a (finite or infinite) place $\mathfrak{p}$ of K we write $\hat{K}_\mathfrak{p}$ for the completion of K at $\mathfrak{p}$ and set

$$\hat{A}_\mathfrak{p} := \hat{K}_\mathfrak{p} \otimes_K A.$$

By [Rei06, Corollary 7.8], $\hat{A}_\mathfrak{p}$ is a central simple $\hat{K}_\mathfrak{p}$-algebra and therefore $\hat{A}_\mathfrak{p} \cong \mathrm{Mat}_{\kappa_\mathfrak{p}}(\hat{S})$ for a skewfield $\hat{S}$ over $\hat{K}_\mathfrak{p}$ and some $\kappa_\mathfrak{p} \in \mathbb{N}$ by [CR81, Theorem 3.28]. In this situation, we call $m_\mathfrak{p} \in \mathbb{N}$ with $m_\mathfrak{p}^2 = [\hat{S} : \hat{K}_\mathfrak{p}]$ the *local index* (also called *Schur index* in the literature) of A at $\mathfrak{p}$ and $\kappa_\mathfrak{p}$ the *local capacity* of A at $\mathfrak{p}$. We say that A *ramifies at* $\mathfrak{p}$ or that $\mathfrak{p}$ *is ramified in* A, if $m_\mathfrak{p} > 1$.

1.1. Norms of elements

Let $\alpha \in A$ and denote by $\alpha_L \in \mathrm{Hom}_K(A, A)$ the left multiplication by α on A. Then the *characteristic polynomial* of α over K is defined to be the characteristic polynomial of α_L over K. Let $f_\alpha(X) \in K[X]$ be this polynomial. Then the *trace* $T(\alpha)$ and the *norm* $N(\alpha)$ of α are the elements of K fulfilling

$$f_\alpha(X) = X^{n^2} - T(\alpha)X^{n^2-1} + \cdots + (-1)^{n^2} N(\alpha).$$

The characteristic polynomial of α is always the n-th power of the so-called *reduced characteristic polynomial* by [Rei06, Theorem 9.5]. Accordingly, we have the *reduced norm* $\mathrm{nr}\,\alpha$ and the *reduced trace* $\mathrm{tr}\,\alpha$, which fulfil $(\mathrm{nr}\,\alpha)^n = N(\alpha)$ and $n\,\mathrm{tr}\,\alpha = T(\alpha)$. If α is integral over R then $\mathrm{nr}\,\alpha$ and $\mathrm{tr}\,\alpha$ are elements of R by [Rei06, Theorem 1.14]. See [Rei06, Chapter 9a] for a precise definition and more properties of these maps.

One can determine the image of the map $\mathrm{nr} : A \to K$. For this, let S_∞^A be the set of all infinite places of K, which are ramified in A. For a place $\mathfrak{p} \in S_\infty^A$ write $\sigma_\mathfrak{p}$ for the corresponding embedding. If $\mathfrak{p}$ is ramified in A, then $\sigma_\mathfrak{p}$ is a real embedding by [Rei06, Theorem 32.2]. Hence we may define

$$K_A^+ := \{a \in K^\times \mid \sigma_\mathfrak{p}(a) > 0 \text{ for each } \mathfrak{p} \in S_\infty^A\}.$$

Theorem 1.1 (Hasse-Schilling-Maass). *Let A be a central simple K-algebra and let $a \in K^\times$. Then a is the reduced norm of an element of A if and only if $a \in K_A^+$, that is,* $\mathrm{nr}(A) = K_A^+ \cup \{0\}$.

Proof. See [Rei06, Theorem 33.15]. □

1.2. Orders

A subring Λ of A having the same unity element as A is called an *R-order* if Λ is a full R-lattice, that is, Λ is a finitely generated R-module and $K\Lambda = A$. Such an order Λ is *maximal* if it is not properly contained in any other R-order of A. Maximal R-orders exist by [Rei06, Corollary 10.4] and most orders considered in this thesis are going to be maximal. We occasionally drop the R in front of the word "order" as there is no danger of ambiguity.

Let $\mathfrak{p} \in \mathbb{P}(R)$, where we write $\mathbb{P}(R)$ for the set of non-zero prime ideals of R. Let $R_\mathfrak{p}$ be the localization of R at $\mathfrak{p}$ and let $\hat{R}_\mathfrak{p}$ be the $\mathfrak{p}$-adic completion of R at $\mathfrak{p}$. For any R-order Λ and any Λ-module M we set

$$\Lambda_\mathfrak{p} := R_\mathfrak{p} \otimes_R \Lambda \text{ and } \hat{\Lambda}_\mathfrak{p} := \hat{R}_\mathfrak{p} \otimes_R \Lambda$$

as well as

$$M_\mathfrak{p} := R_\mathfrak{p} \otimes_R M \text{ and } \hat{M}_\mathfrak{p} := \hat{R}_\mathfrak{p} \otimes_R M.$$

If $M \subseteq A$, we identify $M_\mathfrak{p}$ with the set $\{mr^{-1} \mid m \in M, r \in R \setminus \mathfrak{p}\} \subseteq A$, see [Rei06, p. 32].

The *discriminant* of an R-order Λ is the ideal

$$\mathfrak{d}(\Lambda) := \left\langle \det\bigl((\operatorname{tr} \alpha_i\alpha_j)_{1\leq i,j\leq n^2}\bigr) \;\middle|\; \alpha_1, \ldots, \alpha_{n^2} \in \Lambda \right\rangle_R$$

of R.

The discriminants of any two maximal orders coincide and we can read off information about ramifying prime ideals from the (hence unique) discriminant:

Lemma 1.2. *Let Λ be a maximal R-order in A. Then we have*

$$\mathfrak{d}(\Lambda) = \prod_{\mathfrak{p}\in\mathbb{P}(R)} \mathfrak{p}^{(m_\mathfrak{p}-1)\kappa_\mathfrak{p} n}.$$

Proof. See [Rei06, Corollary 25.10]. □

Remark 1.3. Since

$$(m_\mathfrak{p}\kappa_\mathfrak{p})^2 = \dim_{\hat{K}_\mathfrak{p}} \hat{A}_\mathfrak{p} = \dim_K A = n^2,$$

we have

$$\mathfrak{d}(\Lambda) = \prod_{\mathfrak{p}\in\mathbb{P}(R)} \mathfrak{p}^{n^2 - n\kappa_\mathfrak{p}}.$$

So we can determine the prime ideals at which A ramifies and their local capacities by factoring the discriminant of any maximal order Λ.

Although maximal orders in A are in general not unique, it often suffices to consider a finite set of maximal orders: If Λ is a maximal R-order in A, then for any $\alpha \in A^\times$ the conjugated order $\alpha\Lambda\alpha^{-1}$ is a maximal order too. This conjugation by units of A is clearly an equivalence relation on the set of maximal R-orders in A. The number of equivalence classes of maximal R-orders under conjugation is called the *type number* $t_R(A)$ of A.

Theorem 1.4. *The type number of A is finite.*

Proof. See [Swa86, Proposition 9.12]. It is a consequence of the fact that any maximal order Λ fulfils the Jordan-Zassenhaus condition, see [Rei06, Chapter 26]. □

1.3. Ideals

We call any full R-lattice I in A an *ideal* in A. Note that I is not an ideal of A (or any other ring in general) in the usual ring-theoretical sense. In the rare cases in which we handle ideals in the latter sense, we will explicitly call these left, right, or two-sided ideals. Any ideal I in A possesses a *left order*

$$\mathcal{O}_l(I) := \{\xi \in A \mid \xi I \subset I\}$$

and a *right order*

$$\mathcal{O}_r(I) := \{\xi \in A \mid I\xi \subseteq I\}.$$

These are indeed R-orders in A, see [Rei06, p. 109].

We say that I is a *normal ideal*, if $\mathcal{O}_l(I)$ is a maximal order. Further, if I is normal and $I \subseteq \mathcal{O}_l(I)$, then we call I an *integral ideal*. Then I is also a left ideal of $\mathcal{O}_l(I)$. These definitions could also be formulated with the right order. A normal ideal I is in fact integral if and only if $I \subseteq \mathcal{O}_r(I)$, see [Rei06, Theorem 22.9], and I is normal if and only if $\mathcal{O}_r(I)$ is maximal by [Rei06, Theorem 21.2].

Lemma 1.5. *For any ideal I and $\alpha \in A^\times$ we have*

$$\mathcal{O}_l(\alpha I) = \alpha\mathcal{O}_l(I)\alpha^{-1} \text{ and } \mathcal{O}_r(I\alpha) = \alpha^{-1}\mathcal{O}_r(I)\alpha$$

as well as

$$\mathcal{O}_l(I\alpha) = \mathcal{O}_l(I) \text{ and } \mathcal{O}_r(\alpha I) = \mathcal{O}_r(I).$$

Proof. It holds

$$\begin{aligned}\mathcal{O}_l(\alpha I) &= \{\xi \in A \mid \xi\alpha I \subseteq \alpha I\} = \{\xi \in A \mid (\alpha^{-1}\xi\alpha)I \subseteq I\}\\ &= \{\xi \in A \mid \alpha^{-1}\xi\alpha \in \mathcal{O}_l(I)\} = \alpha\mathcal{O}_l(I)\alpha^{-1}\end{aligned}$$

and

$$\mathcal{O}_l(I\alpha) = \{\xi \in A \mid \xi I\alpha \subseteq I\alpha\} = \{\xi \in A \mid \xi I \subseteq I\} = \mathcal{O}_l(I),$$

since α is a unit of A. The results for the right order follow analogously. □

For two ideals I and J we define the product in the usual way by setting

$$I \cdot J := \langle \alpha\beta \mid \alpha \in I, \beta \in J\rangle_R.$$

This is again an ideal as it is clearly a finitely generated R-module and from $KI = A$ it follows $K \subseteq KI$ and hence $A = KJ \subseteq K(I \cdot J)$ while the other inclusion is trivially fulfilled. For ideals $I_1, \dots, I_k$, $k \in \mathbb{N}_{>1}$, we call the product $I_1 \cdots I_k$ *proper* if $\mathcal{O}_r(I_i) = \mathcal{O}_l(I_{i+1})$ for all $1 \le i \le k-1$.

Theorem 1.6. *(a) A proper product of integral ideals is integral.*

(b) Let I and I' be normal ideals with the same left order Λ. Then it holds $I \subseteq I'$ if and only if $I = I' \cdot J$ for some integral ideal J with $\mathcal{O}_r(J) = \mathcal{O}_r(I)$ and $\mathcal{O}_l(J) = \mathcal{O}_r(I')$.

Proof. See [Rei06, Theorem 22.19]. □

An integral ideal $\mathfrak{P}$ with $\mathcal{O}_l(\mathfrak{P}) = \mathcal{O}_r(\mathfrak{P})$ is a *prime ideal* of $\Lambda := \mathcal{O}_l(\mathfrak{P})$ if $\mathfrak{A}\mathfrak{B} \subseteq \mathfrak{P}$ implies $\mathfrak{A} \subseteq \mathfrak{P}$ or $\mathfrak{B} \subseteq \mathfrak{P}$ for every pair of two-sided ideals $\mathfrak{A}$ and $\mathfrak{B}$ of Λ.

An integral ideal M is called *maximal* if M is a maximal left ideal of $\mathcal{O}_l(M)$. Then M is also a maximal right ideal of $\mathcal{O}_r(M)$ and conversely, see [Rei06, Theorem 22.17].

Theorem 1.7. *Let Λ be a maximal order in A. For each prime ideal $\mathfrak{p}$ of R there exists a unique prime ideal $\mathfrak{P}$ of Λ given by $\mathfrak{P} = \Lambda \cap \operatorname{rad} \Lambda_{\mathfrak{p}}$. Conversely, $\mathfrak{p}$ is uniquely determined by $\mathfrak{P}$ via $\mathfrak{P} \cap R = \mathfrak{p}$.*

For each maximal integral ideal M with left order Λ there is a unique prime ideal $\mathfrak{P}$ of Λ contained in M which is given by $\mathfrak{P} = \operatorname{ann}_\Lambda \Lambda/M$. Conversely, for any prime ideal $\mathfrak{P}$ there exists a maximal integral ideal M with left order Λ containing $\mathfrak{P}$.

Proof. See [Rei06, Theorem 22.4] and [Rei06, Theorem 22.15]. □

Let $\mathfrak{P}$ be a prime ideal of Λ lying over the prime ideal $\mathfrak{p}$, that is $\mathfrak{P} \cap R = \mathfrak{p}$. Note that if the maximal integral ideal M with left order Λ contains $\mathfrak{P}$ then also $M \cap R = \mathfrak{p}$ since $\mathfrak{p}$ is a maximal ideal of R and $1 \notin M$. Conversely, if $M \cap R = \mathfrak{p}$, then $\mathfrak{P}$ is the unique prime ideal of Λ contained in M since $\mathfrak{Q} \cap R \neq \mathfrak{p}$ for each other prime $\mathfrak{Q}$.

In analogy to the factorization of ideals into prime ideals in number fields we have a factorization into maximal ideals.

Theorem 1.8. *Let Λ be a maximal order and I an integral ideal with left order Λ. Suppose that the Λ-module Λ/I has composition length k.*

Then there exist maximal integral ideals $M_1, \ldots, M_k$ such that

$$I = M_1 \cdots M_k$$

is a proper product and $\mathcal{O}_l(I) = \mathcal{O}_l(M_1)$ as well as $O_r(I) = \mathcal{O}_r(M_k)$.

Proof. See [Rei06, Theorem 22.18]. □

In the situation of Theorem 1.8, the maximal integral ideals $M_1, \ldots, M_k$ correspond to the composition factors of Λ/I in the sense that

$$\Lambda/M_1, M_1/M_1M_2, \ldots$$

is a composition series of Λ/I, see [Rei06, p. 200]. The next theorem guarantees that we can control the order of occurrence of the maximal integral ideals.

Theorem 1.9. *Let Λ and I be as in Theorem 1.8 and let $X_1, \ldots, X_k$ be the composition factors of the Λ-module Λ/I in any preassigned order. Then there exists a factorization of I as in Theorem 1.8 such that*

$$\Lambda/M_1 \cong X_1 \text{ and } (M_1 \cdots M_{i-1})/(M_1 \cdots M_i) \cong X_i$$

for all $i \in \{2, \ldots, k\}$.

Proof. See [Rei06, Theorem 22.28]. □

1.4. Norms of ideals

Let X be a non-zero R-torsion module with composition factors $R/\mathfrak{p}_i$ for some prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_k \in \mathbb{P}(R)$. Then the *order ideal* of X is defined to be $\operatorname{ord}_R X := \prod_i \mathfrak{p}_i$. In case $X = 0$ we set $\operatorname{ord}_R X := R$.

Let now I be an integral ideal with left order Λ. Then the *norm* of I is the ideal

$$N(I) := \operatorname{ord}_R \Lambda/I,$$

where Λ/I is indeed an R-torsion module since I is a full R-lattice contained in Λ. If Λ' is the right order of I then we also have $N(I) = \operatorname{ord}_R \Lambda'/I$ by [Rei06, Theorem 24.3].

If I is a normal ideal with left order Λ then there is a non-zero $a \in R$ such that Ia is integral. We then define the norm of I to be $N(I) := a^{-n} N(Ia)$. This does not depend on a, see [Rei06, p. 212].

By [Rei06, Theorem 24.11], the norm of any normal ideal I is always the n-th power of an R-ideal $\operatorname{nr} I$, the *reduced norm* of I.

Lemma 1.10. *For any integral ideal I we have $N(I) \subseteq I$.*

Proof. We follow the hint of [Rei06, Exercise 27.4]. Let Λ be the left order of I. By definition, we have $N(I) = \operatorname{ord}_R \Lambda/I$. But

$$\operatorname{ord}_R \Lambda/I \subseteq \operatorname{ann}_R \Lambda/I \subseteq I. \qquad \square$$

Theorem 1.11. *Let Λ be a maximal order and let $\mathfrak{p}$ be a prime ideal of R. Let $\mathfrak{P}$ be the prime ideal of Λ lying above $\mathfrak{p}$ and let M be a maximal integral ideal with left order Λ containing $\mathfrak{P}$. Then $\operatorname{nr} \mathfrak{P} = \mathfrak{p}^{\kappa_\mathfrak{p}}$ and $\operatorname{nr} M = \mathfrak{p}$.*

Proof. By [Rei06, Theorem 24.13], we have $\operatorname{nr} M = \mathfrak{p}$. The proofs of [Rei06, Corollary 24.8] and [Rei06, Theorem 24.13] show $N(\mathfrak{P}) = N(M)^{\kappa_\mathfrak{p}}$. As both sides are the n-th power of the reduced norm it follows $\operatorname{nr} \mathfrak{P} = \mathfrak{p}^{\kappa_\mathfrak{p}}$. □

We have the following relation between the norms of principal ideals and the norms of elements of A.

Lemma 1.12. *Let Λ be a maximal order and $\alpha \in A^\times$. Then*

$$N(\Lambda\alpha) = RN(\alpha) \text{ and } \operatorname{nr}(\Lambda\alpha) = R \operatorname{nr} \alpha.$$

For the first statement, A is not required to be central or simple.

Proof. Let $I := \Lambda\alpha$. Note that I is indeed an ideal of A since α is a unit and therefore $KI = A\alpha = A$. By [Rei06, Theorem 24.9], it holds

$$N(I) = \langle N(\beta) \mid \beta \in I \rangle_R.$$

So we have

$$N(\Lambda\alpha) = \langle N(\lambda)N(\alpha) \mid \lambda \in \Lambda \rangle_R = RN(\alpha)$$

and the analogous statement holds for the reduced norm by [Rei06, Corollary 24.12]. □

Corollary 1.13. *Let Λ be a maximal order and $\alpha \in \Lambda$ with $\alpha \in A^{\times}$. Then α is a unit of Λ if and only if $N(\alpha)$ and $\operatorname{nr} \alpha$ are units of R.*

Proof. Follows directly from Lemma 1.12 by considering the ideal $\Lambda\alpha$. □

For a normal ideal I and a prime $\mathfrak{p} \in \mathbb{P}(R)$, we also have a norm $N(\hat{I}_{\mathfrak{p}})$ and a reduced norm $\operatorname{nr} \hat{I}_{\mathfrak{p}}$ of the completion which are defined in the same way as for I. There is the following relation.

Lemma 1.14. *Let I be a normal ideal with left order Λ and let $\mathfrak{p} \in \mathbb{P}(R)$. Then it holds $\widehat{(\operatorname{nr} I)}_{\mathfrak{p}} = \operatorname{nr} \hat{I}_{\mathfrak{p}}$.*

Proof. We may assume that I is integral since if Ia is integral for $a \in R$ then also $\hat{I}_{\mathfrak{p}}a$ is integral. Now $N(\hat{I}_{\mathfrak{p}}) = \widehat{N(I)}_{\mathfrak{p}}$ by the same argument as in the proof of [Rei06, Theorem 24.2], see the hint of [Rei06, Exercise 24.1]. Taking the n-th root of the R-ideals on both sides shows the claim. □

2. The Theorems of Eichler

In this chapter we give the precise statements of Eichler's Norm-Theorem and the Theorem of Eichler following [Rei06, Chapter 34].

2.1. Eichler condition and Eichler's Norm-Theorem

Definition 2.1. The central simple K-algebra A satisfies the *Eichler condition relative to R*, if $\dim_K A \neq 4$ or there exists a prime of K at which A does not ramify and which is not induced by a prime of R.

If R is the integral closure of $\mathbb{Z}$ in K then "primes not induced by R" are infinite primes. Hence one could restate the above definition in this case as follows: A satisfies the Eichler condition relative to R if A is not a totally definite quaternion algebra.

From now on, we always assume that A fulfils the Eichler condition relative to R. Additionally we always assume $n > 1$.

We need the following technical lemma. Let S_∞^A and K_A^+ be as in Chapter 1.

Lemma 2.2. *Let $S_1 \neq \emptyset$ be a finite set of primes of R, including all those which ramify in A, and let S_2 be a finite and possibly empty set of primes of R such that $S_1 \cap S_2 = \emptyset$. Let $a \in K_A^+ \cap R$ and assume that for each $\mathfrak{p} \in S_1 \cup S_2$ we are given a polynomial*

$$f_\mathfrak{p}(X) = X^n + b_{1,\mathfrak{p}} X^{n-1} + \cdots + b_{n-1,\mathfrak{p}} X + (-1)^n a \in \hat{R}_\mathfrak{p}[X],$$

such that $f_\mathfrak{p}(X)$ is separable and irreducible over $\hat{K}_\mathfrak{p}$ for each $\mathfrak{p} \in S_1$.

Then for each $\varepsilon > 0$, there exists a polynomial

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + (-1)^n a \in R[X]$$

satisfying all of the following conditions:

(a) For each $\mathfrak{p} \in S_1 \cup S_2$, it holds $v_\mathfrak{p}(a_i - b_{i,\mathfrak{p}}) < \varepsilon$ for $1 \leq i \leq n-1$,

(b) for each $\mathfrak{p} \in S_1$, the polynomial $f(X)$ is irreducible over $\hat{K}_\mathfrak{p}$,

(c) the polynomial $f(X)$ is separable and irreducible over K and

(d) for each $\mathfrak{p} \in S_\infty^A$, the polynomial $f(X)$ has no zeros in the field $\hat{K}_\mathfrak{p}$.

Additionally, the field extension of K defined by f is a splitting field for A.

Proof. For the construction of f see [Rei06, Lemma 34.5]. We now prove the additional claim following step 3 of the proof of [Rei06, Theorem 33.15].

Let x be any root of f in an algebraic closure of K and let $L := K(x)$. By [Rei06, Theorem 32.15], L is a splitting field if and only if for each place $\mathfrak{P}$ of L and each restriction $\mathfrak{p}$ of $\mathfrak{P}$ to K it holds $m_{\mathfrak{p}} \mid [\hat{L}_{\mathfrak{P}} : \hat{K}_{\mathfrak{p}}]$. As $m_{\mathfrak{p}} = 1$ if $\mathfrak{p}$ is not ramified in A, we only need to consider ramified primes and these are either in S_∞^A or in S_1.

If $\mathfrak{p} \in S_\infty^A$, then $\hat{K}_{\mathfrak{p}} \cong \mathbb{R}$ by [Rei06, Theorem 32.2] and hence $\hat{L}_{\mathfrak{P}} \cong \mathbb{C}$ for any $\mathfrak{P}$ extending $\mathfrak{p}$ by condition (d). So, $m_{\mathfrak{p}} = 2 = [\hat{L}_{\mathfrak{P}} : \hat{K}_{\mathfrak{p}}]$.

Let now $\mathfrak{p}$ be a finite prime ramified in A. Then $\mathfrak{p} \in S_1$, so f is irreducible over $\hat{K}_{\mathfrak{p}}$ by (b). But then $[\hat{L}_{\mathfrak{P}} : \hat{K}_{\mathfrak{p}}] = n$ for the (hence) unique prime $\mathfrak{P}$ lying over $\mathfrak{p}$. As $m_{\mathfrak{p}}\kappa_{\mathfrak{p}} = n$ we have $m_{\mathfrak{p}} \mid [\hat{L}_{\mathfrak{P}} : \hat{K}_{\mathfrak{p}}]$ as required. Therefore L is a splitting field for A by [Rei06, Theorem 32.15]. □

We now state Eichler's Norm-Theorem which is an "integral version" of Theorem 1.1.

Theorem 2.3 (Eichler)**.** *If A satisfies the Eichler condition relative to R, then there exists for every $a \in R \cap K_A^+$ an integral element $\alpha \in A$ with $\operatorname{nr} \alpha = a$.*

Sketch of the proof. Let S_1 be as in Lemma 2.2 and let $S_2 = \emptyset$. By [Rei06, Corollary 33.13], there exists for each $\mathfrak{p} \in S_1$ a monic, separable and irreducible polynomial $f_{\mathfrak{p}} \in \hat{R}_{\mathfrak{p}}[X]$ of degree n with constant term $(-1)^n a$. By Lemma 2.2, we may thus find a separable irreducible polynomial

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + (-1)^n a \in R[X]$$

satisfying the conditions (a) to (d) of Lemma 2.2. Let α be any zero of f in some algebraic closure of K. Then $L := K(\alpha)$ is a splitting field for A by Lemma 2.2 and may hence be embedded into A by [Rei06, Corollary 28.10]. Therefore $\alpha \in A$ and it holds $\operatorname{nr} \alpha = a$ and α is integral over R by construction. □

By Theorem 1.1 we also have $\operatorname{nr} \alpha \in R \cap K_A^+$ for any integral element $\alpha \in A \setminus \{0\}$.

2.2. The Theorem of Eichler

The remainder of this chapter is dedicated to the Theorem of Eichler and its proof. We are going to split this proof in some lemmata and propositions, which in some cases correspond to an algorithm presented in the following chapters. We follow [Rei06, Theorem 34.9], although we make some subtle changes:

Remark 2.4. Let Λ be a maximal R-order in A. By Theorem 1.4, there exist finitely many conjugacy classes of maximal R-orders, so let $\Lambda = \Lambda_1, \ldots, \Lambda_t$ be a system of representatives of these classes. As these are finitely generated R-modules, we may choose an $r \in R \setminus \{0\}$ such that $r\Lambda_i \subseteq \Lambda_j$ for all $i, j \in \{1, \ldots, t\}$. In this definition of r, we differ from [Rei06, p. 298] in two aspects. Firstly, we allow r to be a unit. This is just a technicality, we will explain it in the proof of Lemma 2.6, see footnote (2).

The second change is more profound. In [Rei06], r is only required to fulfil $r\Lambda_i \subseteq \Lambda$ for all i. But, quite frankly, we do not see how this is sufficient, as our additional requirements for r appear to be crucial for the proof of Proposition 2.8 (or step 5 of the proof of [Rei06, Theorem 34.9]).

For the remainder of this chapter let $\mathfrak{d}$ be the discriminant of (any) maximal R-order Λ.

Although it may seem a little bit off-topic, we need the following lemma. This is mostly [Rei06, Exercise 34.1] and its hint.

Lemma 2.5. *Let $\mathfrak{p}$ be a prime ideal of R and set $\overline{R} = R/\mathfrak{p}$. There exists a polynomial*

$$f(X) = X^n + c_1 X^{n-1} + \cdots + c_{n-1}X + (-1)^n \in R[X]$$

such that the coefficientwise reduction $\overline{f} \in \overline{R}[X]$ has no zeros in $\overline{R}$.

Proof. Let q be the cardinality of $\overline{R}$. Then there are q^{n-1} polynomials of the form

$$g(X) = X^n + c_1 X^{n-1} + \cdots + c_{n-1}X + (-1)^n \in \overline{R}[X].$$

If such a g has a zero s in $\overline{R}$, then $s \neq 0$, as $g(0) \neq 0$, so we can write

$$g(X) = (X - s)\big(X^{n-1} + \cdots + (-1)^{n-1}s^{-1}\big).$$

There are $q - 1$ possible choices for s and at most q^{n-2} choices for the factor of degree $n - 1$. Therefore the number of polynomials with a zero in $\overline{R}$ is bounded by $(q-1)q^{n-2}$ and this gives at least

$$q^{n-1} - (q-1)q^{n-2} = q^{n-2} \geq 1$$

polynomials without a zero in $\overline{R}$ as $n > 1$. We may choose any such polynomial g and let f be any (coefficientwise) lift to $R[X]$. □

To prove the Theorem of Eichler we need one more technical lemma.

Lemma 2.6. *Let $\Lambda_1, \dots, \Lambda_t$ be a system of representatives*[(1)] *of the maximal R-orders of A and let $r \in R$ be as in Remark 2.4. Let $\Lambda = \Lambda_{i^*}$ for some $i^* \in \{1, \dots, t\}$ and let $\mathfrak{p} \in \mathbb{P}(R)$ such that $\mathfrak{p} \nmid r\mathfrak{d}$. Let finally $\emptyset \neq \{\tau_1, \dots, \tau_k\} \subseteq \Lambda$ be a finite set of units of the localization $\Lambda_{\mathfrak{p}}$.*

Then there exists an element $\lambda \in \Lambda^\times$ such that $\tau_i^{-1}\lambda\tau_i \in \Lambda^\times$ for each $1 \leq i \leq k$ and the minimal polynomial of $\overline{\lambda} \in \Lambda/\mathfrak{p}\Lambda$ has no zeros over $R/\mathfrak{p}$.

Proof. We may choose an element $s \in R \setminus \mathfrak{p}$ such that $s\tau_i^{-1} \in \Lambda$, $i = 1, \dots, k$, where we additionally require $s \notin R^\times$. We want to apply Lemma 2.2. Let S_1 be the set of primes of R which ramify in A or which divide the principal ideal rsR and let $S_2 = \{\mathfrak{p}\}$. Then $S_1 \cap S_2 = \emptyset$ since $\mathfrak{p} \nmid rsR$ by construction and $\mathfrak{p}$ does not ramify as $\mathfrak{p} \nmid \mathfrak{d}$, see Remark 1.3. The set S_1 is non-empty as $s \notin R^\times$.[(2)]

We now construct the polynomials required for Lemma 2.2. For this, fix a $\mathfrak{q} \in S_1$ and let $L = \hat{K}_{\mathfrak{q}}(\zeta)$ be an unramified extension of degree n, where ζ is a primitive $(q^n - 1)$-th root of 1 with q the cardinality of the residue field $\hat{R}_{\mathfrak{q}}/\mathfrak{q}\hat{R}_{\mathfrak{q}}$. Let π be a prime element of $\hat{R}_{\mathfrak{q}}$ and let $n' := v_{\mathfrak{q}}(rs)$. By [Neu15, Lemma II.3.5] (see also the detailed hint to [Rei06, Exercise 34.4]), there exists an $m \geq nn'$ such that $u \equiv 1 \bmod \pi^m \hat{R}_{\mathfrak{q}}$ for an element $u \in \hat{R}_{\mathfrak{q}}$ implies the existence of $v \in \hat{R}_{\mathfrak{q}}$ with

$$u = v^n \text{ and } v \equiv 1 \bmod \pi^{nn'}\hat{R}_{\mathfrak{q}}. \qquad (*)$$

[(1)] We always mean a system of representatives of the conjugacy classes.

[(2)] In [Rei06], $s \in R^\times$ is not excluded. Then this is the only place where $r \notin R^\times$ is required (see Remark 2.4), otherwise S_1 might be empty. We do not want to have this requirement for the following algorithms. Hence we assume $s \notin R^\times$ instead.

Now let $g \in \hat{R}_{\mathfrak{q}}[X]$ be the minimal polynomial of $1+\pi^m\zeta$ over $\hat{K}_{\mathfrak{q}}$. Then the zeros of g are the images of $1+\pi^m\zeta$ under the powers of the Frobenius automorphism, that is

$$\left\{1+\pi^m\zeta^{q^i} \;\middle|\; 0 \le i \le n-1\right\}.$$

Hence g is separable and we have the coefficientwise equivalence

$$g(X) \equiv (X-1)^n \bmod \pi^m\hat{R}_{\mathfrak{q}}.$$

Let $(-1)^n u$ be the constant term of g. By the above, there exists $v \in \hat{R}_{\mathfrak{q}}$ fulfilling $(*)$. Note that v is a unit of $\hat{R}_{\mathfrak{q}}$ and set

$$f_{\mathfrak{q}}(X) := v^{-n}g(vX) = X^n + b_{1,\mathfrak{q}}X^{n-1} + \cdots + b_{n-1,\mathfrak{q}}X + (-1)^n \in \hat{R}_{\mathfrak{q}}[X].$$

Then $f_{\mathfrak{q}}$ is irreducible (as g is a minimal polynomial) and separable and we have $f_{\mathfrak{q}}(X) \equiv (X-1)^n \bmod \pi^m\hat{R}_{\mathfrak{q}}$.

We are left with having to construct a polynomial for $\mathfrak{p}$. Here we choose $f_{\mathfrak{p}} \in \hat{R}_{\mathfrak{p}}[X]$ as in Lemma 2.5.

Applying Lemma 2.2 with $\beta = 1$ now yields a polynomial $f \in R[X]$ which is coefficientwise near $f_{\mathfrak{q}}$ for each $\mathfrak{q} \in S_1 \cup S_2$. Hence f fulfils all of the following conditions (after choosing ε in Lemma 2.2 small enough):

(a) The coefficientwise reduction $\overline{f} \in (R/\mathfrak{p})[X]$ has no zeros in $R/\mathfrak{p}$, since this holds for $f_{\mathfrak{p}}$.

(b) It holds $f(X) \equiv (X-1)^n \bmod (rs)^n$, as this holds for all $f_{\mathfrak{q}}$ with $\mathfrak{q} \in S_1$.

(c) The field extension of K defined by f is a splitting field for A.

Now let λ be a zero of f in some algebraic closure of K and set $L := K(\lambda)$, so L is a splitting field for A by (c). Then we may embed L into A by [Rei06, Corollary 28.10] and have $\lambda \in A$, integral over R, and $\operatorname{nr}\lambda = 1$. Set

$$\mu := \frac{\lambda - 1}{rs} \in A.$$

By (b), we may write $f(X) = (X-1)^n + (rs)^n g(X)$ for some $g \in R[X]$. From $f(\lambda) = 0$ it then follows $\mu^n = -g(\lambda)$ and so μ^n is integral over R by [Rei06, Corollary 1.11]. Then also μ is integral over R and thus there exists a maximal R-order Λ' containing μ by [Swa86, Lemma 9.24]. After replacing λ and μ by suitable conjugates we may assume $\mu \in \Lambda_i$ for some $i \in \{1, \ldots, t\}$. By choice of r in Remark 2.4 we have $r\mu \in \Lambda$, so $\lambda = 1 + rs\mu \in \Lambda$, and

$$\tau_j^{-1}\lambda\tau_j = 1 + \tau_j^{-1}sr\mu\tau_j \in \Lambda$$

for each $j \in \{1, \ldots, k\}$ by choice of s. Further $\operatorname{nr}(\tau_j^{-1}\lambda\tau_j) = \operatorname{nr}\lambda = 1$, so $\lambda \in \Lambda^\times$ and $\tau_j^{-1}\lambda\tau_j \in \Lambda^\times$ for each $j \in \{1, \ldots, k\}$ by Corollary 1.13 (they are units of A since $L \subseteq A$).

Finally note, that the minimal polynomial of $\overline{\lambda} \in \Lambda/\mathfrak{p}\Lambda$ must divide $\overline{f}$. But $\overline{f}$ has no zeros in $R/\mathfrak{p}$ by (a). □

A big step towards the Theorem of Eichler is the next proposition.

Proposition 2.7. *Let $\Lambda_1, \ldots, \Lambda_t$ be a system of representatives of the maximal R-orders of A and let $r \in R$ as in Remark 2.4. Let $\mathfrak{p} \in \mathbb{P}(R)$ with $\mathfrak{p} \nmid r\mathfrak{d}$ and let M and N be maximal integral ideals with left order $\Lambda = \Lambda_{i^*}$, for an $i^* \in \{1, \ldots, t\}$, such that* $\operatorname{nr} M = \operatorname{nr} N = \mathfrak{p}$. *Then there exists $\vartheta \in \Lambda^\times$ with $M = N\vartheta$.*

Proof. We fix some notation before we start the actual proof. By Remark 1.3, A does not ramify at $\mathfrak{p}$ as $\mathfrak{p} \nmid \mathfrak{d}$ and hence we have $\hat{A}_\mathfrak{p} \cong \operatorname{Mat}_n(\hat{K}_\mathfrak{p})$. Now $\hat{\Lambda}_\mathfrak{p}$ is a maximal $\hat{R}_\mathfrak{p}$-order in $\hat{A}_\mathfrak{p}$ by [Rei06, Theorem 11.5], hence $\hat{\Lambda}_\mathfrak{p} \cong \operatorname{Mat}_n(\hat{R}_\mathfrak{p})$ and $\operatorname{rad} \hat{\Lambda}_\mathfrak{p} \cong \mathfrak{p}\hat{\Lambda}_\mathfrak{p}$ by [Rei06, Theorem 17.3] and [Rei06, Corollary 17.5]. Set

$$\overline{\Lambda} := \Lambda/\mathfrak{p}\Lambda \cong \hat{\Lambda}_\mathfrak{p}/\mathfrak{p}\hat{\Lambda}_\mathfrak{p} \text{ and } \overline{R} := R/\mathfrak{p} \cong \hat{R}_\mathfrak{p}/\mathfrak{p}\hat{R}_\mathfrak{p},$$

so $\overline{\Lambda} \cong \operatorname{Mat}_n(\overline{R})$ by [Rei06, Corollary 17.5] again. Note that also $\operatorname{rad} \Lambda_\mathfrak{p} = \mathfrak{p}\Lambda_\mathfrak{p}$ and accordingly $\overline{\Lambda} = \Lambda_\mathfrak{p}/\mathfrak{p}\Lambda_\mathfrak{p}$.

We have $\Lambda/M \cong \Lambda/N \cong \overline{R}^n$ as $\overline{\Lambda}$-modules, as these are simple modules in a matrix algebra (see [Bou58, §5, Proposition 11] and [Bou58, §5, Théorème 2]). This gives short exact sequences of Λ-modules

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r] & \Lambda \arrow[r, "\varphi"] & \overline{R}^n \arrow[r] & 0 \end{tikzcd}$$

and

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r] & \Lambda \arrow[r, "\psi"] & \overline{R}^n \arrow[r] & 0, \end{tikzcd}$$

where the Λ-linear maps φ and ψ are completely defined by the image of 1, that is by $\varphi(1), \psi(1) \in \overline{R}^n$, as there is an isomorphism $\operatorname{Hom}_\Lambda(\Lambda, \overline{R}^n) \cong \overline{R}^n$ defined by $\varphi \mapsto \varphi(1)$, see [Rei06, Theorem 2.7]. Suppose $\varphi(1)$ and $\psi(1)$ are linearly dependent over $\overline{R}^n$, so there exists $a \in R \setminus \mathfrak{p}$ such that $\varphi(1) = a\psi(1)$. Then $(\varphi - a\psi)(1) = 0$, so $\varphi - a\psi = 0$. As $0 \neq \overline{a} \in \overline{R}$, it follows $M = \ker \varphi = \ker \psi = N$, which proves the assertion.

Suppose now that $\varphi(1)$ and $\psi(1)$ are linearly independent over $\overline{R}$. As $\overline{\Lambda}$ is a finite ring, we may choose a finite set of elements $\tau_1, \ldots, \tau_k \in \Lambda$, such that $\overline{\Lambda}^\times = \{\overline{\tau}_1, \ldots, \overline{\tau}_k\}$. Each τ_i is also a unit in $\Lambda_\mathfrak{p}$ (see [Rei06, Exercise 6.2], it is a consequence of Nakayama's Lemma). Let now λ be an element as in Lemma 2.6 and denote by λ_L the map on the $\overline{\Lambda}$-module $\overline{R}^n$ induced by left multiplication by $\overline{\lambda} \in \overline{\Lambda}$. The $\overline{R}$-linear map λ_L has no eigenvalues in $\overline{R}$ since the minimal polynomial of $\overline{\lambda}$ has no zeros in $\overline{R}$. Hence any non-zero vector $v \in \overline{R}^n$ is linear independent of $\overline{\lambda}v$. Choosing any such v there exists an $\overline{R}$-linear transformation T mapping $\varphi(1)$ to v and $\psi(1)$ to $\overline{\lambda}v$. Since

$$\overline{\Lambda} \cong \operatorname{Mat}_n(\overline{R}) \cong \operatorname{Hom}_{\overline{R}}(\overline{R}^n, \overline{R}^n),$$

this T must be given by left multiplication by a unit of $\overline{\Lambda}$, so there exists an $i \in \{1, \ldots, k\}$ such that $\overline{\tau}_i\varphi(1) = v$ and $\overline{\tau}_i\psi(1) = \overline{\lambda}v$. Then

$$\psi(1) = \overline{\tau}_i^{-1}\overline{\lambda}\overline{\tau}_i\varphi(1),$$

so $\psi(1) = \vartheta\varphi(1)$, with $\vartheta := \tau_i^{-1}\lambda\tau_i \in \Lambda^\times$ by Lemma 2.6. It follows

$$\begin{aligned} N = \ker \psi = \ker(\vartheta\varphi) &= \{\alpha \in \Lambda \mid (\vartheta\varphi)(\alpha) = 0\} = \{\alpha \in \Lambda \mid \varphi(\alpha\vartheta) = 0\} \\ &= \{\alpha \in \Lambda \mid \alpha\vartheta \in M\} = M\vartheta^{-1}, \end{aligned}$$

where we have to swap α and ϑ in the fourth step, because the Λ-action on $\operatorname{Hom}_\Lambda(\Lambda, \overline{R}^n)$ arises from the Λ-Λ-bimodule structure of Λ, see [Rei06, p. 9]. Hence $M = N\vartheta$ with $\vartheta \in \Lambda^\times$ as claimed. □

Dropping the maximality of the ideals in Proposition 2.7 gives the following result.

Proposition 2.8. *Let Λ, $\Lambda_1, \dots, \Lambda_t$ and r be as in Proposition 2.7. Let I and J be integral ideals with left order Λ, such that $\operatorname{nr} I = \operatorname{nr} J$ and $\operatorname{nr} I + r\mathfrak{d} = R$. Then there exists $\vartheta \in A^\times$ with $I = J\vartheta$.*

Proof. Let $\operatorname{nr} I = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_k$ for prime ideals $\mathfrak{p}_i \in \mathbb{P}(R)$. By Theorem 1.8, we may factorize I and J into maximal integral ideals

$$I = M_1M_2 \cdots M_k \text{ and } J = N_1N_2 \cdots N_k.$$

The number of factors k is indeed the same in both cases since $\operatorname{nr} I = \operatorname{nr} J$ and each factor corresponds to a prime divisor of the reduced norm (see Lemma 3.9). By Theorem 1.9, we may assume that $\operatorname{nr} M_1 = \operatorname{nr} N_1 = \mathfrak{p}_1$ in the above factorizations.

We now prove the claim by induction on k. In case $k = 0$ there is nothing to show and in case $k = 1$ this is Proposition 2.7.

So let $k > 1$. Since $\mathfrak{p}_1 + r\mathfrak{d} = R$ it follows $M_1 = N_1\vartheta$ by Proposition 2.7 for a $\vartheta \in \Lambda^\times$. Let $I' := M_2 \cdots M_k$, $J' := \vartheta^{-1}N_2 \cdots N_k\vartheta$ and set $\Lambda' := \mathcal{O}_l(I')$. By Lemma 1.5, it holds

$$\begin{aligned}\Lambda' = \mathcal{O}_l(M_2) = \mathcal{O}_r(M_1) = \mathcal{O}_r(N_1\vartheta) = \vartheta^{-1}\mathcal{O}_r(N_1)\vartheta\\ = \vartheta^{-1}\mathcal{O}_l(N_2)\vartheta = \mathcal{O}_l(\vartheta^{-1}N_2) = \mathcal{O}_l(J').\end{aligned}$$

Now I' is an integral ideal of Λ' since proper products of integral ideals are integral by Theorem 1.6. Accordingly $N_2 \cdots N_k$ is an integral ideal of $\mathcal{O}_l(N_2)$, hence $N_2 \cdots N_k \subseteq \mathcal{O}_l(N_2)$, so $J' \subseteq \vartheta^{-1}\mathcal{O}_l(N_2)\vartheta = \Lambda'$ and J' is an integral ideal of Λ' too. Note that $\operatorname{nr} I' = \operatorname{nr} J'$ and $\operatorname{nr} I' + r\mathfrak{d} = R$.

There exists $\alpha \in A^\times$ and $i \in \{1, \dots, t\}$ such that $\Lambda' = \alpha\Lambda_i\alpha^{-1}$. Set $\Lambda'_j := \alpha\Lambda_j\alpha^{-1}$ for each $j = 1, \dots, t$. This is clearly a system of representatives of the maximal R-orders of A and we have

$$r\Lambda'_j = \alpha r\Lambda_j\alpha^{-1} \subseteq \alpha\Lambda_{j'}\alpha^{-1} = \Lambda'_{j'}$$

for any $j, j' \in \{1, \dots, t\}$ by choice of r. So, r and the Λ'_j fulfil the conditions of Remark 2.4. Hence we may assume by induction that there exists $\vartheta' \in A^\times$ with $I' = J'\vartheta'$.

Putting everything together we have

$$I = M_1I' = M_1J'\vartheta' = N_1\vartheta J'\vartheta' = J\vartheta\vartheta',$$

where $\vartheta\vartheta' \in A^\times$ as claimed. □

Lemma 2.9. *Let I be an integral ideal with left order Λ and let $\mathfrak{a}$ be any ideal of R. If $I + \mathfrak{a}\Lambda = \Lambda$ then it holds $\operatorname{nr} I + \mathfrak{a} = R$.*

Proof. Let $\mathfrak{p} \in \mathbb{P}(R)$ divide $\mathfrak{a}$. We have $\hat{I}_\mathfrak{p} + \mathfrak{a}\hat{\Lambda}_\mathfrak{p} = \hat{\Lambda}_\mathfrak{p}$ and hence $\hat{I}_\mathfrak{p} + \mathfrak{p}\hat{\Lambda}_\mathfrak{p} = \hat{\Lambda}_\mathfrak{p}$. By Nakayama's Lemma it follows $\hat{I}_\mathfrak{p} = \hat{\Lambda}_\mathfrak{p}$. By Lemma 1.14, we hence have

$$\widehat{(\operatorname{nr} I)}_\mathfrak{p} = \operatorname{nr} \hat{I}_\mathfrak{p} = \operatorname{nr} \hat{\Lambda}_\mathfrak{p} = \hat{R}_\mathfrak{p},$$

which proves the claim. □

We are now ready to prove the Theorem of Eichler.

Theorem 2.10 (Eichler)**.** *Let A be a central simple K-algebra satisfying the Eichler condition relative to R and let I be any normal ideal in A. Then I is a principal ideal if and only if its reduced norm $\operatorname{nr} I$ is a principal ideal Ra for some $a \in K_A^+$.*

Proof. Let Λ be the left order of I and let $r \in R$ as in Remark 2.4.

If I is a principal ideal, then $I = \Lambda\alpha$ for some $\alpha \in A$. Hence $\operatorname{nr} I = \operatorname{nr}(\Lambda\alpha) = R \operatorname{nr}\alpha$ by Lemma 1.12 and $\operatorname{nr}\alpha \in K_A^+$ by Theorem 1.1.

Now assume $\operatorname{nr} I = Ra$ for some $a \in K_A^+$. By [Rei06, Corollary 27.7], there exists $\beta \in A^\times$ such that $I\beta$ is integral, that is $I\beta \subseteq \Lambda$, and

$$I\beta + r\mathfrak{d}\Lambda = \Lambda.$$

We have $\Lambda = \mathcal{O}_l(I\beta)$ by Lemma 1.5 and by Lemma 1.12 it follows

$$\operatorname{nr}(I\beta) = \operatorname{nr} I \operatorname{nr}\beta = Ra \operatorname{nr}\beta,$$

where $a \operatorname{nr}\beta \in K_A^+$ by Theorem 1.1. Further, if $I\beta = \Lambda\gamma$ for a $\gamma \in A$ then $I = \Lambda\gamma\beta^{-1}$, so it suffices to prove that $I\beta$ is principal. In what follows we may thus assume that I is an integral ideal of Λ and $I + r\mathfrak{d}\Lambda = \Lambda$. Note that then $a \in R \cap K_A^+$.

By Lemma 2.9, it holds

$$\operatorname{nr} I + r\mathfrak{d} = Ra + r\mathfrak{d} = R$$

and by Theorem 2.3, there exists an integral element $\alpha \in A^\times$ with $\operatorname{nr}\alpha = a$. If $\alpha \in \Lambda$ then $\operatorname{nr} I = \operatorname{nr}(\Lambda\alpha)$, hence $I = (\Lambda\alpha)\vartheta$ for some $\vartheta \in A^\times$ by Proposition 2.8.

It remains to show the claim for $\alpha \notin \Lambda$. By [Swa86, Lemma 9.24], there exists a maximal R-order Λ' containing α. Consider the normal ideal $(\Lambda'\Lambda)^{-1}$ with left order Λ and right order Λ'. As at the beginning of this proof there exists $\delta \in A^\times$ such that for $J := (\Lambda'\Lambda)^{-1}\delta$ we have

$$J \subseteq \Lambda \text{ and } J + r\mathfrak{d}\Lambda = \Lambda,$$

and hence $\operatorname{nr} J + r\mathfrak{d} = R$ by Lemma 2.9. Then also $N(J) + r\mathfrak{d} = R$ and we may thus choose $b \in N(J)$ with $bR + r\mathfrak{d} = R$. By Lemma 1.10, it holds $N(J) \subseteq J$, so $b \in J \cap R$. Hence

$$b\delta^{-1}\alpha\delta \in J\delta^{-1}\Lambda'\delta,$$

where $\delta^{-1}\Lambda'\delta = \mathcal{O}_r(J)$ by Lemma 1.5, and it follows

$$b\delta^{-1}\alpha\delta \in J\mathcal{O}_r(J) \subseteq J \subseteq \Lambda.$$

Therefore $I' := \Lambda b\delta^{-1}\alpha\delta$ is an integral ideal with left order Λ and, since $b \in R$, so is Ib. Now

$$\operatorname{nr}(Ib) = \operatorname{nr} I \operatorname{nr} b = Rab^n$$

as well as

$$\operatorname{nr} I' = R \operatorname{nr} b \operatorname{nr}(\delta^{-1}\alpha\delta) = Rb^n a$$

and a and b are coprime to $r\mathfrak{d}$. Hence there exists $\vartheta' \in A^\times$ with $Ib = I'\vartheta'$ by Proposition 2.8 and I is a principal ideal as claimed. □

Following the proof, we can already state an algorithm for Theorem 2.10, making use of the algorithms which we are going to present in the following chapters.

Algorithm 2.11 (Principal generator)**.**

Input: A normal ideal I with left order Λ in a central simple algebra A satisfying the Eichler condition relative to R.

Output: An element $\alpha \in A^\times$ such that $I = \Lambda\alpha$, if such an element exists.

```
 1: Compute a system of representatives $\Lambda = \Lambda_1, \dots, \Lambda_t$ of the maximal $R$-orders using Algorithm 3.13.
 2: Compute $r \in R \setminus \{0\}$ with $r\Lambda_i \subseteq \Lambda_j$ for each $i, j \in \{1, \dots, t\}$ using Algorithm 3.2 (see Remark 3.4).
 3: Compute $\beta \in A^\times$ such that $I\beta \subseteq \Lambda$ and $I\beta + r\mathfrak{d}\Lambda = \Lambda$, where $\mathfrak{d}$ is the discriminant of $\Lambda$, using Algorithm 3.7.
 4: Set $J := I\beta$.
 5: if there does not exist an $a \in K_A^+ \cap R$ such that $\operatorname{nr} J = Ra$ then
 6:     stop $I$ is not a principal ideal.
 7: end if
 8: Find $\alpha \in \Lambda$ with $R(\operatorname{nr} \alpha) = \operatorname{nr} J$ using Algorithm 4.17.
 9: Compute $\vartheta \in A^\times$ with $J = \Lambda\alpha\vartheta$ using Algorithm 5.1.
10: return $\alpha\vartheta\beta^{-1}$.
```

The correctness of Algorithm 2.11 is clear by the previous proof. For the check in line 5 we use [Coh00, Algorithm 4.3.2].

The following chapters are now dedicated to presenting the algorithms used in Algorithm 2.11. Before we start, we state a generalization of Proposition 2.8 for later reference.

Corollary 2.12. *Let Λ be a maximal R-order in A, where A satisfies the Eichler condition relative to R. Let I and J be normal ideals with left order Λ in A. Then it holds*

$$J = I\alpha \textit{ for some } \alpha \in A^\times \textit{ if and only if } \operatorname{nr} J = a \operatorname{nr} I \textit{ for some } a \in K_A^+.$$

Proof. This follows from considering the ideal $I^{-1}J$, see [Rei06, Corollary 34.21] for details. □

3. Algorithms for ideals

In this chapter we present various algorithms mostly concerned with ideals in A.

The first section (3.1) is dedicated to finding integral and coprime representatives of ideals as needed in line 3 of Algorithm 2.11. We then (Section 3.2) consider the problem of computing maximal integral ideals with a chosen left order, as this is needed for the computation of representatives of the maximal orders in Section 3.3. Another application is the factorization of integral ideals, which we discuss in Section 3.4 as we require this in Chapter 5.

For Sections 3.1, 3.2, and 3.4 we do not have to assume that the algebra A fulfils the Eichler condition relative to R.

3.1. Integral and coprime representatives of ideal classes

Let Λ be a maximal R-order, let I be a normal ideal and let J be an integral ideal, both with left order Λ. [Rei06, Corollary 27.7] guarantees the existence of an $\alpha \in A^\times$ such that $I\alpha$ is an integral ideal, which is coprime to J, that is $I\alpha + J = \Lambda$. See also Proposition 3.6 for a proof. In this section we describe an algorithm to compute such an $\alpha \in A^\times$. The main ideas of this algorithm are already hidden in [Rei06, Theorem 27.1] and [Rei06, Exercise 18.3]. Bley and Johnston describe in [BJ11, Section 5.1] a similar algorithm in a more general situation, where I is any module of Λ. We will repeat some of the arguments, but also provide more details since I is an ideal.

Let $a \in J \cap R \setminus \{0\}$ be any element and consider the ideal $\mathfrak{a} := Ra$. Then $\mathfrak{a}\Lambda \subseteq J$, so if $I\alpha + \mathfrak{a}\Lambda = \Lambda$ for an $\alpha \in A^\times$, then $I\alpha + J = \Lambda$. Hence it suffices to consider the case $J = \mathfrak{a}\Lambda$ for an ideal $\mathfrak{a}$ of R.

We first treat the special case where $\mathfrak{a}$ is a prime ideal of R. So let $\mathfrak{p} \in \mathbb{P}(R)$ be any prime. By [Rei06, Theorem 18.10], I is locally free at $\mathfrak{p}$. Hence there exists an $\alpha \in I$ such that $I_\mathfrak{p} = \Lambda_\mathfrak{p}\alpha$, which we may find using the algorithm described in [BW09, Section 4.2]. We call an element with this properties a *local generator* of I at $\mathfrak{p}$ in what follows.

Remark 3.1. Let $\alpha \in I$ be a local generator of I at $\mathfrak{p}$. Then it holds $\alpha \in A^\times$: Indeed, there is a surjective map $\Lambda_\mathfrak{p} \xrightarrow{\cdot\alpha} I_\mathfrak{p}$ of free $R_\mathfrak{p}$-modules of same rank, so this is an isomorphism. This induces an isomorphism $K\Lambda_\mathfrak{p} \cong KI_\mathfrak{p}$ and we have $A = K\Lambda_\mathfrak{p}$ and $A = KI_\mathfrak{p}$, so $\alpha \in A^\times$.

From $I_\mathfrak{p} = \Lambda_\mathfrak{p}\alpha$ it follows $I_\mathfrak{p}\alpha^{-1} = \Lambda_\mathfrak{p}$ and therefore $I\alpha^{-1} \subseteq \Lambda_\mathfrak{p}$. The next task is to find an $x \in R \setminus \mathfrak{p}$ such that $I\alpha^{-1}x \subseteq \Lambda$. For the algorithm solving this, we assume that Λ and I are given by pseudo bases, so

$$\Lambda = \bigoplus_{i=1}^{n^2} \mathfrak{a}_i\alpha_i \text{ and } I = \bigoplus_{i=1}^{n^2} \mathfrak{b}_i\beta_i$$

for fractional ideals $\mathfrak{a}_i$ and $\mathfrak{b}_i$ of R and elements $\alpha_i, \beta_i \in A$.

Algorithm 3.2 (Coprime denominator).

Input: An ideal I with left order Λ and $\mathfrak{p} \in \mathbb{P}(R)$ with $I_{\mathfrak{p}} \subseteq \Lambda_{\mathfrak{p}}$.

Output: $x \in R \setminus \mathfrak{p}$ with $Ix \subseteq \Lambda$.

```
1: Rescale the pseudo bases of $\Lambda$ and $I$ such that the coefficient ideals have no valuation
   at $\mathfrak{p}$ resulting in pseudo bases $(\mathfrak{a}_i, \alpha_i)_{1 \le i \le n^2}$ respectively $(\mathfrak{b}_i, \beta_i)_{1 \le i \le n^2}$, as described
   in Appendix B.
2: Find $c_{ij} \in K$ with $\beta_i = \sum_{j=1}^{n^2} c_{ij}\alpha_j$.
3: Set $\mathfrak{c}_{ij} := \mathfrak{b}_i \cdot \mathfrak{a}_j^{-1} \cdot c_{ij}$ for all $1 \le i, j \le n^2$.
4: Determine the set $S \subseteq \mathbb{P}(R)$ of prime ideals $\mathfrak{q}$ with $v_{\mathfrak{q}}(\mathfrak{c}_{ij}) < 0$ for at least one pair
   of indices $i, j \in \{1, \dots, n^2\}$.
5: for $\mathfrak{q} \in S$ do
6:     $e_{\mathfrak{q}} := \max\big\{ -v_{\mathfrak{q}}(\mathfrak{c}_{ij}) \mid 1 \le i, j \le n^2 \big\}$
7: end for
8: Compute $x \in R$ with $v_{\mathfrak{q}}(x) = e_{\mathfrak{q}}$ for all $\mathfrak{q} \in S$ and $v_{\mathfrak{p}}(x) = 0$.
9: return $x$
```

Lemma 3.3. *Let I be an ideal with left order Λ and $\mathfrak{p} \in \mathbb{P}(R)$ with $I_{\mathfrak{p}} \subseteq \Lambda_{\mathfrak{p}}$. Then Algorithm 3.2 correctly finds an element $x \in R \setminus \mathfrak{p}$ with $Ix \subseteq \Lambda$.*

Proof. With the notation from the algorithm, we have $x\mathfrak{c}_{ij} \subseteq R$ and hence $x\mathfrak{b}_i c_{ij} \subseteq \mathfrak{a}_j$ for all $1 \le i, j \le n^2$. So for $\gamma \in I$ with $\gamma = \sum_{i=1}^{n^2} b_i\beta_i$, $b_i \in \mathfrak{b}_i$, we have

$$\gamma x = \sum_{i=1}^{n^2} b_i \beta_i x = \sum_{i=1}^{n^2} b_i \Big(\sum_{j=1}^{n^2} c_{ij}\alpha_j \Big) x = \sum_{j=1}^{n^2} \underbrace{\Big(\sum_{i=1}^{n^2} b_i c_{ij} x \Big)}_{\in \mathfrak{a}_j} \alpha_j \in \Lambda$$

and therefore it holds $Ix \subseteq \Lambda$.

It remains to show that $\mathfrak{p} \notin S$. The localizations $\Lambda_{\mathfrak{p}}$ and $I_{\mathfrak{p}}$ are free $R_{\mathfrak{p}}$-modules with bases $\{\alpha_1, \dots, \alpha_{n^2}\}$ and $\{\beta_1, \dots, \beta_{n^2}\}$ respectively because of the rescaling in line 1. Since $I_{\mathfrak{p}} \subseteq \Lambda_{\mathfrak{p}}$ by assumption, we have $\beta_i \in \Lambda_{\mathfrak{p}}$ for $1 \le i \le n^2$. Therefore the c_{ij} in line 2 will lie in $R_{\mathfrak{p}}$, so $v_{\mathfrak{p}}(c_{ij}) \ge 0$ for all i and j. As the valuation of the coefficient ideals is 0 at $\mathfrak{p}$, we have $v_{\mathfrak{p}}(\mathfrak{c}_{ij}) \ge 0$ for all $1 \le i, j \le n^2$ and hence $\mathfrak{p} \notin S$. □

Remark 3.4. Let M and N be two full R-lattices in A. Then we can use Algorithm 3.2 to find $x \in R$ such that $Mx \subseteq N$ by omitting line 1 and the requirement $v_{\mathfrak{p}}(x) = 0$ in line 8. However, the algorithm ensures, that the returned element has no valuation at $\mathfrak{p}$. As this is not required, it should usually be faster to compute denominators of the ideals $\mathfrak{c}_{ij}$ in $\mathbb{Z}$ and return the least common multiple of these denominators instead of lines 4 to 8.

Summing up, we can compute a local generator $\alpha \in I \cap A^{\times}$ of I at a prime $\mathfrak{p}$ and then compute an $x \in R \setminus \mathfrak{p}$ using Algorithm 3.2 such that $I\alpha^{-1}x \subseteq \Lambda$. Then $1 \in I\alpha^{-1}$, so $x \in I\alpha^{-1}x$, and therefore $I\alpha^{-1}x + \mathfrak{p}\Lambda = \Lambda$ since $\mathfrak{p}$ is coprime to the ideal Rx. So we have solved the problem for prime ideals. We now come back to the initial problem of an arbitrary ideal $\mathfrak{a}$ and describe how to combine the solutions for different prime ideals.

Lemma 3.5. *Let Λ be a maximal order and let I be a normal ideal with left order Λ and let $\{\mathfrak{p}_1, \dots, \mathfrak{p}_k\} \subseteq \mathbb{P}(R)$. Then there exists $\alpha \in A^\times$ such that the map*

$$\varphi : I \to \Lambda,\ \beta \mapsto \beta\alpha$$

is injective and the induced map $\varphi_{\mathfrak{p}_i} : I_{\mathfrak{p}_i} \to \Lambda_{\mathfrak{p}_i}$ is an isomorphim for each $i \in \{1, \dots, k\}$.

Proof. First assume $k = 0$. Then we can use Algorithm 3.2 (see Remark 3.4) to compute $\alpha \in R \setminus \{0\}$ with $I\alpha \subseteq \Lambda$, which is a unit of A since it is a unit of K. Hence α fulfils the requirements in this case.

Now let $k \geq 1$. Let $\alpha_i \in I \cap A^\times$ for each $1 \leq i \leq k$ be a local generator of I at $\mathfrak{p}_i$. By Lemma 3.3, there exists $x_i \in R \setminus \mathfrak{p}_i$ for each $i \in \{1, \dots, k\}$ such that $I\alpha_i^{-1}x_i \subseteq \Lambda$. Let now $y_i \in R$ such that

$$v_{\mathfrak{p}_i}(y_i) = 0 \text{ and } v_{\mathfrak{p}_j}(y_i) > 0 \text{ for all } j \neq i$$

and set $\alpha := \sum_{i=1}^k \alpha_i^{-1}x_iy_i$. Since y_i is chosen in R it holds $I\alpha_i^{-1}x_iy_i \subseteq \Lambda y_i \subseteq \Lambda$. As this holds for any i we have

$$I\alpha \subseteq I\alpha_1^{-1}x_1y_1 + \dots + I\alpha_k^{-1}x_ky_k \subseteq \Lambda,$$

hence $\varphi : I \to \Lambda,\ \beta \mapsto \beta\alpha$ is well-defined.

We show that the local maps $\varphi_{\mathfrak{p}_i}$ are isomorphisms for all i. For this fix any $i \in \{1, \dots, k\}$ and set $\mathfrak{p} := \mathfrak{p}_i$ for ease of notation. By construction we have

$$I\alpha_j^{-1}x_jy_j \subseteq \mathfrak{p}\Lambda_{\mathfrak{p}} \text{ for all } j \neq i \text{ and } I_{\mathfrak{p}}\alpha_i^{-1}x_iy_i = \Lambda_{\mathfrak{p}}$$

since $v_{\mathfrak{p}}(x_iy_i) = 0$, so $x_iy_i \in (R_{\mathfrak{p}})^\times$. Hence $\varphi_{\mathfrak{p}}$ is surjective by Nakayama's Lemma. By the same argument as in Remark 3.1 it follows that $\varphi_{\mathfrak{p}}$ is an isomorphism and therefore α a unit of A. Then φ must be injective too. □

Proposition 3.6. *Let Λ be a maximal order, let I be a normal ideal and J be an integral ideal, both with left order Λ. Then there exists $\alpha \in A^\times$ such that $I\alpha + J = \Lambda$. In particular, $I\alpha \subseteq \Lambda$.*

Proof. We follow [Rei06, Theorem 27.1] and [Rei06, Corollary 27.7]. Let $\mathfrak{a} \trianglelefteq R$ be any ideal such that $\mathfrak{a}\Lambda \subseteq J$, e. g. choose any $a \in J \cap R \setminus \{0\}$ and set $\mathfrak{a} := aR$. Let $\mathrm{Supp}_R(\mathfrak{a}) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}$. Then Lemma 3.5 yields an $\alpha \in A^\times$ such that the map

$$\varphi : I \to \Lambda,\ \beta \mapsto \beta\alpha$$

is injective and $\varphi_{\mathfrak{p}_i}$ is an isomorphism for each $1 \leq i \leq k$. Hence we have a short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & I \arrow[r, "\varphi"] & \Lambda \arrow[r] & T \arrow[r] & 0, \end{tikzcd}$$

with $T := \operatorname{coker}\varphi$. As $\varphi_{\mathfrak{p}_i}$ is an isomorphism, it follows $T_{\mathfrak{p}_i} = 0$, which implies

$$\operatorname{ann}_R T + \mathfrak{p}_i = R$$

by [Rei06, Theorem 4.20 (iii)] for each $i \in \{1, \dots, k\}$. It follows $\operatorname{ann}_R T + \mathfrak{a} = R$, so there exist $u \in \operatorname{ann}_R T$ and $v \in \mathfrak{a}$ such that $u + v = 1$. It holds $\operatorname{ann}_R T \subseteq \operatorname{im}\varphi$, so $u \in \operatorname{im}\varphi = I\alpha$. This yields $I\alpha + \mathfrak{a}\Lambda = \Lambda$ and finally $I\alpha + J = \Lambda$. □

The proof of Lemma 3.5 gives the following algorithm which is correct by Proposition 3.6.

Algorithm 3.7 (Coprime and integral representative)**.**

Input: A normal ideal I and an integral ideal J, both with left order Λ.

Output: $\alpha \in A^\times$ with $I\alpha + J = \Lambda$ and $I\alpha \subseteq \Lambda$.

```
 1: Choose $\mathfrak{a} \trianglelefteq R$ with $\mathfrak{a}\Lambda \subseteq J$ and let $\mathrm{Supp}_R(\mathfrak{a}) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}$.
 2: if $\mathfrak{a} = R$ then
 3:     Find $x \in R$ with $Ix \subseteq \Lambda$ using Algorithm 3.2 (see Remark 3.4).
 4:     return $x$
 5: end if
 6: for $i \in \{1, \dots, k\}$ do
 7:     Find $\alpha_i \in A^\times$ with $I_{\mathfrak{p}_i} = \Lambda_{\mathfrak{p}_i}\alpha_i$.
 8:     Using Algorithm 3.2 with input $I\alpha_i^{-1}$ and $\mathfrak{p}_i$, compute $x_i \in R \setminus \mathfrak{p}_i$ with
            $$(I\alpha_i^{-1})x_i \subseteq \Lambda.$$
 9:     Compute $y_i \in R$ with $v_{\mathfrak{p}_i}(y_i) = 0$ and $v_{\mathfrak{p}_j}(y_i) = 1$ for all $j \neq i$.
10: end for
11: return $\sum_{i=1}^k \alpha_i^{-1} x_i y_i$
```

For $\mathfrak{a}$ in line 1 we may always choose $a \in J \cap R \setminus \{0\}$ and set $\mathfrak{a} = aR$. However, in our application we will already be given $J = \mathfrak{a}\Lambda$ for an ideal $\mathfrak{a} \trianglelefteq R$. To avoid an unnecessarily large α, one should do lines 7 and 8 for an index $i \in \{1, \dots, k\}$ only if needed, that is, if $I + \mathfrak{p}_i\Lambda \neq \Lambda$.

For line 9 as well as line 8 of Algorithm 3.2 one can use [Hop98, Algorithm 1.7.5].

3.2. Computing maximal ideals

Let Λ be a maximal R-order and $\mathfrak{p}$ a prime ideal of R. We describe an algorithm to compute a maximal integral ideal M with left order Λ and $M \cap R = \mathfrak{p}$.

We first reduce the given problem to finding a maximal left ideal in a matrix algebra over a finite field.

Let $\mathfrak{P}$ be the unique prime ideal of Λ lying over $\mathfrak{p}$ (see Theorem 1.7). The maximal integral ideals with left order Λ, which contain $\mathfrak{p}$ and hence $\mathfrak{P}$, are by definition maximal left ideals[1] of Λ and correspond thus to the maximal left ideals of $\Lambda/\mathfrak{P}$. This algebra $\Lambda/\mathfrak{P}$ is a simple algebra over $R/\mathfrak{p}$: Again, any two-sided ideal of $\Lambda/\mathfrak{P}$ corresponds to a two-sided ideal of Λ containing $\mathfrak{P}$. But $\mathfrak{P}$ is a maximal two-sided ideal of Λ by [Rei06, Theorem 22.3], so $\Lambda/\mathfrak{P}$ contains no non-trivial two-sided ideals. By [CR81, Theorem 3.28], it follows that $\Lambda/\mathfrak{P} \cong \mathrm{Mat}_k(D)$ for a skewfield D over $R/\mathfrak{p}$ and some $k \in \mathbb{N}$. As $R/\mathfrak{p}$ is a finite field, this skewfield D will actually be a field by [Rei06, Theorem 7.24]. So, $\Lambda/\mathfrak{P} \cong \mathrm{Mat}_k(\mathbb{F}_q)$ for a prime power q and we are left with the task of finding a maximal left ideal in this matrix algebra which we discuss in Appendix A, see Remark A.4 (one can also use Algorithm A.5 with input $I = 0$).

This gives the following algorithm.

[1] Recall that we say left respectively two-sided ideal for the "usual" ideals of a ring.

Algorithm 3.8 (Maximal integral ideal containing a given prime ideal)**.**

```
Input: A maximal $R$-order $\Lambda$, a prime ideal $\mathfrak{p} \trianglelefteq R$.
Output: A maximal integral ideal $M$ with left order $\Lambda$ and $M \cap R = \mathfrak{p}$.
Compute the prime ideal $\mathfrak{P}$ lying over $\mathfrak{p}$ and the quotient $\Lambda/\mathfrak{P}$ as an $R/\mathfrak{p}$-algebra together with the canonical map $\pi : \Lambda \to \Lambda/\mathfrak{P}$.
Find the isomorphism $\varphi : \Lambda/\mathfrak{P} \to \mathrm{Mat}_k(\mathbb{F}_q)$, where $\mathbb{F}_q$ is a finite field extension of $R/\mathfrak{p}$ isomorphic to the centre of $\Lambda/\mathfrak{P}$.
Let $v_i$, $1 \leq i \leq k^2 - k$, be an $\mathbb{F}_q$-basis of a maximal left ideal of $\mathrm{Mat}_k(\mathbb{F}_q)$.
Compute elements $\alpha_i \in \Lambda$ such that $\pi(\alpha_i) = \varphi^{-1}(v_i)$ for $1 \leq i \leq k^2 - k$.
Compute the ideal
    $M := \sum_{i=1}^{k^2-k} R\alpha_i + \mathfrak{P}.$
return $M$
```

The correctness of Algorithm 3.8 is clear by the discussion preceding it.

To compute the prime ideal $\mathfrak{P}$ we follow [Fri00, Chapter 5], that means, we compute $\mathfrak{P}$ via the Jacobson radical of the $R/\mathfrak{p}$-algebra $\Lambda/\mathfrak{p}\Lambda$. For more information regarding the computation of this quotient see Appendix B. To compute the Jacobson radical of an algebra over a finite field and to construct the isomorphism φ we use the algorithms described in [Ebe89, Section 2.3.2] and [Ebe89, Section 2.5] respectively.

We are now able to compute any maximal integral ideal. Next, we refine the above techniques to find a maximal integral ideal containing a given integral ideal, as this is needed in the following sections. Let Λ be a maximal order, let I be an integral ideal with left order Λ and let $\mathfrak{p} \in \mathbb{P}(R)$. We want to find a maximal integral ideal M with left order Λ, $M \cap R = \mathfrak{p}$ and $I \subseteq M$. The next lemma gives an criterion for the existence of such an ideal.

Lemma 3.9. *Let $\mathfrak{p} \in \mathbb{P}(R)$ and let I be an integral ideal with left order Λ. There exists a maximal integral ideal M with left order Λ, $M \cap R = \mathfrak{p}$ and $I \subseteq M$ if and only if $\mathfrak{p} \mid \operatorname{nr} I$.*

Proof. If $M \supseteq I$ with $M \cap R = \mathfrak{p}$ is given, then there exists an integral ideal J with left order $\mathcal{O}_r(M)$ such that $I = MJ$ by Theorem 1.6. We have $\operatorname{nr} M = \mathfrak{p}$ by Theorem 1.11 and by the multiplicativity of the norm, it follows $\mathfrak{p} \mid \operatorname{nr} I$.

Let now $\mathfrak{p} \mid \operatorname{nr} I$ and let $X_1, \ldots, X_k$ be the composition factors of the Λ-module Λ/I. Then $\mathfrak{p}$ is the R-annihilator of one of these factors by [Rei06, Corollary 24.14] and after reordering we may assume $\operatorname{ann}_R X_1 = \mathfrak{p}$. By Theorem 1.9, there exists a factorization $I = M_1 \cdots M_k$ of I into maximal integral ideals such that $\Lambda/M_1 \cong X_1$ and by Theorem 1.6 we have $I \subseteq M_1$. Let now $\mathfrak{P}$ be the unique prime ideal of Λ contained in M_1. Then $\mathfrak{P} = \operatorname{ann}_\Lambda \Lambda/M_1$ by Theorem 1.7. But $\mathfrak{p} = \operatorname{ann}_R \Lambda/M_1 \subseteq \operatorname{ann}_\Lambda \Lambda/M_1$, so $M_1 \cap R = \mathfrak{P} \cap R = \mathfrak{p}$. □

Let $\mathfrak{P}$ be the prime ideal of Λ lying over $\mathfrak{p}$. Then any maximal ideal M fulfilling the requirements will also fulfil $\mathfrak{P} \subseteq M$ and hence $I + \mathfrak{P} \subseteq M$. But $I + \mathfrak{P}$ corresponds to a left ideal in the simple $R/\mathfrak{p}$-algebra $\Lambda/\mathfrak{P}$ which is isomorphic to $\mathrm{Mat}_k(\mathbb{F}_q)$ for some $k \in \mathbb{N}$ and an extension $\mathbb{F}_q$ of $R/\mathfrak{p}$ as at the beginning of this section.

Using Algorithm A.5 we obtain the following algorithm.

Algorithm 3.10 (Maximal integral ideal containing a given ideal)**.**

```
Input: An integral ideal $I$ with left order $\Lambda$, a prime ideal $\mathfrak{p} \trianglelefteq R$ with $\mathfrak{p} \mid \operatorname{nr} I$ (see Lemma 3.9).
Output: A maximal integral ideal $M$ with left order $\Lambda$, $M \cap R = \mathfrak{p}$ and $I \subseteq M$.
Compute the prime ideal $\mathfrak{P}$ lying over $\mathfrak{p}$ and the quotient $\Lambda/\mathfrak{P}$ together with the canonical map $\pi : \Lambda \to \Lambda/\mathfrak{P}$.
Find the isomorphism $\varphi : \Lambda/\mathfrak{P} \to \mathrm{Mat}_k(\mathbb{F}_q)$, where $\mathbb{F}_q$ is a finite field extension of $R/\mathfrak{p}$ isomorphic to the centre of $\Lambda/\mathfrak{P}$.
Compute $J := \varphi(\pi(I + \mathfrak{P})) \trianglelefteq \mathrm{Mat}_k(\mathbb{F}_q)$.
Using Algorithm A.5 compute an $\mathbb{F}_q$-basis $v_1, \dots, v_{k^2-k}$ of a maximal left ideal of $\mathrm{Mat}_k(\mathbb{F}_q)$ containing $J$.
Compute elements $\alpha_i \in \Lambda$ such that $\pi(\alpha_i) = \varphi^{-1}(v_i)$ for $1 \leq i \leq k^2 - k$. Compute the ideal
    $M := \sum_{i=1}^{k^2-k} R\alpha_i + \mathfrak{P}.$
return $M$
```

The correctness of Algorithm 3.10 is again clear by the above discussion.

It should be pointed out that the main idea of Algorithm 3.10 is actually the reduction to $I' := I + \mathfrak{P}$, since one can then work in the finite algebra $\Lambda/\mathfrak{P}$. From this point on, one wants to find a maximal submodule of the $\Lambda/\mathfrak{P}$-module Λ/I', which could also be done using the Meat-Axe-Algorithm [Par84]. However, we are only interested in finding any maximal submodule, which is why we have chosen the given less elaborate approach.

3.3. Computing a system of representatives of the maximal orders

As we are now able to compute maximal integral ideals, we are prepared to describe an algorithm which computes a system of representatives for the conjugacy classes of maximal orders. In this section we rely again on the fact that A fulfils the Eichler condition relative to R. Let Λ be a maximal R-order in A. Firstly, we establish some notation: Let $\mathcal{I}(\Lambda)$ be the group of ideals with left and right order Λ (this *is* a group by [Rei06, Theorem 22.10]) and let

$$\mathcal{P}(\Lambda) := \{\alpha\Lambda \mid \alpha \in A^\times \text{ with } \alpha\Lambda = \Lambda\alpha\}$$

be the subgroup of principal ideals. Then we call

$$\mathrm{Cl}(\Lambda) := \mathcal{I}(\Lambda)/\mathcal{P}(\Lambda)$$

the *class group* of ideals with left and right order Λ.(2)

Let $S := S_\infty^A$ and K_A^+ be as in Chapter 1. We define $\mathrm{Cl}_S(R)$ to be the *ray class group* given by the quotient

$$\mathrm{Cl}_S(R) := \mathcal{I}(R)/\mathcal{P}_S(R),$$

(2) We differ here from the notation in [Rei06] where $\mathrm{Cl}(\Lambda)$ is the group of stable isomorphism classes of ideals with left order Λ.

where $\mathcal{I}(R)$ is the group of fractional ideals of R and $\mathcal{P}_S(R) := \{aR \mid a \in K_A^+\}$.

With this notation we can state the following lemmata (which are actually Exercise 38 in [Kir17]), whose proofs already give an algorithm for the computation of a system of representatives of conjugacy classes.

Lemma 3.11. *Let Λ be a maximal R-order in A. The map*

$$\varphi_\Lambda : \mathrm{Cl}(\Lambda) \to \mathrm{Cl}_S(R),\ [I] \mapsto [\mathrm{nr}\, I]_S$$

is an injective group homomorphism whose image is the group

$$H := \big\langle \{[\mathfrak{a}]_S^n \mid [\mathfrak{a}]_S \in \mathrm{Cl}_S(R)\} \cup \{[\mathfrak{p}]_S^{\kappa_\mathfrak{p}} \mid \mathfrak{p} \in \mathbb{P}(R) \text{ ramifying in } A\}\big\rangle.$$

In particular, the image does not depend on the choice of Λ, but is the same for each maximal R-order.

Proof. The map φ_Λ is well-defined by Corollary 2.12 and Theorem 1.1. It is a group homomorphism by the multiplicativity of the reduced norm.

For injectivity, let $[I], [J] \in \mathrm{Cl}(\Lambda)$ such that $[\mathrm{nr}\, I]_S = [\mathrm{nr}\, J]_S$, so $\mathrm{nr}\, I = a \,\mathrm{nr}\, J$ for some $a \in K_A^+$. Then there exists $\alpha \in A^\times$ such that $I = J\alpha$ by Corollary 2.12. Now we have

$$\Lambda = \mathcal{O}_r(I) = \mathcal{O}_r(J\alpha) = \alpha^{-1}\mathcal{O}_r(J)\alpha = \alpha^{-1}\Lambda\alpha$$

by Lemma 1.5. Hence $\alpha\Lambda = \Lambda\alpha$ and therefore $[I] = [J]$.

Since $\mathcal{I}(\Lambda)$ is generated by the prime ideals of Λ by [Rei06, Theorem 22.10], it suffices to consider the reduced norms of prime ideals for the last claim. Let $\mathfrak{P}$ be a prime ideal of Λ lying over the prime $\mathfrak{p}$ of R. As $\mathrm{nr}\,\mathfrak{P} = \mathfrak{p}^{\kappa_\mathfrak{p}}$ by Theorem 1.11, we already have $\operatorname{im}\varphi_\Lambda = \langle [\mathfrak{p}]_S^{\kappa_\mathfrak{p}} \mid \mathfrak{p} \in \mathbb{P}(R)\rangle$. Since $\kappa_\mathfrak{p} \mid n$ for all $\mathfrak{p}$ and $\kappa_\mathfrak{p} = n$, if $\mathfrak{p}$ does not ramify in A, we have

$$\operatorname{im}\varphi_\Lambda = \big\langle \{[\mathfrak{p}]_S^n \mid \mathfrak{p} \in \mathbb{P}(R)\} \cup \{[\mathfrak{p}]_S^{\kappa_\mathfrak{p}} \mid \mathfrak{p} \in \mathbb{P}(R) \text{ ramifies}\}\big\rangle = H$$

as claimed. □

Lemma 3.12. *It holds $[\mathrm{Cl}_S(R) : H] = t_R(A)$, where $t_R(A)$ is the type number of A and H is as in Lemma 3.11.*

Proof. Let $[R]_S, [\mathfrak{p}_1]_S, \ldots, [\mathfrak{p}_k]_S \in \mathrm{Cl}_S(R)$, $k = [\mathrm{Cl}_S(R) : H] - 1$, be a system of representatives for the equivalence classes of the quotient $\mathrm{Cl}_S(R)/H$. We may choose the first representative to be R as $[R]_S$ is the neutral element of the group and we may choose $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ to be prime ideals, since any ideal class in $\mathrm{Cl}_S(R)$ contains a prime ideal by [Nar04, Section 7.2, Corollary 7]. Now let Λ be any maximal R-order in A and let M_i be a maximal integral ideal with left order Λ such that $M_i \cap R = \mathfrak{p}_i$ for each i, so $\mathrm{nr}\, M_i = \mathfrak{p}_i$ by Theorem 1.11. We write $\mathfrak{p}_0 = R$ and $M_0 = \Lambda$ and claim that the orders $\mathcal{O}_r(M_i)$ for $0 \le i \le k$ form a system of representatives for the conjugacy classes of maximal orders.

Each of them is maximal by [Rei06, Theorem 21.2]. Assume that there exists $\alpha \in A^\times$ such that $\mathcal{O}_r(M_i) = \alpha^{-1}\mathcal{O}_r(M_j)\alpha$ for $0 \le i, j \le k$. Following [Kir17, Lemma 2.8.4], let $I := M_i^{-1}M_j\alpha$, so $M_iI = M_j\alpha$. Then

$$\mathcal{O}_l(I) = \mathcal{O}_l(M_i^{-1}) = \mathcal{O}_r(M_i)$$

by [Rei06, Corollary 22.8] and

$$\mathcal{O}_r(I) = \mathcal{O}_r(M_j\alpha) = \alpha^{-1}\mathcal{O}_r(M_j)\alpha = \mathcal{O}_r(M_i)$$

by Lemma 1.5, so $I \in \mathcal{I}(O_r(M_i))$ and hence $[\operatorname{nr} I]_S \in H$ by applying Lemma 3.11 to $\mathcal{O}_r(M_i)$. But

$$[\mathfrak{p}_i]_S[\operatorname{nr} I]_S = [\operatorname{nr} M_i]_S[\operatorname{nr} I]_S = [\operatorname{nr}(M_j\alpha)]_S = [\operatorname{nr} M_j]_S = [\operatorname{nr} \mathfrak{p}_j]_S,$$

so the classes $[\mathfrak{p}_i]_S$ and $[\mathfrak{p}_j]_S$ are equivalent modulo H which implies $i = j$. This shows that no two of the right orders are conjugated and hence $[\mathrm{Cl}_S(R) : H] \leq t_R(A)$.

Let Λ' be any maximal R-order. We have to show $\Lambda' = \alpha\Lambda_i\alpha^{-1}$ for some $\alpha \in A^\times$ and $i \in \{0, \dots, k\}$. Consider the ideal $I := \Lambda\Lambda'$ with left order Λ and right order Λ' (since clearly $\Lambda \subseteq \mathcal{O}_l(I)$ and Λ is maximal). Then $[\operatorname{nr} I]_S \in \mathrm{Cl}_S(R)$, so there exists $[\mathfrak{a}]_S \in H$ and $i \in \{0, \dots, k\}$ such that

$$[\operatorname{nr} I]_S[\mathfrak{a}]_S = [\mathfrak{p}_i]_S.$$

Applying Lemma 3.11 to Λ', we have $\operatorname{im} \varphi_{\Lambda'} = H$, so there exists $J \in \mathcal{I}(\Lambda')$ with $[\operatorname{nr} J]_S = [\mathfrak{a}]_S$. Hence $\operatorname{nr}(IJ) = (\operatorname{nr} M_i)a$ for an $a \in K_A^+$ and thus $IJ = M_i\alpha$ with $\alpha \in A^\times$ by Corollary 2.12. Now

$$\Lambda' = \mathcal{O}_r(IJ) = \mathcal{O}_r(M_i\alpha) = \alpha^{-1}\mathcal{O}_r(M_i)\alpha = \alpha^{-1}\Lambda_i\alpha$$

by Lemma 1.5, so we have indeed $[\mathrm{Cl}_S(R) : H] = t_R(A)$. □

The previous lemmata now give the following algorithm.

Algorithm 3.13 (Representatives of the conjugacy classes of maximal orders)**.**

Input: A maximal R-order Λ in A.

Output: Maximal R-orders $\Lambda_1, \dots, \Lambda_t$, such that each maximal order in A is conjugated to Λ_i for exactly one $i \in \{1, \dots, t\}$.

```
1: Determine the set $S$ and compute the ray class group $\mathrm{Cl}_S(R)$.
2: Determine the ramifying prime ideals of $R$ and their local capacities.
3: Compute $H := \langle \mathrm{Cl}_S(R)^n \cup \{[\mathfrak{p}^{\kappa_\mathfrak{p}}]_S \mid \mathfrak{p} \in \mathbb{P}(R), A \text{ ramified at } \mathfrak{p}\}\rangle$ and the quotient $\mathrm{Cl}_S(R)/H$.
4: Choose a system of representatives $[R]_S, [\mathfrak{p}_1]_S, \dots, [\mathfrak{p}_{t-1}]_S$ for the equivalence classes in $\mathrm{Cl}_S(R)/H$, where $\mathfrak{p}_i \trianglelefteq R$ is prime for each $i$.
5: For each $\mathfrak{p}_i$ find a maximal integral ideal $M_i$ with left order $\Lambda$ such that $M_i \cap R = \mathfrak{p}_i$ using Algorithm 3.8.
6: Compute the right orders $\mathcal{O}_r(M_1), \dots, \mathcal{O}_r(M_{t-1})$.
7: return $\Lambda, \mathcal{O}_r(M_1), \dots, \mathcal{O}_r(M_{t-1})$
```

The correctness of Algorithm 3.13 is ensured by Lemma 3.12.

To determine the set $S = S_\infty^A$ we compute the local indices of the algebra at all real places of K as described in [NS09] and to find the ramifying prime ideals we factor the discriminant of Λ, see Remark 1.3. For the computation of the ray class group and quotients of groups one may use [Coh00, Algorithm 4.3.1] and [Coh00, Algorithm 4.1.7] respectively. To find the prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_{t-1}$ we test “small” primes. This is a reasonable approach since each ideal class contains infinitely many prime ideals by [Nar04, Section 7.2, Corollary 7]. To compute right orders we use [Fri00, Algorithmus 2.16].

3.4. Factorizing ideals

Another application of the computation of maximal integral ideals is the factorization of an ideal. In this section, let I be an integral ideal with left order Λ. Recall that I can be written as a proper product of maximal integral ideals by Theorem 1.8.

Algorithm 3.14 (Factorization of integral ideals)**.**

Input: An integral ideal I with left order Λ.

Output: Maximal integral ideals $M_1, \dots, M_k$ as in Theorem 1.8.

```
1: Factorize the reduced norm: $\operatorname{nr} I = \mathfrak{p}_1 \cdots \mathfrak{p}_k$ with $\mathfrak{p}_i \in \mathbb{P}(R)$, $k \in \mathbb{N}$.
2: $J := I$
3: for $i = 1, \dots, k-1$ do
4:     Using Algorithm 3.10 compute a maximal ideal $M_i$ containing $J$ and $\mathfrak{p}_i$.
5:     Set $J := M_i^{-1} J$.
6: end for
7: return $M_1, \dots, M_{k-1}, J$
```

To prove the correctness of the algorithm we need the following lemma.

Lemma 3.15. *An integral ideal M with left order Λ is maximal if and only if its reduced norm $\operatorname{nr} M$ is a prime ideal.*

Proof. If M is maximal, then $\operatorname{nr} M \in \mathbb{P}(R)$ by Theorem 1.11.

On the other hand, if $\operatorname{nr} M$ is prime, then Λ/M is a simple Λ-module by [Rei06, Corollary 24.14], so M is a maximal left Λ-submodule. □

Proposition 3.16. *Given an integral ideal I with left order Λ, Algorithm 3.14 correctly computes a factorization into maximal integral ideals as in Theorem 1.8.*

Proof. We show that at the beginning of the i-th run of the `for`-loop it holds $I = M_1 \cdots M_{i-1} \cdot J$ and that this is a proper product as well as $\mathcal{O}_l(I) = \mathcal{O}_l(M_1)$ and $\mathcal{O}_r(I) = \mathcal{O}_r(J)$ by induction on i. This is clearly fulfilled for $i = 1$, so let $i > 1$. By induction the claim holds at the beginning of the $(i-1)$-st run, so we have to prove it is preserved during that run. Algorithm 3.10 returns a maximal integral ideal $M_{i-1} \supseteq J$ with left order $\mathcal{O}_l(M_{i-1}) = \mathcal{O}_l(J)$ in line 4. Let $J' := M_{i-1}^{-1} J$, so $J = M_{i-1} J'$. Then we have $\mathcal{O}_l(M_{i-1}) = \mathcal{O}_l(J)$ and $\mathcal{O}_r(M_{i-1}) = \mathcal{O}_l(J')$ by [Rei06, Corollary 22.8], so the product $M_1 \cdots M_{i-1} J'$ is proper. Furthermore, it holds $\mathcal{O}_r(I) = \mathcal{O}_r(J) = \mathcal{O}_r(J')$. Putting everything together, the claim is indeed still fulfilled at the end of the $(i-1)$-st run, so at the beginning of the i-th run.

Then this will also be fulfilled after the `for`-loop (or at "the beginning of the k-th run"). Note that J is indeed maximal after the `for`-loop by Lemma 3.15, as $\operatorname{nr} J = \mathfrak{p}_k$ by construction. This means that all requirements of Theorem 1.8 are fulfilled.

It is worth pointing out, that all involved orders are maximal, since we start with a maximal order Λ and the right order of an ideal is maximal if and only if the left order is maximal, see [Rei06, Theorem 21.2]. □

For the computation of $M_i^{-1} J$ in line 5 in Algorithm 3.14 we may use [Fri00, Algorithmus 2.16].

4. Integral norm equations

We want to make Eichler's Norm-Theorem (Theorem 2.3) constructive, that is, given an element $a \in R \cap K_A^+$ we want to construct an integral element $\alpha \in A$ with $\operatorname{nr} \alpha = a$. We will now look at this problem in the case, where A is a finite field extension of K (and not a central algebra) and after that go back to a central simple algebra A.

4.1. Solving integral norm equations in number fields

Let L be a finite extension of K and let S be the integral closure of R in L. Recall that S is a Dedekind ring by [Neu07, Satz I.8.1]. Given $a \in R$ we want to find $b \in S$ with $N_{L/K}(b) = a$ or decide, that no such b exists. Since there is no danger of ambiguity we will write N for the norm map $N_{L/K} : L \to K$ from now on. If $a = 0$, then this is solved by $b = 0$, so we assume $a \neq 0$ in the following.

We are going to present an algorithm to solve this problem which has been developed by Prof. Dr. Claus Fieker. However, besides an implementation in Hecke [Fie+17], it has not been published, as far as we know.

Let $S_R := \operatorname{Supp}_R(a) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$. If $S_R = \emptyset$, that is $a \in R^\times$, one may skip the following discussion and use Algorithm 4.5. Assume now $S_R \neq \emptyset$ and let $\overline{S}_R$ be the set of places of K containing the ideals in S_R and all places of K which do not correspond to a prime ideal of R. Extending the definition in [Neu07] to possibly infinite sets we set

$$K^{\overline{S}_R} := \{x \in K^\times \mid v_\mathfrak{p}(x) = 0 \text{ for all places } \mathfrak{p} \notin \overline{S}_R\}$$

to be the group of $\overline{S}_R$-units of K.

Let $S_S := \{\mathfrak{P} \in \mathbb{P}(S) \mid \mathfrak{P} \cap R \in S_R\}$ and define $\overline{S}_S$ analogously to $\overline{S}_R$. Let $L^{\overline{S}_S}$ be the group of $\overline{S}_S$-units. It holds $L^{\overline{S}_S}/S^\times \cong \mathbb{Z}^l$ where $l = |S_S|$ by Theorem C.3.

We have the following easy observation.

Lemma 4.1. *Let $b \in S$ be any solution of the norm equation, that is $N(b) = a$. Then $b \in L^{\overline{S}_S}$.*

Proof. We may write $\langle b \rangle = \prod_{\mathfrak{P} \in \mathbb{P}(S)} \mathfrak{P}^{n_\mathfrak{P}}$ for some $n_\mathfrak{P} \in \mathbb{Z}_{\geq 0}$ and so using Lemma 1.12 it holds

$$\langle a \rangle = N(\langle b \rangle) = \prod_{\mathfrak{p} \in \mathbb{P}(R)} \prod_{\mathfrak{P} \mid \mathfrak{p}} \mathfrak{p}^{n_\mathfrak{P} f_{\mathfrak{P}|\mathfrak{p}}},$$

where $f_{\mathfrak{P}|\mathfrak{p}}$ is the inertia degree of $\mathfrak{P}$ over $\mathfrak{p}$. Now let $\mathfrak{P} \in \mathbb{P}(S) \setminus S_S$ and $\mathfrak{p} = \mathfrak{P} \cap R$. Then $\mathfrak{p} \notin S_R$, so $v_\mathfrak{p}(a) = 0$ and hence $\sum_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}|\mathfrak{p}} n_\mathfrak{P} = 0$. Thus $n_\mathfrak{P} = 0$ as all summands are non-negative integers. □

As a first step, we now want to determine the set

$$\mathcal{M} := \bigl\{ b \in S \bigm| N(b) \equiv a \text{ in } K^{\overline{S}_R}/R^\times \bigr\} \subseteq L^{\overline{S}_S} \cap S.$$

If this set is not empty, then it may contain infinitely many elements since one may always multiply any $b \in \mathcal{M}$ by units of S. However, it suffices to find a system of representatives of the elements of $\mathcal{M}$ modulo $S^\times$. This is done by the following algorithm. We represent a as an element of $K^{\overline{S}_R}/R^\times$ in form of its valuations $v_i := v_{\mathfrak{p}_i}(a)$ at the primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$, so we have

$$\mathcal{M} = \{ b \in S \mid v_{\mathfrak{p}_i}\bigl(N(b)\bigr) = v_i \text{ for } 1 \le i \le k \text{ and } v_{\mathfrak{q}}\bigl(N(b)\bigr) = 0 \text{ for all } \mathfrak{q} \in \mathbb{P}(R) \setminus S_R \}.$$

Algorithm 4.2 (Integral norm equation in a number field – non-unit case)**.**

```
Input: A set $S_R = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ of prime ideals of $R$ and integers $v_1, \ldots, v_k \in \mathbb{Z}_{>0}$.
Output: Elements $b_1, \ldots, b_t \in \mathcal{M}$ such that for each element $b \in \mathcal{M}$ there exist a unit
    $u \in S^\times$ and an index $j \in \{1, \ldots, t\}$ such that $b = ub_j$.
1: Determine the set $S_S := \{\mathfrak{P}_1, \ldots, \mathfrak{P}_l\}$ of primes $\mathfrak{P}$ of $S$ with $\mathfrak{P} \cap R \in S_R$.
2: Compute a minimal(1) set of generators $g_1, \ldots, g_l$ of $L^{\overline{S}_S}/S^\times$.
3: Build the following matrices
       $\mathbf{M} := \begin{pmatrix} v_{\mathfrak{p}_1}\bigl(N(g_1)\bigr) & \cdots & v_{\mathfrak{p}_1}\bigl(N(g_l)\bigr) \\ \vdots & & \vdots \\ v_{\mathfrak{p}_k}\bigl(N(g_1)\bigr) & \cdots & v_{\mathfrak{p}_k}\bigl(N(g_l)\bigr) \end{pmatrix} \in \mathbb{Z}^{k \times l}, \quad \mathbf{a} := \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} \in \mathbb{Z}^k$
   and
       $\mathbf{N} := \begin{pmatrix} v_{\mathfrak{P}_1}(g_1) & \cdots & v_{\mathfrak{P}_1}(g_l) \\ \vdots & & \vdots \\ v_{\mathfrak{P}_l}(g_1) & \cdots & v_{\mathfrak{P}_l}(g_l) \end{pmatrix} \in \mathbb{Z}^{l \times l}.$
4: Find the set $\mathcal{B}$ of vectors $\mathbf{b} \in \mathbb{Z}^l$ such that $\mathbf{Mb} = \mathbf{a}$ and $\mathbf{Nb} \in \mathbb{Z}^l_{\ge 0}$.
5: return elements $\prod_{i=1}^l g_i^{b_i}$ for each $\mathbf{b} = (b_1, \ldots, b_l) \in \mathcal{B}$ (where $\mathcal{B}$ might be empty).
```

To prove the correctness of Algorithm 4.2 we need the following lemma.

Lemma 4.3. *The set of solutions $\mathcal{B}$ in line 4 of Algorithm 4.2 is finite.*

Proof. Let $\mathbf{F} = (f_{ij})_{ij} \in \mathbb{Z}^{k \times l}$ be the matrix defined by

$$f_{ij} := \begin{cases} f_{\mathfrak{P}_j | \mathfrak{p}_i}, & \text{if } \mathfrak{P}_j \text{ lies over } \mathfrak{p}_i, \\ 0, & \text{otherwise.} \end{cases}$$

We claim $\mathbf{M} = \mathbf{FN}$. Indeed we have

$$(\mathbf{M})_{ij} = v_{\mathfrak{p}_i}\bigl(\langle N(g_j)\rangle\bigr) = v_{\mathfrak{p}_i}\bigl(N(\langle g_j\rangle)\bigr) = \sum_{\mathfrak{P}|\mathfrak{p}_i} f_{\mathfrak{P}|\mathfrak{p}_i} v_{\mathfrak{P}}(g_j) = \sum_{t=1}^{l} f_{it} v_{\mathfrak{P}_t}(g_j) = (\mathbf{FN})_{ij}$$

for all $1 \le i \le k$ and $1 \le j \le l$.

(1) That is $g_i \notin \langle g_j \mid j \ne i \rangle$ for all $i = 1, \ldots, l$.

Let $\mathbf{b} \in \mathbb{Z}^l$ be any vector fulfilling $\mathbf{Nb} \in \mathbb{Z}^l_{\geq 0}$. Set $\mathbf{c} := \mathbf{Nb}$. Then $\mathbf{b}$ is uniquely determined by $\mathbf{c}$, as $\{g_1, \ldots, g_l\}$ is a minimal set of generators and so the columns of $\mathbf{N}$ are $\mathbb{Z}$- and hence $\mathbb{Q}$-linearly independent. Now $\mathbf{b} \in \mathcal{B}$ if and only if $\mathbf{Mb} = \mathbf{a}$, so $\mathbf{Fc} = \mathbf{a}$. We now show that there are only finitely many possibilities for $\mathbf{c}$, so $|\mathcal{B}| < \infty$.

Write $\mathbf{c} = (c_1, \ldots, c_l)$ for integers c_i and $\mathbf{a} = (v_1, \ldots, v_k)$ and recall $c_i \geq 0$ and $v_i > 0$ for all i. Every column of $\mathbf{F}$ contains exactly one non-zero entry (as there is exactly one prime ideal of R lying under a prime ideal of S). Then we have for each c_i the upper bound $c_i \leq \frac{v_j}{f_{ji}}$, where f_{ji} is the unique non-zero entry of column i of $\mathbf{F}$. It follows, that there can only be finitely many solutions $\mathbf{c}$ and so only finitely many vectors $\mathbf{b} \in \mathcal{B}$. □

Proposition 4.4. *Algorithm 4.2 is correct.*

Proof. By Lemma 4.3, $\mathcal{B}$ is finite, so line 5 of Algorithm 4.2 is feasible and the algorithm returns only finitely many elements. Let $b \in L$ be any element returned by the algorithm when given $S_R = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ and $v_1, \ldots, v_k \in \mathbb{Z}_{>0}$. Then we have $v_{\mathfrak{Q}}(b) = 0$ for each prime $\mathfrak{Q} \in \mathbb{P}(S) \setminus S_S$, as b is a $\overline{S}_S$-unit, and

$$v_{\mathfrak{P}_i}(b) = \sum_{j=1}^{l} b_j v_{\mathfrak{P}_i}(g_j) \geq 0$$

by the second condition on $\mathbf{b}$ in line 4. It follows $b \in S$. Similarly we have

$$v_{\mathfrak{p}_i}\big(N(b)\big) = \sum_{j=1}^{l} b_j v_{\mathfrak{p}_i}\big(N(g_j)\big) = v_i$$

by the first condition on $\mathbf{b}$ in line 4 and $v_{\mathfrak{q}}\big(N(b)\big) = 0$ for all $\mathfrak{q} \notin S_R$. So $b \in \mathcal{M}$ as required.

Now assume there exists $b \in S$ with $v_{\mathfrak{p}_i}\big(N(b)\big) = v_i$ for all $i = 1, \ldots, k$ and $v_{\mathfrak{q}}\big(N(b)\big) = 0$ for all other primes $\mathfrak{q}$, so $N(b)$ is a $\overline{S}_R$-unit and therefore b a $\overline{S}_S$-unit by Lemma 4.1. Then there exist $b_1, \ldots, b_l \in \mathbb{Z}$ such that

$$b \equiv \prod_{i=1}^{l} g_i^{b_i} \text{ in } L^{\overline{S}_S}/S^{\times}.$$

Now, $\mathbf{b} := (b_1, \ldots, b_l) \in \mathbb{Z}^l$ is a solution in line 4 of the algorithm since $\mathbf{Mb} = \mathbf{a}$ as $N(b)$ has the correct valuations and $\mathbf{Nb} \in \mathbb{Z}^l_{\geq 0}$ as b is integral. Thus b is indeed equivalent to one of the returned solutions modulo units of S. □

To find solutions of the linear system in line 4 of Algorithm 4.2 we use polymake [GJ00; Ass+17], which itself uses the Parma Polyhedra Library [BHZ08].

So far, we have only approached a up to a unit. The next two algorithms do the remaining part.

Algorithm 4.5 (Integral norm equation in a number field – unit case)**.**
Input: $c \in R^{\times}$
Output: $d \in S^{\times}$ with $N(d) = c$ if such an element exists.

```
Let $u_1, \ldots, u_t$ be generators of $S^{\times}$.
```

```
Build the group homomorphism $\nu : S^\times \to R^\times$ defined by $\nu(u_i) = N(u_i)$ for $i = 1, \dots, t$.
if $c \in \operatorname{im} \nu$ then
    return some $d \in \nu^{-1}\big(\{c\}\big)$
else
    There does not exist a solution.
end if
```

The correctness of Algorithm 4.5 is clear since an integral element is a unit if and only if its norm is a unit, see Corollary 1.13.

Putting everything together we have an algorithm to solve integral norm equations in a number field as follows.

Algorithm 4.6 (Integral norm equation in a number field)**.**
Input: $a \in R$
Output: $b \in S$ with $N(b) = a$ if such an element exists.

```
 1: if $a = 0$ then
 2:     return 0
 3: end if
 4: Determine $S_R := \operatorname{Supp}_R(a) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}$ and $v_i := v_{\mathfrak{p}_i}(a)$ for $i = 1, \dots, k$.
 5: if $S_R = \emptyset$ then
 6:     return the output of Algorithm 4.5 with input $a$.
 7: end if
 8: Let $b_1, \dots, b_t$ be the output of Algorithm 4.2 given $S_R$ and $v_1, \dots, v_k$.
 9: for $i = 1, \dots, t$ do
10:     Set $c := a/N(b_i)$.
11:     if Algorithm 4.5 finds an element $d \in S^\times$ with $N(d) = c$ then
12:         return $d \cdot b_i$
13:     end if
14: end for
15: There does not exist a solution.
```

Proposition 4.7. *Given $a \in R$, Algorithm 4.6 correctly returns $b \in S$ with $N(b) = a$ if such an element exists.*

Proof. If Algorithm 4.6 returns $b = d \cdot b_i$ given $a \in R$, then

$$N(b) = N(d)N(b_i) = (a/N(b_i))N(b_i) = a,$$

so b is a solution of the norm equation. Furthermore b is integral as both d and b_i in line 12 are integral.

Now assume there exists $b \in S$ with $N(b) = a$. Then we have $b = ub_i$ for an index $i \in \{1, \dots, t\}$ and a unit $u \in S^\times$ by Proposition 4.4 (in particular $t \neq 0$). It follows $c = a/N(b_i) = N(u)$ in line 10 and so $c \in \operatorname{im} \nu$ in Algorithm 4.5. Hence the `if`-condition in line 11 is fulfilled and the algorithm terminates with a solution. □

Before we move on to norm equations in algebras, we want to discuss a generalization of Algorithm 4.6 for non-maximal orders of L. Let from now on $T \subsetneq S$ be a non-maximal

R-order in L. In analogy to the situation for maximal orders, we want to determine a system of representatives of the set

$$\mathcal{M}_T := \left\{ b \in T \;\middle|\; N(b) \equiv a \text{ in } K^{\overline{S}_R}/R^\times \right\}$$

modulo units of T.

Making use of Algorithm 4.2 this is done by the following algorithm.

Algorithm 4.8 (Integral norm equation in a non-maximal order – non-unit case)**.**
Input: A set $S_R = \{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}$ of prime ideals of R and integers $v_1, \dots, v_k \in \mathbb{Z}_{>0}$.
Output: Elements $b_1, \dots, b_t \in \mathcal{M}_T$ such that for each element $b \in \mathcal{M}_T$ there exist a unit $u \in T^\times$ and an index $j \in \{1, \dots, t\}$ such that $b = ub_j$.

```
 1: Let $c_1, \dots, c_s$ be the output of Algorithm 4.2 given $S_R$ and $v_1, \dots, v_k$.
 2: Compute the conductor $\mathcal{F}$ of $T$ in $S$ and compute the quotient $(S/\mathcal{F})^\times/(T/\mathcal{F})^\times$
    together with the projection $\pi : S^\times \to (S/\mathcal{F})^\times/(T/\mathcal{F})^\times$.
 3: Choose a system of representatives $u_1, \dots, u_r \in S^\times$ for the residue classes in $S^\times/T^\times$.
 4: Initialize a list $\mathcal{B}$.
 5: for $i \in \{1, \dots, s\}$ do
 6:     Let $\overline{c}_i$ be the residue class of $c_i$ in $S/\mathcal{F}$.
 7:     if $\overline{c}_i \in (S/\mathcal{F})^\times$ then
 8:         if there exists $u \in S^\times$ with $\pi(u) = \overline{c}_i$[2] then
 9:             Append $u^{-1}c_i$ to $\mathcal{B}$.
10:         end if
11:     else
12:         for $j \in \{1, \dots, r\}$ do
13:             if $u_j c_i \in T$ then
14:                 Append $u_j c_i$ to $\mathcal{B}$.
15:             end if
16:         end for
17:     end if
18: end for
19: return $\mathcal{B}$
```

Proposition 4.9. *Algorithm 4.8 is correct.*

Proof. Before we prove the correctness of any results, we should explain why line 3 is feasible. This is indeed the case since the index $[S^\times : T^\times]$ is always finite by [Neu07, Satz I.12.9], [Neu07, Satz I.12.11] and the fact that the Picard group of S is finite (the argument is the same as for [Neu07, Satz I.12.12]).

Let now $c_1, \dots, c_s$ and $u_1, \dots, u_r$ be as in the algorithm. We first show that a system of representatives of $\mathcal{M}_T$ is given by the set

$$\{u_j c_i \mid 1 \le i \le s,\ 1 \le j \le r\} \cap T = \bigcup_{i=1}^{s} \left(\{c_i u_j \mid 1 \le j \le r\} \cap T \right). \qquad (*)$$

[2] By abuse of notation, we write $\overline{c}_i$ for the residue class of c_i in $S/\mathcal{F}$ as well as the one in $(S/\mathcal{F})^\times/(T/\mathcal{F})^\times$.

Indeed, if $b \in \mathcal{M}_T$, then there exist $i \in \{1, \dots, s\}$ and $u \in S^\times$ such that $b = uc_i$ by Proposition 4.4. Further, there are $j \in \{1, \dots, r\}$ and $v \in T^\times$ such that $u = vu_j$. Hence $b = vu_jc_i$ and $u_jc_i = v^{-1}b \in T$ as claimed.

Now fix any $i \in \{1, \dots, s\}$. We claim that lines 6 to 17 compute the set

$$\mathcal{M}_i := \{c_iu_j \mid 1 \leq j \leq r\} \cap T,$$

at least up to units of T, so that $\mathcal{B}$ is in the end the set in $(*)$. If the reduction $\overline{c}_i$ of c_i is not a unit in $S/\mathcal{F}$, then there is nothing to show, as lines 12 to 16 clearly build the set $\mathcal{M}_i$.

So let $\overline{c}_i \in (S/\mathcal{F})^\times$. By [Neu07, Satz I.12.9] and [Neu07, Satz I.12.11], there is a exact sequence

$$1 \longrightarrow T^\times \longrightarrow S^\times \xrightarrow{\pi} (S/\mathcal{F})^\times/(T/\mathcal{F})^\times.$$

If there exists a unit $u \in S^\times$ with $\pi(u) = \overline{c}_i$, there hence exists exactly one $j \in \{1, \dots, r\}$ such that $\pi(u_j^{-1}) = \overline{c}_i$.

It remains to be shown that for any $j \in \{1, \dots, r\}$ it holds $\pi(u_j^{-1}) = \overline{c}_i$ if and only if $u_jc_i \in T$. If $\pi(u_j^{-1}) = \overline{c}_i$, then $\pi(u_j)\overline{c}_i \in (T/\mathcal{F})^\times$, so $u_jc_i \in T$ as claimed and the implication in the other direction follows by the same arguments. □

To compute $T^\times$, $\mathcal{F}$ and $(S/\mathcal{F})^\times/(T/\mathcal{F})^\times$ we use the algorithms described in [KP05].

Lines 12 to 16 may appear a little bit unsatisfying as the order of $S^\times/T^\times$ may be quite large. However, we can in general not do any better: If $c_i \in \mathcal{F}$ for an $i \in \{1, \dots, s\}$, then $S^\times c_i \subseteq T$ by definition of $\mathcal{F}$. That means, that in this case we have $u_jc_i \in T$ for *all* $1 \leq j \leq r$, and we need all those elements as $u_{j_1}c_i \neq vu_{j_2}c_i$ for any choice of $j_1, j_2 \in \{1, \dots, r\}$, $j_1 \neq j_2$, and $v \in T^\times$ by construction.

Replacing any "*S*" by a "*T*", we can now use Algorithms 4.5 and 4.6 to solve norm equations in non-maximal orders.

4.2. Solving integral norm equations in algebras

Let $a \in R \cap K_A^+$, which implies $a \in K^\times$, so $a \neq 0$. Motivated by the proof of Theorem 2.3 we want to find $\alpha \in A$ integral over R with $\operatorname{nr} \alpha = a$ by finding a number field $K \subseteq L \subseteq A$ such that there exists $b \in L$ with $N_{L/K}(b) = a$. By the following lemma it then holds $\operatorname{nr} b = a$ if $[L : K] = n$.

Lemma 4.10. *Let $\alpha \in A$ and set $L := K(\alpha)$ with $[L : K] = m$. Then*

$$\operatorname{nr} b = \big(N_{L/K}(b)\big)^{\frac{n}{m}}$$

for any $b \in L$. In particular, if $m = n$, then $\operatorname{nr} b = N_{L/K}(b)$ for any $b \in L$.

Proof. For $b \in L$ we have

$$N_{L/K}(b) = N_{L/K(b)}\big(N_{K(b)/K}(b)\big) = N_{K(b)/K}(b)^{[L:K(b)]}.$$

Let f_b be the reduced characteristic polynomial of b over K and m_b be the minimal polynomial of b over K. Following the hint of [Rei06, Exercise 9.1], we show

$$f_b = m_b^{\frac{n}{[K(b):K]}}:$$

Indeed, m_b has degree $[K(b) : K]$ and f_b is a power of m_b of degree n. Now $\operatorname{nr} b$ is the constant term of f_b and $N_{K(b)/K}(b)$ is the constant term of m_b, so

$$(\operatorname{nr} b)^m = \left(N_{K(b)/K}(b)\right)^{\frac{nm}{[K(b):K]}} = N_{L/K}(b)^n.$$

Finally it holds $m \mid n$ since n is the degree of the reduced characteristic polynomial of α which is a power of the minimal polynomial of α whose degree is m as above. □

The proof of Theorem 2.3 constructs an irreducible polynomial f over R by making heavy use of the approximation theorem and then argues that the primitive element of the field extension given by f has the desired norm. One then has to embed this field into A to obtain the respective element of A. It is not at all clear how to make this feasible in practice. Therefore we will present a different (less elegant) approach to solve norm equations. The basic idea is to look at many fields and try to combine partial solutions. That is to say we try to find fields $L_1, \dots, L_t$ in A and elements $b_i \in L_i$ such that $\operatorname{nr}(b_1 \cdots b_t) = a$.

There are some pitfalls regarding the choice of these fields one has to avoid, the first one being the following: If we have $\alpha, \beta \in A$ both integral over R, we can in general not assume that the product $\alpha\beta$ is also integral over R (this holds of course if $\alpha\beta = \beta\alpha$, see [Rei06, Corollary 1.11] and also the remark after that for a counterexample). To avoid this problem we have to make sure that the partial solutions we want to combine (that is multiply) are always elements of the same maximal order in A.

Another problem comes from the fact, that Theorem 2.3 only guarantees us an integral element $\alpha \in A$ solving $\operatorname{nr} \alpha = a$, but we cannot choose a particular maximal order, in which we would like to find a solution. Also, if we choose an element $\gamma \in \Lambda$ where Λ is a fixed maximal R-order and set $L := K(\gamma)$ we cannot assume that $\operatorname{IntCls}_L(R) \subseteq \Lambda$. Slightly changing the proof of [Swa86, Lemma 9.24], we obtain the following existence result, which will be refined later (see Proposition 4.16).

Lemma 4.11. *Let $a \in R \cap K_A^+$. Then there exists a maximal R-order Λ and an element $\alpha \in \Lambda$ fulfilling all of the following properties.*

(a) $\operatorname{nr} \alpha = a$,

(b) $[K(\alpha) : K] = n$ *and*

(c) $\operatorname{IntCls}_{K(\alpha)}(R) \subseteq \Lambda$.

Proof. Let $f \in R[X]$ be the polynomial constructed in the proof of Theorem 2.3. Let α be any root of f in some algebraic closure of K and set $L := K(\alpha)$. Then $[L : K] = n$ and we may embed L into A as in Theorem 2.3. Set $S := \operatorname{IntCls}_L(R)$ and consider the R-module $M := \sum_{i=1}^{n^2} S\omega_i$, where $\omega_1, \dots, \omega_{n^2}$ is a K-basis of A. Then M is finitely generated and we have $KM = A$. Hence the left order of M is indeed an order of A and it holds $S \subseteq \mathcal{O}_l(M)$. By [Rei06, Corollary 10.4], $\mathcal{O}_l(M)$ is contained in a maximal R-order Λ. Thus $S \subseteq \Lambda$ and in particular $\alpha \in \Lambda$. □

For the next algorithm we assume that we have an oracle which returns a maximal R-order Λ fulfilling the assertions in Lemma 4.11 when given an element $a \in R \cap K_A^+$.

Algorithm 4.12 (Integral norm equation in a fixed maximal order)**.**

Input: $a \in R \cap K_A^+$ and a maximal R-order Λ as in Lemma 4.11.

Output: $\alpha \in \Lambda$ with $\operatorname{nr} \alpha = a$.

```
 1: Determine the set $S_R := \{\mathfrak{p} \in \mathbb{P}(R) \mid v_\mathfrak{p}(a) \neq 0\}$.
 2: Initialize lists $\mathcal{L}_1$ and $\mathcal{L}_2$.
 3: Initialize a group $G$ as the trivial group $\{1\}$ and a map $\nu : G \to R^\times$ with $\nu(1) := 1$.
 4: repeat
 5:     Choose $\lambda \in A$, integral over $R$, and set $L := K(\lambda)$ and $S := \operatorname{IntCls}_L(R)$.
 6:     if $[L : K] \neq n$ or $S \not\subseteq \Lambda$ then
 7:         continue
 8:     end if
 9:     Determine the subset $S_R' := \{\mathfrak{p} \in S_R \mid \exists \mathfrak{P} \in \mathbb{P}(S),\ \mathfrak{P} \mid \mathfrak{p}$ and $f_{\mathfrak{P}|\mathfrak{p}} \leq v_\mathfrak{p}(a)\}$.
10:     Find (modulo units) all $b \in S$ with $v_\mathfrak{p}\big(N_{L/K}(b)\big) = v_\mathfrak{p}(a)$ for all $\mathfrak{p} \in S_R'$ and
        $v_\mathfrak{q}\big(N_{L/K}(b)\big) = 0$ for all primes $\mathfrak{q} \notin S_R'$ using Algorithm 4.2.
11:     for any such $b$ do
12:         Append the tuple $(S_R', b)$ to $\mathcal{L}_1$.
13:         if there exist elements $(S_1, b_1), \dots, (S_t, b_t)$ of $\mathcal{L}_1$ such that $\bigcup_{i=1}^t S_i \cup S_R' = S_R$
        and $S_i \cap S_R' = \emptyset$ as well as $S_i \cap S_j = \emptyset$ for all $i, j \in \{1, \dots, t\}$, $i \neq j$ then
14:             Append $b \cdot \prod_{i=1}^t b_i$ to $\mathcal{L}_2$.
15:         end if
16:     end for
17:     Set $G := G \times S^\times$ and extend $\nu$ by setting $\nu(u) := N_{L/K}(u)$ for all $u \in S^\times$.
18: until $a/\operatorname{nr} \beta \in \nu(G)$ for some $\beta \in \mathcal{L}_2$.
19: Let $\gamma \in G$ with $\nu(\gamma) = a/\operatorname{nr} \beta$.
20: return $\gamma \cdot \beta$
```

Proposition 4.13. *Algorithm 4.12 is correct.*

Proof. Let $a \in R \cap K_A^+$ and let Λ be a maximal R-order as in Lemma 4.11. Assume the algorithm terminates with the product $\gamma \cdot \beta$, where $\nu(\gamma) = a/\operatorname{nr} \beta$. Then $\gamma = g_1 \cdots g_t$ for integral units g_i of number fields L_i, where $[L_i : K] = n$ by line 6. Hence Lemma 4.10 applies and we have

$$\operatorname{nr} \gamma = \prod_{i=1}^t N_{L_i/K}(g_i) = \nu(\gamma).$$

It follows $\operatorname{nr}(\gamma\beta) = a$ as required.

It remains to be shown, that the algorithm terminates at all. For this, let $\alpha \in \Lambda$ be an element as in Lemma 4.11. We claim that the algorithm terminates at the latest when the field $K(\alpha)$ is considered in line 5. By construction, this field fulfils the conditions in line 6. Further it holds $S_R' = S_R$ in line 9: We have

$$N_{K(\alpha)/K}(\alpha)R = \prod_{\mathfrak{p} \in S_R} \prod_{\mathfrak{P} | \mathfrak{p}} \mathfrak{p}^{n_\mathfrak{P} f_{\mathfrak{P}|\mathfrak{p}}}$$

for some $n_\mathfrak{P} \in \mathbb{Z}_{\geq 0}$ analogously to the proof of Lemma 4.1. Fix any $\mathfrak{p} \in S_R$. Then there exists $\mathfrak{P}^* \mid \mathfrak{p}$ with $n_{\mathfrak{P}^*} > 0$, so

$$v_\mathfrak{p}(a) = v_\mathfrak{p}\big(N_{K(\alpha)/K}(\alpha)\big) = \sum_{\mathfrak{P}|\mathfrak{p}} n_\mathfrak{P} f_{\mathfrak{P}|\mathfrak{p}} \geq f_{\mathfrak{P}^*|\mathfrak{p}}.$$

But now we are back in the situation of Section 4.1, as the `if`-condition in line 13 is trivially fulfilled. Hence the algorithm finds a solution by the same arguments as in the proof of Proposition 4.7. □

Remark 4.14. Since we assert with the `if`-condition in line 6 of Algorithm 4.12, that $S \subseteq \Lambda$, we can be sure that $\beta \in \Lambda$ for all $\beta \in \mathcal{L}_2$ and also $\gamma\beta \in \Lambda$ in line 20, which takes care of the first problem mentioned above.

The set S_R' in line 9 is chosen to be a subset of S_R for which we can hope to find a solution: If $\mathfrak{p} \in S_R$ and $f_{\mathfrak{P}|\mathfrak{p}} > v_\mathfrak{p}(a)$ for all $\mathfrak{P}$ lying above $\mathfrak{p}$, then there cannot exist an ideal $\mathfrak{a} \trianglelefteq S$ with $v_\mathfrak{p}\big(N_{L/K}(\mathfrak{a})\big) = v_\mathfrak{p}(a)$, so we do not need to try to find an element with that property.

The condition $[L : K] = n$ in line 6 is not necessarily needed. If $[L : K] = m < n$, then one can restrict the set S_R' further to only contain primes $\mathfrak{p} \in S_R$ for which $\frac{n}{m} \mid v_\mathfrak{p}(a)$ and then search all $b \in S$ (modulo units) with $v_\mathfrak{p}\big(N_{L/K}(b)\big) = \frac{m}{n} v_\mathfrak{p}(a)$ for all $\mathfrak{p} \in S_R'$ and $v_\mathfrak{q}\big(N_{L/K}(b)\big) = 0$ for all other primes $\mathfrak{q} \notin S_R'$. It then holds

$$v_\mathfrak{p}(\operatorname{nr} b) = v_\mathfrak{p}\big(N_{L/K}(b)^{\frac{n}{m}}\big) = v_\mathfrak{p}(a)$$

by Lemma 4.10. However, for a unit $\gamma \in G$ we require $\operatorname{nr}\gamma = \nu(\gamma)$, so one should extend this group in line 17 only if $[L : K] = n$.

Also the condition $S \subseteq \Lambda$ in line 6 is not required, if one uses Algorithm 4.8 in line 10 to find all solutions in the order $R[\alpha]$. But the computations in non-maximal orders require more work than the ones in maximal orders (after all Algorithm 4.8 calls Algorithm 4.2), so we decided to be a little more "picky" in the choice of the number fields.

Unfortunately, we do not have the aforementioned oracle, that means, we do not know in advance in which maximal order we might find a solution. However, we only need to look in finitely many maximal R-orders, namely a system of representatives of the conjugacy classes of maximal orders.

Algorithm 4.15 (Integral norm equation in algebras)**.**

```
Input: $a \in R \cap K_A^+$
Output: An integral element $\alpha \in A$ such that $\operatorname{nr}\alpha = a$.
Compute a system of representatives $\Lambda_1, \dots, \Lambda_t$ of the maximal $R$-orders of $A$ using Algorithm 3.13.
run Algorithm 4.12 in parallel for each order $\Lambda_i$ until it terminates for one of these with an element $\alpha$.
return $\alpha$
```

Proposition 4.16. *Given $a \in R \cap K_A^+$, Algorithm 4.15 determines an integral element $\alpha \in A$ with $\operatorname{nr}\alpha = a$.*

Proof. Let $\Lambda_1, \dots, \Lambda_t$ be a system of representatives of the maximal R-orders of A. It only remains to be shown that one of these orders fulfils the assertions in Lemma 4.11. The correctness then follows by Proposition 4.13.

Let Λ be a maximal R-order and $\alpha \in \Lambda$ an element as in Lemma 4.11. Then there exist $\beta \in A$ and $i \in \{1, \dots, t\}$ with $\Lambda = \beta\Lambda_i\beta^{-1}$. Let f be the minimal polynomial of α over K and set $L := K(\alpha)$ as well as $S := \operatorname{IntCls}_L(R) \subseteq \Lambda$. Set $\alpha' := \beta^{-1}\alpha\beta \in \Lambda_i$

and observe that $f(\alpha') = \beta^{-1}f(\alpha)\beta = 0$ as $(\beta^{-1}\alpha\beta)^i = \beta^{-1}\alpha^i\beta$ for each $i \in \mathbb{N}$ and the coefficients of f lie in K. Then $L \cong K(\alpha')$ and $\operatorname{IntCls}_{K(\alpha')}(R) = \beta^{-1}S\beta$ and in conclusion we have $\operatorname{nr}\alpha' = \operatorname{nr}\beta \operatorname{nr}\alpha \operatorname{nr}\beta^{-1} = a$ and $\operatorname{IntCls}_{K(\alpha')}(R) \subseteq \Lambda_i$ as claimed. □

4.3. A special algorithm for Chapter 2

We now want to adapt Algorithm 4.15 to solve the problem arising in Algorithm 2.11: Let I be an integral ideal in A with left order Λ such that $\operatorname{nr} I = Ra$ for some $a \in K_A^+$. We want to find $\alpha \in \Lambda$ such that $R(\operatorname{nr}\alpha) = \operatorname{nr} I$. After all, such an element must exist since there exists $\alpha \in \Lambda$ such that $I = \Lambda\alpha$ by Theorem 2.10, and hence $(\operatorname{nr}\alpha)R = \operatorname{nr} I$ by Lemma 1.12.

One could of course use Algorithm 4.15 with input a and obtain $\beta \in \Lambda'$ with $(\operatorname{nr}\beta)R = \operatorname{nr} I$ for a maximal order Λ'. If then $\Lambda' \neq \Lambda$ one has to carry out operations as in the end of the proof of Theorem 2.10. Although this is possible, we would prefer to find a solution directly in the maximal order Λ.

We now present an adapted version of Algorithm 4.12 and, after proving its correctness, discuss the reasons for the changes.

Algorithm 4.17 (Integral norm equation – special case for Algorithm 2.11)**.**
Input: An integral ideal I with left order Λ such that $\operatorname{nr} I = Ra$ for some $a \in K_A^+$.
Output: $\alpha \in \Lambda$ such that $(\operatorname{nr}\alpha)R = \operatorname{nr} I$.

```
 1: Determine the set $S_R := \{\mathfrak{p} \in \mathbb{P}(R) \mid v_\mathfrak{p}(\operatorname{nr} I) \neq 0\}$.
 2: Initialize a list $\mathcal{L}$.
 3: repeat
 4:     Choose $\lambda \in A$, integral over $R$, and set $L := K(\lambda)$ and $S := \operatorname{IntCls}_L(R)$.
 5:     Let $m := [L : K]$. Determine the subset $S'_R := \{\mathfrak{p} \in S_R \mid \frac{m}{n} v_\mathfrak{p}(\operatorname{nr} I) \in \mathbb{Z}\}$.
 6:     Determine the subset $S''_R := \{\mathfrak{p} \in S'_R \mid \exists \mathfrak{P} \in \mathbb{P}(S),\ \mathfrak{P} \mid \mathfrak{p}$ and $f_{\mathfrak{P}|\mathfrak{p}} \leq \frac{m}{n} v_\mathfrak{p}(\operatorname{nr} I)\}$.
 7:     if $S''_R = \emptyset$ or there already exists an element $(T, c) \in \mathcal{L}$ with $T = S''_R$ then
 8:         continue
 9:     end if
10:     Using Algorithm 4.8 with input $S''_R$ and the valuations $\frac{m}{n} v_\mathfrak{p}(\operatorname{nr} I)$ for $\mathfrak{p} \in S''_R$
        search for an element $b \in R[\alpha]$ with $v_\mathfrak{p}(N_{L/K}(b)) = \frac{m}{n} v_\mathfrak{p}(\operatorname{nr} I)$ for all $\mathfrak{p} \in S''_R$ and
        $v_\mathfrak{q}(N_{L/K}(b)) = 0$ for all other primes $\mathfrak{q} \notin S''_R$.
11:     if such an element $b$ exists then
12:         Append the tuple $(S''_R, b)$ to $\mathcal{L}$.
13:     end if
14: until there exist elements $(S_1, c_1), \dots, (S_t, c_t)$ of $\mathcal{L}$ such that $\bigcup_{i=1}^t S_i = S_R$ and
    $S_i \cap S_j = \emptyset$ for all $i, j \in \{1, \dots, t\}$, $i \neq j$
15: return $\prod_{i=1}^t c_i$ for elements $c_i$ as in line 14.
```

Proposition 4.18. *Given an integral ideal I with left order Λ such that $\operatorname{nr} I = Ra$ for some $a \in K_A^+$, Algorithm 4.17 correctly computes an $\alpha \in \Lambda$ such that $(\operatorname{nr}\alpha)R = \operatorname{nr} I$.*

Proof. Assume the algorithm returns $\gamma := \prod_{i=1}^t c_i$ with elements $(S_1, c_1), \dots, (S_t, c_t) \in \mathcal{L}$ in line 14, where $c_i \in L_i$ for field extensions L_i of K, $1 \leq i \leq t$. We have to show that $v_\mathfrak{p}(\operatorname{nr}\gamma) = v_\mathfrak{p}(\operatorname{nr} I)$ for any $\mathfrak{p} \in \mathbb{P}(R)$. For primes $\mathfrak{p}$ with $v_\mathfrak{p}(\operatorname{nr} I) = 0$ we have $\mathfrak{p} \notin S_R$

so $v_{\mathfrak{p}}\big(N_{L_i/K}(c_i)\big) = 0$ for all $1 \leq i \leq t$ and hence $v_{\mathfrak{p}}(\operatorname{nr}\gamma) = 0$. So, let $\mathfrak{p} \in \mathbb{P}(R)$ with $v_{\mathfrak{p}}(\operatorname{nr} I) \neq 0$ that is $\mathfrak{p} \in S_R$. Then there exists exactly one index $i \in \{1, \dots, t\}$ such that $v_{\mathfrak{p}}\big(N_{L_i/K}(c_i)\big) \neq 0$ by the condition in line 14. Here it holds

$$v_{\mathfrak{p}}(\operatorname{nr} c_i) = \frac{n}{m_i} v_{\mathfrak{p}}\big(N_{L_i/K}(c_i)\big) = v_{\mathfrak{p}}(\operatorname{nr} I)$$

by Lemma 4.10, where $m_i := [L_i : K]$. Hence $v_{\mathfrak{p}}(\operatorname{nr}\gamma) = v_{\mathfrak{p}}(\operatorname{nr} I)$ for all primes $\mathfrak{p} \in \mathbb{P}(R)$ as claimed.

It remains to be shown, that the algorithm terminates. By Theorem 2.10, there exists $\alpha \in \Lambda$ with $I = \Lambda\alpha$, so $(\operatorname{nr}\alpha)R = \operatorname{nr} I$ by Lemma 1.12. We claim that Algorithm 4.17 terminates at the latest if the field $L := K(\alpha)$ is considered in line 4. Note, that then $S_R'' = S_R$ as

$$v_{\mathfrak{p}}\big(N_{L/K}(\alpha)\big) = \frac{m}{n} v_{\mathfrak{p}}(\operatorname{nr}\alpha) = \frac{m}{n} v_{\mathfrak{p}}(\operatorname{nr} I)$$

for all $\mathfrak{p} \in \mathbb{P}(R)$ by Lemma 4.10 with $m := [L : K]$. Then Algorithm 4.8 called in line 10 will find an element $b \in R[\alpha]$ satisfying the conditions as $\alpha \in R[\alpha]$ is such an element. Hence (S_R'', b) is appended to $\mathcal{L}$ in line 12 and the algorithm terminates since the conditions in line 14 are trivially fulfilled (as $S_R'' = S_R$). □

As announced we now give reason for the differences between Algorithms 4.12 and 4.17. As input of Algorithm 4.17 we do not need any particular generator a of $\operatorname{nr} I$ but only the valuations of $\operatorname{nr} I$ since it suffices to find $\alpha \in \Lambda$ such that $\operatorname{nr}\alpha$ is a generator of $\operatorname{nr} I$, so $v_{\mathfrak{p}}(\operatorname{nr}\alpha) = v_{\mathfrak{p}}(\operatorname{nr} I)$ for all $\mathfrak{p} \in \mathbb{P}(R)$. This allows us to omit the search for a unit as in Algorithm 4.12 and we only need to find any element $b \in R[\alpha]$ (and not all of them) whose norm has the correct valuations in line 10.

In Algorithm 4.17, we do not impose any conditions on the number field L in contrast to line 6 in Algorithm 4.12. As already explained in Remark 4.14, these were mostly made out of "convenience" in the first algorithm. Although we would like to have $\operatorname{IntCls}_L(R) \subseteq \Lambda$, we are unable to proof the correctness of Algorithm 4.17 if we would only choose such number fields. To show the correctness of Algorithm 4.12 we required that there exists an element fulfilling the conditions of Lemma 4.11. Translated to the new problem this would mean to prove that there exists $\alpha \in \Lambda$ with $(\operatorname{nr}\alpha)R = \operatorname{nr} I$ and $\operatorname{IntCls}_{K(\alpha)}(R) \subseteq \Lambda$. Although we can be sure that there is $\alpha \in \Lambda$ with $(\operatorname{nr}\alpha)R = \operatorname{nr} I$, it could be the case that the second condition is not fulfilled. For a system of representatives of the maximal orders $\Lambda = \Lambda_1, \dots, \Lambda_t$ we only have $\operatorname{IntCls}_{K(\alpha)}(R) \subseteq \beta\Lambda_i\beta^{-1}$ for a $\beta \in A^\times$ and $i \in \{1, \dots, t\}$ as in Proposition 4.16. Given that there are infinitely many elements in Λ whose reduced norm generate $\operatorname{nr} I$ by multiplying any such element by units of Λ and that each of the corresponding integral closures must (after conjugation) be contained in one of the finitely many representatives Λ_i, one would expect that there exists one which is contained in Λ. Still, a proof for this currently eludes us. Hence we have to search for a solution in $R[\alpha]$ in line 10 instead of the maximal order S in general.

5. An algorithm for Proposition 2.8

As the title already suggests we now discuss an algorithm which makes Proposition 2.8 constructive. The first section (5.1) reduces this problem to finding a representative of an orbit of a certain group action and hence a completely group-theoretical problem, which we then consider in Section 5.2. The last section (5.3) provides a different algorithmic idea as a starting point for further work on the subject.

5.1. Reducing to a group-theoretical problem

Let I and J be integral ideals with the same left order Λ, $\operatorname{nr} I = \operatorname{nr} J$ and $\operatorname{nr} I + r\mathfrak{d} = R$, where r and $\mathfrak{d}$ are as in Proposition 2.8. We want to find $\vartheta \in A^\times$ such that $I = J\vartheta$.

If we assume for a moment, that we have an algorithm for Proposition 2.7 (see Algorithm 5.2 below), the proof of Proposition 2.8 already tells us, what we need to do.

Algorithm 5.1 ("Transforming unit" as in Proposition 2.8).

Input: Integral ideals I and J with left order Λ such that $\operatorname{nr} I = \operatorname{nr} J$ and $\operatorname{nr} I + r\mathfrak{d} = R$ (see Proposition 2.8).

Output: $\vartheta \in A^\times$ with $I = J\vartheta$.

```
$\vartheta := 1$
while $\operatorname{nr} I \neq R$ do
    Choose a prime $\mathfrak{p}$ dividing $\operatorname{nr} I$.
    Compute maximal integral ideals $M$ and $N$ containing $I$ respectively $J$ and $\mathfrak{p}$ using Algorithm 3.10.
    Find $\tilde{\vartheta} \in \mathcal{O}_l(M)^\times$ with $M = N\tilde{\vartheta}$ using Algorithm 5.2.
    $\vartheta := \vartheta \cdot \tilde{\vartheta}$
    $I := M^{-1}I$
    $J := \tilde{\vartheta}^{-1}(N^{-1}J)\tilde{\vartheta}$
end while
return $\vartheta$
```

By Proposition 3.16, we may compute a factorization of I in the given way. Hence the correctness of Algorithm 5.1 is clear by Proposition 2.8.

We are now left with making Proposition 2.7 constructive. In the following let M and N be maximal integral ideals with the same left order Λ and $\operatorname{nr} M = \operatorname{nr} N = \mathfrak{p}$ where $\mathfrak{p} \nmid r\mathfrak{d}$ (see Proposition 2.7). As in the proof of the proposition, we consider Λ/M and Λ/N as modules of $\Lambda/\mathfrak{p}\Lambda \cong \operatorname{Mat}_n(R/\mathfrak{p})$ and obtain mappings $\varphi : \Lambda \to (R/\mathfrak{p})^n$ and $\psi : \Lambda \to (R/\mathfrak{p})^n$ such that $\ker\varphi = M$ and $\ker\psi = N$. This reduces the task to finding a unit $\vartheta \in \Lambda^\times$ such that $\psi(1) = \bar{\vartheta}\varphi(1)$, where $\bar{\vartheta}$ is the image of ϑ under the canonical projection $\pi : \Lambda \to \Lambda/\mathfrak{p}\Lambda$.

Here we cannot follow the proof further, as this would mean to construct an element λ as in Lemma 2.6. But it is not clear how to (practically) embed a splitting field in the algebra. Even if this were possible, then one still would have to lift all elements of $\mathrm{GL}_n(R/\mathfrak{p})$ to Λ to find an element s as in the proof of Lemma 2.6. Taking into account that $\mathrm{GL}_n(\mathbb{F}_q)$ has $\prod_{i=0}^{n-1}(q^n - q^i) \approx q^{n^2-n}$ elements, this is surely not feasible in practice even for small input sizes.

Set $v := \varphi(1)$ and $w := \psi(1)$, so clearly $v, w \in (R/\mathfrak{p})^n \setminus \{0\}$. It is, of course, no problem to find a matrix $g \in \mathrm{GL}_n(R/\mathfrak{p})$ such that $gv = w$. But it is far from clear, whether there exists a preimage of g under the map $\Lambda^\times \to \mathrm{GL}_n(R/\mathfrak{p})$ induced by π, let alone how to find such a unit of Λ.[1] Our approach is now as follows: We choose units $\vartheta_1, \dots, \vartheta_k \in \Lambda^\times$ for some $k \in \mathbb{N}$ and consider the group $G := \langle \bar{\vartheta}_1, \dots, \bar{\vartheta}_k \rangle \leq \mathrm{GL}_n(R/\mathfrak{p})$ generated by the residue classes of these units. This group acts naturally on $(R/\mathfrak{p})^n$ and w lies in the orbit of v under this action, if we have chosen k big enough as this is certainly the case for $\langle \vartheta_1, \dots, \vartheta_k \rangle = \Lambda^\times$ by Proposition 2.7. We then have to find an element $g \in G$ with $gv = w$ given by $g = \prod_{i=1}^t \bar{\vartheta}_{j_i}^{e_i}$, where $j_i \in \{1, \dots, k\}$, $e_i \in \mathbb{Z}$ and $t \in \mathbb{N}$. Then $\vartheta := \prod_{i=1}^t \vartheta_{j_i}^{e_i} \in \Lambda^\times$ is the searched unit. For this, we need to solve two problems. The first one is how to find g given G, v and w. As this is a surprisingly hard problem and certainly of interest on its own, we dedicated a whole section to it; see Section 5.2 and in particular Algorithm 5.5. Here, we discuss the second problem, being how to find $\vartheta_1, \dots, \vartheta_k$.

Bley and Johnston [BJ11] present an algorithm, which determines a set of representatives $U \subseteq \Lambda^\times$ of the image of the projection map. However, this algorithm seems not to be feasible in practice as it requires embedding a splitting field in the algebra (see [BJ11, Lemma 7.4]). We should also mention that there exist algorithms to compute (a presentation of) the group $\Lambda^\times$ by Braun et al. [Bra+15] and Page [Pag14b], the latter one being restricted to divison algebras. As we do not require to know the whole group $\Lambda^\times$ and these algorithms appear only to be feasible for small input sizes we are not going to use them.

Instead, we want to suggest the following approach. Firstly, we can find units of Λ by considering rings of type $R[\alpha]$ for an $\alpha \in \Lambda$. As $R[\alpha]$ is a subring of Λ, we obtain units of Λ by mapping units of $R[\alpha]$ to Λ. But $R[\alpha]$ is an order in the number field $K(\alpha)$, so its group of units can be computed comparatively easy (see [Coh93, Section 4.9] for maximal orders and [KP05] for non-maximal orders). Hence, we can generate units of Λ by choosing a random element α and computing the units of $R[\alpha]$.

This leaves us with the question, how many units we need or how to choose k in the above notation. One could of course start with only one unit ϑ_1 and check, whether v and w lie in the same orbit under the action of G. If this is not the case, one adds another unit ϑ_2 and so on, thereby minimizing the number of units one needs to compute. However, it is not clear, how to efficiently add an element in Algorithm 5.5, so many computations would have to be repeated in each step. Therefore we should try to start with enough units, that we can hope do find a solution in G. For this a choice of $k \geq \log_2(|\mathrm{GL}_n(R/\mathfrak{p})|)$ proved to be a useful heuristic. This is motivated by the fact, that any group H can be generated by $\log_2(|H|)$ elements. Indeed, if $h_1, \dots, h_m \in H$ is a minimal set of generators, then $h_{i+1} \notin \langle h_1, \dots, h_i \rangle$ for each $1 \leq i \leq m-1$. Hence $|\langle h_1, \dots, h_{i+1} \rangle| \geq 2|\langle h_1, \dots, h_i \rangle|$, so inductively $|H| \geq 2^m$ and $\log_2(|H|) \geq m$. This does,

[1] In Section 5.3, we describe a probabilistic algorithm which occasionally succeeds in constructing such a preimage.

however, not mean that any set of $\log_2(|H|)$ elements generators H, since we require the set of generators to be minimal. As we choose the units $\vartheta_1, \ldots, \vartheta_k$ randomly, we can expect that there are not "too much" dependencies between them, so that G is "almost" $\pi(\Lambda^\times)$.

This gives the following algorithm.

Algorithm 5.2 ("Transforming unit" as in Proposition 2.7)**.**

Input: Maximal integral ideals M and N with left order Λ, such that $\operatorname{nr} M = \operatorname{nr} N = \mathfrak{p}$ and $\mathfrak{p} + r\mathfrak{d} = R$ (see Proposition 2.7).

Output: $\vartheta \in \Lambda^\times$ with $M = N\vartheta$.

```
1: Compute the projection $\pi : \Lambda \to \Lambda/\mathfrak{p}\Lambda$ and the isomorphism $\Lambda/\mathfrak{p}\Lambda \cong \mathrm{Mat}_n(R/\mathfrak{p})$.
2: Find the $R/\mathfrak{p}$-isomorphisms $\varphi : \Lambda/M \to (R/\mathfrak{p})^n$ and $\psi : \Lambda/N \to (R/\mathfrak{p})^n$.
3: Set $v := \varphi(1)$ and $w := \psi(1)$.
4: Initialize a list $\mathcal{L}$.
5: while $|\mathcal{L}| \leq \log_2(|\mathrm{GL}_n(R/\mathfrak{p})|)$ do
6:     Choose $\alpha \in \Lambda$.
7:     Compute generators $u_1, \ldots, u_s$ for $R[\alpha]^\times$.
8:     Append $u_1, \ldots, u_s$ to $\mathcal{L}$.
9: end while
10: Let $\mathcal{L} = \{\vartheta_1, \ldots, \vartheta_k\}$ and set $G := \langle \pi(\vartheta_1), \ldots, \pi(\vartheta_k) \rangle \leq \mathrm{GL}_n(R/\mathfrak{p})$.
11: Using Algorithm 5.5, find $g \in G$ with $gv = w$ given by $g = \prod_{i=1}^t \pi(\vartheta_{j_i})^{e_i}$ for $j_i \in \{1, \ldots, k\}$, $e_i \in \mathbb{Z}$ and $t \in \mathbb{N}$.
12: if no such $g$ exists then
13:     Generate more units and go to line 10.
14: end if
15: return $\prod_{i=1}^t \vartheta_{ji}^{e_i}$
```

Proposition 5.3. *Given maximal integral ideals M and N with left order Λ satisfying the conditions of Proposition 2.7, Algorithm 5.2 correctly computes a unit $\vartheta \in \Lambda^\times$ with $M = N\vartheta$.*

Proof. If the algorithm terminates with an element ϑ, then $\vartheta \in \Lambda^\times$ and $\pi(\vartheta)\varphi(1) = \psi(1)$ by construction. It follows $M = N\vartheta$ as in the proof of Proposition 2.7.

If $\vartheta' \in \Lambda^\times$ is an element with $M = N\vartheta'$, then the algorithm terminates at the latest when ϑ' is chosen in line 6 respectively 13. □

It is of course desirable to keep α or rather the minimal polynomial of α in line 6 of Algorithm 5.2 small. Therefore in the implementation we compute an LLL-reduced $\mathbb{Z}$-basis of Λ and take linear combinations with small coefficients of these basis elements.

5.2. The action of $\mathrm{GL}_k(\mathbb{F}_q)$ on $\mathbb{F}_q^k$

This section is concerned with the group-theoretical problem already mentioned above. We state this in full generality. Let $\mathbb{F}_q$ be a finite field and let $k \in \mathbb{N}$. Let $g_1, \ldots, g_m \in \mathrm{GL}_k(\mathbb{F}_q)$ and set $G := \langle g_1, \ldots, g_m \rangle$. Then G acts naturally on $\mathbb{F}_q^k$ by multiplication from the left. Let finally $v, w \in \mathbb{F}_q^k \setminus \{0\}$. We want to find $g \in G$ explicitly given as a word in the generators $g_1, \dots, g_m$ with $gv = w$, or decide, that no such g exists, that is, that v and w do not lie in the same orbit under the action of G.

We now try to give reason why this is a pretty hard problem and then give an algorithm, which works considerably better than a naive enumeration of the orbit.

Since G is a finite group one could apply [But91, Chapter 7, Algorithm 1], which computes the whole orbit $G.v$ with $\mathcal{O}(|G.v|m)$ matrix-vector-multiplications [But91, p. 58]. However, for $G = \mathrm{GL}_k(\mathbb{F}_q)$ we have $G.v = \mathbb{F}_q^k \setminus \{0\}$, so $|G.v| = q^k - 1$, which makes this approach infeasible even for relatively small q and k. One could argue of course, that one does not have to write down the whole orbit in our situation, but can stop as soon as one has reached w. Here one can convince oneself that

$$\frac{|\{h \in \mathrm{GL}_k(\mathbb{F}_q) \mid hv = w\}|}{|\mathrm{GL}_k(\mathbb{F}_q)|} = \frac{1}{q^k - 1} =: P.$$

Indeed, one can partition $\mathrm{GL}_k(\mathbb{F}_q)$ in the sets $M_{v'} := \{h \in \mathrm{GL}_k(\mathbb{F}_q) \mid hv = v'\}$ for $v' \in \mathbb{F}_q^k \setminus \{0\}$ and each of these has the same cardinality as we have a bijection $M_{v'} \to M_{v''}$ by multiplying by a matrix $h \in \mathrm{GL}_k(\mathbb{F}_q)$ with $hv' = v''$ for each pair $v', v'' \in \mathbb{F}_q^k \setminus \{0\}$.

Hence a randomly chosen uniformly distributed matrix $h \in \mathrm{GL}_k(\mathbb{F}_q)$ will fulfil $hv = w$ with probability P. This means, that the expected value of the number of matrices we have to pick at random until we find a matching one (for the first time) is given by

$$\sum_{i=1}^{\infty} iP(1-P)^{i-1} = \frac{P}{1-P} \sum_{i=0}^{\infty} i(1-P)^i = \frac{P}{1-P} \frac{1-P}{P^2} = \frac{1}{P} = q^k - 1.$$

Therefore any algorithm which writes down the group G until it finds a matching group element (in whatever fashion) will have a runtime of at least $\mathcal{O}(q^k - 1)$ on average, if not G has some special properties which would change the probability P.

Unfortunately, the author is not aware of any algorithm specialized for matrix groups which solves the problem faster and algorithms for matrix groups seem to be scarce in general (see also the introducing words to the short section on matrix groups in [EHO05, Section 7.8]). We are now going to present an algorithm which still has a (provable) runtime of $\mathcal{O}(q^k)$ (if $G.v = \mathbb{F}_q^k$), but is a big improvement in comparison to just writing down the orbit.

Like in [But91, Chapter 7], we consider the following graph $\mathcal{G}$: The vertices of $\mathcal{G}$ are the elements of $\mathbb{F}_q^k \setminus \{0\}$ and there is a (directed) edge from a vertex v_1 to a vertex v_2, if there exists a generator g_i with $g_i v_1 = v_2$. Note that the graph may have parallel edges and that v_1 and v_2 need not be distinct, that is, there may be loops. An example of such a graph can be seen in Figure 5.1, where we have $G = \mathrm{GL}_2(\mathbb{F}_3)$.

In graph theoretical terms, we are searching for a path from the vertex v to the vertex w in $\mathcal{G}$ and "writing down the orbit" translates to a traversal of the graph, where starting from v each vertex in the same connected component is explored. The two standard ways to traverse a graph are depth first search and breadth first search (we refer the reader to [KN12, Kapitel 7] for basic facts on these algorithms). Both have a linear runtime in the number of vertices and edges of the connected component of the starting vertex, that is $\mathcal{O}(|G.v|m)$ in our case (as from each vertex in $\mathcal{G}$ there are m edges going out). However, breadth first search has the advantage of producing a path of minimal length by [KN12, Satz 7.15]. This is preferable since given the path $g_{j_1}, \dots, g_{j_t}$, $j_i \in \{1, \dots, m\}$, we need

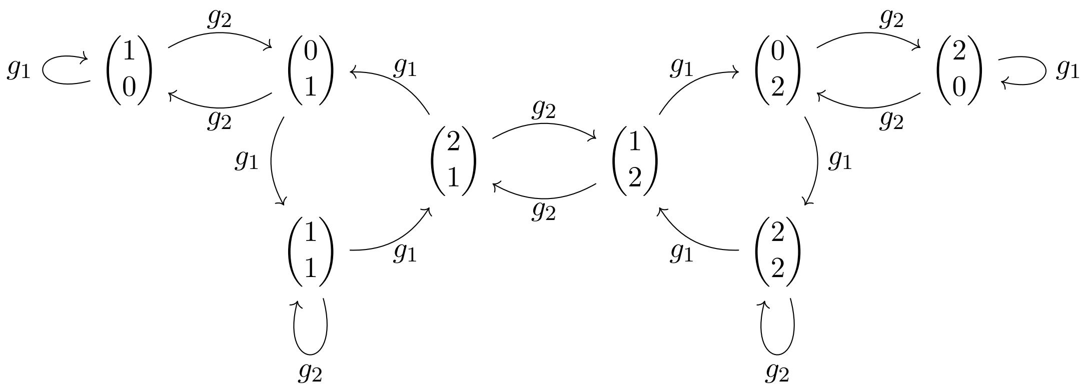


Figure 5.1.: The graph $\mathcal{G}$ for $\mathbb{F}_q = \mathbb{F}_3$, $k = 2$, $g_1 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $g_2 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

to compute the product $g_{j_1} \cdots g_{j_t}$. Especially in light of our application in Section 5.1 we would appreciate it, if this product were as "short" as possible.

For later reference, we state our version of breadth first search as an algorithm. The pseudo code is inspired by [KN12, Algorithmus 7.5].

Algorithm 5.4 (Orbit inclusion test – plain BFS)**.**
Input: A group $G := \langle g_1, \ldots, g_m \rangle \leq \mathrm{GL}_k(\mathbb{F}_q)$ and vectors $v, w \in \mathbb{F}_q^k \setminus \{0\}$.
Output: Indices $j_1, \ldots, j_t \in \{1, \ldots, m\}$ with $(\prod_{i=1}^t g_{j_i})v = w$ if $w \in G.v$.

```
if $v = w$ then
    return the empty sequence $()$.
end if
Initialize a queue $\mathcal{Q} := \{v\}$ and a dictionary $\mathcal{D}$ with $\mathcal{D}(v) = ()$.
while $\mathcal{Q} \neq \emptyset$ do
    Remove an element $u$ from $\mathcal{Q}$ whose entry $\mathcal{D}(u)$ has minimal length.
    for $i \in \{1, \ldots, m\}$ do
        $u' := g_i u$
        if $\mathcal{D}(u')$ exists then
            continue
        end if
        if $u' = w$ then
            return $(i, \mathcal{D}(u))$
        end if
        $\mathcal{D}(u') := (i, \mathcal{D}(u))$
        $\mathcal{Q} := \mathcal{Q} \cup \{u'\}$
    end for
end while
$w$ is not an element of $G.v$.
```

Carrying out a traversal on $\mathcal{G}$ one obtains a tree, whose vertices are the elements of $G.v$ and in which there is an edge g_i from v_1 to v_2 if one explored v_2 coming from v_1 using the edge g_i in $\mathcal{G}$. See Figure 5.2 for the search tree coming from a traversal on the graph in Figure 5.1. Interestingly the tree is the same for depth first search and breadth

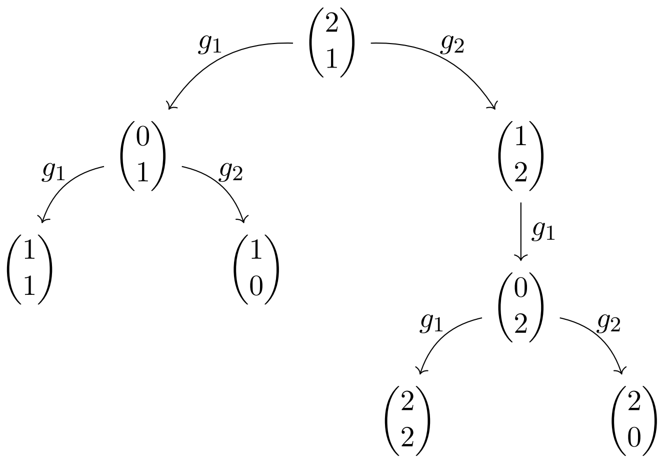


Figure 5.2.: The search tree of a depth or breadth first search on the graph in Figure 5.1 starting in $\binom{2}{1}$.

first search. However, depth first search always (recursively) explores all children of a vertex, starting with the leftmost, whereas breadth first search traverses the tree level per level.

The "usual" strategy to optimize Algorithm 5.4 is to "prune" the search tree, see [EHO05, Section 4.6], that means to find a property Q for which one can prove, that if a vertex u fulfilling Q is added to the tree, then one need not explore the neighbours of u since none of the possible children of u in the search tree can be w. However, in our situation, it appears that such a property Q does not exist (without imposing further requirements on G), since for any $u \in \mathbb{F}_q^k \setminus \{0\}$ there exists $g \in \mathrm{GL}_k(\mathbb{F}_q)$ with $gu = w$. So, in whatever vertex we are in the search tree it might be possible that we find w as a child.

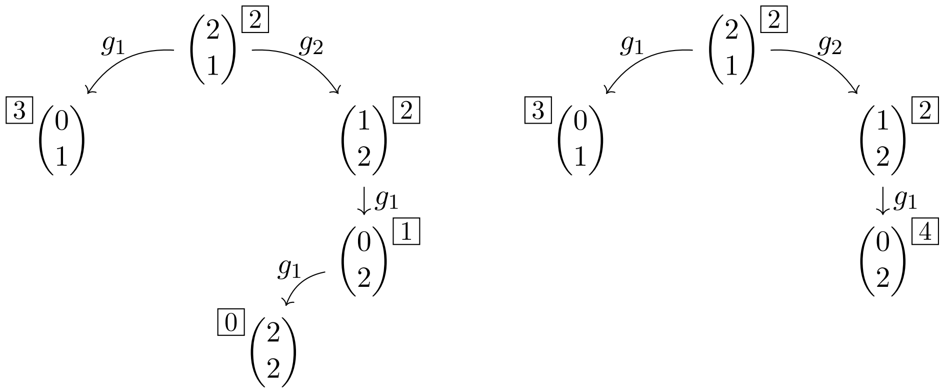
In short, the algorithm, which we want to present, nevertheless prunes the search tree, but only in a first run. If w is not found in this first run, the algorithm falls back to plain breadth first search.

For the pruning, we introduce a weight function $|\cdot| : \mathbb{F}_q^k \to \mathbb{Z}_{\geq 0}$ in the following way. Let $\mathbb{F}_p$, p prime, be the prime field of $\mathbb{F}_q$ and $[\mathbb{F}_q : \mathbb{F}_p] = l$. Then we can write each $\lambda \in \mathbb{F}_q$ as $\lambda = \sum_{i=0}^{l-1} \lambda_i a^i$ where a is a primitive element of $\mathbb{F}_q$ over $\mathbb{F}_p$ and $\lambda_i \in \mathbb{F}_p$. Identifying $\mathbb{F}_p$ with $\mathbb{Z}/p\mathbb{Z}$ we may assume $\lambda_i \in \mathbb{Z}$ and $0 \leq \lambda_i \leq p-1$. This gives a bijection (of sets)

$$f_a : \mathbb{F}_q \to \{0, \dots, p-1\}^{[\mathbb{F}_q : \mathbb{F}_p]}$$

which clearly depends on the choice of a. This dependence is, however, not important for the following arguments. The weight $|\lambda|$ of a $\lambda \in \mathbb{F}_q$ is now defined to be $|\lambda| := \sum_{i=1}^{l} (f_a(\lambda))_i$. One directly sees that $|\lambda| \geq 0$ for all $\lambda \in \mathbb{F}_q$ and $|\lambda| = 0$ if and only if $\lambda = 0$. We finally extend $|\cdot|$ on $\mathbb{F}_q^k$ by setting $|u| := \sum_{i=1}^{k} |u_i|$ where $u \in \mathbb{F}_q^k$ with $u = (u_1, \dots, u_k)$. We have $|u| \geq 0$ and $|u| = 0$ if and only if $u = 0$.

The pruning is then done in the following way: If we are in a vertex u and consider an edge g during the algorithm, we only explore gu if $|gu - w| \leq |u - w|$. In Figure 5.3 one can see the tree from Figure 5.2 with pruning with respect to two different target vertices



(a) $w = \left(\begin{smallmatrix}2\\2\end{smallmatrix}\right)$: Pruning successful

(b) $w = \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$: Pruning fails

Figure 5.3.: Pruned versions of the tree in Figure 5.2.

w. The numbers in the squares indicate the weights of the vertices. In Figure 5.3a, the pruning is successful: one avoids exploring two vertices in the left branch. Figure 5.3b shows, that this will not always work. Here, we have no chance to find w any more.

In practice, it turned out, that depth first search is much faster than breadth first search during the "pruning phase" of our algorithm. A reason for this might be that breadth first search always explores all vertices of distance one to v, then all the ones of distance two, and so on. If w has distance d then one has to write down all vertices of shorter distance $1, \dots, d-1$ and the pruning does not seem to help much here. In contrast, depth first search with pruning resembles a random walk on the graph, so the actual distance of w to v does not play such a big role. Also, the pruning makes long paths very unlikely, so breadth first search has no advantage any more.

Speaking of random walks, we should also mention that we considered carrying out a depth first search where the search tree is pruned at random. But this did not perform as well as the pruning with the weight function does.

This yields the following algorithm which is mostly depth first search.

Algorithm 5.5 (Orbit inclusion test)**.**
Input: A group $G := \langle g_1, \dots, g_m \rangle \leq \mathrm{GL}_k(\mathbb{F}_q)$ and vectors $v, w \in \mathbb{F}_q^k \setminus \{0\}$.
Output: Indices $j_1, \dots, j_t \in \{1, \dots, m\}$ with $(\prod_{i=1}^t g_{j_i})v = w$ if $w \in G.v$.

```
if $v = w$ then
    return the empty sequence ().
end if
Initialize a dictionary $\mathcal{D}$ with $\mathcal{D}(v) := 0$ and an empty sequence $\mathcal{P} := ()$.
$u := v$
while $|u - w| \neq 0$ do
    Find the minimal index $j \in \{\mathcal{D}(u) + 1, \dots, m\}$ such that $\mathcal{D}(g_j u)$ does not exist
    and $|g_j u - w| \leq |u - w|$.
    if $j$ exists then
        $\mathcal{D}(u) := j$
        $\mathcal{D}(g_j u) := 0$
```

```
11:         $\mathcal{P} := (j, \mathcal{P})$
12:         $u := g_j u$
13:     else
14:         if $|\mathcal{P}| = 0$ then
15:             Pruning failed: Use Algorithm 5.4.
16:         end if
17:         Remove the first entry $j$ of $\mathcal{P}$.
18:         $u := g_j^{-1} u$
19:     end if
20: end while
21: return $\mathcal{P}$
```

Proposition 5.6. *Algorithm 5.5 is correct.*

Proof. Any solution returned by Algorithm 5.5 is correct since if the `while`-loop terminates, then $|u - w| = 0$, so $u = w$.

If the pruning is not successful, Algorithm 5.4 is called, which is correct by the above discussion. □

If $|\mathcal{P}| = 0$ in line 14, then the algorithm is back at the starting vertex and has no edges left to test. In a normal depth first search, this would mean that the algorithm has explored the whole connected component of the starting vertex. But here this might not be the case as Figure 5.3b illustrates. Hence we have to fall back to a provable correct algorithm.

To avoid situations as in Figure 5.3b, one may add more edges to the graph to overcome "local maxima". In the implementation we add all products $g_i g_j$ for $1 \leq i, j \leq m$ and $g_i g_j g_k$ for $1 \leq i, j, k \leq m$ dynamically, that is, "a few" new edges whenever we reach $|\mathcal{P}| = 0$.

One might attempt to cache information so that the breadth first search started in line 15 does not have to start from scratch. However, one would have to cache all vertices, at which the algorithm did not explore further (pruned the tree). This quickly requires huge memory resources.

The algorithm explores only few vertices (in comparison to Algorithm 5.4) and needs little memory accordingly.

5.3. Another approach to Proposition 2.7

The previous section is surely the most unsatisfying part of this thesis, both from a theoretical and a practical point of view. To conclude the thesis, we want to present another approach to making Proposition 2.7 constructive, that is, an algorithm which could be used instead of Algorithm 5.2 and which does not rely on Algorithm 5.5. Although this algorithm turned out to be not as efficient as Algorithm 5.2 in practice, we still like the idea behind it and expect that there is a certain potential of optimization. As this section is only meant to present an idea, it is more "sketchy" then the previous ones.

We now give the algorithm and then discuss some starting points for improvements.

Algorithm 5.7 ("Transforming unit" as in Proposition 2.7 – alternative approach)**.**

```
Input: Maximal integral ideals $M$ and $N$ with left order $\Lambda$, such that $\operatorname{nr} M = \operatorname{nr} N = \mathfrak{p}$
    and $\mathfrak{p} + r\mathfrak{d} = R$ (see Proposition 2.7).
Output: $\vartheta \in \Lambda^\times$ with $M = N\vartheta$.
 1: Carry out lines 1 to 3 of Algorithm 5.2 resulting in vectors $v, w \in (R/\mathfrak{p})^n \setminus \{0\}$.
 2: Choose any $g \in \mathrm{GL}_n(R/\mathfrak{p})$ with $gv = w$ and choose any lift $\alpha$ of $g$ in $\Lambda$.
 3: Set $L := K(\alpha)$ and $S := \mathrm{IntCls}_L(R)$.
 4: if $S \not\subseteq \Lambda$ then
 5:     go to line 2.
 6: end if
 7: Compute the ideal $\mathfrak{a} := S \cap \mathfrak{p}\Lambda$ and the group $(S/\mathfrak{a})^\times$. Denote the reduction of $\alpha$
    modulo $\mathfrak{a}$ by $\overline{\alpha}$.
 8: if $\overline{\alpha} \notin (S/\mathfrak{a})^\times$ then
 9:     go to line 2.
10: end if
11: Compute the group $S^\times$ and the canonical map $\pi : S^\times \to (S/\mathfrak{a})^\times$.
12: if $\overline{\alpha} \notin \pi(S^\times)$ then
13:     go to line 2.
14: end if
15: Choose any $u \in S^\times$ with $\pi(u) = \overline{\alpha}$.
16: return $u$
```

The correctness of the algorithm is clear: If it returns an element $u \in S^\times \subseteq \Lambda^\times$ coming from a field extension $K(\alpha)$, then $u \equiv \alpha \mod \mathfrak{p}\Lambda \cap S$, so $u \equiv \alpha \mod \mathfrak{p}\Lambda$. Hence u is another preimage of g in line 2. Further, the algorithm terminates at the latest, when α itself is a unit of Λ.

This is, of course, a purely theoretical argument. In practice we had the impression, that the number of different fields one needs to consider lies in $\mathcal{O}(p)$, where p is the characteristic of $R/\mathfrak{p}$.

Although, this would result in an encouraging probability of success,[2] there are two simple reasons why we have chosen Algorithm 5.2 in favour of Algorithm 5.7:

(a) Algorithm 5.2 is in general faster.

(b) The element returned by Algorithm 5.2 is in general smaller.

However, we have hope that Algorithm 5.7 can be improved regarding both points. A major part of the runtime of the algorithm is used for the computation of the unit group $S^\times$ in line 11. This is not a surprise as the computation of unit groups is not an easy problem and the algorithm has to compute such a group for almost every field since it appears to rarely go back to line 2 from line 5 or 9. Therefore it seems worthwhile to try to improve the performance of lines 11 to 14 in light of problem (a). A point of improvement would be to choose a representative of α modulo $\mathfrak{p}\Lambda$ with a minimal polynomial with particularly small coefficients. Further, one does not need to compute the whole unit group but only a subgroup $H \leq S^\times$ such that $\pi(H) = \pi(S^\times)$. In fact, even this is in principle not needed, as one only needs to decide whether $\overline{\alpha} \in \pi(S^\times)$.

[2] In comparison to the orbit length in Section 5.2.

These ideas could also be ways to remedy problem (b). If one can find a "nice" subgroup H of $S^\times$, then its generators may be smaller, resulting in a smaller element u.

Another very standard way to at least circumvent problem (b) is to compute u in a factorized form, that is as a product of (comparatively) small factors. As far as Algorithm 5.7 is concerned there is nothing to change to do this, as the algorithm is done as soon as it finds u. If Algorithm 5.7 is called by Algorithm 5.1 we suggest the following adjustments in the latter algorithm. At the start of any iteration of the `for`-loop of Algorithm 5.1 let J be given by an R-generating system, that is $J = \sum_{i=1}^{k} R\alpha_i$, where $\alpha_i \in A$ and $k \in \mathbb{N}$. Here, $\alpha_1, \dots, \alpha_k$ may be represented in factorized form. Use the elements α_i as input for Algorithm 3.10 called in line 4. In this algorithm one maps these to a finite algebra where it is no problem to compute the actual elements from the product representations and to compute a maximal integral ideal N containing J. Let now $\tilde{\vartheta}$ be the element returned by Algorithm 5.7 in line 5 of Algorithm 5.1 and let $N^{-1} = \sum_{i=1}^{l} R\beta_i$, where $\beta_i \in A$, $l \in \mathbb{N}$. Then the product in line 8 of Algorithm 5.1 is given by

$$\tilde{\vartheta}^{-1} N^{-1} J \tilde{\vartheta} = \sum_{i=1}^{l} \sum_{j=1}^{k} R\big(\tilde{\vartheta}^{-1} \beta_i \alpha_j \tilde{\vartheta}\big),$$

so one obtains again an R-generating system of the ideal J of the next iteration.

Appendix

A. Computing maximal ideals in matrix algebras

In this section we discuss the analogue of Section 3.2 for matrix algebras over a field. Let F be any field and set $B := \mathrm{Mat}_k(F)$ for a $k \in \mathbb{N}$. Especially for algorithmic purposes, we fix an F-basis of B as follows: Let $E_{i,j} = (e_{i',j'})_{i',j'}$ for fixed $1 \leq i, j \leq k$ be the element of B with

$$e_{i',j'} = \begin{cases} 1, & i = i' \text{ and } j = j', \\ 0, & \text{otherwise.} \end{cases}$$

Then $\{E_{1,1}, E_{1,2}, \ldots, E_{k,k}\}$ is clearly an F-basis of B. One immediately sees that

$$E_{i,j}E_{i',j'} = \begin{cases} E_{i,j'}, & j = i', \\ 0, & \text{otherwise.} \end{cases}$$

and $E_{i,i} = E_{i,1}E_{1,1}E_{1,i}$ for all $i, i', j, j' \in \{1, \ldots, k\}$.

Before we start to consider maximal ideals we need the following proposition whose proof is inspired by [BW09, Lemma 4.1].

Proposition A.1. *Every left ideal of B is a principal ideal.*

Proof. Let $I \subseteq B$ be a left ideal. Let furthermore $v_1, \ldots, v_m$ be a F-basis for $E_{1,1}I$. Set $x := \sum_{i=1}^{m} E_{i,1}v_i \in I$. We claim $Bx = I$.

Indeed, we clearly have $Bx \subseteq I$, as $x \in I$. On the other hand, it holds $I = 1I \subseteq E_{1,1}I + \cdots + E_{k,k}I$. We have

$$E_{i,i}I = E_{i,1}E_{1,1}E_{1,i}I \subseteq E_{i,1}E_{1,1}I = \left\langle E_{i,1}v_1, \ldots, E_{i,1}v_m \right\rangle_F,$$

for all $i \in \{1, \ldots, k\}$, so

$$I \subseteq \sum_{i=1}^{k} \left\langle E_{i,1}v_1, \ldots, E_{i,1}v_m \right\rangle_F.$$

Finally it holds $E_{i,j}x = E_{i,1}v_j$, hence $E_{i,1}v_j \in Bx$ for all $1 \leq i \leq k$ and $1 \leq j \leq m$ and therefore $I \subseteq Bx$. □

We can easily extract an algorithm from the previous proof.

Algorithm A.2 (Principal generator of a left ideal).
Input: A left ideal I in a matrix algebra $B = \mathrm{Mat}_k(F)$.
Output: $x \in I$ such that $I = Bx$.

```
Compute an $F$-basis $v_1, \ldots, v_m$ for $E_{1,1}I$.
return $\sum_{i=1}^{m} E_{i,1}v_i$
```

The maximal left ideals of B can be characterized in the following way.

Lemma A.3. *Let $x \in B$ and $I := Bx$. Then $\operatorname{rk} x = k - 1$ if and only if I is a maximal left ideal of B.*

Proof. Let x_i be the i-th row of x. As an F-vector space, I is generated by $E_{i,j}x$ for all $1 \leq i, j \leq k$, which are the matrices with x_j in the i-th row. We now consider these matrices as vectors in F^{k^2} by mapping a matrix $(y_{i,j})_{i,j}$ to the vector $(y_{1,1}, y_{1,2}, \ldots, y_{2,1}, \ldots, y_{k,k})$. By writing these vectors in the order

$$E_{1,1}x, E_{1,2}x, \ldots, E_{2,1}x, \ldots, E_{k,k}x$$

in the rows of a $k^2 \times k^2$ matrix we obtain

$$M := \operatorname{diag}(x, x, \ldots, x).$$

The span of the rows of M is isomorphic to I as F-vector spaces and one directly sees $\operatorname{rk} M = k \operatorname{rk} x$, so $\dim_F I = k \operatorname{rk} x$. The maximality of I is equivalent to B/I being a simple module. Combining [Bou58, §5, Proposition 11] and [Bou58, §5, Théorème 2], each simple module of B has F-dimension k, so I is maximal if and only if $\dim_F I = k(k-1)$. Therefore I is maximal if and only if $\operatorname{rk} x = k - 1$. □

Remark A.4. By Lemma A.3, one can construct a maximal left ideal of B by choosing any matrix of rank $k - 1$, e. g. $\operatorname{diag}(1, \ldots, 1, 0)$, as generator.

Lemma A.3 is also helpful in the following problem: Given a left ideal I of B, find a maximal left ideal J containing I. This is solved by the following algorithm.

Algorithm A.5 (Maximal ideal containing a given ideal).
Input: A left ideal I in a matrix algebra $B = \operatorname{Mat}_k(F)$.
Output: A maximal left ideal J in B with $I \subseteq J$.

```
Use Algorithm A.2 to find $x \in I$ with $Bx = I$.
Compute a row reduced echelon form $\tilde{x}$ of $x$ and set $r := \operatorname{rk} x$.
while $r < k - 1$ do
    Find a column $j$ of $\tilde{x}$ without a pivot.[1]
    Find a row $i$ of $\tilde{x}$ containing only zeros.
    Set $\tilde{x} := \tilde{x} + E_{i,j}$ and $r := r + 1$.
end while
return $B\tilde{x}$
```

Lemma A.6. *Given a left ideal I, Algorithm A.5 correctly computes a maximal left ideal J with $I \subseteq J$.*

Proof. By construction, $\tilde{x}$ will have rank $k - 1$ at the end of the `while`-loop. Then $J := B\tilde{x}$ is maximal by Lemma A.3.

Let now $I = Bx$ and $\tilde{x}$ be the row reduced echelon form of x. We have to show that $I \subseteq B\tilde{x}$ at any point of the algorithm. Before the start of the `while`-loop it holds

[1] That is a column in which no non-zero entry is the leftmost non-zero entry of its row, if the row reduced echelon form is "upper right".

$Bx = B\tilde{x}$ since $\tilde{x} = ux$ for a matrix $u \in \mathrm{GL}_k(F) = B^\times$. Consider now any iteration of the `while`-loop and assume that $I \subseteq B\tilde{x}$ at the beginning of this iteration. Let (i, j) be a tuple chosen in lines 4 and 5. As in the proof of Lemma A.3, $B\tilde{x}$ is generated as an F-vector space by the matrices $E_{i',j'}\tilde{x}$ for $1 \leq i', j' \leq k$. We have

$$E_{i',j'}(\tilde{x} + E_{i,j}) = E_{i',j'}\tilde{x}$$

whenever $j' \neq i$ and in case $j' = i$ it holds

$$E_{i',j'}(\tilde{x} + E_{i,j}) = E_{i',j}$$

since the i-th row of $\tilde{x}$ was chosen to be zero, so $E_{i',j'}\tilde{x} = 0$. This means that

$$B(\tilde{x} + E_{i,j}) = B\tilde{x} + BE_{i,j}$$

as vector spaces, so clearly $I \subseteq B\tilde{x} \subseteq B(\tilde{x} + E_{i,j})$. □

B. Quotients of modules over Dedekind rings

This section is mostly a translation of (unpublished) notes by Dr. Tommy Hofmann.

Let $R \neq K$ be a Dedekind ring with quotient field K and $\mathfrak{p}$ a prime ideal in R with residue field $\kappa = R/\mathfrak{p}$ and let $\rho : R \to \kappa$ be the canonical projection. Let M and N be finitely generated torsion-free R-modules with $\mathfrak{p}M \subseteq N \subseteq M$. We want to find a κ-basis of the module M/N.[2]

By [CR62, Theorem 22.12], we can write $M = \bigoplus_{i=1}^k \mathfrak{a}_i m_i$ and $N = \bigoplus_{i=1}^k \mathfrak{b}_i n_i$ with $\mathfrak{a}_i$ and $\mathfrak{b}_i$ fractional ideals of R, $m_i \in KM$ and $n_i \in KN$ for all $1 \leq i \leq k$, where $k \in \mathbb{N}$. As $N \subseteq M$, there exist $b_{ij} \in \mathfrak{a}_j$ with $n_i = \sum_{j=1}^k b_{ij} m_j$ for all $1 \leq i, j \leq k$. This yields the matrix $B := (b_{ij})_{i,j} \in \mathrm{Mat}_k(K)$ and the basis pseudo-matrix of N:

$$\mathcal{B} := \begin{array}{c} \mathfrak{b}_1 \\ \vdots \\ \mathfrak{b}_k \end{array} \begin{pmatrix} b_{11} & \cdots & b_{1k} \\ \vdots & & \vdots \\ b_{k1} & \cdots & b_{kk} \end{pmatrix}.$$

We may assume that B is a lower-left triangular matrix, since we can compute a pseudo Hermite Normal Form of $\mathcal{B}$ (see [Coh00, Section 1.4]). Note that this matrix has rank k, since $\mathfrak{p}M \subseteq N$.

Set $I := \{i \in \{1, \dots, k\} \mid v_\mathfrak{p}(b_{ii}) > 0\}$ and $l := |I|$.

Free modules

At first we assume that M and N are free modules, that is $\mathfrak{a}_i = R$ and $\mathfrak{b}_i = R$ for all $1 \leq i \leq k$. This implies $b_{ij} \in R$ for $1 \leq i, j \leq k$. Then the situation is quite simple:

Theorem B.1. *The tuple $(\overline{m}_i)_{i \in I}$ is a κ-basis of M/N.*

Proof. Since we have $M = \bigoplus_{i=1}^k Rm_i$ and $N = \bigoplus_{i=1}^k Rn_i$ as R-modules, we also have $M = \bigoplus_{i=1}^k \kappa m_i$ and $N = \bigoplus_{i=1}^k \kappa n_i$ as κ-vector spaces. Now $\rho(b_{ii}) = 0$ if and only if $i \in I$. Therefore the claim follows by basic linear algebra. □

[2] More exactly: We view M and N and hence M/N as κ-modules via restriction of scalars with respect to the map ρ.

For algorithmic purposes we are also interested in an R-linear map $f : M \to \kappa^l$, which factors through M/N. We construct such a map as follows. The first step is to write $v \in M$ as $v = \sum_{i \in I} a_i m_i + w$ for some $w \in N$ and $a_i \in R$. For this, let $v = \sum_{i=1}^k x_i m_i$ with $x_i \in R$ and fix a $j \in \{1, \ldots, k\} \setminus I$. Now $\rho(b_{jj}) \neq 0$, so there exists $c_j \in R$ such that $\rho(b_{jj} c_j) = 1$ and then $\rho(x_j) - \rho(x_j b_{jj} c_j) = 0$. So we can reduce the coefficients $x_1, \ldots, x_k$ with the rows of B for each $j \in \{1, \ldots, k\} \setminus I$ (sorting the indices in decreasing order by size, if B is lower-left triangular) and obtain a representation

$$v = \sum_{i \in I} a_i m_i + \sum_{i \notin I} a_i m_i + \tilde{w}$$

for some $\tilde{w} \in N$ and $a_i \in R$ such that $v_{\mathfrak{p}}(a_i) > 0$ for $i \notin I$. But $\mathfrak{p}M \subseteq N$, so $a_i m_i \in N$ for $i \notin I$, that is, we have $w := \sum_{i \notin I} a_i m_i + \tilde{w} \in N$, so $v = \sum_{i \in I} a_i m_i + w$ as claimed.

We then set $f(v) := \sum_{i \in I} a_i e_i$, where $(e_i)_{i \in I}$ is some basis of κ^l. We now also construct a section s for f. By abuse of notation let ρ^{-1} be any section of ρ. We obtain a section of f by setting

$$s : \kappa^l \to M, \ \sum_{i \in I} \lambda_i e_i \mapsto \sum_{i \in I} \rho^{-1}(\lambda_i) m_i.$$

By Theorem B.1, it is clear, that f factors through M/N.

General case

We now return to the general case, where M and N are not free over R. The key idea is to consider the localization at $\mathfrak{p}$. Recall that $\kappa = R/\mathfrak{p} \cong R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ and $M_{\mathfrak{p}}/N_{\mathfrak{p}} \cong M/N$, as $\mathfrak{p}M \subseteq N$.

We assume that $v_{\mathfrak{p}}(\mathfrak{a}_i) = 0 = v_{\mathfrak{p}}(\mathfrak{b}_i)$ for all $1 \leq i \leq n$. This can be achieved as follows: Let $\pi \in \mathfrak{p}$ be an element with $v_{\mathfrak{p}}(\pi) = 1$ and let $v_i := v_{\mathfrak{p}}(\mathfrak{a}_i)$. Set $\tilde{\mathfrak{a}}_i := \pi^{-v_i} \mathfrak{a}_i$ and $\tilde{m}_i := \pi^{v_i} m_i$. Then it holds $v_{\mathfrak{p}}(\tilde{\mathfrak{a}}_i) = 0$ and

$$M = \bigoplus_{i=1}^k \mathfrak{a}_i m_i = \bigoplus_{i=1}^k \mathfrak{a}_i \pi^{-v_i} \pi^{v_i} m_i = \bigoplus_{i=1}^k \tilde{\mathfrak{a}}_i \tilde{m}_i.$$

So we may choose $(\tilde{\mathfrak{a}}_i, \tilde{m}_i)_{1 \leq i \leq k}$ as pseudo basis for M. By analogously scaling the pseudo basis for N, we obtain the desired valuations. This now means that $(R \setminus \mathfrak{p})^{-1} \mathfrak{a}_i = R_{\mathfrak{p}}$ and $(R \setminus \mathfrak{p})^{-1} \mathfrak{b}_i = R_{\mathfrak{p}}$ for all $1 \leq i \leq k$ and we have well-defined images of the entries of B in κ, as these entries lie in the coefficient ideals $\mathfrak{a}_i$.

Theorem B.2. *The elements $(\overline{m}_i)_{i \in I}$ form a κ-basis of $M_{\mathfrak{p}}/N_{\mathfrak{p}} \cong M/N$.*

Proof. From the definition of M we obtain

$$M_{\mathfrak{p}} = \bigoplus_{i=1}^k (R \setminus \mathfrak{p})^{-1} \mathfrak{a}_i m_i = \bigoplus_{i=1}^k R_{\mathfrak{p}} m_i$$

for the localization. Analogously, we have $N_{\mathfrak{p}} = \bigoplus_{i=1}^k R_{\mathfrak{p}} n_i$ and therefore M and N are free $R_{\mathfrak{p}}$-modules. Now the claim follows with Theorem B.1. □

As in the case of free modules, we want to construct a map $f : M \to \kappa^l$, which factors through M/N for $l = |I|$, and a section s of f. For $v \in M$ we obtain a representation $v = \sum_{i\in I} a_i m_i + w$ with $a_i \in R_\mathfrak{p}$ and $w \in N_\mathfrak{p}$ by reducing v with the j-th row of B for $j \in \{1, \ldots, n\} \setminus I$ as before. Then we may set $f(v) = \sum_{i\in I} \tilde{\rho}(a_i)e_i$, where $\tilde{\rho} : R_\mathfrak{p} \to \kappa$ is the canonical projection.

For the construction of a section we have to take more care as in the case of free modules: For $\sum_{i\in I} \lambda_i e_i \in \kappa^l$ we cannot just choose any preimages $a_i = \rho^{-1}(\lambda_i) \in R$, as a_i might not be an element of the coefficient ideal $\mathfrak{a}_i$. Therefore we choose for each $i \in I$ an element $\alpha_i \in \mathfrak{a}_i$ with $v_\mathfrak{p}(\alpha_i) = 0$, so $\rho(\alpha_i) \neq 0$ in κ, and define

$$s : \kappa^l \to M,\ \sum_{i\in I} \lambda_i e_i \mapsto \sum_{i\in I} \rho^{-1}(\lambda_i)\rho^{-1}\big(\tilde{\rho}(\alpha_i)^{-1}\big)\alpha_i m_i,$$

where we implicitly consider the α_i as elements of $R_\mathfrak{p}$. Then $s\big(\sum_{i\in I} \lambda_i e_i\big)$ is indeed an element of M, since $\rho^{-1}(\lambda_i)\rho^{-1}\big(\tilde{\rho}(\alpha_i)^{-1}\big) \in R$ and $\alpha_i \in \mathfrak{a}_i$. Clearly s is a section of f as

$$f\Big(s\Big(\sum_{i\in I} \lambda_i e_i\Big)\Big) = f\Big(\sum_{i\in I} \rho^{-1}(\lambda_i)\rho^{-1}\big(\tilde{\rho}(\alpha_i)^{-1}\big)\alpha_i m_i\Big) = \sum_{i\in I} \lambda_i \tilde{\rho}(\alpha_i)^{-1}\tilde{\rho}(\alpha_i)e_i = \sum_{i\in I} \lambda_i e_i,$$

since $\tilde{\rho}|_R = \rho$.

C. S-units and unit groups of Dedekind rings

Let, as always, K be an algebraic number field and $R \neq K$ a Dedekind ring with quotient field K. Let S be a (possibly infinite) set of places of K containing all infinite places. Extending the definition of S-units in [Neu07] to infinite sets we set

$$K^S := \{x \in K^\times \mid v_\mathfrak{p}(x) = 0 \text{ for all places } \mathfrak{p} \notin S\},$$

which is clearly a multiplicative group.

Write $\mathcal{O}_K$ for the integral closure of $\mathbb{Z}$ in K, so R is a localization of $\mathcal{O}_K$ by [Swa86, Proposition A21]. Let T be the set of places of K which do not correspond to a prime ideal of R. Note that the cardinality of T might be infinite, e. g., if R is the localization of $\mathcal{O}_K$ at one prime ideal. The aim of this section is to prove

$$K^{S_R \cup T}/R^\times \cong \mathbb{Z}^{|S_R|}$$

for any finite set $S_R \subseteq \mathbb{P}(R)$, where we always identify prime ideals of R respectively $\mathcal{O}_K$ with places of K.

We need two preliminary results.

Lemma C.1. *It holds $R^\times = K^T$.*

Proof. By choice of T it holds

$$K^T = \{x \in K^\times \mid v_\mathfrak{p}(x) = 0 \text{ for all } \mathfrak{p} \in \mathbb{P}(R)\}.$$

For $r \in K$, we then have the following chain of equivalences:

$$r \in R^\times \iff rR = R \iff v_\mathfrak{p}(r) = 0 \text{ for all } \mathfrak{p} \in \mathbb{P}(R) \iff r \in K^T. \qquad \square$$

Lemma C.2. *Let $S_R \subseteq \mathbb{P}(R)$ be a finite set and set $S := S_R \cup T$. Then it holds $K^S/R^\times \cong \mathbb{Z}^r$ for some $r \in \mathbb{Z}_{\geq 0}$ with $r \leq |S_R|$.*

Proof. Write $S_R = \{\mathfrak{p}_1, \dots, \mathfrak{p}_k\}$, so $|S_R| = k$, and consider the map

$$\varphi : K^S \to \mathbb{Z}^k,\ x \mapsto (v_{\mathfrak{p}_1}(x), \dots, v_{\mathfrak{p}_k}(x)),$$

which is clearly a homomorphism of groups.

We claim $\ker \varphi = K^T$. Indeed, if $x \in K^T$, then $v_\mathfrak{p}(x) = 0$ for all $\mathfrak{p} \in \mathbb{P}(R)$, so in particular $v_{\mathfrak{p}_i}(x) = 0$ for all $1 \leq i \leq k$ which implies $x \in \ker \varphi$. On the other hand, if $x \in \ker \varphi$, then $v_{\mathfrak{p}_i}(x) = 0$ for all $1 \leq i \leq k$. But also $v_\mathfrak{p}(x) = 0$ for all $\mathfrak{p} \in \mathbb{P}(R) \setminus S_R$, since $x \in K^S$, so $x \in K^T$.

By Lemma C.1, we hence have $\ker \varphi = R^\times$, so there is an injection

$$K^S/R^\times \hookrightarrow \mathbb{Z}^k,$$

which implies that $K^S/R^\times$ is isomorphic to a subgroup of $\mathbb{Z}^k$. Each subgroup of the free abelian group $\mathbb{Z}^k$ is itself a free abelian group of smaller or equal rank by [Lan02, Theorem I.7.3]. Hence $K^S/R^\times \cong \mathbb{Z}^r$ for some $0 \leq r \leq k$ as claimed. □

We are now ready to prove the main result.

Theorem C.3. *For any finite set $S_R \subseteq \mathbb{P}(R)$ it holds $K^{S_R \cup T}/R^\times \cong \mathbb{Z}^{|S_R|}$.*

Proof. There exists a set of prime ideals $S_{\mathcal{O}_K} \subseteq \mathbb{P}(\mathcal{O}_K)$ corresponding to S_R, since prime ideals of the localization R correspond to prime ideals of $\mathcal{O}_K$ via contraction with respect to the canonical inclusion map $\mathcal{O}_K \hookrightarrow R$. This means, that the prime ideals in $S_{\mathcal{O}_K}$ and in S_R correspond to the same finite places of K.

Let S_∞ be the set of infinite places of K and note that $S_\infty \subseteq T$. Set $S := S_R \cup T$ and $S' := S_{\mathcal{O}_K} \cup S_\infty$. The arguments are now quite similar to the ones in Lemma C.2.

Consider the group homomorphism

$$\psi : K^{S'} \to K^S/R^\times,\ x \mapsto \overline{x},$$

where we denote the residue class of the reduction of x modulo $R^\times$ by $\overline{x}$. This is a well-defined map, since, considered as sets of places of K, we have $S' \subseteq S$ and therefore $K^{S'} \leq K^S$.

We claim $\ker \psi = \mathcal{O}_K^\times$. Indeed, if $x \in \mathcal{O}_K^\times$, then $x \in K^{S_\infty}$ by Lemma C.1, so $x \in K^T$, since $S_\infty \subseteq T$. Hence $\psi(x) = \overline{1}$ since $R^\times = K^T$ by Lemma C.1 again. If $x \in \ker \psi$, then $x \in K^T$, which means $v_\mathfrak{p}(x) = 0$ for all finite places $\mathfrak{p}$ of K not in T. But we also have $x \in K^{S'}$, so $v_\mathfrak{p}(x) = 0$ for all finite places $\mathfrak{p}$ of K not in $S_{\mathcal{O}_K}$. Since $S_{\mathcal{O}_K}$ and T are disjoint by construction it follows $x \in K^{S_\infty} = \mathcal{O}_K^\times$.

Hence there is an injection

$$K^{S'}/\mathcal{O}_K^\times \hookrightarrow K^S/R^\times,$$

and $K^{S'}/\mathcal{O}_K^\times$ is isomorphic to a subgroup of $\mathbb{Z}^r$ with $r \leq k$ by Lemma C.2, where $k = |S_R| = |S_{\mathcal{O}_K}|$.

But by [Neu07, Korollar I.11.7] and [Neu07, Theorem I.7.4], we have

$$K^{S'}/\mathcal{O}_K^\times \cong \mathbb{Z}^k.$$

Therefore we must have $r = k$ by [Lan02, Theorem I.7.3] and thus

$$K^S/R^\times \cong \mathbb{Z}^k,$$

which finishes the proof. □

Bibliography

[Ass+17] Benjamin Assarf, Ewgenij Gawrilow, Katrin Herr, Michael Joswig, Benjamin Lorenz, Andreas Paffenholz and Thomas Rehn. 'Computing convex hulls and counting integer points with `polymake`'. In: *Math. Program. Comput.* 9.1 (2017), pp. 1–38.

[Bez+17] Jeff Bezanson, Alan Edelman, Stefan Karpinski and Viral B. Shah. 'Julia: A Fresh Approach to Numerical Computing'. In: *Siam Review* 59 (2017), pp. 65–98.

[BHZ08] Roberto Bagnara, Patricia M. Hill and Enea Zaffanella. 'The Parma Polyhedra Library: Toward a Complete Set of Numerical Abstractions for the Analysis and Verification of Hardware and Software Systems'. In: *Science of Computer Programming* 72.1–2 (2008), pp. 3–21.

[BJ11] Werner Bley and Henri Johnston. 'Computing generators of free modules over orders in group algebras II'. In: *Math. Comp.* 80.276 (2011), pp. 2411–2434.

[Bou58] Nicolas Bourbaki. *Algèbre. Modules et anneaux semi-simples.* Chapitre 8. Paris: Hermann, 1958.

[Bra+15] Oliver Braun, Renaud Coulangeon, Gabriele Nebe and Sebastian Schönnenbeck. 'Computing in arithmetic groups with Voronoï's algorithm'. In: *Journal of Algebra* 435 (2015), pp. 263–285.

[But91] Gregory Butler. *Fundamental Algorithms for Permutation Groups.* Vol. 559. Lecture Notes in Computer Science. Berlin, Heidelberg, New York: Springer-Verlag, 1991.

[BW09] Werner Bley and Stephen M. J. Wilson. 'Computations in relative algebraic K-groups'. In: *LMS J. Comput. Math.* 12 (2009), pp. 166–194.

[Coh00] Henri Cohen. *Advanced Topics in Computational Number Theory.* Vol. 193. Graduate Texts in Mathematics. Berlin, Heidelberg, New York: Springer-Verlag, 2000.

[Coh93] Henri Cohen. *A Course in Computational Algebraic Number Theory.* Vol. 138. Graduate Texts in Mathematics. Berlin, Heidelberg, New York: Springer-Verlag, 1993.

[CR62] Charles W. Curtis and Irving Reiner. *Representation Theory of Finite Groups and Associative Algebras.* New York: John Wiley & Sons (Interscience), 1962.

[CR81] Charles W. Curtis and Irving Reiner. *Methods of representation theory – with applications to finite groups and orders.* Vol. 1. New York: John Wiley & Sons (Interscience), 1981.

[Ebe89] Wayne Eberly. 'Computations for Algebras and Group Representations'. PhD thesis. University of Toronto, 1989.

[EHO05] Bettina Eick, Derek F. Holt and Eamonn A. O'Brien. *Handbook of Computational Group Theory.* Discrete mathematics and its applications. Boca Raton: Chapman & Hall/CRC, 2005.

[Eic37] Martin Eichler. 'Bestimmung der Idealklassenzahl in gewissen normalen einfachen Algebren'. In: *Journ. für r. u. a. Math.* 176 (1937), pp. 192–202.

[Fie+17] Claus Fieker, William Hart, Tommy Hofmann and Fredrik Johansson. 'Nemo/ Hecke: Computer Algebra and Number Theory Packages for the Julia Programming Language'. In: *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation.* ISSAC '17. New York, NY, USA: ACM, 2017, pp. 157–164.

[Fri00] Carsten Friedrichs. 'Berechnung von Maximalordnungen über Dedekindringen'. PhD thesis. Technische Universität Berlin, 2000.

[GJ00] Ewgenij Gawrilow and Michael Joswig. '`polymake`: a framework for analyzing convex polytopes'. In: *Polytopes – combinatorics and computation (Oberwolfach, 1997).* Vol. 29. DMV Sem. Birkhäuser, Basel, 2000, pp. 43–73.

[HJ18] Tommy Hofmann and Henri Johnston. 'Computing isomorphisms between lattices'. Preprint available at `https://www.mathematik.uni-kl.de/~thofmann/publications.html`. 2018.

[Hop98] Andreas Hoppe. 'Normal forms over Dedekind domains, efficient implementation in the computer algebra system KANT'. PhD thesis. Technische Universität Berlin, 1998.

[Kir17] Markus Kirschmer. *Arithmetik.* Aachen: Lecture notes, 2017.

[KN12] Sven O. Krumke and Hartmut Noltemeier. *Graphentheoretische Konzepte und Algorithmen.* Third edition. Leitfäden der Informatik. Wiesbaden: Springer Vieweg, 2012.

[KP05] Jürgen Klüners and Sebastian Pauli. 'Computing residue class rings and Picard groups of orders'. In: *Journal of Algebra* 292 (2005), pp. 47–64.

[KV10] Markus Kirschmer and John Voight. 'Algorithmic enumeration of ideal classes for quaternion orders'. In: *SIAM J. Comput.* 39.5 (2010), pp. 1714–1747.

[Lan02] Serge Lang. *Algebra.* Vol. 211. Graduate Texts in Mathematics. New York, Berlin, Heidelberg: Springer-Verlag, 2002.

[Nar04] Władysław Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers.* Third edition. Berlin, Heidelberg, New York: Springer-Verlag, 2004.

[Neu07] Jürgen Neukirch. *Algebraische Zahlentheorie.* Berlin, Heidelberg, New York: Springer-Verlag, 2007.

[Neu15] Jürgen Neukirch. *Klassenkörpertheorie.* Fourth edition. Berlin, Heidelberg, New York: Springer-Verlag, 2015.

[NS09] Gabriele Nebe and Allan Steel. 'Recognition of Division Algebras'. In: *Journal of Algebra* 322.3 (2009), pp. 903–909.

[Pag14a] Aurel Page. ‘An algorithm for the principal ideal problem in indefinite quaternion algebras’. In: *LMS J. Comput. Math.* 17 (Special issue A 2014), pp. 366–384.

[Pag14b] Aurel Page. ‘Méthodes explicites pour les groupes arithmétiques’. PhD thesis. Université de Bordeaux, 2014.

[Par84] Richard A. Parker. ‘The computer calculation of modular characters (the meat-axe)’. In: *Computational group theory* (1984), pp. 267–274.

[Rei06] Irving Reiner. *Maximal Orders.* Vol. 28. London Mathematical Society Monographs New Series. Oxford: Oxford University Press, 2006.

[Swa86] Richard G. Swan. *K-Theory of Finite Groups and Orders.* Second edition. Vol. 149. Lecture Notes in Mathematics. Berlin, Heidelberg, New York: Springer-Verlag, 1986.

I hereby declare that I wrote this thesis on my own and did not use any references or resources other than the named ones.

Ich erkläre hiermit, dass ich diese Arbeit selbst verfasst habe und außer den angegebenen keine weiteren Hilfsmittel oder Quellen genutzt habe.

Kaiserslautern, 23rd October 2019

Johannes Schmitt