CLASS FIELD THEORY FOR ORDERS OF NUMBER FIELDS

GENE S. KOPP AND JEFFREY C. LAGARIAS

ABSTRACT. This paper defines a generalized notion of *ray class group* associated to an arbitrary order in a number field together with an arbitrary ray class modulus for that order. It shows existence of ray class fields corresponding to these ray class groups. These ray class groups (resp., ray class fields) specialize to classical ray class groups (resp., fields) of a number field in the case of the maximal order, and they specialize to the ring class group (resp., field) of an order in the case of trivial modulus. The paper gives an exact sequence for simultaneous change of order and change of modulus. As a consequence, we identify the ray class field of an order with a given modulus as a specific subfield of a ray class field of the maximal order with a larger modulus. We also uniquely identify each ray class field of an order in terms of the splitting behavior of primes. An appendix extends some structural results of the paper to *ray class monoids* of the order (which include non-invertible elements).

CONTENTS

Date: December 17, 2022 (preliminary draft).

1. INTRODUCTION

The first complete version of class field theory for number fields was developed by Takagi [35] in 1920, building on work of Weber, Hilbert, and Fueter; see [18] and [20]. In Takagi's treatment, the ray class fields of a number field K comprise an infinite set of finite abelian extensions of K which are cofinal in the set of abelian extensions: That is, every finite abelian extension is contained in some ray class field. The ray class fields $H_{\mathfrak{m},\Sigma}$ are associated to ray class moduli $(\mathfrak{m}, \Sigma)$, where $\mathfrak{m}$ is an ideal of the ring of integers $\mathcal{O}_K$ of K, and Σ is a subset of the real embeddings of K. The ray class field associated to the modulus $(\mathcal{O}_K, \emptyset)$ is the Hilbert class field.

An *order* $\mathcal{O}$ of a number field K is a subring of K having finite rank equal to $[K : \mathbb{Q}]$ as a $\mathbb{Z}$-module. It may be shown that any element of an order is an algebraic integer, so the ring of all algebraic integers $\mathcal{O}_K$ is the maximal order of K. Associated to each nonmaximal order $\mathcal{O}$ of K, there is a separate classical notion of *ring class field* $H^{\mathcal{O}}$. When $K/\mathbb{Q}$ is an imaginary quadratic field, the set of ring class fields arise naturally as the fields $K(j(\tau))$ generated by values of the Klein j-invariant at points $\tau \in K$. The set of all ring class fields of a field K, obtained by varying

the order $\mathcal{O}$, are generally not cofinal in the set of abelian extensions of K and do not generate the maximal abelian extension K^{ab}.

This paper formulates a notion of *class field theory for orders* of number fields, in the Takagi sense. We define *ray class fields* $H^{\mathcal{O}}_{\mathfrak{m},\Sigma}$ *of an order* $\mathcal{O}$ that unify the perspective of ray class fields and ring class fields. We define these fields as associated to *ray class groups of an order* $\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$. Here, $\mathcal{O}$ is an order of K, $\mathfrak{m}$ is an ideal of $\mathcal{O}$, and Σ is a subset of the real embeddings of K; the ray class datum $(\mathcal{O};\mathfrak{m},\Sigma)$ specifies the level of a given ray class group. Classical ring class fields appear as "unramified" ray class fields of an order $\mathcal{O}$, in the sense that the ring class field of $\mathcal{O}$ is the ray class field of $\mathcal{O}$ for which the associated ray ideal is $\mathfrak{m} = \mathcal{O}$ and the associated set of real embeddings is $\Sigma = \emptyset$. An "unramified" ray class field H of a nonmaximal order $\mathcal{O}$ will usually have H/K a ramified extension of K, whose ramification will be only at prime ideals of K dividing the conductor ideal $\mathfrak{f}(\mathcal{O})$ of the order.

1.1. **Main Results.** This paper formulates appropriate notions of ray class groups and ray class fields of orders and establishes exact sequences relating these objects when the order and modulus are varied.

The first result states that the ray class field of an order $\mathcal{O}$ with modulus $(\mathfrak{m},\Sigma)$ is uniquely specified by its splitting of primes associated to the principal ray class in the ray class group with the given data. This definition is in the spirit of Weber's original definition of a class field in terms of a law of decomposition of prime ideals (see [40, p. 164], [18, p. 266], and also [39]), motivated by special values of modular functions.

Theorem 1.1. *Let K be a number field, $\mathcal{O}$ an order of K, $\mathfrak{m}$ an ideal of $\mathcal{O}$, and Σ a (possibly empty) subset of the set of real embeddings of K. Then for the ray class datum $(\mathcal{O};\mathfrak{m},\Sigma)$, there exists a unique abelian Galois extension $H^{\mathcal{O}}_{\mathfrak{m},\Sigma}/K$ with the property that a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ that is relatively prime to the quotient ideal $(\mathfrak{m}:\mathcal{O}_K)$ splits completely in $H^{\mathcal{O}}_{\mathfrak{m},\Sigma}/K$ if and only if $\mathfrak{p}\cap\mathcal{O} = \pi\mathcal{O}$, a principal prime $\mathcal{O}$-ideal, having $\pi\in\mathcal{O}$ with $\pi \equiv 1 \pmod{\mathfrak{m}}$ and $\rho(\pi) > 0$ for $\rho\in\Sigma$.*

Theorem 1.1 is an existence theorem which, when given the ray class datum $(\mathcal{O};\mathfrak{m},\Sigma)$, produces an associated ray class field. The map $(\mathcal{O};\mathfrak{m},\Sigma)\mapsto H^{\mathcal{O}}_{\mathfrak{m},\Sigma}$ is neither one-to-one nor onto: A given abelian extension H/K might be a ray class field for none or many different triples $(\mathcal{O}';\mathfrak{m}',\Sigma')$, allowing the order to vary.

To understand Theorem 1.1, it is helpful to compare the quotient ideal $(\mathfrak{m}:\mathcal{O}_K)$ to more familiar ideals. Given any integral ideal $\mathfrak{m}$ of $\mathcal{O}$, the quotient ideal $(\mathfrak{m}:\mathcal{O}_K)$ is the largest ideal of $\mathcal{O}_K$ contained in $\mathfrak{m}$. An important invariant of an order $\mathcal{O}$ of an algebraic number field K is its (absolute) conductor $\mathfrak{f} = \mathfrak{f}(\mathcal{O}) = (\mathcal{O}:\mathcal{O}_K)$, which is the (set-theoretically) largest integral ideal $\mathfrak{f}\subseteq\mathcal{O}$ of $\mathcal{O}$ that is also an ideal of the maximal order $\mathcal{O}_K$. The conductor ideal $\mathfrak{f}(\mathcal{O})$ encodes information on all the non-invertible ideals in the order $\mathcal{O}$; see Lemma 2.12. The ideal $(\mathfrak{m}:\mathcal{O}_K)$ always satisfies the

inclusions (as $\mathcal{O}_K$-ideals)

$$\mathfrak{f}(\mathcal{O})\mathfrak{m} \subseteq (\mathfrak{m} : \mathcal{O}_K) \subseteq \mathfrak{f}(\mathcal{O}) \cap \mathfrak{m}\mathcal{O}_K, \tag{1.1}$$

where $\mathfrak{f} = \mathfrak{f}(\mathcal{O})$ is the conductor ideal of the order; these inclusions are proven in Lemma 2.18 (taking $\mathcal{O}' = \mathcal{O}_K$ in its statement). In particular $(\mathfrak{m} : \mathcal{O}_K) \subseteq \mathfrak{f}(\mathcal{O})$. The three ideals in eq. (1.1) have the same prime divisors: A prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ such that $\mathfrak{p} \supseteq \mathfrak{f}(\mathcal{O})\mathfrak{m} = \mathfrak{f}(\mathcal{O})\mathfrak{m}\mathcal{O}_K$ satisfies either $\mathfrak{p} \supseteq \mathfrak{f}(\mathcal{O})$ or $\mathfrak{p} \supseteq \mathfrak{m}\mathcal{O}_K$, and thus, $\mathfrak{p} \supseteq \mathfrak{f}(\mathcal{O}) \cap \mathfrak{m}\mathcal{O}_K$.

The smallest ray class field $H^{\mathcal{O}}_{\mathcal{O},\emptyset}$ of the order $\mathcal{O}$ is the ring class field associated to $\mathcal{O}$, which always contains the (wide) Hilbert class field of $\mathcal{O}_K$ and which has ramification over K at prime $\mathcal{O}_K$-ideals containing the conductor ideal $\mathfrak{f}(\mathcal{O})$.

The second result locates the ray class field $H^{\mathcal{O}}_{\mathfrak{m},\Sigma}/K$ of an order $\mathcal{O}$ for the datum $(\mathcal{O}; \mathfrak{m}, \Sigma)$ as falling between two ray class fields on the maximal order.

Theorem 1.2. *For an order $\mathcal{O}$ in a number field K and any ray class datum $(\mathcal{O}; \mathfrak{m}, \Sigma)$, there are inclusions of ray class fields $H^{\mathcal{O}_K}_{\mathfrak{m}\mathcal{O}_K,\Sigma} \subseteq H^{\mathcal{O}}_{\mathfrak{m},\Sigma} \subseteq H^{\mathcal{O}_K}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}$.*

It follows from Theorem 1.2 and eq. (1.1) that the set of all ray class fields of a fixed order $\mathcal{O}$ are confinal in the set of all finite abelian extensions of K.

The third result gives the correspondence between class groups and Galois groups of class fields. The *ray class group of an order* $\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ for datum $(\mathcal{O}; \mathfrak{m}, \Sigma)$ is defined using a notion of invertible fractional ideals of orders. The correspondence asserts that the ray class field $H^{\mathcal{O}}_{\mathfrak{m},\Sigma}$ of an order $\mathcal{O}$ is associated to an appropriate $\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ in such a way that a Galois correspondence holds: $\mathrm{Gal}(H^{\mathcal{O}}_{\mathfrak{m},\Sigma}/K) = \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ as abelian groups.

Theorem 1.3. *For an order $\mathcal{O}$ in a number field K and any ray class datum $(\mathcal{O}; \mathfrak{m}, \Sigma)$, with associated ray class field $H_0 := H^{\mathcal{O}}_{\mathfrak{m},\Sigma}$, there is an isomorphism $\mathrm{Art}_{\mathcal{O}} : \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) \to \mathrm{Gal}(H_0/K)$, uniquely determined by its behavior on prime ideals $\mathfrak{p}$ of $\mathcal{O}$ that are relatively prime to $\mathfrak{f}(\mathcal{O}) \cap \mathfrak{m}$, having the property that*

$$\mathrm{Art}_{\mathcal{O}}([\mathfrak{p}])(\alpha) \equiv \alpha^p \pmod{\mathfrak{P}}, \tag{1.2}$$

where $\mathfrak{P}$ is any prime of $\mathcal{O}_{H_0}$ lying over $\mathfrak{p}\mathcal{O}_K$. For any (not necessarily prime) ideal $\mathfrak{a}$ relatively prime to $\mathfrak{f}(\mathcal{O}) \cap \mathfrak{m}$,

$$\mathrm{Art}_{\mathcal{O}}([\mathfrak{a}]) = \mathrm{Art}([\mathfrak{a}\mathcal{O}_K])|_{H_0}, \tag{1.3}$$

where $\mathrm{Art} : \mathrm{Cl}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K) \to \mathrm{Gal}(H_1/K)$ is the usual Artin map in class field theory, with $H_1 = H_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}$.

In this result the set of prime ideals coprime to $\mathfrak{f}(\mathcal{O}) \cap \mathfrak{m}$ includes all but finitely many prime ideals.

The proofs in the paper first define and study ray class groups of orders, which are given in terms of groups of invertible fractional ideals, and relate them to Takagi ray class groups. A main part of the paper gives exact sequences which detail the effect on ray class groups of simultaneous change of orders inside a fixed number field, together with change of ideals between different

orders, allowing also changes in the number of real places considered, where positivity conditions are imposed. The class groups of the orders are then related to suitable subgroups of Takagi ray class groups in the maximal order $\mathcal{O}_K$, permitting the known results of global class field theory to obtain the theorems, via the Galois correspondence given by the Artin isomorphism of global class field theory. The significant content of the paper is these exact sequences, which yield also a formula for the cardinality of such ray class groups (Theorem 5.6).

The ray class groups of orders are defined in terms of groups of invertible fractional ideals of the order, but many calculations and proofs use possibly non-invertible integral ideals, sometimes in semilocal rings obtained by inverting elements relatively prime to a single auxiliary ideal $\mathfrak{d}$. Therefore the paper necessarily treats integral ideals along with a discussion of the conductor ideal.

The notion of class group of an order may be extended to a more general notion of *class monoid* (or *class semigroup*) of an order, which includes classes for the non-invertible elements of such orders. Such monoids were introduced by Dade, Taussky and Zassenhaus [13]. Some non-invertible ideals in an order $\mathcal{O}$ are actually equal (as sets) to invertible ideals in an order $\mathcal{O}'$ with $\mathcal{O} \subset \mathcal{O}'$. The class monoid of an order includes monoid classes which are associated with the classes in the class groups of all intermediate orders $\mathcal{O}'$ with $\mathcal{O} \subseteq \mathcal{O}' \subseteq \mathcal{O}_K$. In addition there may be classes in the class monoid which do not correspond to any invertible ideal in any order. Appendix A formulates results extending the group-theoretic constructions of this paper to *ray class monoids* of orders. These results are included because they are needed for some of the applications discussed below.

1.2. **Applications.** We discuss three applications involving ray class groups of orders of (real and imaginary) quadratic fields, motived by problems outside of pure class field theory.

(1) Special configurations of complex lines, called *SIC-POVMs (symmetric informationally complete positive operator-valued measures)* or *SICs*, are of interest in quantum information theory. A SIC is a special optimal complex projective code corresponding to a maximal set of d^2 complex lines in $\mathbb{C}^d$ that are "equiangular" with respect to the Hermitian inner product. They are known to exist in at least dimensions $d \leq 25$ and were conjectured by Zauner [42, 43] to exist in all dimensions.

Recently, a surprising connection has been made between SICs and the explicit class field theory of real quadratic fields [2, 3, 22]. The connection was originally discovered through numerical experimentation. Work in preparation by these authors and others [1, 24] incorporates ray class fields of real quadratic orders as part of a conjectural framework for classifying SICs.

(2) Recent progress toward p-adic analogues of the Stark conjectures has involved algebraicity results for *real multiplication values* of certain rigid meromorphic *modular cocycles* [14]. Work by the first author [23] introduces complex meromorphic modular cocycles whose real multiplication values are (essentially) the classical Stark class invariants conjectured to be algebraic units by Stark in the real quadratic case. The real multiplication values studied are

naturally parametrized by elements of ray class groups of orders, and they are conjectured to lie in ray class fields of orders.

(3) Certain ray class groups of a (real or complex) quadratic order have a characterization in terms of quadratic forms, generalizing the theory of Gauss composition. The first author and Olivia Beckwith [6] are developing a theory of "Gauss composition with level structure" associated a rational integral modulus $\mathfrak{m} = N\mathcal{O}$ in a quadratic order $\mathcal{O}$, generalizing the work of Eum, Koo, and Shin [15] in the imaginary quadratic maximal order case and Koda [21] in the real and imaginary quadratic case. This theory has applications to the theory of polyharmonic Maass forms for the congruence subgroup $\Gamma_1(N)$ of $\mathrm{SL}_2(\mathbb{Z})$.

1.3. **Prior Work.** There has been an extensive algebraic study of the structure of orders of number fields. Two general references are Stevenhagen [34] and Neukirch [30]. Neukirch views orders of number fields as number rings with "singularities" at the primes dividing the conductor ideal [30, Chap. 1, Sect. 12].

An important 1962 paper of Dade, Taussky, and Zassenhaus [13] obtained fundamental results on the structure of invertible ideals and class groups of orders; we discuss it in more detail. They developed a structure theory for one-dimensional Noetherian domains; see [13, p. 32]. An integral domain $\mathcal{D}$ has dimension one if and only if all nonzero prime ideals are maximal. Orders in number fields form a strict subclass of one-dimensional Noetherian integral domains. Dade, Taussky, and Zassenhaus gave a general definition of *fractional ideals* valid for all integral domains $\mathcal{D}$ (with quotient field denoted K) in [13, Defn. 1.1.6]. The set $\mathrm{J}(\mathcal{D})$ of all such fractional ideals of $\mathcal{D}$ is closed under four operations: $+, \cdot, \cap, (\ :\ )$, in which $\cdot$ is ideal multiplication and $(\mathfrak{a} : \mathfrak{b}) = \{x \in K \mid x\mathfrak{b} \subseteq \mathfrak{a}\}$ is ideal quotient [13, Prop. 1.10]. The set $\mathrm{J}(\mathcal{D})$ carries the structure of a semigroup under ideal multiplication. Dade, Taussky, and Zassenhaus define an $\mathcal{D}$-*order* of an integral domain to be any fractional ideal $\mathfrak{a}$ of $\mathcal{D}$ that is also an integral domain [13, p. 32]. Every fractional ideal $\mathfrak{a}$ has an associated $\mathcal{D}$-order $\mathrm{ord}(\mathfrak{a}) := (\mathfrak{a} : \mathfrak{a})$, which in other contexts is called its *multiplier ring*. For Noetherian integral domains, they gave a general definition of *invertible fractional ideal* and a characterization of them using ideal quotient [13, Defn. (p. 41), Prop. 1.3.6].

Ring class groups and ring class fields go back to fundamental work of Weber in 1897–1898 [39], motivated in part by complex multiplication; see his books [37, 38, 40]. The ring class groups associated to orders of imaginary quadratic fields appear in the theory of complex multiplication, because ideal classes of orders of imaginary quadratic fields are classified by homothety classes of lattices in $\mathbb{C}$ having a given endomorphism ring $\mathcal{O} \neq \mathbb{Z}$; see [12, Corollary 10.20]. The Weber prime splitting criteria for ring class fields of orders $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ $(n > 0)$ over imaginary quadratic fields are expressible in terms primes represented by the principal quadratic forms $x^2 + ny^2$. Explaining this connection is the main objective of the book of Cox [12], stated in Theorem 9.2.

In 1989 Stevenhagen [33] formulated an abstract development of *unramified class field theory for orders*, which extends beyond orders of number fields (see also [32]). In the case of orders of number fields, his results would specialize to the "unramified case" $(\mathcal{O}; \mathfrak{m}, \Sigma) = (\mathcal{O}; \mathcal{O}, \emptyset)$ treated

here. In 2015 Lv and Deng [25] treated ring class fields for arbitrary orders in number fields, in a more classical setting, again corresponding to the case $(\mathcal{O}; \mathfrak{m}, \Sigma) = (\mathcal{O}; \mathcal{O}, \emptyset)$. We are not aware of prior treatment of class field theory for orders in the general "ramified" case. Our work was motivated by the potential applications described in Section 1.2.

It is known that the compositum of all ring class fields of a field K (i.e., all "unramified class fields of orders" of K) need not be equal to the maximal abelian extension K^{ab}. That is, there can be abelian extensions of K that are not contained in any ring class field. In 1914 Fueter [16, p. 178] showed that the field $\mathbb{Q}(i, \sqrt[4]{1+2i})$ is not contained in any ring class field of $\mathbb{Q}(i)$; see also Schappacher [31, p. 258]. Moreover, Bruckner [8, Satz 8] showed for a quadratic field K that the compositum of ring class fields for K is the compositum of all Galois fields containing K that have Galois group over $\mathbb{Q}$ a generalized dihedral group. The case of imaginary quadratic fields is also treated in Cox [12, Theorem 9.18, Corollary 11.35].

1.4. **Contents of the paper.** The main theorems are proved by first defining ray class groups of orders as ray groups of invertible fractional ideals of the order quotiented by suitable ray groups of principal ideals. The proofs determine homomorphisms between these ray groups and Takagi ray groups of the maximal order $\mathcal{O}_K$, through study of extension and contraction maps between the invertible fractional ideals of $\mathcal{O}$ and $\mathcal{O}_K$. These maps in turn are induced from extension and contraction maps between integral ideal groups of $\mathcal{O}$ and $\mathcal{O}_K$.

Section 2 reviews the structure of the set of integral ideals of an order of a number field, which forms a monoid under ideal multiplication. It defines various monoids of fractional ideal of the order, which allow inversion of certain integral ideals. Ideal quotient of two fractional ideals is well-defined; however, not all integral ideals are invertible in general. Each non-invertible integral ideal contains some non-invertible prime ideal, and the non-invertible prime ideals are exactly those prime ideals containing the conductor ideal of the order. These monoids of fractional ideals are groups when restricted to ideals relatively prime to the conductor ideal of the order.

Section 3 studies the effect of change of order inside a fixed number fields K on the structure of ideals, via the contraction and extension maps on integral and fractional ideals.

Section 4 defines ray class groups of orders for a ray class datum $(\mathcal{O}; \mathfrak{m}, \Sigma)$. It relates such groups under extension and contraction of order. In particular Section 4.4 determines a surjective map from such a ray class group to a particular ray class group of the maximal order.

Section 5 first relates the effect of change of order $\mathcal{O} \subset \mathcal{O}'$ on unit groups and principal ideal groups of varying orders, in Proposition 5.3. The exact sequence of Theorem 5.4 in Section 5.2, which relates unit groups and class groups of different orders, is the main formula of this paper for applications. Section 5.3 gives a formula for the class number of a given ray class group of an order. This formula generalizes a formula in Neukirch [30, Theorem I. 12.12] for the cardinality of the ring class group (Picard group) of an order.

Section 6 gives the construction of ray class fields of orders. For this purpose it is necessary to obtain a given ray class group of an order $\mathcal{O}$ as a quotient group of a particular Takagi ray class

group of the maximal order $\mathcal{O}_K$. This is done in Section 6.1. The kernel of the map ψ in eq. (6.3) defining the quotient under the global class field correspondence via the Artin map then identifies a suitable subfield L of the Takagi ray class field as the desired ray class field of the order. Section 6.2 recalls the main existence theorems of class field theory with in a suitable form encoding both the formulation of Takagi (in terms of prime splitting) and of Artin (in terms of an isomorphism between ray class group and Galois groups). Section 6.3 proves Theorem 1.1 by identifying the map ψ in eq. (6.3) with the contraction map between fractional ideals of the maximal order $\mathcal{O}_K$ and the given order $\mathcal{O}$. Section 6.4 states and proves a result generalizing Theorem 1.2, replacing the maximal order $\mathcal{O}_K$ with a general order $\mathcal{O}'$ with $\mathcal{O} \subseteq \mathcal{O}' \subseteq \mathcal{O}_K$. Section 6.5 proves Theorem 1.3.

Section 7 presents some examples of ray class groups and ray class fields of quadratic orders.

Section 8 presents some remarks on extending results of the paper.

Appendix A discusses more general ray class monoids of orders. It gives a taxonomy of several classes of such monoids. These results are relevant to the applications discussed in Section 1.2, in particular to work in progress [6, 22, 24].

Appendix B discusses norms of ideals of an order and the (consistent) extension of the norm to monoids fractional ideals of an order. The norm is multiplicative when multiplying two fractional ideas, at least one of which is invertible, but is not multiplicative in general.

1.5. **Notation.**

- $\mathcal{O}$ = arbitrary order of a number field K.
- $\mathcal{O}'$ = another arbitrary order of K satisfying $\mathcal{O} \subseteq \mathcal{O}'$.
- $\mathfrak{f}_{\mathcal{O}'}(\mathcal{O}) = (\mathcal{O} : \mathcal{O}')$ = relative conductor ideal.
- $\mathrm{ord}(\mathfrak{a}) = (\mathfrak{a} : \mathfrak{a})$ = multiplier ring of the $\mathcal{O}$-ideal $\mathfrak{a}$.
- $\mathrm{I}(\mathcal{O})$ = monoid of integral ideals of the order $\mathcal{O}$.
- $\mathrm{I}^*(\mathcal{O})$ = submonoid of $\mathrm{I}(\mathcal{O})$ of integral ideals invertible as fractional ideals of $\mathcal{O}$.
- $\mathrm{I}_{\mathfrak{m}}(\mathcal{O})$ = monoid of integral ideals of $\mathcal{O}$ relatively prime to the integral ideal $\mathfrak{m}$.
- $\mathrm{I}^*_{\mathfrak{m}}(\mathcal{O})$ = submonoid of $\mathrm{I}_{\mathfrak{m}}(\mathcal{O})$ of integral ideals invertible as fractional ideals of $\mathcal{O}$.
- $\mathrm{J}(\mathcal{O})$ = monoid of all (possibly not invertible) fractional ideals of $\mathcal{O}$
- $\mathrm{J}^*(\mathcal{O})$ = group of invertible fractional ideals of $\mathcal{O}$.
- $\mathrm{J}_{\mathfrak{m}}(\mathcal{O})$ = monoid of fractional ideals relatively prime to the (nonzero) integral ideal $\mathfrak{m}$ of $\mathcal{O}$.
- $\mathrm{J}^*_{\mathfrak{m}}(\mathcal{O})$ = group of invertible fractional ideals relatively prime to $\mathfrak{m}$.
- $\mathrm{P}(\mathcal{O})$ = group of nonzero principal fractional ideals $\alpha\mathcal{O}$, with $\alpha \in K^\times$.
- $\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})$ = group of nonzero principal fractional ideals $\alpha\mathcal{O}$, $\alpha \in K^\times$, with $\alpha \equiv 1 \pmod{\mathfrak{m}}$, and positive on a given set Σ of real places of K.
- $\mathrm{P}^{\mathfrak{d}}_{\mathfrak{m},\Sigma}(\mathcal{O})$ = subgroup of $\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})$ of all $\alpha\mathcal{O} = (\mathfrak{a} : \mathfrak{b}) = \mathfrak{a}\mathfrak{b}^{-1}$ an ideal quotient of invertible integral ideals $\mathfrak{a}$, $\mathfrak{b}$, each relatively prime to a given integral ideal $\mathfrak{d}$ of $\mathcal{O}$.

2. IDEALS OF AN ORDER

Let $\mathcal{O}_K$ be the maximal order of all algebraic integers in a number field K. Then $\mathcal{O}_K$ is a Dedekind domain, having unique prime factorization of nonzero integral ideals. All nonzero fractional ideals are invertible, and they form a free abelian group. One has an ideal class group defined as the quotient of the group of nonzero fractional ideals by the group of nonzero principal ideals. One can define ray class groups by restricting to ideals relatively prime to a modulus $\mathfrak{m}$ and quotienting by the group of principal prime ideals having a generator $\alpha \equiv 1 \pmod{\mathfrak{m}}$ and with some positivity conditions at a subset Σ of real places.

Orders of a number field other than $\mathcal{O}_K$ are never Dedekind domains; they are one-dimensional arithmetic objects with "singularities" in the viewpoint of Neukirch [30, p. 73]. The ideal theory of non-maximal orders of number fields have the following differences from the maximal order. Not all integral ideals factor uniquely into prime ideals. Not all fractional ideals are invertible; so the set of fractional ideals under ideal multiplication has the structure of a monoid (a semigroup with identity). In addition the group of invertible fractional ideals need not be free; it may contain (a finite number of) torsion elements. Instead of an ideal class group, one can define an *ideal class monoid* by quotienting the monoid of fractional ideals by the group of nonzero principal ideals (which are always invertible); ideal class monoids and ray class monoids are discussed in Appendix A. One can also define an ideal class group (or Picard group) by restricting to invertible fractional ideals. Moreover, we will be able to define ray class groups on orders, by restricting to invertible fractional ideals relatively prime to a modulus $\mathfrak{m}$.

In the rest of Section 2, we state and prove required foundational results at varying levels of generality, always restricted to commutative rings with identity. In decreasing generality, these include integral domains, Noetherian integral domains, Noetherian integral domains of dimension one, finally orders of algebraic number fields.

Compared to more general integral domains, orders of a number field K have extra finiteness properties arising from the $\mathbb{Q}$-lattice structure on K. A *full rank $\mathbb{Z}$-lattice* of K is any $\mathbb{Z}$-module $\Lambda = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \cdots + \alpha_n\mathbb{Z}$ with each $\alpha_i \in K$, having $\mathbb{Z}$-rank $n = [K : \mathbb{Q}]$. The *multiplier ring* $\mathrm{ord}(\Lambda)$ of a full rank $\mathbb{Z}$-lattice Λ of a number field K is given by

$$\mathrm{ord}(\Lambda) := \{\alpha \in K : \alpha\Lambda \subseteq \Lambda\}, \tag{2.1}$$

and it is an order of K.

In general, $\mathrm{ord}(\Lambda)$ is the largest order (as a set) such that Λ is a fractional ideal of that order; see Section 2.5. Each order $\mathcal{O}$ of K is the multiplier ring of some full rank $\mathbb{Z}$-lattice, namely itself: $\mathcal{O} = \mathrm{ord}(\mathcal{O})$. Finiteness properties of orders of number fields include the finiteness of the invertible class group of an order and the uniform finiteness bound in Proposition 2.22.

2.1. Integral ideals, prime ideals, and primary ideals.

An *(integral) ideal* $\mathfrak{a}$ of a Noetherian integral domain $\mathcal{D}$ is a $\mathcal{D}$-submodule $\mathfrak{a} \subseteq \mathcal{D}$. The *$\mathcal{D}$-ideal product* $\mathfrak{ab}$ of two integral $\mathcal{D}$-ideals $\mathfrak{a}, \mathfrak{b}$

is the $\mathcal{D}$-ideal

$$\mathfrak{ab} := \left\{ \sum_j \alpha_j \beta_j : \alpha_j \in \mathfrak{a}, \beta_j \in \mathfrak{b} \right\}. \tag{2.2}$$

A $\mathcal{D}$-ideal $\mathfrak{p}$ is *prime* if $xy \in \mathfrak{p}$ implies $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$, and $\mathfrak{p} \neq \mathcal{D}$. There is a also notion of relative primality of $\mathcal{D}$-integral ideals.

Definition 2.1 (Relative primality of integral ideals)**.** An integral ideal $\mathfrak{a} \subseteq \mathcal{D}$ of an integral domain $\mathcal{D}$ is said to be *relatively prime* (or *coprime*) to another integral ideal $\mathfrak{m} \subseteq \mathcal{D}$ if $\mathfrak{a} + \mathfrak{m} = \mathcal{D}$.

Commutative Noetherian rings generally do not have unique factorization into products of powers of prime ideals; they possess a weaker form of decomposition of ideals under intersection, called *primary decomposition*. A *primary ideal* $\mathfrak{q}$ is an ideal such that, if $xy \in \mathfrak{q}$, then either $x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$ for some $n \geq 1$, and $\mathfrak{q} \neq \mathcal{D}$. Any power of a prime ideal $\mathfrak{p}^n$ is primary. The primary decomposition for a Noetherian ring is a decomposition of an ideal into an *intersection* of primary ideals. In a commutative Noetherian ring, all ideals have a primary decomposition (Lasker-Noether theorem); however, a primary decomposition is not necessarily unique.

For a one-dimensional commutative Noetherian domain $\mathcal{D}$, stronger results hold. A primary decomposition always exists and is unique. In addition, relevant to our situation, the primary decomposition given as an intersection of ideals coincides with its decomposition as a product of the same primary ideals. This case covers all orders $\mathcal{O}$ of number fields. To state the result precisely, recall that the *radical* of an ideal is

$$\mathrm{rad}(\mathfrak{m}) := \{x \in A : \, x^n \in \mathfrak{m} \text{ for some } n \geq 1\}. \tag{2.3}$$

The radical $\mathrm{rad}(\mathfrak{q})$ of a primary ideal is the unique prime ideal $\mathfrak{p}$ containing $\mathfrak{q}$. We say that such a primary ideal $\mathfrak{q}$ is *associated* to the prime ideal $\mathfrak{p}$.

Proposition 2.2 (Primary decomposition in dimension 1)**.** *Let $\mathcal{D}$ be a commutative Noetherian integral domain in which all nonzero prime ideals are maximal (i.e., $\mathcal{D}$ has Krull dimension 1). Then*

(1) *Every non-zero ideal $\mathfrak{m}$ in $\mathcal{D}$ has a unique primary decomposition*

$$\mathfrak{m} = \bigcap_i \mathfrak{q}_i, \tag{2.4}$$

in which $\mathfrak{q}_i$ are primary ideals whose radicals $\mathfrak{p}_i = \mathrm{rad}(\mathfrak{q}_i)$ are pairwise distinct.

(2) *The primary decomposition agrees with its product decomposition*

$$\mathfrak{m} = \prod_i \mathfrak{q}_i. \tag{2.5}$$

Proof. This is [4, Proposition 9.1]. The last assertion (2.5) is established in its proof. □

Proposition 2.2 (2) gives a form of unique factorization into pairwise relatively prime ideals, in which every ideal is primary.

A prime ideal $\mathfrak{p}$ of A is *regular* if all the $\mathfrak{p}$-primary ideals are powers of $\mathfrak{p}$; it is *singular* otherwise. The singular prime ideals of orders of number fields are characterized in Lemma 2.12 below. Each order $\mathcal{O}$ of K has finitely many singular prime ideals; the maximal order $\mathcal{O}_K$ is the only order having no singular prime ideals.

2.2. **Invertible integral ideals of orders of number fields.** Recall that there is associated to each integral $\mathcal{O}$-ideal $\mathfrak{a}$ of a number field a *multiplier ring*

$$\mathrm{ord}(\mathfrak{a}) := (\mathfrak{a} : \mathfrak{a}) = \{x \in K : x\mathfrak{a} \subseteq \mathfrak{a}\}. \tag{2.6}$$

Necessarily $(\mathfrak{a} : \mathfrak{a}) \subseteq \mathcal{O}_K$, and it always is an order $\mathcal{O}'$ of K having $\mathcal{O} \subseteq \mathcal{O}' \subseteq \mathcal{O}_K$. All orders $\mathcal{O}'$ between $\mathcal{O}$ and $\mathcal{O}_K$ occur this way; one may choose $\mathfrak{a} = \gamma\mathcal{O}' \subseteq \mathcal{O}$ so that $\mathfrak{a}$ is an integral $\mathcal{O}$-ideal, while $(\mathfrak{a} : \mathfrak{a}) = \mathcal{O}'$.

Definition 2.3. (Invertible integral ideal) An integral ideal $\mathfrak{a}$ of $\mathcal{O}$ is *invertible* if there exists another integral $\mathcal{O}$-ideal $\mathfrak{b}$ and a nonzero $\gamma \in \mathcal{O}$ such that the $\mathcal{O}$-ideal product $\mathfrak{a}\mathfrak{b} = \gamma\mathcal{O}$.

The invertibility property is preserved under ideal multiplication. Moreover, the converse holds: If $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ is invertible then necessarily both $\mathfrak{a}$ and $\mathfrak{b}$ are invertible. This is because, if $\mathfrak{c}\mathfrak{d} = \gamma\mathcal{O}$, then $\mathfrak{a}(\mathfrak{b}\mathfrak{d}) = \gamma\mathcal{O}$ and $\mathfrak{b}(\mathfrak{a}\mathfrak{d}) = \gamma\mathcal{O}$. We let $\mathrm{I}^*(\mathcal{O})$ denote the monoid (semigroup with identity) of invertible integral ideals under ideal multiplication.

All nonzero principal ideals $\mathfrak{a} = \alpha\mathcal{O}$ are invertible for $\mathcal{O}$; take $\mathfrak{b} = \mathcal{O}$. For orders in general, not all ideals of $\mathcal{O}$ are invertible; a necessary condition for invertibility of an ideal $\mathfrak{a}$ of $\mathcal{O}$ is that $\mathrm{ord}(\mathfrak{a}) = \mathcal{O}$. This fact follows from the property of integral $\mathcal{O}$-ideals that $\mathrm{ord}(\mathfrak{a})\mathrm{ord}(\mathfrak{b}) \subseteq \mathrm{ord}(\mathfrak{a}\mathfrak{b})$. Consequently if $\mathrm{ord}(\mathfrak{a}\mathfrak{b}) = \mathcal{O}$ then necessarily $\mathrm{ord}(\mathfrak{a}) = \mathrm{ord}(\mathfrak{b}) = \mathcal{O}$; the next example shows the converse does not hold in general.

Example 2.4. [Non-invertible ideal $\mathfrak{q}$ of $\mathcal{O}$ with $\mathrm{ord}(\mathfrak{q}) = \mathcal{O}$] (This phenomenon occurs only for number fields K with $[K : \mathbb{Q}] \geq 3$ and with a non-maximal order $\mathcal{O}$ of K.) Take $K = \mathbb{Q}(\sqrt[3]{2})$, $\mathcal{O}_K = \mathbb{Z} + \sqrt[3]{2}\mathbb{Z} + \sqrt[3]{4}\mathbb{Z}$, $\mathcal{O}' = \mathbb{Z} + 2\sqrt[3]{2}\mathbb{Z} + \sqrt[3]{4}\mathbb{Z}$, and $\mathcal{O} = \mathbb{Z} + 2\sqrt[3]{2}\mathbb{Z} + 2\sqrt[3]{4}\mathbb{Z}$. Take $\mathfrak{q} = 2\mathbb{Z} + 2\sqrt[3]{2}\mathbb{Z} + 4\sqrt[3]{4}\mathbb{Z}$. Now $\mathfrak{q}$ is of index 4 in $\mathcal{O}$ and is a primary ideal, which is contained in $\mathfrak{p} = 2\mathcal{O}_K = 2\mathbb{Z} + 2\sqrt[3]{2}\mathbb{Z} + 2\sqrt[3]{4}\mathbb{Z} \subseteq \mathcal{O}$, which is of index 2 in $\mathcal{O}$ and therefore a prime ideal of $\mathcal{O}$. Here $\mathfrak{p} = 2\mathcal{O}$ is not invertible as an $\mathcal{O}$-ideal because its multiplier ring $\mathrm{ord}(\mathfrak{p}) = (\mathfrak{p} : \mathfrak{p}) = \mathcal{O}_K$. In addition $\mathfrak{q}$ is also not invertible as an $\mathcal{O}$-ideal because $\mathfrak{q}^2 = 4\mathbb{Z} + 4\sqrt[3]{2}\mathbb{Z} + 4\sqrt[3]{4}\mathbb{Z} = \mathcal{O}_K$ has $\mathrm{ord}(\mathfrak{q}^2) = (\mathfrak{q}^2 : \mathfrak{q}^2) = \mathcal{O}_K$, so $\mathfrak{q}^2$ is not invertible for $\mathcal{O}$. But $\mathfrak{q}$ has multiplier ring $\mathrm{ord}(\mathfrak{q}) = (\mathfrak{q} : \mathfrak{q}) = \mathcal{O}$. The only orders containing $\mathcal{O}$ are $\mathcal{O}'$ and $\mathcal{O}_K$. It suffices to note $\mathfrak{q}\mathcal{O}' \neq \mathfrak{q}$, because $2 \in \mathfrak{q}$, and $\sqrt[3]{4} \in \mathcal{O}'$ have product $2\sqrt[3]{4} \notin \mathfrak{q}$.

There is a factorization theory for invertible integral ideals, based on a notion of irreducible integral ideals.

Definition 2.5 (Irreducible integral ideal)**.** An integral ideal $\mathfrak{q}$ is said to be *irreducible* for the one-dimensional Noetherian domain $\mathcal{D}$ if $\mathfrak{q} \neq \mathcal{D}$ and the factorization $\mathfrak{q} = \mathfrak{a}\mathfrak{b}$ for invertible ideals $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{D}$ implies that $\mathfrak{a} = \mathcal{D}$ or $\mathfrak{b} = \mathcal{D}$.

Irreducible invertible ideals of one-dimensional Noetherian domains $\mathcal{D}$ are necessarily primary ideals. (If they were not primary, they would have a nontrivial primary decomposition.) There may be more than one irreducible invertible ideal whose radical is a given prime ideal, as well as more than one irreducible invertible ideal associated to a given non-Archimedean valuation on K; both of these phenomena are illustrated by Example 2.7.

Example 2.6 (Primary and prime ideals in non-maximal orders; invertibility)**.** Consider $K = \mathbb{Q}(\sqrt{-13})$, which has ring of integers $\mathcal{O}_K = \mathbb{Z} + \sqrt{-13}\mathbb{Z}$ of discriminant -52. Let q be an inert prime in $\mathcal{O}_K$, for example $q = 5$. Then $\mathfrak{m} = q\mathcal{O}_K = q\mathbb{Z} + q\sqrt{-13}\mathbb{Z}$ is a maximal ideal of $\mathcal{O}_K$ of norm q^2 in O_K. It is an invertible principal ideal in the maximal order $\mathcal{O}_K$.

Consider the non-maximal order $\mathcal{O} = \mathbb{Z}+q\sqrt{-13}\mathbb{Z}$. The lattice $\mathfrak{m} = q\mathbb{Z}+q\sqrt{-13}\mathbb{Z}$ is a maximal $\mathcal{O}$-ideal; hence, it is a prime ideal of $\mathcal{O}$. It has $\mathrm{ord}(\mathfrak{m}) = \mathcal{O}_K$, so it is not an invertible integral ideal of $\mathcal{O}$. Since it is not invertible, it cannot be a principal ideal of $\mathcal{O}$.

On the other hand, the ideal $\mathfrak{q} := q\mathcal{O} = q\mathbb{Z} + q^2\sqrt{-13}\mathbb{Z}$, which has $\mathfrak{q} \subseteq \mathfrak{m}$, is a principal ideal of $\mathcal{O}$; hence, it is an invertible $\mathcal{O}$-ideal. It is is a primary ideal of $\mathcal{O}$, and its associated prime ideal in $\mathcal{O}$ is $\mathrm{rad}(\mathfrak{q}) = \mathfrak{m}$, noting that $(q\sqrt{-13})^2 \in \mathfrak{q}$.

Example 2.7 (Nonunique factorization into irreducible factors)**.** Let $K = \mathbb{Q}(\sqrt{2})$ with $\mathcal{O}_K = \mathbb{Z} + \sqrt{2}\mathbb{Z}$, and $\mathcal{O} = \mathbb{Z} + 2\sqrt{2}\mathbb{Z}$. Then $\mathcal{O}$ does not contain the fundamental unit $\varepsilon = 1 + \sqrt{2}$, but it does contain $\varepsilon^2 = 3 + 2\sqrt{2}$. Now the two ideals $\mathfrak{q}_1 = (2\varepsilon)\mathcal{O} = 4\mathbb{Z} + (2 + 2\sqrt{2})\mathbb{Z}$ and $\mathfrak{q}_2 = 2\mathcal{O} = 2\mathbb{Z} + 4\sqrt{2}\mathbb{Z}$ are principal, hence invertible. They are both primary with associated prime ideal $\mathfrak{p} = 2\mathbb{Z} + (2 + \sqrt{2})\mathbb{Z}$, which is not invertible. It follows that $\mathfrak{q}_1$ and $\mathfrak{q}_2$, which are of index 4 in $\mathcal{O}$ and index 2 in $\mathfrak{p}$, are irreducible. One has $(\mathfrak{q}_1)^2 = (\mathfrak{q}_2)^2 = 4\mathcal{O} = 4\mathbb{Z} + 8\sqrt{2}\mathbb{Z}$. Thus $4\mathcal{O}$ has two different irreducible factorizations.

2.3. **Conductors and relative conductors of orders of number fields.** The conductor ideal $\mathfrak{f}(\mathcal{O})$ of an order $\mathcal{O}$ of a number field contains information on the non-invertible ideals of an order.

Definition 2.8. (1) The *(absolute) conductor* of $\mathcal{O}$ (in $\mathcal{O}_K$) is

$$\mathfrak{f}(\mathcal{O}) := \mathfrak{f}_{\mathcal{O}_K}(\mathcal{O}) = (\mathcal{O} : \mathcal{O}_K) = \{\alpha \in \mathcal{O}_K : \alpha\mathcal{O}_K \subseteq \mathcal{O}\}. \tag{2.7}$$

It is the largest $\mathcal{O}_K$-ideal in $\mathcal{O}$.

(2) More generally, if $\mathcal{O} \subseteq \mathcal{O}'$, then the *relative conductor* of $\mathcal{O}$ in $\mathcal{O}'$ is

$$\mathfrak{f}_{\mathcal{O}'}(\mathcal{O}) = (\mathcal{O} : \mathcal{O}') = \{\alpha \in \mathcal{O}' : \alpha\mathcal{O}' \subseteq \mathcal{O}\}. \tag{2.8}$$

It is the largest $\mathcal{O}'$-ideal in $\mathcal{O}$.

The absolute conductor ideal $\mathfrak{f}(\mathcal{O}) = \mathfrak{f}_{\mathcal{O}_K}(\mathcal{O})$ is contained in all relative conductor ideals $\mathfrak{f}_{\mathcal{O}'}(\mathcal{O})$.

Example 2.9 (Conductors of quadratic orders)**.** If K is a quadratic field of discriminant Δ, then the maximal order of K is given by $\mathcal{O}_K = \mathcal{O}_\Delta = \mathbb{Z}\left[\frac{\Delta+\sqrt{\Delta}}{2}\right]$. The orders of K are of the form

$$\mathcal{O}_{f^2\Delta} = \mathbb{Z}\left[\frac{f^2\Delta + \sqrt{f^2\Delta}}{2}\right] = \mathbb{Z} + f\frac{\Delta+\sqrt{\Delta}}{2}\mathbb{Z} \tag{2.9}$$

for $f \in \mathbb{N}$. The order $\mathcal{O}_{f^2\Delta}$ has discriminant $f^2\Delta$. We have $\mathcal{O}_{f^2\Delta} \subseteq \mathcal{O}_{(f')^2\Delta}$ if and only if $f'|f$, and the relative conductor is $\mathfrak{f}_{\mathcal{O}_{(f')^2\Delta}}(\mathcal{O}_{f^2\Delta}) = \frac{f}{f'}\mathcal{O}_{(f')^2\Delta}$.

In the quadratic field case, the absolute conductor determines the order. This does not hold in general, as the following biquadratic example shows.

Example 2.10 (The absolute conductor does not determine the order)**.** Let K be the field generated by the 12-th roots of unity, and write it as a biquadratic field $K = \mathbb{Q}(\omega, i)$, where $\omega^2 + \omega + 1 = 0$ and $i^2 + 1 = 0$. The maximal order of K is $\mathcal{O}_K = \mathbb{Z}[\omega, i]$.

Consider the two orders $\mathcal{O} \subsetneq \mathcal{O}' \subsetneq \mathcal{O}_K$ given by

$$\mathcal{O} = \mathbb{Z}[5\omega, 5i, 5\omega i] = \mathbb{Z} + 5\omega\mathbb{Z} + 5i\mathbb{Z} + 5\omega i\mathbb{Z} \text{ and} \tag{2.10}$$

$$\mathcal{O}' = \mathbb{Z}[\omega, 5i] = \mathbb{Z} + \omega\mathbb{Z} + 5i\mathbb{Z} + 5\omega i\mathbb{Z}. \tag{2.11}$$

If $\alpha = w + \omega x + iy + \omega iz \in \mathfrak{f}(\mathcal{O})$, then $\alpha \in \mathcal{O} \implies 5|x, 5|y, 5|z$, and $i\alpha \in \mathcal{O} \implies 5|w$, so we see that $\mathfrak{f}(\mathcal{O}) = 5\mathcal{O}_K$. On the other hand, if $\alpha = w + \omega x + iy + \omega iz \in \mathfrak{f}(\mathcal{O}')$, then $\alpha \in \mathcal{O}' \implies 5|y, 5|z$, and $i\alpha \in \mathcal{O}' \implies 5|w, 5|x$, so we see that $\mathfrak{f}(\mathcal{O}') = 5\mathcal{O}_K$. Thus, $\mathcal{O}$ and $\mathcal{O}'$ have the same absolute conductor $5\mathcal{O}_K$.

Example 2.11 (Noninvertible relative conductor)**.** We compute the relative conductor for orders $\mathcal{O}$ and $\mathcal{O}'$ in Example 2.10. Taking $\alpha = w + \omega x + iy + \omega iz \in \mathfrak{f}_{\mathcal{O}'}(\mathcal{O})$, then $\alpha \in \mathcal{O} \implies 5|x, 5|y, 5|z$, and $\omega\alpha \in \mathcal{O} \implies 5|(w - x)$ and thus $5|w$; we see that the relative conductor $\mathfrak{f}_{\mathcal{O}'}(\mathcal{O}) = 5\mathcal{O}_K$. This relative conductor is not only an $\mathcal{O}$-ideal, it is also an $\mathcal{O}_K$-ideal. This relative conductor is not invertible as a fractional $\mathcal{O}$-ideal; it is invertible as an $\mathcal{O}_K$-ideal.

The conductor determines all singular prime ideals.

Lemma 2.12. *Let $\mathcal{O}$ be an order of a number field and $\mathfrak{p}$ a nonzero prime ideal of $\mathcal{O}$. The following are equivalent.*

1. *$\mathfrak{p}$ is a singular prime ideal of $\mathcal{O}$.*
2. *$\mathfrak{p}$ is not relatively prime to the $\mathfrak{f}(\mathcal{O})$. In that case $\mathfrak{p} + \mathfrak{f}(\mathcal{O}) = \mathfrak{p}$; equivalently, the conductor $\mathfrak{f}(\mathcal{O}) \subseteq \mathfrak{p}$.*
3. *$\mathfrak{p}$ is a non-invertible prime ideal of $\mathcal{O}$.*

Proof. We have $\mathfrak{p} \subseteq \mathfrak{p} + \mathfrak{f}(\mathcal{O}) \subseteq \mathcal{O}$. Since all nonzero prime ideals $\mathfrak{p}$ are maximal, $\mathfrak{p}$ is not relatively prime to $\mathfrak{f}(\mathcal{O})$ if and only if $\mathfrak{p} + \mathfrak{f}(\mathcal{O}) = \mathfrak{p}$.

$(1) \Leftrightarrow (2)$. The contrapositive of this assertion says: $\mathfrak{p}$ is a invertible prime ideal of $\mathcal{O}$ if and only if $\mathfrak{p} \nmid \mathfrak{f}(\mathcal{O})$, meaning $\mathfrak{f}(\mathcal{O}) \notin \mathfrak{p}$, which since $\mathfrak{p}$ is maximal means $\mathfrak{p} + \mathfrak{f}(\mathcal{O}) = \mathcal{O}$, i.e., $\mathfrak{p}$ is relatively

prime to $\mathfrak{f}(\mathcal{O})$. The contrapositive is proved as Proposition 12.10 of Chapter I of Neukirch [30, p. 79].

$(1) \Leftrightarrow (3)$. The contrapositive of the assertion $(1) \Rightarrow (2)$ says: $\mathfrak{p}$ is an invertible prime ideal of $\mathcal{O}$ if and only if $\mathfrak{p}$ is a regular prime ideal of $\mathcal{O}$. Now a prime ideal $\mathfrak{p}$ is invertible if and only if $\mathfrak{p}\mathcal{O}_{\mathfrak{p}} = \alpha_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}$ is a principal ideal, where $\mathcal{O}_{\mathfrak{p}}$ denotes the localization of $\mathcal{O}$ at the maximal ideal $\mathfrak{p}$. (See Lemma 12.4 of Chap. 1 of [30, p. 87].) Equivalently $\mathcal{O}_{\mathfrak{p}}$ is a discrete valuation ring, so, equivalently, the set of all nonzero ideals in the local ring are powers of the maximal ideal $\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$, i.e., $\mathfrak{p}$ is regular, as required. □

2.4. **Fractional ideals for integral domains.** There is a theory of fractional ideals for general integral domains.

Definition 2.13 (Fractional ideal)**.** A *fractional ideal* $\mathfrak{a}$ of an integral domain $\mathcal{D}$ is a finitely generated $\mathcal{D}$-submodule of its quotient field K.

The *ideal product* operation $\cdot$ is defined for $\mathcal{D}$-modules by

$$\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cdot \mathfrak{b} = \left\{ \sum_j \alpha_j \beta_j : \alpha_j \in \mathfrak{a}, \beta_j \in \mathfrak{b} \right\}. \tag{2.12}$$

This operation is well-defined for fractional ideals: If $\mathfrak{a}$ and $\mathfrak{b}$ are finitely generated as $\mathcal{D}$-modules, then $\mathfrak{a}\mathfrak{b}$ is also a finitely generated $\mathcal{D}$-module.

The *ideal quotient* (or *colon ideal*) operation $(\ :\ )$ is defined on fractional ideals of an integral domain $\mathcal{D}$ by

$$(\mathfrak{a} : \mathfrak{b}) := \{x \in K \mid x\mathfrak{b} \subseteq \mathfrak{a}\}. \tag{2.13}$$

The conductor ideal defined in Definition 2.8 is an example of an ideal quotient: $\mathfrak{f}_{\mathcal{O}'}(\mathcal{O}) = (\mathcal{O} : \mathcal{O}')$.

Proposition 2.14. *The set* $\mathrm{J}(\mathcal{D})$ *of all fractional ideals of an integral domain* $\mathcal{D}$ *is closed under the four operations,* $+, \cdot, \cap, (\ :\ )$ *(addition, multiplication, intersection, and ideal quotient.)*

Proof. This is Proposition 1.1.11 of [13]. □

The set $\mathrm{J}(\mathcal{D})$ is a monoid with the ideal product operation. The ideal quotients $\mathrm{ord}(\mathfrak{a}) = (\mathfrak{a} : \mathfrak{a})$ for ideals $\mathfrak{a}$ in $\mathrm{J}(\mathcal{D})$ are always orders, and they comprise the complete set of idempotent elements of the monoid $\mathrm{J}(\mathcal{D})$.

Definition 2.15 (Invertible fractional ideal)**.** A fractional ideal $\mathfrak{a}$ of an integral domain $\mathcal{D}$ is *invertible for* $\mathcal{D}$ if there is another fractional ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathcal{D}$. More generally, a fractional ideal of $\mathcal{D}$ is called *potentially invertible* if it is invertible for its associated order $\mathrm{ord}(\mathfrak{a}) = (\mathfrak{a} : \mathfrak{a})$. (This order contains $\mathcal{D}$ but may be larger.)

We let $\mathrm{J}^*(\mathcal{D})$ denote the set of all invertible fractional ideals of $\mathcal{D}$; they form a group under multiplication in which $\mathcal{D}$ is the identity element.

Proposition 2.16. *If $\mathcal{D}$ is a Noetherian integral domain, then a fractional ideal $\mathfrak{a} \in \mathrm{J}(\mathcal{D})$ is invertible for its associated order $\mathrm{ord}(\mathfrak{a})$ if and only if $\mathfrak{a}\,(\mathrm{ord}(\mathfrak{a}) : \mathfrak{a}) = \mathrm{ord}(\mathfrak{a})$. If this condition holds, then $\mathfrak{a} \in \mathrm{J}^*(\mathrm{ord}(\mathfrak{a}))$, and the ideal quotient $\mathfrak{b} := (\mathrm{ord}(\mathfrak{a}) : \mathfrak{a})$ is its inverse in this group, which has identity element $\mathrm{ord}(\mathfrak{a})$.*

Proof. This is Proposition 1.3.6 of [13]. □

Invertible fractional ideals can be characterized by local data.

Proposition 2.17. *If $\mathcal{D}$ is any integral domain, then a fractional ideal $\mathfrak{a} \in \mathrm{J}(\mathcal{D})$ is invertible for $\mathcal{D}$ if and only if each localized ideal $\mathfrak{a}_{\mathfrak{m}}$ is a principal $\mathcal{D}_{\mathfrak{m}}$-ideal for each maximal ideal $\mathfrak{m}$ of $\mathcal{D}$.*

Proof. This is Corollary 2.1.7 of [13]. □

Some basic properties of ideal quotients will be used throughout the paper.

Lemma 2.18. *Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ be fractional ideals in an integral domain $\mathcal{D}$.*

(1) $(\mathfrak{a} : \mathfrak{b}) \subseteq (\mathfrak{ac} : \mathfrak{bc})$*, with equality if $\mathfrak{c}$ is invertible.*
(2) $(\mathfrak{a} : \mathfrak{b})\,\mathfrak{c} \subseteq (\mathfrak{ac} : \mathfrak{b})$*, with equality if $\mathfrak{c}$ is invertible.*
(3) $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{bc})$.
(4) *If $\mathfrak{a} \subseteq \mathfrak{b} \subseteq \mathfrak{c}$, then $(\mathfrak{a} : \mathfrak{c}) \subseteq (\mathfrak{a} : \mathfrak{b})$ and $(\mathfrak{a} : \mathfrak{c}) \subseteq (\mathfrak{b} : \mathfrak{c})$.*

Now, let $\mathfrak{m}$ be an integral ideal of an order $\mathcal{O}$ in a number field K, and let $\mathcal{O}' \supseteq \mathcal{O}$ be a larger order of K. Then,

(5) $\mathfrak{f}_{\mathcal{O}'}(\mathcal{O})\mathfrak{m} \subseteq (\mathfrak{m} : \mathcal{O}') \subseteq \mathfrak{f}_{\mathcal{O}'}(\mathcal{O}) \cap \mathfrak{m}\mathcal{O}'$.

Proof. Properties (1), (2), (3) and (4) follow directly from the definitions of the quotient and product ideals. To prove the left-hand inclusion of property (5), observe using (2) that

$$\mathfrak{f}_{\mathcal{O}'}(\mathcal{O})\mathfrak{m} = (\mathcal{O} : \mathcal{O}')\,\mathfrak{m} \subseteq (\mathcal{O}\mathfrak{m} : \mathcal{O}') = (\mathfrak{m} : \mathcal{O}')\,. \tag{2.14}$$

To prove the right-hand inclusion, use (1) and (4):

$$(\mathfrak{m} : \mathcal{O}') \subseteq (\mathfrak{m}\mathcal{O}' : \mathcal{O}'\mathcal{O}') = (\mathfrak{m}\mathcal{O}' : \mathcal{O}') = \mathfrak{m}\mathcal{O}', \tag{2.15}$$

and $(\mathfrak{m} : \mathcal{O}') \subseteq (\mathcal{O} : \mathcal{O}') = \mathfrak{f}_{\mathcal{O}'}(\mathcal{O})$. □

2.5. **Fractional ideals for orders of number fields.** We specialize to the case of orders $\mathcal{O}$ of number fields. For the maximal order $\mathcal{O}_K$ (more generally for Dedekind domains), $\mathrm{J}^*(\mathcal{O}_K)$ it is a free abelian group. For non-maximal orders $\mathcal{O}$, $\mathrm{J}^*(\mathcal{O})$ may contain a (finite) nontrivial torsion subgroup.

Definition 2.19 (Relative primality of fractional ideals)**.** A fractional ideal $\mathfrak{d}$ of $\mathcal{O}$ is *coprime* (or *relatively prime*) to an integral ideal $\mathfrak{a} \subseteq \mathcal{O}$ if it may be written as a quotient $\mathfrak{d} = (\mathfrak{b} : \mathfrak{c})$, where $\mathfrak{b}$ is an integral ideal of $\mathcal{O}$ coprime to $\mathfrak{a}$, and $\mathfrak{c}$ is an invertible integral ideal of $\mathcal{O}$ coprime to $\mathfrak{a}$.

Each nonzero fractional ideal $\mathfrak{d}$ of an order $\mathcal{O}$ is coprime to all but a finite set of nonzero prime ideals (i.e., maximal ideals) of $\mathcal{O}$.

The next two lemmas show that the definitions of invertibility and coprimality for fractional ideals are consistent with the earlier definitions for integral ideals.

Lemma 2.20. *Let $\mathcal{O}$ be an order in a number field, and let $\mathfrak{a}$ and $\mathfrak{b}$ be integral $\mathcal{O}$-ideals. If $\mathfrak{b}$ is invertible, then $(\mathfrak{a} : \mathfrak{b}) = \mathfrak{a}\mathfrak{b}^{-1}$.*

Proof. We show that $(\mathfrak{a} : \mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b}^{-1}$. Since $\mathfrak{b}$ is invertible, this inclusion is equivalent to showing that $(\mathfrak{a} : \mathfrak{b})\,\mathfrak{b} \subseteq \mathfrak{a}$. Let $c \in (\mathfrak{a} : \mathfrak{b})$ and $b \in \mathfrak{b}$. Thus $c\mathfrak{b} \subseteq \mathfrak{a}$ by the definition of $(\mathfrak{a} : \mathfrak{b})$, so in particular, $cb \in \mathfrak{a}$ as required.

We show the reverse inclusion $(\mathfrak{a} : \mathfrak{b}) \supseteq \mathfrak{a}\mathfrak{b}^{-1}$. Let $a \in \mathfrak{a}$ and $d \in \mathfrak{b}^{-1}$. Then, $d\mathfrak{b} \subseteq \mathcal{O}$, so $ad\mathfrak{b} \subseteq a\mathcal{O} \subseteq \mathfrak{a}$. By definition of the quotient ideal, $ad \in (\mathfrak{a} : \mathfrak{b})$, as required. □

Lemma 2.21. *Let $\mathcal{O}$ be an order in a number field K.*

(1) *Any fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ with $\mathfrak{a} \subseteq \mathcal{O}$ is an integral ideal, and conversely.*

(2) *Any invertible fractional ideal of $\mathcal{O}$ with $\mathfrak{a} \subseteq \mathcal{O}$ is an invertible integral ideal, and conversely.*

(3) *If two integral ideals $\mathfrak{a}, \mathfrak{b}$ are coprime as integral ideals, then $\mathfrak{b}$ as a fractional ideal is coprime to $\mathfrak{a}$, and conversely.*

Proof. (1) Immediate, by comparing the definitions of integral ideals and fractional ideals.

(2) An invertible integral ideal $\mathfrak{a}$ is an invertible fractional ideal, because $\mathfrak{a}\mathfrak{b} = \gamma\mathcal{O}$ implies $\mathfrak{a}(\gamma^{-1}\mathfrak{b}) = \mathcal{O}$.

Conversely, if $\mathfrak{a}$ is an integral ideal that is invertible as a fractional ideal, then $\mathfrak{a}\mathfrak{b} = \mathcal{O}$ for some fractional ideal $\mathfrak{b}$. Since $\mathfrak{b}$ is a sublattice of $K = \mathbb{Q}\mathcal{O}$, there exists a nonzero integer n such that $n\mathfrak{b}$ is an integral ideal, and $\mathfrak{a}(n\mathfrak{b}) = n\mathcal{O}$.

(3) Given integral ideals satisfying $\mathfrak{a} + \mathfrak{b} = \mathcal{O}$, view $\mathfrak{b}$ as a fractional ideal, and use the decomposition $\mathfrak{b} = (\mathfrak{b} : \mathcal{O})$, noting that $\mathcal{O}$ is invertible as a fractional ideal. Conversely, given an integral ideal $\mathfrak{b} = (\mathfrak{b}_1 : \mathfrak{b}_2)$ with $\mathfrak{b}_1, \mathfrak{b}_2$ integral and $\mathfrak{b}_2$ invertible, satisfying $\mathfrak{a} + \mathfrak{b}_1 = \mathcal{O}$ and $\mathfrak{a} + \mathfrak{b}_2 = \mathcal{O}$, use Lemma 2.20 to write $\mathfrak{b} = \mathfrak{b}_1\mathfrak{b}_2^{-1}$. Thus, $\mathfrak{b}\mathfrak{b}_2 = \mathfrak{b}_1$, so $\mathfrak{b} \supseteq \mathfrak{b}_1$. There exists $a \in \mathfrak{a}$ and $b_1 \in \mathfrak{b}_1$ such that $a + b_1 = 1$, and $b_1 \in \mathfrak{b}$, so $\mathfrak{a} + \mathfrak{b} = \mathcal{O}$. □

The group of invertible fractional ideals of an order $\mathcal{O}$ coprime to a given integral ideal $\mathfrak{m}$ is denoted $\mathrm{J}^*_{\mathfrak{m}}(\mathcal{O})$. The submonoid of (integral) ideals of $\mathcal{O}$ coprime to $\mathfrak{m}$ is denoted by $\mathrm{I}_{\mathfrak{m}}(\mathcal{O})$.

Although not all fractional ideals are potentially invertible, every sufficiently large power of every nonzero fractional ideal $\mathfrak{a}$ is potentially invertible, with a uniform bound on the power.

Proposition 2.22. *Let $\mathcal{O}$ be an order of an algebraic number field K. Then for any nonzero fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ there is a positive power $N_{\mathfrak{a}} \geq 1$ such that the ideal $\mathfrak{a}^N$ is an potentially invertible ideal if and only if $N \geq N_{\mathfrak{a}}$. Furthermore $N_{\mathfrak{a}}$ is bounded uniformly by $N_{\mathfrak{a}} \leq n-1$, where $n = [K : \mathbb{Q}]$.*

Proof. The proposition is a special case of [13, Theorem C, Cor. 2.2.17], taking $\mathcal{O}_E = \mathbb{Z}$, $E = \mathbb{Q}$, and $\mathcal{O}$ an order of $F = K$. (Dade, Taussky, and Zassenhaus define invertibility of a fractional ideal $\mathfrak{a}$ to mean invertibility with respect to the order $\mathrm{ord}(\mathfrak{a}) = (\mathfrak{a} : \mathfrak{a})$; it is possible that $\mathrm{ord}(\mathfrak{a})$ is a strict subset of $\mathrm{ord}(\mathfrak{a}^k)$.) □

3. Change of orders in a number field: extension and contraction of ideals

We consider the effect on integral ideals and fractional ideals of a change of orders between two orders $\mathcal{O} \subseteq \mathcal{O}'$ having the same quotient field K.

Definition 3.1. The inclusion map $\mathcal{O} \hookrightarrow \mathcal{O}'$ defines extension and contraction maps on integral ideals.

(1) If $\mathfrak{a}$ is an integral ideal of $\mathcal{O}$, then the *extension* $\mathrm{ext}(\mathfrak{a}) := \mathfrak{a}\mathcal{O}'$ is the integral $\mathcal{O}'$-ideal generated by the elements of $\mathfrak{a}$.
(2) If $\mathfrak{a}'$ is an integral ideal of $\mathcal{O}'$, then the *contraction* $\mathrm{con}(\mathfrak{a}') := \mathfrak{a}' \cap \mathcal{O}$ is an integral $\mathcal{O}$-ideal.

This is a special case of extension and contraction of ideals under ring homomorphism [4, p. 9]. In Section 3.1 we study the effect of ext and con on general integral ideals. In Section 3.2 we show these maps are bijective monoid homomorphisms when restricted to submonoids of integral ideals coprime to the relative conductor ideal $f_{\mathcal{O}'}(\mathcal{O})$ of $\mathcal{O}$ in $\mathcal{O}'$. In Section 3.3 we extend ext and con to bijective homomorphisms on groups of invertible fractional ideals coprime to $f_{\mathcal{O}'}(\mathcal{O})$.

3.1. Extension and contraction of general integral ideals.

Given the inclusion of two orders $\iota : \mathcal{O} \to \mathcal{O}'$ of a fixed algebraic number field K, we have well-defined functions $\mathrm{ext} : \mathrm{I}(\mathcal{O}) \to \mathrm{I}(\mathcal{O}')$ and $\mathrm{con} : \mathrm{I}(\mathcal{O}') \to \mathrm{I}(\mathcal{O}')$.

The extension map $\mathrm{ext} : \mathrm{I}(\mathcal{O}) \to \mathrm{I}(\mathcal{O}')$ is a monoid homomorphism for ideal multiplication. It is easy to check that this map preserves the property of invertibility of ideals, and it preserves the property of being a principal ideal. The map ext may not be surjective; see Example 3.4.

The contraction map $\mathrm{con} : \mathrm{I}(\mathcal{O}') \to \mathrm{I}(\mathcal{O})$ is a well-defined function but in general is not a monoid homomorphism. One always has $\mathrm{con}(\mathfrak{a}')\,\mathrm{con}(\mathfrak{b}') \subseteq \mathrm{con}(\mathfrak{a}'\mathfrak{b}')$, but strict inclusion may sometimes hold; see Example 3.5. Contraction need not preserve invertibility of ideals nor the property of being a principal ideal; see Example 3.6. We will show in Section 3.2 that con is a monoid homomorphism (and thus preserves invertibility) when restricted to $\mathrm{I}_{\mathfrak{f}}(\mathcal{O}')$, where $\mathfrak{f} = \mathfrak{f}_{\mathcal{O}'}(\mathcal{O})$.

For later use we study the effect of ext and con on maximal ideals.

Lemma 3.2. *Let $\mathcal{O} \subseteq \mathcal{O}'$ be orders of a number field K, and let* con *and* ext *be the contraction and extension maps on integral ideals.*

(1) *If $\mathfrak{p}$ is a maximal ideal of $\mathcal{O}$, then* $\mathrm{con}(\mathrm{ext}(\mathfrak{p})) = \mathfrak{p}$.
(2) *If $\mathfrak{p}'$ is a maximal ideal of $\mathcal{O}'$, then $\mathfrak{p} = \mathrm{con}(\mathfrak{p}')$ is a maximal ideal of $\mathcal{O}$.*
(3) *If $\mathfrak{p}$ is a maximal ideal of $\mathcal{O}$, then $\mathfrak{p} = \mathrm{con}(\mathfrak{p}')$ for some maximal ideal $\mathfrak{p}'$ of $\mathcal{O}'$.*
(4) *If $\mathfrak{p}'$ is a maximal ideal of $\mathcal{O}'$, then $\mathrm{ext}(\mathrm{con}(\mathfrak{p}')) \subseteq \mathfrak{p}'$, and strict inequality may occur.*

To prove Lemma 3.2, we will need a standard result in commutative algebra.

Lemma 3.3. *Let $A \subseteq B$ and C be commutative rings with unity such that C is the integral closure of A in B. Let $\mathfrak{a}$ be an ideal of A, and let $\mathrm{ext}(\mathfrak{a})$ the extension of $\mathfrak{a}$ to C. Let $\overline{\mathfrak{a}}$ be the integral closure of $\mathfrak{a}$ in B, that is,*

$$\overline{\mathfrak{a}} = \{\alpha \in C : f(\alpha) = 0 \textit{ for a monic polynomial } f(x) \textit{ with all coefficients in } \mathfrak{a}\}. \tag{3.1}$$

Then, $\overline{\mathfrak{a}} = \mathrm{rad}(\mathrm{ext}(\mathfrak{a}))$, so in particular $\overline{\mathfrak{a}}$ is a B-ideal.

Proof. This is Lemma 5.14 in Atiyah-MacDonald [4]. □

Proof of Lemma 3.2. (1) The inclusion $\mathfrak{a} \subseteq \mathrm{con}(\mathrm{ext}(\mathfrak{a}))$ holds for all $\mathfrak{a} \in \mathrm{I}(\mathcal{O})$ [4, Prop. I.17]. Since $\mathfrak{p}$ is maximal, either $\mathrm{con}(\mathrm{ext}(\mathfrak{p})) = \mathcal{O}$ or $\mathrm{con}(\mathrm{ext}(\mathfrak{p})) = \mathfrak{p}$. Suppose for a contradiction that $\mathrm{con}(\mathrm{ext}(\mathfrak{p})) = \mathcal{O}$. Then, $\mathrm{ext}(\mathfrak{p})$ contains $\mathcal{O}$, so it contains $\mathcal{O}'\mathcal{O} = \mathcal{O}'$, so $\mathrm{ext}(\mathfrak{p}) = \mathcal{O}'$. It follows that the extension to the maximal order $\mathrm{ext}_{\mathcal{O}_K}(\mathfrak{p}) = \mathcal{O}_K$. But $\mathcal{O}_K$ is the integral closure of $\mathcal{O}$ in K, so by Lemma 3.3, $\overline{\mathfrak{p}} = \mathrm{rad}(\mathcal{O}_K) = \mathcal{O}_K$. Thus, $1 \in \overline{\mathfrak{p}}$, so $f(1) = 0$ for some monic polynomial $f(x) = x^n + \mu_{n-1}x^{n-1} + \cdots + \mu_0$ with $\mu_j \in \mathfrak{p}$. So $1 = -(\mu_{n-1} + \cdots + \mu_0) \in \mathfrak{p}$, which means $\mathfrak{p} = \mathcal{O}$, contradicting the hypothesis that $\mathfrak{p}$ is a maximal ideal of $\mathcal{O}$. It follows that $\mathrm{con}(\mathrm{ext}(\mathfrak{p})) = \mathfrak{p}$.

(2) Consider any $a \in \mathcal{O}$ such that $a \notin \mathrm{con}(\mathfrak{p}')$. Then, $\mathfrak{p}' + a\mathcal{O}'$ is an ideal of $\mathcal{O}'$ strictly containing $\mathfrak{p}'$, so $\mathfrak{p}' + a\mathcal{O}' = \mathcal{O}'$. Thus, a is invertible in $\mathcal{O}'/\mathfrak{p}'$, and $\mathcal{O}'/\mathfrak{p}'$ is finite (indeed, a finite field), so there is some $n \in \mathbb{N}$ such that $a^n \equiv 1 \pmod{\mathfrak{p}'}$. That is, $a^n = 1 + p'$ for some $p' \in \mathfrak{p}'$. However, $p' = a^n - 1 \in \mathcal{O}$, so in fact $a^n \equiv 1 \pmod{\mathrm{con}(\mathfrak{p}')}$. Thus, $\mathrm{con}(\mathfrak{p}') + a\mathcal{O} = \mathcal{O}$. Since this holds for any $a \in \mathcal{O} \setminus \mathrm{con}(\mathfrak{p}')$, we have shown that $\mathrm{con}(\mathfrak{p}')$ is a maximal ideal.

(3) By (1) we have $\mathrm{con}(\mathrm{ext}(\mathfrak{p})) = \mathfrak{p}$. Let $\mathfrak{p}'$ is any maximal ideal containing $\mathrm{ext}(\mathfrak{p})$. By maximality of $\mathfrak{p}$, either $\mathrm{con}(\mathfrak{p}') = \mathfrak{p}$ or $\mathrm{con}(\mathfrak{p}') = \mathcal{O}$. The latter case implies $1 \in \mathfrak{p}'$, a contradiction.

(4) The inclusion $\mathrm{ext}(\mathrm{con}(\mathfrak{a})) \subseteq \mathfrak{a}$ holds for general ideals in $\mathrm{I}(\mathcal{O}')$ [4, Prop. I.17]. An example of strict inclusion is given in Example 3.4 below. □

Example 3.4. [For a maximal $\mathcal{O}$-ideal $\mathfrak{p}$, $\mathrm{ext}(\mathfrak{p})$ need not be a maximal $\mathcal{O}'$-ideal.] Consider the orders $\mathcal{O} = \mathbb{Z} + 5^2\sqrt{2}\mathbb{Z}$ and $\mathcal{O}' = \mathbb{Z} + 5\sqrt{2}\mathbb{Z}$ in $K = \mathbb{Q}(\sqrt{2})$, with $\mathcal{O} \subset \mathcal{O}'$. Both these orders are strictly smaller than the maximal order $\mathcal{O}_K = \mathbb{Z} + \sqrt{2}\mathbb{Z}$. Consider $\mathrm{ext} : \mathrm{I}(\mathcal{O}) \to \mathrm{I}(\mathcal{O}')$ and $\mathrm{con} : \mathrm{I}(\mathcal{O}') \to \mathrm{I}(\mathcal{O})$. Set $\mathfrak{p} = 5\mathbb{Z} + 5^2\sqrt{2}\mathbb{Z}$. By inspection $\mathfrak{p}$ is an integral ideal of $\mathcal{O}$, and since it is of prime index 5 in $\mathcal{O}$, it is a maximal ideal of $\mathcal{O}$. By Lemma 3.3(3) there is a maximal ideal $\mathfrak{p}'$ of $\mathcal{O}'$ such that $\mathrm{con}(\mathfrak{p}') = \mathfrak{p}$. We may in fact choose $\mathfrak{p}' = 5\mathbb{Z} + 5\sqrt{2}\mathbb{Z}$.

On the other hand, $\mathfrak{p} = 5\mathcal{O}'$ is by inspection a principal $\mathcal{O}'$-ideal. It follows that $\mathrm{ext}(\mathfrak{p}) = \mathfrak{p}$. Now $\mathfrak{p} \subsetneq \mathfrak{p}' \subsetneq \mathcal{O}'$, so $\mathfrak{p} = \mathrm{ext}(\mathrm{con}(\mathfrak{p}'))$ is not maximal as an $\mathcal{O}'$-ideal.

The maximal ideal $\mathfrak{p}'$ of $\mathcal{O}'$ is not in range of the map ext: Suppose it were, and let $\mathfrak{p}' = \mathrm{ext}(\mathfrak{a})$ for some $\mathfrak{a} \in \mathrm{I}(\mathcal{O})$. We would have $\mathrm{ext}(\mathrm{con}(\mathrm{ext}(\mathfrak{a}))) = \mathrm{ext}(\mathfrak{a})$ by [4, Prop. I.17]. But

$$\mathrm{ext}(\mathrm{con}(\mathrm{ext}(\mathfrak{a}))) = \mathrm{ext}(\mathrm{con}(\mathfrak{p}')) = \mathrm{ext}(\mathfrak{p}) = \mathfrak{p}. \tag{3.2}$$

so we would get $\mathfrak{p} = \mathrm{ext}(\mathfrak{a}) = \mathfrak{p}'$, which is false.

Example 3.5. [The contraction map is not a monoid homomorphism on $\mathrm{I}(\mathcal{O}')$] As in Example 3.4, consider the orders $\mathcal{O} = \mathbb{Z} + 5^2\sqrt{2}\mathbb{Z}$ and $\mathcal{O}' = \mathbb{Z} + 5\sqrt{2}\mathbb{Z}$ in $K = \mathbb{Q}(\sqrt{2})$, with $\mathcal{O} \subset \mathcal{O}'$. We consider $\mathrm{con} : \mathrm{I}(\mathcal{O}') \to \mathrm{I}(\mathcal{O})$. Also, as in Example 3.4, let $\mathfrak{p} = 5\mathbb{Z} + 5^2\sqrt{2}\mathbb{Z}$ and $\mathfrak{p}' = 5\mathbb{Z} + 5\sqrt{2}\mathbb{Z}$; we have $\mathrm{con}(\mathfrak{p}') = \mathfrak{p}$.

Take $\mathfrak{a}' = \mathfrak{b}' = \mathfrak{p}'$. As an $\mathcal{O}'$-ideal,

$$\mathfrak{a}'\mathfrak{b}' = (\mathfrak{p}')^2 = \left(5\mathbb{Z} + 5\sqrt{2}\mathbb{Z}\right)^2 = 5^2\mathbb{Z} + 5^2\sqrt{2}\mathbb{Z}. \tag{3.3}$$

Now $\mathfrak{a}'\mathfrak{b}' = (\mathfrak{p}')^2$ is also an $\mathcal{O}$-ideal, so that

$$\mathrm{con}(\mathfrak{a}'\mathfrak{b}') = \mathrm{con}((\mathfrak{p}')^2) = (\mathfrak{p}')^2 = 5^2\mathbb{Z} + 5^2\sqrt{2}\mathbb{Z}. \tag{3.4}$$

Since $\mathrm{con}(\mathfrak{p}') = \mathfrak{p} = (5\mathbb{Z} + 5^2\sqrt{2}\mathbb{Z})$, we have

$$\mathrm{con}(\mathfrak{a}')\,\mathrm{con}(\mathfrak{b}') = (\mathrm{con}(\mathfrak{p}))^2 = (\mathfrak{p}^2) = 5^2\mathbb{Z} + 5^3\sqrt{2}\mathbb{Z}. \tag{3.5}$$

We have shown $\mathrm{con}(\mathfrak{a}')\,\mathrm{con}(\mathfrak{b}') \subsetneq \mathrm{con}(\mathfrak{a}'\mathfrak{b}')$.

Example 3.6. [Contraction and extension of ideals in non-maximal orders] Consider $K = \mathbb{Q}(\sqrt{-13})$ with maximal order $\mathcal{O}_K = \mathbb{Z} + \sqrt{-13}\mathbb{Z}$, and consider a nonmaximal order $\mathcal{O} = \mathbb{Z} + q\sqrt{-13}\mathbb{Z}$ where q is an odd inert prime (for example, $q = 5$). Recall from Example 2.6 that $\mathfrak{m} = q\mathcal{O}_K = q\mathbb{Z} + q\sqrt{-13}\mathbb{Z}$ is a maximal $\mathcal{O}_K$-ideal of norm q^2, and $\mathfrak{m}$ is principal in $\mathcal{O}_K$, hence invertible.

Now $\mathfrak{m}$ is also an $\mathcal{O}$-ideal and is a maximal ideal for $\mathcal{O}$. It is the conductor ideal for $\mathcal{O}$, so it is non-invertible as an $\mathcal{O}$-ideal. It is immediate that $\mathrm{ext}(\mathfrak{m}) = \mathfrak{m}$. For the contraction map $\mathcal{O}_K \to \mathcal{O}$ sending $\mathfrak{a}' \mapsto \mathfrak{a}' \cap \mathcal{O}$, we have

$$\mathrm{con}(\mathfrak{m}) = \mathfrak{m} \cap \mathcal{O} = \mathfrak{m}. \tag{3.6}$$

This example verifies $\mathrm{con}(\mathrm{ext}(\mathfrak{m})) = \mathfrak{m}$, and also $\mathrm{ext}(\mathrm{con}(\mathfrak{m})) = \mathfrak{m}$, preserving the maximal ideal property. However, the contracted ideal $\mathfrak{m}$, viewed as an $\mathcal{O}$-ideal, is not an invertible fractional ideal in $\mathcal{O}$, hence also not a principal ideal in $\mathcal{O}$

Furthermore, consider $\mathfrak{q} := q\mathcal{O} = q\mathbb{Z} + q^2\sqrt{-13}\mathbb{Z}$. It is a principal $\mathcal{O}$-ideal, so it is an invertible $\mathcal{O}$-ideal; hence, it cannot be an $\mathcal{O}_K$-ideal. We have $\mathfrak{q} \subsetneq \mathfrak{m}$. It is easy to see that $\mathrm{ext}(\mathfrak{q}) = \mathfrak{m}$. So we now have $\mathrm{con}(\mathrm{ext}(\mathfrak{q})) = \mathrm{con}(\mathfrak{m}) = \mathfrak{m}$ and $\mathfrak{q} \subsetneq \mathrm{con}(\mathrm{ext}(\mathfrak{q})) = \mathfrak{m}$. (Thus $\mathrm{con}(\mathrm{ext}(\mathfrak{a}))$ can be a maximal ideal while $\mathfrak{a}$ is not maximal.)

3.2. **Extension and contraction of integral ideals relatively prime to the relative conductor.** Extension and contraction operations behave well when restricted to integral ideals relatively prime to the relative conductor ideal.

Lemma 3.7. *On the set of integral ideals $\mathrm{I}_{\mathfrak{f}}(\mathcal{O})$ coprime to the (relative) conductor $\mathfrak{f} = \mathfrak{f}_{\mathcal{O}'}(\mathcal{O}) \in \mathrm{I}(\mathcal{O}) \cap \mathrm{I}(\mathcal{O}')$, contraction $\mathrm{con} : \mathrm{I}_{\mathfrak{f}}(\mathcal{O}') \to \mathrm{I}_{\mathfrak{f}}(\mathcal{O})$ defines an isomorphism of monoids, with inverse the extension map $\mathrm{ext} : \mathrm{I}_{\mathfrak{f}}(\mathcal{O}) \to \mathrm{I}_{\mathfrak{f}}(\mathcal{O}')$.*

Proof. We first show that con and ext are bijections inverse to each other. For general ring maps, it is easily seen that $\mathrm{ext}(\mathrm{con}(\mathfrak{a}')) \subseteq \mathfrak{a}'$ and $\mathfrak{a} \subseteq \mathrm{con}(\mathrm{ext}(\mathfrak{a}))$ [4, Prop. I.17]. The reverse inclusions

are not true in general, even in our case of the inclusion map of a suborder in an order. We must use coprimality to the conductor.

For the first, consider $\mathfrak{a}' \in \mathrm{I}_{\mathfrak{f}}(\mathcal{O}')$, and set $\mathfrak{a} = \mathrm{con}(\mathfrak{a}') = \mathfrak{a}' \cap \mathcal{O}$. We will show $\mathrm{ext}(\mathrm{con}(\mathfrak{a}')) = \mathfrak{a}'$. By comprimality of $\mathfrak{a}'$ to the relative conductor $\mathfrak{f} = \mathfrak{f}_{\mathcal{O}'}(\mathcal{O})$ we have

$$1 = a' + c' \tag{3.7}$$

for some $a' \in \mathfrak{a}'$ and $c \in \mathfrak{f} \subseteq \mathcal{O}$. Then $a' = 1 - c \in \mathcal{O}$, so $a' \in \mathfrak{a} = \mathrm{con}(\mathfrak{a}')$. Then eq. (3.7) certifies that $\mathfrak{a}$ is coprime to $\mathfrak{f}$ in the order $\mathcal{O}$. Also $a' \in \mathrm{ext}(\mathrm{con}(\mathfrak{a}'))$, so $\mathrm{ext}(\mathrm{con}(\mathfrak{a}'))$ is coprime to $\mathfrak{f}$. We must show $\mathfrak{a}' \subseteq \mathrm{ext}(\mathrm{con}(\mathfrak{a}'))$. We have $\mathfrak{a}'\mathfrak{f} \subseteq \mathrm{con}(\mathfrak{a})$, because $\mathfrak{a}'\mathfrak{f} \subseteq \mathcal{O}'\mathfrak{f} \subseteq \mathcal{O}$ and $\mathfrak{a}'\mathfrak{f} \subseteq \mathfrak{a}'\mathcal{O}' = \mathfrak{a}'$. Now given $b' \in \mathfrak{a}'$ we have from eq. (3.7) that

$$b' = b'a + b'c'. \tag{3.8}$$

Now $ab' \in \mathrm{ext}(\mathrm{con}(\mathfrak{a}))$ since $a \in \mathrm{con}(\mathfrak{a}), b' \in \mathcal{O}$, while $b'c' \in \mathfrak{a}'\mathfrak{f} \subseteq \mathrm{con}(\mathfrak{a}) \subseteq \mathrm{ext}(\mathrm{con}(\mathfrak{a}))$, hence $b' \in \mathrm{ext}(\mathrm{con}(\mathfrak{a}'))$; thus $\mathfrak{a}' \subseteq \mathrm{ext}(\mathrm{con}(\mathfrak{a}'))$, so we conclude $\mathrm{ext}(\mathrm{con}(\mathfrak{a}')) = \mathfrak{a}'$.

For the second, consider $\mathfrak{a} \in \mathrm{I}_{\mathfrak{f}}(\mathcal{O})$, and set $\mathfrak{a}' = \mathrm{ext}(\mathfrak{a})$. We will show $\mathrm{con}(\mathrm{ext}(\mathfrak{a})) = \mathfrak{a}$. By the coprimality assumption, there exist $a \in \mathfrak{a}$ and $f \in \mathfrak{f} = \mathfrak{f}_{\mathcal{O}'}(\mathcal{O})$ with $1 = a + f$. Since $a \in \mathfrak{a}' = \mathrm{ext}(\mathfrak{a})$ the ideals $\mathfrak{a}'$ and $\mathfrak{f}$ are coprime in $\mathcal{O}'$, and in addition $a \in \mathrm{con}(\mathrm{ext}(\mathfrak{a}))$. We must show $\mathrm{con}(\mathrm{ext}(\mathfrak{a})) \subseteq \mathfrak{a}$. Suppose $b \in \mathrm{con}(\mathrm{ext}(\mathfrak{a})) \subseteq \mathcal{O}$; then the coprimality equation implies $b = ba + bf$. We show $b \in \mathfrak{a}$ by showing both summands of the right hand side are in $\mathfrak{a}$. Now $b \in \mathcal{O}$, so $ba \in \mathcal{O}\mathfrak{a} = \mathfrak{a}$. Now

$$bf \in \mathrm{ext}(\mathfrak{a})\mathfrak{f} = (\mathfrak{a}\mathcal{O}')\mathfrak{f} = \mathfrak{a}(\mathcal{O}'\mathfrak{f}) = \mathfrak{a}\mathfrak{f} \subseteq \mathfrak{a}\mathcal{O} = \mathfrak{a}. \tag{3.9}$$

Thus $\mathrm{con}(\mathrm{ext}(\mathfrak{a})) \subseteq \mathfrak{a}$, whence $\mathrm{con}(\mathrm{ext}(\mathfrak{a})) = \mathfrak{a}$.

Finally, for two ideals $\mathfrak{a}, \mathfrak{b} \in \mathrm{I}_{\mathfrak{f}}(\mathcal{O})$, it follows from the definition of the extension map that $\mathrm{ext}(\mathfrak{a}\mathfrak{b}) = \mathrm{ext}(\mathfrak{a})\,\mathrm{ext}(\mathfrak{b})$. Because con defines an inverse to ext, it follows that con is also a homomorphism from $\mathrm{I}_{\mathfrak{f}}(\mathcal{O}')$ onto $\mathrm{I}_{\mathfrak{f}}(\mathcal{O})$. □

3.3. **Extension and contraction of fractional ideals relatively prime to the relative conductor.** The extension and contraction maps between orders $\mathcal{O} \subseteq \mathcal{O}'$ of a number field K consistently extend from integral ideals to fractional ideals, provided that one restricts to fractional ideals coprime to the relative conductor $\mathfrak{f}_{\mathcal{O}'}(\mathcal{O})$.

Proposition 3.8. *Consider two orders $\mathcal{O} \subseteq \mathcal{O}'$ of the number field K. Let $\mathfrak{f} = \mathfrak{f}_{\mathcal{O}'}(\mathcal{O})$ denote the relative conductor. Let $\mathfrak{m}'$ be an integral ideal of $\mathcal{O}'$ having $\mathfrak{m}' \subseteq \mathfrak{f}$. Then the contraction and extension maps extend uniquely to isomorphisms between groups of fractional ideals coprime to $\mathfrak{m}'$. That is, the maps*

$$\mathrm{con} : \mathrm{J}_{\mathfrak{m}'}(\mathcal{O}') \to \mathrm{J}_{\mathfrak{m}'}(\mathcal{O}) \text{ and} \tag{3.10}$$

$$\mathrm{ext} : \mathrm{J}_{\mathfrak{m}'}(\mathcal{O}) \to \mathrm{J}_{\mathfrak{m}'}(\mathcal{O}') \tag{3.11}$$

are well-defined and are inverses of each other.

Remark 3.9. The extension map on fractional ideals coprime to $\mathfrak{f}$ is $\mathrm{ext}(\mathfrak{a}) = \mathfrak{a}\mathcal{O}'$, as in the case for integral ideals in Definition 3.1(1). However, the contraction map on fractional ideals coprime to $\mathfrak{f}$ requires a new definition different from Definition 3.1(2) for integral ideals. That is, the contraction map on fractional ideals does not always have $\mathrm{con}(\mathfrak{a}') = \mathfrak{a}' \cap \mathcal{O}$, although the inclusion $\mathfrak{a}' \cap \mathcal{O} \subseteq \mathrm{con}(\mathfrak{a}')$ holds. For example, let $\mathfrak{b}'$ be any proper integral $\mathcal{O}'$-ideal relatively prime to $\mathfrak{f}_{\mathcal{O}'}(\mathcal{O})$, and set $\mathfrak{a}' = (\mathfrak{b}')^{-1}$. Then $\mathcal{O}' \subsetneq \mathfrak{a}'$, so $\mathfrak{a}' \cap \mathcal{O} = \mathcal{O}$. However, by Proposition 3.8, we will have $\mathrm{con}(\mathfrak{a}') = \mathrm{con}(\mathfrak{b}')^{-1} = (\mathfrak{b} \cap \mathcal{O})^{-1} = \mathfrak{b}^{-1} = \mathfrak{a}'$. Since $\mathfrak{b}'$ is a proper ideal, $\mathrm{con}(\mathfrak{a}') \neq \mathfrak{a}' \cap \mathcal{O}$.

Proof of Proposition 3.8. Note that $\mathfrak{m}'$ is both an integral $\mathcal{O}$-ideal and an integral $\mathcal{O}'$-ideal, the latter by assumption, and the former because $\mathcal{O} \subseteq \mathcal{O}'$ (so $\mathfrak{m}'$ is a fractional $\mathcal{O}$-ideal) and $\mathfrak{m}' \subseteq \mathfrak{f} \subseteq \mathcal{O}$ (so in fact $\mathfrak{m}'$ is integral as an $\mathcal{O}$-ideal).

We first claim that the maps $\mathrm{con} : \mathrm{I}_{\mathfrak{m}'}(\mathcal{O}') \to \mathrm{I}_{\mathfrak{m}'}(\mathcal{O})$ and $\mathrm{ext} : \mathrm{I}_{\mathfrak{m}'}(\mathcal{O}) \to \mathrm{I}_{\mathfrak{m}'}(\mathcal{O}')$ send integral ideals in the specified domains into integral ideals in the specified codomains.

To prove the claim for con, suppose $\mathfrak{a}' \in \mathrm{I}_{\mathfrak{m}'}(\mathcal{O}')$, which means $\mathfrak{a}' \subseteq \mathcal{O}'$ is coprime to $\mathfrak{m}'$ in $\mathcal{O}'$; that is, $\mathfrak{a}' + \mathfrak{m}' = \mathcal{O}'$. Then there exist $a' \in \mathfrak{a}'$ and $m' \in \mathfrak{m}'$ such that $a' + m' = 1$. Now $m' \in \mathfrak{m}' \subseteq \mathfrak{f} \subseteq \mathcal{O}$, so $a' = 1 - m' \in \mathcal{O}$, showing that $a' \in \mathrm{con}(\mathfrak{a}')$. Therefore $\mathrm{con}(\mathfrak{a}')$ is coprime to $\mathfrak{m}'$ in $\mathcal{O}$.

To prove the claim for ext, suppose $\mathfrak{a} \in \mathrm{I}_{\mathfrak{m}'}(\mathcal{O})$, which means $\mathfrak{a} \subseteq \mathcal{O}$ is coprime to $\mathfrak{m}'$; that is, $\mathfrak{a} + \mathfrak{m}' = \mathcal{O}$. Then, there exist $a \in \mathfrak{a}$ and $m \in \mathfrak{m}'$ such that $a + m = 1$. Clearly, $a \in \mathrm{ext}(\mathfrak{a})$. Therefore, $\mathrm{ext}(\mathfrak{a})$ is coprime to $\mathfrak{m}'$ in $\mathcal{O}'$. This proves the claim.

Now Lemma 3.7 asserts that $\mathrm{con}(\mathrm{ext}(\mathfrak{a})) = \mathfrak{a}$ holds and $\mathrm{ext}(\mathrm{con}(\mathfrak{a}')) = \mathfrak{a}'$ holds for all integral ideals in their respective domains. Because the domains and codomains of the maps above match on integral ideals, the bijection of con and ext on integral ideals $\mathrm{I}_{\mathfrak{f}}(\mathcal{O}')$ and $\mathrm{I}_{\mathfrak{f}}(\mathcal{O})$ given by Lemma 3.7 restricts to bijective homomorphisms $\mathrm{con} : \mathrm{I}_{\mathfrak{m}'}(\mathcal{O}') \to \mathrm{I}_{\mathfrak{m}'}(\mathcal{O})$ and $\mathrm{ext} : \mathrm{I}_{\mathfrak{m}'}(\mathcal{O}) \to \mathrm{I}_{\mathfrak{m}'}(\mathcal{O}')$ that are inverses of each other.

We now consider a general fractional ideal $\mathfrak{d} = (\mathfrak{a} : \mathfrak{b}) = \mathfrak{a}\mathfrak{b}^{-1} \in \mathrm{J}_{\mathfrak{m}'}(\mathcal{O})$ with $\mathfrak{a} \in \mathrm{I}_{\mathfrak{m}'}(\mathcal{O})$ and $\mathfrak{b} \in \mathrm{I}^*_{\mathfrak{m}'}(\mathcal{O})$, where we have used Lemma 2.20 to write $\mathfrak{d} = \mathfrak{a}\mathfrak{b}^{-1}$. We define $\mathrm{ext}(\mathfrak{d}) = \mathrm{ext}(\mathfrak{a})\,\mathrm{ext}(\mathfrak{b})^{-1}$; any group homomorphisms extending ext must be defined this way. To show this definition is independent of the choice expression of $\mathfrak{d}$ as a ratio of integral ideals, consider two such expressions $\mathfrak{d} = \mathfrak{a}_1\mathfrak{b}_1^{-1} = \mathfrak{a}_2\mathfrak{b}_2^{-1}$. Then, $\mathfrak{a}_1\mathfrak{b}_2 = \mathfrak{a}_2\mathfrak{b}_1$, so $\mathrm{ext}(\mathfrak{a}_1)\,\mathrm{ext}(\mathfrak{b}_2) = \mathrm{ext}(\mathfrak{a}_2)\,\mathrm{ext}(\mathfrak{b}_1)$, so $\mathrm{ext}(\mathfrak{a}_1)\,\mathrm{ext}(\mathfrak{b}_1)^{-1} = \mathrm{ext}(\mathfrak{a}_2)\,\mathrm{ext}(\mathfrak{b}_2)^{-1}$, whence $\mathrm{ext}(\mathfrak{d})$ is well-defined. By a similar argument, defining $\mathrm{con}(\mathfrak{d}') = \mathrm{con}(\mathfrak{a}')\,\mathrm{con}(\mathfrak{b}')^{-1}$ for $\mathfrak{d}' = \mathfrak{a}'(\mathfrak{b}')^{-1}$ with $\mathfrak{a}' \in \mathrm{I}_{\mathfrak{m}'}(\mathcal{O}')$ and $\mathfrak{b}' \in \mathrm{I}^*_{\mathfrak{m}'}(\mathcal{O}')$ gives a unique well-defined homomorphism. The fact that con and ext are inverses of each other then follows from the same fact for integral ideals. □

Remark 3.10. (1) The set of integral ideals $\mathrm{I}_{\mathfrak{f}(\mathcal{O})}(\mathcal{O})$ coprime to the absolute conductor $\mathfrak{f}(\mathcal{O})$ forms a free abelian monoid; the corresponding set of fractional ideals $\mathrm{J}_{\mathfrak{f}(\mathcal{O})}(\mathcal{O})$ is a free abelian group. In both cases there is unique factorization into powers of prime ideals. If an

additional congruence constraint $(\mathrm{mod}\ \mathfrak{m}')$ is imposed as in Proposition 3.8, then unique factorization is inherited for both integral and fractional ideals .

(2) In contrast, for $\mathcal{O} \subsetneq \mathcal{O}_K$, the larger group $\mathrm{J}^*(\mathcal{O})$ of all fractional ideals of $\mathcal{O}$ that are invertible as fractional ideals may contain torsion elements and may also fail to have unique factorization into powers of prime ideals. For an example of the former, $\varepsilon\mathcal{O}$ for any unit $\varepsilon \in \mathcal{O}_K \setminus \mathcal{O}$ is a nontrivial torsion element of $\mathrm{J}^*(\mathcal{O})$.

4. Ray class groups of orders

In this section, we define ray class groups of an order $\mathcal{O}$ as quotients of certain groups of fractional ideals, and we show that those groups can be taken to satisfy auxiliary coprimeness conditions for an auxiliary modulus $\mathfrak{d}$.

4.1. Definition of ray class groups of orders.

Let $\mathcal{O}$ be an order of a number field K.

Definition 4.1. A fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ is *principal* if it may be written as $\mathfrak{a} = \alpha\mathcal{O}$ for some $\alpha \in K$. The group of principal fractional ideals is denoted by $\mathrm{P}(\mathcal{O})$.

When working with ray class groups, one needs to talk about modular congruences between non-integral elements of K. This requires a bit of care. Technically, the following definition depends on the order, so we should really write $\alpha \equiv_{\mathcal{O}} \beta \pmod{\mathfrak{m}}$, but we generally leave the order out of the notation when it is clear from context.

Definition 4.2. Given $\alpha, \beta \in K$, we say that $\alpha \equiv_{\mathcal{O}} \beta \pmod{\mathfrak{m}}$ (abbreviated $\alpha \equiv \beta \pmod{\mathfrak{m}}$ when $\mathcal{O}$ is known from context) if $\alpha = \frac{\alpha_1}{\alpha_2}$ and $\beta = \frac{\beta_1}{\beta_2}$ for some $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathcal{O}$ with $\alpha_2\mathcal{O}$ and $\beta_2\mathcal{O}$ coprime to $\mathfrak{m}$, satisfying $\alpha_1\beta_2 - \alpha_2\beta_1 \in \mathfrak{m}$. This is equivalent to saying that $\alpha - \beta \in \mathfrak{m}\mathcal{O}[S_{\mathfrak{m}}^{-1}]$, where $\mathcal{O}[S_{\mathfrak{m}}^{-1}]$ is the semilocal ring obtained by inverting the elements of $\mathcal{O}$ coprime to $\mathfrak{m}$ (see also Definition 4.7).

Definition 4.3 (Principal ray class)**.** Given an integral ideal $\mathfrak{m}$ in $\mathcal{O}$ and a subset Σ of the real places of K (possibly empty), define the group of *principal ray ideals of $\mathcal{O}$ (modulo $\mathfrak{m}$)*, denoted $\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})$, is given by:

$$\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O}) = \{\alpha\mathcal{O}\colon\ \alpha \in K^\times \text{ such that } \alpha \equiv 1 \pmod{\mathfrak{m}} \text{ and } \rho(\alpha) > 0 \text{ for all } \rho \in \Sigma\}. \tag{4.1}$$

Definition 4.4. The *ray class group* of $\mathcal{O}$ modulo $(\mathfrak{m}, \Sigma)$ is

$$\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) = \frac{\mathrm{J}_{\mathfrak{m}}^*(\mathcal{O})}{\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})}. \tag{4.2}$$

That is,

$$\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) = \frac{\{\text{invertible fractional ideals of } \mathcal{O} \text{ coprime to } \mathfrak{m}\}}{\{\alpha\mathcal{O}\colon\ \alpha \in K^\times \text{ such that } \alpha \equiv 1 \pmod{\mathfrak{m}} \text{ and } \rho(\alpha) > 0 \text{ for all } \rho \in \Sigma\}}. \tag{4.3}$$

This definition of ray class group for an order $\mathcal{O}$ parallels the definition of ray class group for the maximal order. To make the definition flexible, we will show in Section 4.3 that one may add auxiliary congruence conditions without changing the group; for example, requiring relative primality to the conductor ideal $\mathfrak{f}(\mathcal{O})$.

Definition 4.5. The *(wide) ring class group* (or *Picard group*) $\mathrm{Cl}(\mathcal{O})$ of an order $\mathcal{O}$ is the special case of ray class datum modulo $(\mathcal{O}, \emptyset)$, so that

$$\mathrm{Cl}(\mathcal{O}) := \mathrm{Cl}_{\mathcal{O},\emptyset}(\mathcal{O}) = \frac{\mathrm{J}^*_{\mathcal{O}}(\mathcal{O})}{\mathrm{P}_{\mathcal{O},\emptyset}(\mathcal{O})}. \tag{4.4}$$

That is,

$$\mathrm{Cl}_{\mathcal{O},\emptyset}(\mathcal{O}) = \frac{\{\text{invertible fractional ideals of } \mathcal{O}\}}{\{\alpha\mathcal{O}\colon \alpha \in K^\times\}}. \tag{4.5}$$

One can show this definition of ring class field is consistent with the classical definitions in the case of quadratic fields, as given in [11, pp. 114–115], [12, pp. 162–163].

4.2. **Local behavior of ideals.** Before proving results about the ray class group, we need to establish some facts about the interaction of localization with invertibility and ideal inclusion.

Proposition 4.6. *Let $\mathcal{O}$ be an order in a number field K. Invertible fractional ideals of $\mathcal{O}$ are locally principal. Moreover, the correspondence $\mathfrak{a} \mapsto (\mathfrak{a}_\mathfrak{p}) := (\mathfrak{a}\mathcal{O}_\mathfrak{p})$ defines an isomorphism*

$$\mathrm{J}^*(\mathcal{O}) \cong \bigoplus_{\mathfrak{p}} \mathrm{P}(\mathcal{O}_\mathfrak{p}), \tag{4.6}$$

where $\mathfrak{p}$ varies over the prime ideals of $\mathcal{O}$.

Proof. This is Proposition 12.6 on page 75 of Neukirch [30]. □

In the next proposition, we recall a basic fact from commutative algebra: Fractional ideal containment (and more generally, injectivity of module maps) is a local property. We first introduce a notation for localization of rings, for later use.

Definition 4.7. For a commutative ring with unity R and an ideal I of R, we denote by S_I the multiplicatively closed set of elements coprime to I,

$$S_I := \{a \in R : aR + I = R\}. \tag{4.7}$$

We denote by $R[S_I^{-1}]$ the ring defined by inverting the elements of S_I. (We avoid the notation $S_I^{-1}R$ to prevent any confusion with multiplication of ideals.)

The construction extends to R-modules M, yielding $M[S_I^{-1}]$; see [4, Chap. 3]. If R is a Noetherian ring of dimension 1 (such as an order in a number field), then for any nonzero ideal I, the ring $R[S_I^{-1}]$ is a *semilocal ring*—a ring with finitely many maximal ideals. For example, the ring $\mathbb{Z}[S_{(6)}^{-1}]$ consists of those rational numbers whose denominators are contain no factors of 2 or 3, and the only maximal ideals are (2) and (3). If $\mathfrak{p}$ is a maximal ideal of R, then $R[S_\mathfrak{p}^{-1}] = R[(R \setminus \mathfrak{p})^{-1}] = R_\mathfrak{p}$ is the localization away from $\mathfrak{p}$.

We use the notation $M_{\mathfrak{p}} := \mathcal{O}_{\mathfrak{p}}M$ for the localization of an $\mathcal{O}$-module M away from a prime ideal $\mathfrak{p}$.

Proposition 4.8. *For any commutative ring R and a map of R-modules $\phi : M \to N$, the following are equivalent:*

(i) *ϕ is injective.*
(ii) *The induced map $\phi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective for every prime ideal $\mathfrak{p}$ of R.*
(iii) *The induced map $\phi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective for every maximal ideal $\mathfrak{p}$ of R.*

In particular, for an order $\mathcal{O}$ and fractional ideals $\mathfrak{a}, \mathfrak{b} \in \mathrm{J}(\mathcal{O})$,

$$\mathfrak{a} \subseteq \mathfrak{b} \iff \mathfrak{a}_{\mathfrak{p}} \subseteq \mathfrak{b}_{\mathfrak{p}} \text{ for all nonzero prime ideals } \mathfrak{p} \subseteq \mathcal{O}. \tag{4.8}$$

Proof. The statement for R-modules is [4, Proposition 3.9]. The statement for fractional $\mathcal{O}$-ideals follows by taking ϕ to be the inclusion map. □

We now show that the group of invertible fractional ideals coprime to $\mathfrak{m}$ is determined by the set of nonzero prime ideals containing $\mathfrak{m}$.

Lemma 4.9. *Let $\mathcal{O}$ be an order in a number field K, and let $\mathfrak{m}_1, \mathfrak{m}_2$ be nonzero ideals of $\mathcal{O}$. Then:*

(i) *One has $\{\mathfrak{p} : \mathfrak{p} \text{ a prime ideal with } \mathfrak{m}_1 \subseteq \mathfrak{p}\} \subseteq \{\mathfrak{p} : \mathfrak{p} \text{ a prime ideal with } \mathfrak{m}_2 \subseteq \mathfrak{p}\}$ if and only if $\mathrm{I}_{\mathfrak{m}_2}(\mathcal{O}) \subseteq \mathrm{I}_{\mathfrak{m}_1}(\mathcal{O})$.*
(ii) *If $\mathrm{I}_{\mathfrak{m}_2}(\mathcal{O}) \subseteq \mathrm{I}_{\mathfrak{m}_1}(\mathcal{O})$ then $\mathrm{J}^*_{\mathfrak{m}_2}(\mathcal{O}) \subseteq \mathrm{J}^*_{\mathfrak{m}_1}(\mathcal{O})$.*
(iii) *For any nonzero $\mathcal{O}$-ideal $\mathfrak{m}$, there exists an invertible ideal $\widetilde{\mathfrak{m}} \in \mathrm{I}^*(\mathcal{O})$ such that $\widetilde{\mathfrak{m}} \subseteq \mathfrak{m}$ and $\mathrm{I}_{\mathfrak{m}}(\mathcal{O}) = \mathrm{I}_{\widetilde{\mathfrak{m}}}(\mathcal{O})$ (and thus $\mathrm{J}^*_{\mathfrak{m}}(\mathcal{O}) = \mathrm{J}^*_{\widetilde{\mathfrak{m}}}(\mathcal{O})$).*

Proof. If $\mathfrak{m}_1 \subseteq \mathfrak{p}$ but $\mathfrak{m}_2 \not\subseteq \mathfrak{p}$, then $\mathfrak{p} \in \mathrm{I}_{\mathfrak{m}_2}(\mathcal{O})$ (because $\mathfrak{p}$ is maximal and hence $\mathfrak{p} + \mathfrak{m}_2 = \mathcal{O}$) but $\mathfrak{p} \notin \mathrm{I}_{\mathfrak{m}_1}(\mathcal{O})$ (because $\mathfrak{p} + \mathfrak{m}_1 = \mathfrak{p} \neq \mathcal{O}$). This proves the "if" direction of (i) (by proving the contrapositive). To prove the "only if" direction of (i), suppose

$$\{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\} = \{\text{nonzero prime ideals } \mathfrak{p} \text{ with } \mathfrak{m}_1 \subseteq \mathfrak{p}\} \subseteq \{\text{nonzero prime ideals } \mathfrak{p} \text{ with } \mathfrak{m}_2 \subseteq \mathfrak{p}\}. \tag{4.9}$$

For any *integral* ideal $\mathfrak{b} \in \mathrm{I}(\mathcal{O})$, we have

$$\begin{aligned}
\mathfrak{b} + \mathfrak{m}_2 = \mathcal{O} &\implies \mathfrak{b}\mathcal{O}_{\mathfrak{p}_j} + \mathfrak{m}_2\mathcal{O}_{\mathfrak{p}_j} = \mathcal{O}_{\mathfrak{p}_j} \text{ for } 1 \le j \le m && (4.10)\\
&\implies \mathfrak{b}\mathcal{O}_{\mathfrak{p}_j} = \mathcal{O}_{\mathfrak{p}_j} \text{ for } 1 \le j \le m, \text{ because } \mathfrak{m}_2\mathcal{O}_{\mathfrak{p}_j} \subseteq \mathfrak{p}_j\mathcal{O}_{\mathfrak{p}_j} \\
&\qquad \text{and } \mathfrak{p}_j\mathcal{O}_{\mathfrak{p}_j} \text{ is the unique maximal ideal of } \mathcal{O}_{\mathfrak{p}_j} && (4.11)\\
&\implies \mathfrak{b}\mathcal{O}_{\mathfrak{p}} + \mathfrak{m}_1\mathcal{O}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}} \text{ for all nonzero prime } \mathcal{O}\text{-ideals } \mathfrak{p}, \\
&\qquad \text{because } \mathfrak{m}_1\mathcal{O}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}} \text{ for } \mathfrak{p} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\} && (4.12)\\
&\implies \mathfrak{b} + \mathfrak{m}_1 = \mathcal{O} \text{ by Proposition 4.8.} && (4.13)
\end{aligned}$$

In other words, $\mathrm{I}_{\mathfrak{m}_2}(\mathcal{O}) \subseteq \mathrm{I}_{\mathfrak{m}_1}(\mathcal{O})$.

To prove (ii), by definition $\mathrm{J}^*_{\mathfrak{m}}(\mathcal{O})$ consists of fractional ideals of the form $\mathfrak{a}\mathfrak{b}^{-1}$ where $\mathfrak{a}, \mathfrak{b} \in \mathrm{I}^*_{\mathfrak{m}}(\mathcal{O})$. Thus, $\mathrm{I}_{\mathfrak{m}_2}(\mathcal{O}) \subseteq \mathrm{I}_{\mathfrak{m}_1}(\mathcal{O}) \implies \mathrm{I}^*_{\mathfrak{m}_2}(\mathcal{O}) \subseteq \mathrm{I}^*_{\mathfrak{m}_1}(\mathcal{O}) \implies \mathrm{J}^*_{\mathfrak{m}_2}(\mathcal{O}) \subseteq \mathrm{J}^*_{\mathfrak{m}_1}(\mathcal{O})$, so (ii) follows from (i).

To prove (iii), consider a nonzero $\mathcal{O}$-ideal $\mathfrak{m}$. Let $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ be the set of all prime ideals $\mathfrak{p}$ containing $\mathfrak{m}$. For each j with $1 \le j \le m$, choose some nonzero element $\mu_j \in \mathfrak{m}\mathcal{O}_{\mathfrak{p}_j}$, so that the ideal $\mathfrak{q}_j := \mu_j \mathcal{O}_{\mathfrak{p}_j}$ in the local ring $\mathcal{O}_{\mathfrak{p}_j}$ is a principal primary ideal associated to its maximal ideal $\mathfrak{p}_j\mathcal{O}_{\mathfrak{p}_j}$, which is contained in the primary component of $\mathfrak{m}$ that is associated to $\mathfrak{p}_j$. By Proposition 4.6, there exists a unique invertible ideal $\widetilde{\mathfrak{m}} \in \mathrm{J}^*(\mathcal{O})$ such that $\widetilde{\mathfrak{m}}\mathcal{O}_{\mathfrak{p}_j} = \mu_j \mathcal{O}_{\mathfrak{p}_j}$ for $1 \le j \le m$ and $\widetilde{\mathfrak{m}}\mathcal{O}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}$ for $\mathfrak{p} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$. We have

$$\{\text{nonzero prime ideals } \mathfrak{p} \text{ with } \mathfrak{m} \subseteq \mathfrak{p}\} = \{\text{nonzero prime ideals } \mathfrak{p} \text{ with } \widetilde{\mathfrak{m}} \subseteq \mathfrak{p}\}. \tag{4.14}$$

Thus, by (i), both $\mathrm{I}_{\widetilde{\mathfrak{m}}}(\mathcal{O}) \subseteq \mathrm{I}_{\mathfrak{m}}(\mathcal{O})$ and $\mathrm{I}_{\mathfrak{m}}(\mathcal{O}) \subseteq \mathrm{I}_{\widetilde{\mathfrak{m}}}(\mathcal{O})$. Then by (ii) we have $\mathrm{J}^*_{\mathfrak{m}}(\mathcal{O}) = \mathrm{J}^*_{\widetilde{\mathfrak{m}}}(\mathcal{O})$. □

4.3. **Auxiliary coprimality conditions on ray class groups of orders.** In the definition of the ray class group for the maximal order $\mathcal{O}_K$, it is well known that restricting to the fractional ideal group to fractional ideals relatively prime to some ideal $\mathfrak{d}$, and restricting principal ideals similarly, yields the same class group. In this subsection we show this is true for arbitrary orders.

Definition 4.10 (Principal ray class relatively prime to $\mathfrak{d}$)**.** Given an integral $\mathcal{O}$-ideal $\mathfrak{d}$, the group of *principal ray ideals (modulo* $\mathfrak{m}$*) relatively prime to* $\mathfrak{d}$, denoted $\mathrm{P}^{\mathfrak{d}}_{\mathfrak{m},\Sigma}(\mathcal{O})$, is given by:

$$\mathrm{P}^{\mathfrak{d}}_{\mathfrak{m},\Sigma}(\mathcal{O}) = \{\alpha\mathcal{O}\colon \ \alpha \in K^\times \text{ such that } \alpha \equiv 1 \pmod{\mathfrak{m}},\ \alpha\mathcal{O} \text{ coprime to } \mathfrak{d},\ \rho(\alpha) > 0 \text{ for all } \rho \in \Sigma\}. \tag{4.15}$$

The following lemma show that, without loss of generality, we may suppose $\mathfrak{d} \subseteq \mathfrak{m}$.

Lemma 4.11. *If* $\mathfrak{d}$ *is an integral* $\mathcal{O}$*-ideal, then* $\mathrm{P}^{\mathfrak{d}}_{\mathfrak{m},\Sigma}(\mathcal{O}) = \mathrm{P}^{\mathfrak{d}\cap\mathfrak{m}}_{\mathfrak{m},\Sigma}(\mathcal{O}) = \mathrm{P}^{\mathfrak{d}\mathfrak{m}}_{\mathfrak{m},\Sigma}(\mathcal{O})$*. In particular,* $\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O}) = \mathrm{P}^{\mathfrak{m}}_{\mathfrak{m},\Sigma}(\mathcal{O})$.

Proof. Clearly $\mathrm{P}^{\mathfrak{d}\mathfrak{m}}_{\mathfrak{m},\Sigma}(\mathcal{O}) \subseteq \mathrm{P}^{\mathfrak{d}\cap\mathfrak{m}}_{\mathfrak{m},\Sigma}(\mathcal{O}) \subseteq \mathrm{P}^{\mathfrak{d}}_{\mathfrak{m},\Sigma}(\mathcal{O})$. To show the reverse inclusions, suppose $\mathfrak{a} \in \mathrm{P}^{\mathfrak{d}}_{\mathfrak{m},\Sigma}(\mathcal{O})$. Write $\mathfrak{a} = \alpha\mathcal{O}$ for $\alpha \in K^\times$ such that $\alpha \equiv 1 \pmod{\mathfrak{m}}$, α coprime to $\mathfrak{d}$, and $\rho(\alpha) > 0$ for all $\rho \in \Sigma$. Write $\alpha = \frac{\alpha_1}{\alpha_2}$ for $\alpha_1, \alpha_2 \in \mathcal{O}$ with α_2 coprime to $\mathfrak{m}$ (which is possible by Definition 4.2). Then $\alpha_1 \equiv \alpha_2 \pmod{\mathfrak{m}}$, so α_1 is also coprime to $\mathfrak{m}$, so α is coprime to $\mathfrak{m}$. Since α is coprime to $\mathfrak{d}$ and to $\mathfrak{m}$, α is also coprime to $\mathfrak{d}\mathfrak{m}$ and to $\mathfrak{d} \cap \mathfrak{m}$.

The equality $\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O}) = \mathrm{P}^{\mathfrak{m}}_{\mathfrak{m},\Sigma}(\mathcal{O})$ follows by taking $\mathfrak{d} = \mathcal{O}$. □

Lemma 4.12. *For any nonzero ideals* $\mathfrak{d} \subseteq \mathfrak{m} \subseteq \mathcal{O}$ *and any set* Σ *of real places of* K *(possibly empty),*

$$\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) = \frac{\mathrm{J}^*_{\mathfrak{d}}(\mathcal{O})}{\mathrm{P}^{\mathfrak{d}}_{\mathfrak{m},\Sigma}(\mathcal{O})}. \tag{4.16}$$

Proof. Consider the inclusion $\mathrm{J}^*_{\mathfrak{d}}(\mathcal{O}) \hookrightarrow \mathrm{J}^*_{\mathfrak{m}}(\mathcal{O})$, and compose with the quotient map to get a homomorphism

$$\phi : \mathrm{J}^*_{\mathfrak{d}}(\mathcal{O}) \to \frac{\mathrm{J}^*_{\mathfrak{m}}(\mathcal{O})}{\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})} = \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}). \tag{4.17}$$

The kernel $\ker \phi = \mathrm{J}^*_{\mathfrak{d}}(\mathcal{O}) \cap \mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O}) = \mathrm{P}^{\mathfrak{d}}_{\mathfrak{m},\Sigma}(\mathcal{O})$. For the equality (4.16) it suffices to prove that ϕ is surjective.

Consider $\mathfrak{b} \in \mathrm{J}^*_{\mathfrak{m}}(\mathcal{O})$; we want to find some $\mathfrak{a} \in \mathrm{J}^*_{\mathfrak{d}}(\mathcal{O})$ such that $\mathfrak{a}\mathfrak{b}^{-1} \in \mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})$. By Proposition 4.6, for each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$, $\mathfrak{b}\mathcal{O}_{\mathfrak{p}} = \beta_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}$ for some $\beta_{\mathfrak{p}} \in K^{\times}$, and we may take $\beta_{\mathfrak{p}} = 1$ for all but finitely many $\mathfrak{p}$; specifically we take $\beta_{\mathfrak{p}} = 1$ whenever $\mathfrak{p}$ is relatively prime to $\mathfrak{b}$. For every $\mathfrak{p}$, either $\mathfrak{d} \subseteq \mathfrak{p}$ or $\mathfrak{p}+\mathfrak{d} = \mathcal{O}$, and there are only finitely many satisfying the former condition; let $\mathfrak{p}_1, \dots \mathfrak{p}_m$ be those for which $\mathfrak{d} \subseteq \mathfrak{p}_j$ *and* $\mathfrak{m} \not\subseteq \mathfrak{p}_j$. Note that $\beta_{\mathfrak{p}} \neq 1 \implies \mathfrak{p} \in \{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}$.

By Lemma 4.9, there exists some invertible ideal $\widetilde{\mathfrak{m}} \subseteq \mathfrak{m}$ with the property that the set $\{\mathfrak{q}_1, \dots \mathfrak{q}_n\}$ of all nonzero prime ideals of $\mathcal{O}$ for which $\widetilde{\mathfrak{m}} \subseteq \mathfrak{q}_j$ is the same as the set of nonzero prime ideals containing $\mathfrak{m}$. For each nonzero prime ideal $\mathfrak{q}$ of $\mathcal{O}$, use Proposition 4.6 to write $\widetilde{\mathfrak{m}}\mathcal{O}_{\mathfrak{q}} = \mu_{\mathfrak{q}}\mathcal{O}_{\mathfrak{q}}$ for some $\mu_{\mathfrak{q}} \in K^{\times}$, where we set $\mu_{\mathfrak{q}} = 1$ whenever $\mathfrak{q} \notin \{\mathfrak{q}_1, \dots, \mathfrak{q}_n\}$. Note that the sets $\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$ and $\{\mathfrak{q}_1, \dots, \mathfrak{q}_n\}$ are disjoint, and their union is the set of all primes dividing $\mathfrak{d}$.

For $1 \le j \le m$, write $\mathfrak{p}_j = \mathrm{con}(\mathfrak{p}'_j)$ for some nonzero prime ideal $\mathfrak{p}'_j$ of $\mathcal{O}_K$; this is possible by Lemma 3.2. Similarly, for $1 \le j \le n$, write $\mathfrak{q}_j = \mathrm{con}(\mathfrak{q}'_j)$ for some nonzero prime ideal $\mathfrak{q}'_j$ of $\mathcal{O}_K$. These primes $\mathfrak{p}'_j, \mathfrak{q}'_j$ are all distinct, because the primes $\mathfrak{p}_j, \mathfrak{q}_j$ are all distinct. Thus, there are pairwise independent multiplicative valuations (absolute values) $|\cdot|_{v_1}, \dots, |\cdot|_{v_m}, |\cdot|_{w_1}, \dots, |\cdot|_{w_n}$ on K corresponding to $\mathfrak{p}'_1, \dots, \mathfrak{p}'_m, \mathfrak{q}'_1, \dots \mathfrak{q}'_n$, respectively.

Let $\mathfrak{f}_{\mathfrak{p}}$ be the "local conductor" at $\mathfrak{p}$, that is,

$$\mathfrak{f}_{\mathfrak{p}} = \{x \in \mathcal{O}_{\mathfrak{p}} : x\overline{\mathcal{O}}_{\mathfrak{p}} \subseteq \mathcal{O}_{\mathfrak{p}}\}, \tag{4.18}$$

where $\overline{\mathcal{O}}_{\mathfrak{p}}$ is the integral closure of $\mathcal{O}_{\mathfrak{p}}$ in its fraction field $K_{\mathfrak{p}}$. Let $\tilde{f}_{\mathfrak{p}}$ be any nonzero element of $\mathfrak{f}_{\mathfrak{p}}$, so $\tilde{f}_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}$ is a nonzero principal ideal contained in $\mathfrak{f}_{\mathfrak{p}}$.

By the Approximation Theorem [30, Theorem 3.4], we can find $\beta \in K$ such that

(1) $\left|\beta - \beta_{\mathfrak{p}_j}\right|_{v_j} < |\beta|_{v_j}$ for $1 \le j \le m$,
(2) $|\beta - 1|_{w_j} \le \left|f_{\mathfrak{q}_j}\mu_{\mathfrak{q}_j}\right|^{-1}_{w_j}$ for $1 \le j \le n$, and
(3) $\rho(\beta) > 0$ for $\rho \in \Sigma$, via the archimedean real bound $|\beta - 1|_{\rho} < 1$.

Define $\mathfrak{a}$ by $\mathfrak{a} = \beta^{-1}\mathfrak{b}$.

Note that, for $1 \le j \le m$, $\mathfrak{a}\mathcal{O}_{\mathfrak{p}_j} = \beta^{-1}\beta_{\mathfrak{p}_j}\mathcal{O}_{\mathfrak{p}_j}$. By (1), $\left|\beta^{-1}\beta_{\mathfrak{p}_j} - 1\right|_{v_j} < 1$, so in particular, $\beta^{-1}\beta_{\mathfrak{p}_j}$ is a unit in $\mathcal{O}_{\mathfrak{p}'_j} = \overline{\mathcal{O}}_{\mathfrak{p}_j}$. But $\overline{\mathcal{O}}^{\times}_{\mathfrak{p}_j} \cap \mathcal{O}_{\mathfrak{p}_j} = \mathcal{O}^{\times}_{\mathfrak{p}_j}$, so $\beta^{-1}\beta_{\mathfrak{p}_j}$ is a unit in $\mathcal{O}_{\mathfrak{p}_j}$, and thus $\mathfrak{a}\mathcal{O}_{\mathfrak{p}_j} = \mathcal{O}_{\mathfrak{p}_j}$. On the other hand, for $1 \le j \le n$, $\mathfrak{a}\mathcal{O}_{\mathfrak{q}_j} = \beta^{-1}\mathcal{O}_{\mathfrak{q}_j}$ because $\mathfrak{q}_j \supseteq \mathfrak{m}$ and thus $\beta_{\mathfrak{q}_j} = 1$. It follows from (2) that $|\beta^{-1} - 1|_{w_j} < 1$, so in particular, β^{-1} is a unit in $\mathcal{O}_{\mathfrak{q}'_j} = \overline{\mathcal{O}}_{\mathfrak{q}_j}$ and thus a unit in $\mathcal{O}_{\mathfrak{q}_j}$, so $\mathfrak{a}\mathcal{O}_{\mathfrak{q}_j} = \mathcal{O}_{\mathfrak{q}_j}$. Since $\mathfrak{a}\mathcal{O}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}$ for all $\mathfrak{p} \in \{\mathfrak{p}_1, \dots, \mathfrak{p}_m\} \cup \{\mathfrak{q}_1, \dots, \mathfrak{q}_n\}$, it follows that $\mathfrak{a}$ is coprime to $\mathfrak{d}$, so $\mathfrak{a} \in \mathrm{J}^*_{\mathfrak{d}}(\mathcal{O})$.

Moreover, for $1 \le j \le n$, $|\beta^{-1} - 1|_{w_j} \le \left|f_{\mathfrak{q}_j}\mu_{\mathfrak{q}_j}\right|^{-1}_{w_j}$ by (2), so $\beta^{-1} - 1 \in \tilde{f}_{\mathfrak{q}_j}\mu_{\mathfrak{q}_j}\mathcal{O}_{\mathfrak{q}'_j}$. We have the inclusion of ideals

$$\tilde{f}_{\mathfrak{q}_j}\mu_{\mathfrak{q}_j}\mathcal{O}_{\mathfrak{q}'_j} = \mu_{\mathfrak{q}_j}(\tilde{f}_{\mathfrak{q}_j}\overline{\mathcal{O}}_{\mathfrak{q}_j}) \subseteq \mu_{\mathfrak{q}_j}\mathcal{O}_{\mathfrak{q}_j} = \widetilde{\mathfrak{m}}\mathcal{O}_{\mathfrak{q}_j}, \tag{4.19}$$

so $\beta^{-1} - 1 \in \widetilde{\mathfrak{m}}\mathcal{O}_{\mathfrak{q}_j}$ for each j. It follows that $\beta^{-1} \equiv 1 \pmod{\widetilde{\mathfrak{m}}}$, so in particular, $\beta^{-1} \equiv 1 \pmod{\mathfrak{m}}$. Combining this congruence with the positivity condition (3), we have $\mathfrak{a}\mathfrak{b}^{-1} = \beta^{-1}\mathcal{O} \in \mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O}_K)$. □

4.4. **Effect of change of order on ray class groups of orders.** We show that for orders $\mathcal{O} \subseteq \mathcal{O}'$, the extension map on ideals induces well-defined extension maps $\overline{\mathrm{ext}}$ relating ray class groups of orders. This result will be applied in Proposition 5.5.

Lemma 4.13. *For K-orders $\mathcal{O} \subseteq \mathcal{O}'$ and an $\mathcal{O}$-ideal $\mathfrak{m}$, the map*

$$\overline{\mathrm{ext}} : \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) \to \mathrm{Cl}_{\mathfrak{m}\mathcal{O}',\Sigma}(\mathcal{O}') \tag{4.20}$$

induced by extension of ideals is well-defined and surjective.

Proof. To see that the map $\overline{\mathrm{ext}}$ in eq. (4.20) is a well-defined homomorphism, it suffices to show the image of $\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})$ under ring extension from $\mathcal{O}$ to $\mathcal{O}'$ is contained in $\mathrm{P}_{\mathfrak{m}\mathcal{O},\Sigma}(\mathcal{O}')$. So consider an ideal $\mathfrak{b} \in \mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})$. Then $\mathfrak{b} = b\mathcal{O}$ for some $b \in K$, $b \equiv 1 \pmod{\mathfrak{m}}$, and $\rho(b) > 0$ for $\rho \in \Sigma$. Since $\mathfrak{m} \subseteq \mathfrak{m}\mathcal{O}'$, we have $b \equiv 1 \pmod{\mathfrak{m}\mathcal{O}'}$. Moreover, $\mathrm{ext}(\mathfrak{b}) = \mathfrak{b}\mathcal{O}' = b\mathcal{O}'$, and $\mathrm{ext}(\mathfrak{b})$ is coprime to $\mathfrak{m}\mathcal{O}'$. Thus, $\mathrm{ext}(\mathfrak{b}) \in \mathrm{P}_{\mathfrak{m}\mathcal{O}',\Sigma}(\mathcal{O}')$.

Let $\mathfrak{f} = \mathfrak{f}_{\mathcal{O}'}(\mathcal{O})$ be the relative conductor of $\mathcal{O}$ in $\mathcal{O}'$. Let $\mathfrak{d}$ be an ideal of $\mathcal{O}'$ contained in both $\mathfrak{m}$ and $\mathfrak{f}$. Using Lemma 4.12, under the inclusion map on ideals, we have

$$\mathrm{Cl}_{\mathfrak{m}\mathcal{O}',\Sigma}(\mathcal{O}') := \frac{\mathrm{J}^*_{\mathfrak{m}\mathcal{O}'}(\mathcal{O}')}{\mathrm{P}_{\mathfrak{m}\mathcal{O}',\Sigma}(\mathcal{O}')} = \frac{\mathrm{J}^*_{\mathfrak{d}}(\mathcal{O}')}{\mathrm{P}^{\mathfrak{d}}_{\mathfrak{m}\mathcal{O}',\Sigma}(\mathcal{O}')}. \tag{4.21}$$

To see that the map (4.20) is surjective, let $A \in \mathrm{Cl}_{\mathfrak{m}\mathcal{O}',\Sigma}(\mathcal{O}')$, and let $\mathfrak{a} \in \mathrm{J}_{\mathfrak{d}}$ be a representative of the class A. Because $\mathfrak{a}$ is coprime to the conductor $\mathfrak{f}$, we have $\mathrm{ext}(\mathrm{con}(\mathfrak{a})) = \mathfrak{a}$ by Lemma 3.7, so $[\mathrm{con}(\mathfrak{a})] \mapsto [\mathfrak{a}] = A$. □

5. Exact sequences for ray class groups of orders

5.1. **Exact sequences relating unit groups and principal ideals for varying orders.** We describe unit groups that we will relate by exact sequences to groups of principal ideals of varying orders.

Definition 5.1. For a commutative ring with unity R and an ideal I of R, define the group

$$\mathrm{U}_I(R) := \{\alpha \in R^\times : \alpha \equiv 1 \bmod I\} = (1 + I) \cap R^\times. \tag{5.1}$$

If R has real embeddings and Σ is a subset of the real embeddings of R, define

$$\mathrm{U}_{I,\Sigma}(R) := \{\alpha \in R^\times : \alpha \equiv 1 \bmod I \text{ and } \rho(\alpha) > 0 \text{ for } \rho \in \Sigma\}. \tag{5.2}$$

We also make use of the following extension of this notation: If there is an obvious map $\phi : R_1 \to R_2$ implicit in the discussion, and if I is an ideal of R_1, then we will let $\mathrm{U}_I(R_2) := \mathrm{U}_{\phi(I)R_2}(R_2)$ and $\mathrm{U}_{I,\Sigma}(R_2) := \mathrm{U}_{\phi(I)R_2,\Sigma}(R_2)$.

Proposition 5.2. *Let K be a number field. For any order $\mathcal{O}$ in the field K, any ideals $\mathfrak{d} \subseteq \mathfrak{m} \subseteq \mathcal{O}$, and any set of real embeddings $\Sigma \subseteq \{$embeddings $K \to \mathbb{R}\}$, we have an exact sequence*

$$1 \to \mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O}) \to \mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O}[S_{\mathfrak{d}}^{-1}]) \to \mathrm{P}^{\mathfrak{d}}_{\mathfrak{m},\Sigma}(\mathcal{O}) \to 1, \tag{5.3}$$

where $S_{\mathfrak{d}} = \{\alpha \in \mathcal{O} : \alpha\mathcal{O} + \mathfrak{d} = \mathcal{O}\}$.

Proof. By definition,

$$\mathrm{P}^{\mathfrak{d}}_{\mathfrak{m},\Sigma}(\mathcal{O}) = \{\alpha\mathcal{O} : \alpha \in \mathcal{O}[S_{\mathfrak{d}}^{-1}],\ \alpha \equiv 1 \pmod{\mathfrak{m}},\ \rho(\alpha) > 0 \text{ for all } \rho \in \Sigma\}, \tag{5.4}$$

so $\phi(\alpha) := \alpha\mathcal{O}$ defines a surjective map $\phi : \mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O}[S_{\mathfrak{d}}^{-1}]) \to \mathrm{P}^{\mathfrak{d}}_{\mathfrak{m},\Sigma}(\mathcal{O})$. Moreover,

$$\ker(\phi) = \{\alpha \in \mathcal{O}[S_{\mathfrak{d}}^{-1}] : \alpha\mathcal{O} = \mathcal{O},\ \alpha \equiv 1 \pmod{\mathfrak{m}},\ \rho(\alpha) > 0 \text{ for all } \rho \in \Sigma\} \tag{5.5}$$

$$= \mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O}). \tag{5.6}$$

The proposition follows. □

We now relate unit groups and principal ideal groups of varying orders.

Proposition 5.3. *Let K be a number field and $\mathcal{O} \subseteq \mathcal{O}' \subseteq \mathcal{O}_K$ be orders of K. Let $\mathfrak{m}$ be an ideal of $\mathcal{O}$, $\mathfrak{m}'$ an ideal of $\mathcal{O}'$ with $\mathfrak{m}\mathcal{O}' \subseteq \mathfrak{m}'$, and $\Sigma' \subseteq \Sigma \subseteq \{$embeddings $K \hookrightarrow \mathbb{R}\}$. Let $\mathfrak{d}$ be any $\mathcal{O}'$-ideal such that $\mathfrak{d} \subseteq (\mathfrak{m} : \mathcal{O}')$. We have a short exact sequence of the form*

$$1 \to \frac{\mathrm{U}_{\mathfrak{m}',\Sigma'}(\mathcal{O}')}{\mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O})} \to \frac{\mathrm{U}_{\mathfrak{m}'}(\mathcal{O}'/\mathfrak{d})}{\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/\mathfrak{d})} \times \{\pm 1\}^{|\Sigma \setminus \Sigma'|} \to \frac{\mathrm{P}^{\mathfrak{d}}_{\mathfrak{m}',\Sigma'}(\mathcal{O}')}{\mathrm{P}^{\mathfrak{d}}_{\mathfrak{m},\Sigma}(\mathcal{O})} \to 1. \tag{5.7}$$

Proof. Here $\mathfrak{d}$ is an integral $\mathcal{O}$-ideal because $\mathfrak{d} \subseteq (\mathfrak{m} : \mathcal{O}') = \{a \in K : a\mathcal{O} \subseteq \mathfrak{m}\} \subseteq \mathfrak{m} \subseteq \mathcal{O}$, and $\mathfrak{d}\mathcal{O} \subseteq \mathfrak{d}\mathcal{O}' = \mathfrak{d}$. Thus $\mathcal{O}/\mathfrak{d}$ is well-defined. We localize away from $\mathfrak{d}$ by inverting $S_{\mathfrak{d}}$, for the two rings $\mathcal{O}$ and $\mathcal{O}'$ separately. By Proposition 5.2, we have short exact sequences

$$\begin{array}{ccccccccc} 1 & \to & \mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O}) & \to & \mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O}[S_{\mathfrak{d}}^{-1}]) & \to & \mathrm{P}^{\mathfrak{d}}_{\mathfrak{m},\Sigma}(\mathcal{O}) & \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & \mathrm{U}_{\mathfrak{m}',\Sigma'}(\mathcal{O}') & \to & \mathrm{U}_{\mathfrak{m}',\Sigma'}(\mathcal{O}'[S_{\mathfrak{d}}^{-1}]) & \to & \mathrm{P}^{\mathfrak{d}}_{\mathfrak{m}',\Sigma'}(\mathcal{O}') & \to & 1. \end{array} \tag{5.8}$$

The downward maps are all injective—in particular, the rightmost map is—so, by the snake lemma, the sequence of cokernels is exact:

$$1 \to \frac{\mathrm{U}_{\mathfrak{m}',\Sigma'}(\mathcal{O}')}{\mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O})} \to \frac{\mathrm{U}_{\mathfrak{m}',\Sigma'}(\mathcal{O}'[S_{\mathfrak{d}}^{-1}])}{\mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O}[S_{\mathfrak{d}}^{-1}])} \to \frac{\mathrm{P}^{\mathfrak{d}}_{\mathfrak{m}',\Sigma'}(\mathcal{O}')}{\mathrm{P}^{\mathfrak{d}}_{\mathfrak{m},\Sigma}(\mathcal{O})} \to 1. \tag{5.9}$$

This is the short exact sequence in the proposition statement, except for the middle group. We now must show the middle group is isomorphic to the group in the proposition statement.

First of all, note that the localization maps induces compatible isomorphisms

$$\begin{array}{rccc} \iota: & \mathrm{U}_{\mathfrak{m}'}(\mathcal{O}/\mathfrak{d}) & \xrightarrow{\sim} & \mathrm{U}_{\mathfrak{m}'}(\mathcal{O}[S_{\mathfrak{d}}^{-1}]/\mathfrak{d}\mathcal{O}[S_{\mathfrak{d}}^{-1}]) \\ & \downarrow & & \downarrow \\ \iota': & \mathrm{U}_{\mathfrak{m}}(\mathcal{O}'/\mathfrak{d}) & \xrightarrow{\sim} & \mathrm{U}_{\mathfrak{m}}(\mathcal{O}'[S_{\mathfrak{d}}^{-1}]/\mathfrak{d}\mathcal{O}'[S_{\mathfrak{d}}^{-1}]). \end{array} \tag{5.10}$$

Let $\Upsilon = \{$embeddings $K \hookrightarrow \mathbb{R}\}$. Consider the map

$$\phi : \mathrm{U}_{\mathfrak{m}',\Sigma'}(\mathcal{O}'[S_{\mathfrak{d}}^{-1}]) \to \mathrm{U}_{\mathfrak{m}'}(\mathcal{O}'/\mathfrak{d}) \times \{\pm 1\}^{\Upsilon \setminus \Sigma'} \tag{5.11}$$

given by $\phi(u) = \left(\iota'^{-1}\left(u \pmod{\mathfrak{d}\mathcal{O}'[S_\mathfrak{d}^{-1}]}\right), (\mathrm{sign}(\rho(u)))_{\rho\in\Upsilon\setminus\Sigma'}\right)$.

We see that ϕ is surjective as follows: Consider $(u,\varepsilon) \in \mathrm{U}_{\mathfrak{m}'}(\mathcal{O}'/\mathfrak{d}) \times \{\pm 1\}^{\Upsilon\setminus\Sigma'}$. Choose a lift $\widetilde{u} \in \mathcal{O}'$ of u; $\widetilde{u} \in \mathrm{U}_{\mathfrak{m}'}(\mathcal{O}'[S_\mathfrak{d}^{-1}])$ because it is coprime to $\mathfrak{d}$ and congruent to 1 modulo $\mathfrak{m}'$. We may replace $\widetilde{u}$ with $\widetilde{u}+\lambda$ for any $\lambda \in \mathfrak{d}\cap\mathfrak{m}' = \mathfrak{d}$ without affecting its image in $\mathrm{U}_{\mathfrak{m}'}(\mathcal{O}'/\mathfrak{d})$. Since $\mathfrak{d}$ forms a lattice in $K\otimes\mathbb{R}$, we may choose λ appropriately so that $\mathrm{sign}(\rho(\widetilde{u}+\lambda)) = +1$ for $\rho\in\Sigma'$ and $\mathrm{sign}(\rho(\widetilde{u}+\lambda)) = \varepsilon_\rho$ for $\rho \in \Upsilon\setminus\Sigma$. Thus, $\widetilde{u}+\lambda \in \mathrm{U}_{\mathfrak{m}',\Sigma'}(\mathcal{O}'[S_\mathfrak{d}^{-1}])$, and $\phi(\widetilde{u}+\lambda) = (u,\varepsilon)$.

Now, define

$$\overline{\phi} : \mathrm{U}_{\mathfrak{m}',\Sigma'}(\mathcal{O}'[S_\mathfrak{d}^{-1}]) \to \frac{\mathrm{U}_{\mathfrak{m}'}(\mathcal{O}'/\mathfrak{d})\times\{\pm1\}^{\Upsilon\setminus\Sigma'}}{\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/\mathfrak{d})\times\{\pm1\}^{\Upsilon\setminus\Sigma}} \tag{5.12}$$

by $\overline{\phi}(u) := \phi(u) \pmod{\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/\mathfrak{d})\times\{\pm1\}^{E\setminus\Sigma}}$; $\overline{\phi}$ is surjective because ϕ is. Furthermore, we compute the kernel of $\overline{\phi}$ as follows.

$$\overline{\phi}(u) = 1 \iff \iota'^{-1}\left(u \pmod{\mathfrak{d}\mathcal{O}'[S_\mathfrak{d}^{-1}]}\right) \in \mathrm{U}_{\mathfrak{m}}(\mathcal{O}/\mathfrak{d}) \text{ and } \mathrm{sign}(\rho(u)) = 1 \text{ for all } \rho\in\Sigma\setminus\Sigma'. \tag{5.13}$$

We already knew that $\mathrm{sign}(\rho(u)) = 1$ for all $\rho\in\Sigma'$, so in fact, the second condition tells us that $\rho(u) > 0$ for all $\rho\in\Sigma$. We now reformulate the first condition.

$$\iota'^{-1}\left(u \pmod{\mathfrak{d}\mathcal{O}'[S_\mathfrak{d}^{-1}]}\right) \in \mathrm{U}_{\mathfrak{m}}(\mathcal{O}/\mathfrak{d}) \tag{5.14}$$

$$\iff u \pmod{\mathfrak{d}\mathcal{O}'[S_\mathfrak{d}^{-1}]} \in \iota'\left(\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/\mathfrak{d})\right) = \iota\left(\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/\mathfrak{d})\right) = \mathrm{U}_{\mathfrak{m}}\left(\mathcal{O}_\mathfrak{d}/\mathfrak{d}\mathcal{O}[S_\mathfrak{d}^{-1}]\right) \tag{5.15}$$

$$\iff u \equiv 1 \pmod{\mathfrak{m}\mathcal{O}[S_\mathfrak{d}^{-1}]}. \tag{5.16}$$

This last condition also implies that $u\in\mathcal{O}[S_\mathfrak{d}^{-1}]$ (rather than simply in $\mathcal{O}'[S_\mathfrak{d}^{-1}]$). Thus, we have shown that

$$\ker\left(\overline{\phi}\right) = \{u\in\mathrm{U}_{\mathfrak{m}',\Sigma'}(\mathcal{O}'[S_\mathfrak{d}^{-1}]) : u\in\mathcal{O}[S_\mathfrak{d}^{-1}],\ u\equiv 1 \pmod{\mathfrak{m}\mathcal{O}[S_\mathfrak{d}^{-1}]},\ \rho(u)>0 \text{ for all } \rho\in\Sigma\} \tag{5.17}$$

$$= \mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O}[S_\mathfrak{d}^{-1}]). \tag{5.18}$$

Therefore, $\overline{\phi}$ induces an isomorphism

$$\frac{\mathrm{U}_{\mathfrak{m}',\Sigma'}(\mathcal{O}'[S_\mathfrak{d}^{-1}])}{\mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O}[S_\mathfrak{d}^{-1}])} \xrightarrow{\sim} \frac{\mathrm{U}_{\mathfrak{m}'}(\mathcal{O}'/\mathfrak{d})\times\{\pm1\}^{E\setminus\Sigma'}}{\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/\mathfrak{d})\times\{\pm1\}^{E\setminus\Sigma}} \cong \frac{\mathrm{U}_{\mathfrak{m}'}(\mathcal{O}'/\mathfrak{d})}{\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/\mathfrak{d})}\times\{\pm1\}^{|\Sigma\setminus\Sigma'|}, \tag{5.19}$$

proving the proposition. □

5.2. **Exact sequences for ray class groups of varying orders.** We relate class groups of varying orders; the formula (5.20) is important for applications.

Theorem 5.4. *Let K be a number field and $\mathcal{O}\subseteq\mathcal{O}'\subseteq\mathcal{O}_K$ be orders of K, and let $\mathfrak{f} = \mathfrak{f}_{\mathcal{O}'}(\mathcal{O})$. Let $\mathfrak{m}$ be an ideal of $\mathcal{O}$, $\mathfrak{m}'$ an ideal of $\mathcal{O}'$ such that $\mathfrak{m}\mathcal{O}'\subseteq\mathfrak{m}'$, and $\Sigma'\subseteq\Sigma\subseteq\{$embeddings $K\hookrightarrow\mathbb{R}\}$. Let $\mathfrak{d}$ be any $\mathcal{O}'$-ideal such that $\mathfrak{d}\subseteq(\mathfrak{m}:\mathcal{O}')$. With the* U*-groups defined as in Definition 5.1, we have the following exact sequence.*

$$1\to\frac{\mathrm{U}_{\mathfrak{m}',\Sigma'}(\mathcal{O}')}{\mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O})}\to\frac{\mathrm{U}_{\mathfrak{m}'}(\mathcal{O}'/\mathfrak{d})}{\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/\mathfrak{d})}\times\{\pm1\}^{|\Sigma\setminus\Sigma'|}\to\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})\to\mathrm{Cl}_{\mathfrak{m}',\Sigma'}(\mathcal{O}')\to 1. \tag{5.20}$$

To prove this result, we use the following proposition.

Proposition 5.5. *Let K be a number field and $\mathcal{O} \subseteq \mathcal{O}' \subseteq \mathcal{O}_K$ be orders of K. Let $\mathfrak{m}$ be an ideal of $\mathcal{O}$, $\mathfrak{m}'$ an ideal of $\mathcal{O}'$ with $\mathfrak{m}\mathcal{O}' \subseteq \mathfrak{m}'$, and $\Sigma' \subseteq \Sigma \subseteq \{$embeddings $K \hookrightarrow \mathbb{R}\}$. Let $\mathfrak{d}$ be any $\mathcal{O}'$-ideal such that $\mathfrak{d} \subseteq (\mathfrak{m} : \mathcal{O}')$. We have an exact sequence of the form*

$$1 \to \frac{\mathrm{P}^{\mathfrak{d}}_{\mathfrak{m}',\Sigma'}(\mathcal{O}')}{\mathrm{P}^{\mathfrak{d}}_{\mathfrak{m},\Sigma}(\mathcal{O})} \to \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) \to \mathrm{Cl}_{\mathfrak{m}',\Sigma'}(\mathcal{O}') \to 1. \tag{5.21}$$

Proof. The extension map $\overline{\mathrm{ext}} : \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) \to \mathrm{Cl}_{\mathfrak{m}',\Sigma}(\mathcal{O}')$ is surjective by Lemma 4.13, so the sequence is exact at $\mathrm{Cl}_{\mathfrak{m}',\Sigma'}(\mathcal{O}')$.

Note that $\mathfrak{d}$ is both an $\mathcal{O}'$-ideal and $\mathcal{O}$-ideal, because it is an $\mathcal{O}'$-ideal and $\mathfrak{d} \subseteq (\mathfrak{m} : \mathcal{O}') \subseteq \mathfrak{m} \subseteq \mathcal{O}$. In addition $\mathfrak{d} \subseteq \mathfrak{m}$, so that $\mathfrak{d} \subseteq \mathfrak{m}'$ (because $\mathfrak{m} \subseteq \mathfrak{m}'$). By Lemma 4.12,

$$\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) = \frac{\mathrm{I}_{\mathfrak{d}}(\mathcal{O})}{\mathrm{P}^{\mathfrak{d}}_{\mathfrak{m},\Sigma}(\mathcal{O})} \text{ and } \mathrm{Cl}_{\mathfrak{m}',\Sigma'}(\mathcal{O}') = \frac{\mathrm{I}_{\mathfrak{d}}(\mathcal{O}')}{\mathrm{P}^{\mathfrak{d}}_{\mathfrak{m}',\Sigma'}(\mathcal{O}')}. \tag{5.22}$$

The kernel of the extension map is

$$\ker(\overline{\mathrm{ext}}) = \{[\mathfrak{a}] \in \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) : \mathfrak{a}\mathcal{O}' = \alpha\mathcal{O}',\ \alpha \in \mathcal{O}'_{\mathfrak{d}},\ \alpha \equiv 1 \pmod{\mathfrak{m}'},\ \rho(\alpha) > 0 \text{ for all } \rho \in \Sigma'\}. \tag{5.23}$$

The ideal $\mathfrak{d} \subseteq (\mathcal{O} : \mathcal{O}') = \mathfrak{f}_{\mathcal{O}'}(\mathcal{O})$, so fractional ideals (of $\mathcal{O}$ or $\mathcal{O}'$) coprime to $\mathfrak{d}$ are also coprime to the conductor $\mathfrak{f}_{\mathcal{O}'}(\mathcal{O})$. By Proposition 3.8, con and ext act as inverses on ideals coprime to the conductor, so setting $\phi(\alpha\mathcal{O}') = [\mathrm{con}(\alpha\mathcal{O}')]$ defines a surjective map

$$\phi : \mathrm{P}^{\mathfrak{d}}_{\mathfrak{m}',\Sigma'}(\mathcal{O}') \to \ker(\overline{\mathrm{ext}}). \tag{5.24}$$

Moreover,

$$\ker\phi = \{\alpha\mathcal{O}' : \alpha \in \mathcal{O}[S_{\mathfrak{d}}^{-1}],\ \alpha \equiv 1 \pmod{\mathfrak{m}},\ \rho(\alpha) > 0 \text{ for all } \rho \in \Sigma\} = \mathrm{P}^{\mathfrak{d}\cap\mathfrak{m}}_{\mathfrak{m},\Sigma}(\mathcal{O}) = \mathrm{P}^{\mathfrak{d}}_{\mathfrak{m},\Sigma}(\mathcal{O}). \tag{5.25}$$

The proposition follows. □

We now prove the main exact sequence.

Proof of Theorem 5.4. The result follows by gluing together the two short exact sequences in Proposition 5.3 and Proposition 5.5. □

5.3. **Cardinality of ray class groups of orders.** The following result gives a formula for the "class number" of the ray class group of an order with ray class datum $(\mathcal{O}; \mathfrak{m}, \Sigma)$. It generalizes a formula in Neukirch [30, Theorem I.12.12] for the cardinality of the Picard group of an order (corresponding to ray class datum $(\mathcal{O}; \mathcal{O}, \emptyset)$).

Theorem 5.6. *Let K be an algebraic number field having r real places and s conjugate pairs of complex places. Let $\mathcal{O}_K$ be the maximal order, and let $(\mathcal{O}; \mathfrak{m}, \Sigma)$ be a ray class datum of K.*

The groups $\frac{\mathcal{O}_K^\times}{\mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O})}$ *and* $\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ *are finite, and one has*

$$\#\,\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) = \frac{h_K}{[\mathcal{O}_K^\times : \mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O})]} \cdot \frac{2^{|\Sigma|}\#(\mathcal{O}_K/(\mathfrak{m}:\mathcal{O}_K))^\times}{\#\,\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/(\mathfrak{m}:\mathcal{O}_K))} \tag{5.26}$$

where h_K *is the class number of* K*. In particular, one has*

$$\mathrm{rank}(\mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O})) = \mathrm{rank}(\mathcal{O}_K^\times) = r + s - 1. \tag{5.27}$$

Proof. We specialize the short exact sequence in Theorem 5.4, given $\mathfrak{m} \subseteq \mathcal{O}$, to the case where $\mathfrak{m}' = \mathcal{O}' = \mathcal{O}_K$, $\Sigma' = \emptyset$, and $\mathfrak{d} = (\mathfrak{m} : \mathcal{O}')$. Certainly $\mathfrak{m} \subseteq \mathfrak{m}'\mathcal{O}_K = \mathcal{O}_K$, whence

$$1 \to \frac{\mathcal{O}_K^\times}{\mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O})} \to \frac{(\mathcal{O}_K/(\mathfrak{m}:\mathcal{O}_K))^\times}{\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/(\mathfrak{m}:\mathcal{O}_K))} \times \{\pm 1\}^{|\Sigma|} \to \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_K) \to 1. \tag{5.28}$$

The second nontrivial term in this exact sequence is obviously finite, and the fourth term is finite of order h_K by the finiteness of the class group. It follows that the other two terms are also finite. Equation (5.27) follows from the finiteness of the first term and from Dirichlet's Unit Theorem. Moreover, the alternating product of the cardinality of the terms in an exact sequence of finite groups is 1. Writing this product down and solving for $\#\,\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ yields eq. (5.26). □

5.4. **Ring class groups of orders.** Theorem 5.4 allows us to express the (wide) ring class group $\mathrm{Cl}(\mathcal{O})$ of an order $\mathcal{O}$, as given in Definition 4.5, as a quotient of the Takagi ray class group $\mathrm{Cl}_{\mathfrak{f},\emptyset}(\mathcal{O}_K)$ for the conductor ideal $\mathfrak{f}(\mathcal{O})$, permitting us to quantify the difference between them.

To understand the structure of the (principal) ring class group of $\mathcal{O}$, take $\mathfrak{m} = \mathcal{O}$, let $\mathcal{O}' = \mathcal{O}_K$, take $\mathfrak{m}' = \mathcal{O}_K$, and let Σ, Σ' to be empty. Set $\mathfrak{d} = \mathfrak{f} = \mathfrak{f}(\mathcal{O})$. In particular, this is the case used in eq. (5.28) with the further specialization $(\mathfrak{m}, \Sigma) = (\mathcal{O}, \emptyset)$. We obtain the exact sequence

$$1 \to \frac{\mathcal{O}_K^\times}{\mathcal{O}^\times} \to \frac{(\mathcal{O}_K/\mathfrak{f})^\times}{(\mathcal{O}/\mathfrak{f})^\times} \to \mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_K) \to 1. \tag{5.29}$$

For the ray class group, choose $\mathfrak{m}', \mathcal{O}' = \mathcal{O}_K$ and Σ, Σ' to be empty, but take $\mathfrak{m} = \mathfrak{f}(\mathcal{O})$. Again set $\mathfrak{d} = \mathfrak{f} = \mathfrak{f}(\mathcal{O})$. Note that the unit group $\mathrm{U}_{\mathfrak{f}}(\mathcal{O}_K/\mathfrak{f}) = \{1\}$, so we obtain the exact sequence

$$1 \to \frac{\mathcal{O}_K^\times}{\mathrm{U}_{\mathfrak{f}}(\mathcal{O}_K)} \to (\mathcal{O}_K/\mathfrak{f})^\times \to \mathrm{Cl}_{\mathfrak{f}}(\mathcal{O}_K) \to \mathrm{Cl}(\mathcal{O}_K) \to 1. \tag{5.30}$$

There are natural quotient maps making the following diagram commute (because $\mathrm{U}_{\mathfrak{f}}(\mathcal{O}_K)$ is a subgroup of $\mathcal{O}^\times$), so there is a surjective induced map ψ from the ray class group to the ring class group.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \frac{\mathcal{O}_K^\times}{\mathrm{U}_{\mathfrak{f}}(\mathcal{O}_K)} & \longrightarrow & (\mathcal{O}_K/\mathfrak{f})^\times & \longrightarrow & \mathrm{Cl}_{\mathfrak{f}}(\mathcal{O}_K) & \longrightarrow & \mathrm{Cl}(\mathcal{O}_K) \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \vdots\ \psi & & \| \\
1 & \longrightarrow & \frac{\mathcal{O}_K^\times}{\mathcal{O}^\times} & \longrightarrow & \frac{(\mathcal{O}_K/\mathfrak{f})^\times}{(\mathcal{O}/\mathfrak{f})^\times} & \longrightarrow & \mathrm{Cl}(\mathcal{O}) & \longrightarrow & \mathrm{Cl}(\mathcal{O}_K) \longrightarrow 1.
\end{array} \tag{5.31}$$

In the next section, we generalize this comparison by introducing a ray class modulus.

6. RAY CLASS FIELDS OF ORDERS

In this section, we define and prove existence of class fields associated to the ray class groups defined in Section 4. As usual, let K be a number field, $\mathcal{O}$ an order of K, $\mathfrak{m}$ an integral ideal of $\mathcal{O}$, and Σ a subset of the real embeddings of K.

6.1. **Ray class fields of orders defined via Takagi ray class groups.** We define ray class fields of orders by the following recipe. We are given the ray class datum $(\mathcal{O}; \mathfrak{m}, \Sigma)$, and we also consider the ray class datum $(\mathcal{O}_K; (\mathfrak{m} : \mathcal{O}_K), \Sigma)$. We define a homomorphism ψ from the group $\mathrm{Cl}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K)$ to the given ray class group $\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ and show that it is surjective. We let $J = J(\mathcal{O}; \mathfrak{m}, \Sigma) = \ker \psi$ be the kernel. As a subgroup of $\mathrm{Cl}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K)$, J has an associated Takagi ray class (sub)field $L = L_J$ (of $H_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}$), given in Theorem 6.2(1) below. We define the field L obtained this way to be the ray class field $H^{\mathcal{O}}_{\mathfrak{m},\Sigma}$ assigned to the ray class datum $(\mathcal{O}; \mathfrak{m}, \Sigma)$ for the order $\mathcal{O}$.

To construct ψ, we start from the exact sequence from Theorem 5.4 for $(\mathcal{O}, \mathfrak{m}, \Sigma)$, taking $(\mathcal{O}', \mathfrak{m}', \Sigma') := (\mathcal{O}_K, \mathcal{O}_K, \emptyset)$ and $\mathfrak{d} := (\mathfrak{m} : \mathcal{O}_K)$. It is

$$1 \to \frac{\mathcal{O}_K^\times}{\mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O})} \to \frac{(\mathcal{O}_K/(\mathfrak{m} : \mathcal{O}_K))^\times}{\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/(\mathfrak{m} : \mathcal{O}_K))} \times \{\pm 1\}^{|\Sigma|} \to \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_K) \to 1, \tag{6.1}$$

since $\mathrm{U}_{\mathfrak{m}'}(\mathcal{O}'/\mathfrak{d}) = (\mathcal{O}_K/(\mathfrak{m} : \mathcal{O}_K))^\times$.

Consider also the exact sequence in Theorem 5.4, taking $(\mathcal{O}, \mathfrak{m}, \Sigma) := (\mathcal{O}_K, (\mathfrak{m} : \mathcal{O}_K), \Sigma)$, $(\mathcal{O}', \mathfrak{m}', \Sigma') := (\mathcal{O}_K, \mathcal{O}_K, \emptyset)$, and $\mathfrak{d} := (\mathfrak{m} : \mathcal{O}_K)$. In this sequence the denominator in the second term is $\mathrm{U}_{(\mathfrak{m}:\mathcal{O}_K)}(\mathcal{O}_K/(\mathfrak{m} : \mathcal{O}_K))$ (since $((\mathfrak{m} : \mathcal{O}_K) : \mathcal{O}_K) = (\mathfrak{m} : \mathcal{O}_K)$)), which is the trivial group. We obtain

$$1 \to \frac{\mathcal{O}_K^\times}{\mathrm{U}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K)} \to (\mathcal{O}_K/(\mathfrak{m} : \mathcal{O}_K))^\times \times \{\pm 1\}^{|\Sigma|} \to \mathrm{Cl}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K) \to \mathrm{Cl}(\mathcal{O}_K) \to 1. \tag{6.2}$$

As in Section 5.3, there are natural quotient maps between the objects in these two exact sequences corresponding to the downward maps labeled κ, π, and id in the following diagram. The map κ exists and is surjective because $\mathrm{U}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K)$ is a subgroup of $\mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O})$; the map π is a quotient in the first coordinate; and the map id is the identity map. Moreover, it is straightforward to check that the diagram commutes, which implies that there is an induced surjective map ψ in the position shown.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \frac{\mathcal{O}_K^\times}{\mathrm{U}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K)} & \longrightarrow & (\mathcal{O}_K/(\mathfrak{m} : \mathcal{O}_K))^\times \times \{\pm 1\}^{|\Sigma|} & \longrightarrow & \mathrm{Cl}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K) & \longrightarrow & \mathrm{Cl}(\mathcal{O}_K) \longrightarrow 1 \\
 & & \downarrow \kappa & & \downarrow \pi & & \vdots\ \psi & & \| \mathrm{id} \\
1 & \longrightarrow & \frac{\mathcal{O}_K^\times}{\mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O})} & \longrightarrow & \frac{(\mathcal{O}_K/(\mathfrak{m}:\mathcal{O}_K))^\times}{\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/(\mathfrak{m}:\mathcal{O}_K))} \times \{\pm 1\}^{|\Sigma|} & \longrightarrow & \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) & \longrightarrow & \mathrm{Cl}(\mathcal{O}_K) \longrightarrow 1
\end{array} \tag{6.3}$$

We have thus constructed a surjective map $\psi : \mathrm{Cl}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K) \twoheadrightarrow \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$.

We make the following definition.

Definition 6.1. The *ray class field of the order $\mathcal{O}$ with modulus* $(\mathfrak{m}, \Sigma)$ is the subfield $H^{\mathcal{O}}_{\mathfrak{m},\Sigma}$ of $H^{\mathcal{O}_K}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}$ associated to $J(\mathcal{O}, \mathfrak{m}, \Sigma) := \ker \psi$ in eq. (6.3) under the Galois correspondence between subgroups of the Galois group $\mathrm{Gal}(H^{\mathcal{O}_K}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}/K) \cong \mathrm{Cl}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K)$ and subfields of $H^{\mathcal{O}_K}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}$ containing K.

Theorem 1.1 will identify this field $H^{\mathcal{O}}_{\mathfrak{m},\Sigma}$ in terms of data associated to the splitting of primes in $\mathcal{O}_K$, their contractions to $\mathcal{O}$, and a ray class congruence condition on those contractions. Namely, we will show the field $L = H^{\mathcal{O}}_{\mathfrak{m},\Sigma}$ produced by this definition is the unique extension field of K whose set of prime ideals $\mathfrak{p}$ over $\mathcal{O}_K$ that split completely in L/K agrees (with symmetric difference a finite set) with the set of prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ whose contraction $\mathfrak{p} \cap \mathcal{O}$ to $\mathcal{O}$ is a principal prime ideal $\pi\mathcal{O}$ having a generator $\pi \equiv_{\mathcal{O}} 1 \pmod{\mathfrak{m}}$ and $\rho(\pi) > 0$ for $\rho \in \Sigma$.

6.2. **The classical existence theorem.** We state the classical existence theorem of class field theory, called the Weber–Hilbert–Artin–Takagi [WHAT] correspondence by Cohn [11, Chapter 7], in our notation.

Theorem 6.2 (WHAT correspondence)**.** *Let K be a number field, $\mathfrak{m}$ an ideal of $\mathcal{O}_K$, and Σ a subset of the set of real embeddings of K.*

(1) (Weber-Takagi) *Let J be a subgroup of the (Takagi) ray class group $\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}_K)$. Then, there is a unique abelian extension L_J/K with property that a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ splits completely in L_J if and only if the ray class $[\mathfrak{p}]$ lies in J, with finitely many exceptions. (The exceptions are among the prime ideals dividing $\mathfrak{m}$.) If $J_1 \subseteq J_2$ then $L_{J_2} \subseteq L_{J_1}$. For $J = \{\mathcal{I}\}$, where $\mathcal{I} = [\mathcal{O}_K]$ is the principal ray class modulo $(\mathfrak{m}, \Sigma)$, the field $L = L_{\{\mathcal{I}\}} = H^{\mathcal{O}_K}_{\mathfrak{m},\Sigma}$, the principal ray class field.*

(2) (Artin) *Under the correspondence (1), for $L = L_{\{\mathcal{I}\}} = H^{\mathcal{O}_K}_{\mathfrak{m},\Sigma}$ there is an isomorphism $\mathrm{Art} : \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}_K) \to \mathrm{Gal}(L/K)$, the so-called Artin isomorphism $\mathrm{Art} = \mathrm{Art}_{\mathfrak{m},\Sigma}$, which is determined by sending prime ideals $[\mathfrak{p}]$ of $\mathcal{O}_K$ (relatively prime to $\mathfrak{m}$) to $\left[\frac{L/K}{\mathfrak{p}}\right] \in \mathrm{Gal}(L/K)$, and extending this map multiplicatively to all ray ideals $[\mathfrak{a}]$ relatively prime to $\mathfrak{m}$. Under this isomorphism, L_J is the fixed field of the principal ray class field $L = L_{\{\mathcal{I}\}}$ under the action of the group of automorphisms $\mathrm{Art}(J) \subseteq \mathrm{Gal}(L/K)$, i.e.,*

$$L_J := \left(H^{\mathcal{O}_K}_{\mathfrak{m},\Sigma}\right)^{\mathrm{Art}(J)}. \tag{6.4}$$

In the statement of (2), the Artin symbol $\left[\frac{L/K}{\mathfrak{p}}\right]$ denotes the Frobenius automorphism $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$ computed for a prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ lying over $\mathfrak{p}$ as $x^p \equiv x^{\sigma_{\mathfrak{p}}} \pmod{\mathfrak{P}}$ for all $x \in \mathcal{O}_L$.

Proof. This statement (1) is extracted from Theorem 7.4.1 of Cohn [11]. The statement (2) follows from Theorem 7.4.2 of Cohn [11]. □

Remark 6.3. For J a subgroup of $\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}_K)$, with $L = H^{\mathcal{O}_K}_{\mathfrak{m},\Sigma}$ and $L_J = L^{\mathrm{Art}(J)}$ as in Theorem 6.2, one can also define an Artin isomorphism Art_J making the diagram

$$\begin{array}{ccc} \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}_K) & \xrightarrow{\mathrm{Art}_{\mathfrak{m},\Sigma}} & \mathrm{Gal}(L/K) \\ \Big\downarrow & & \Big\downarrow \\ \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}_K)/J & \xrightarrow{\mathrm{Art}_J} & \mathrm{Gal}(L_J/K) \end{array} \tag{6.5}$$

commute, as a direct consequence of the Galois correspondence. Moreover, the Artin maps with different class field moduli are compatible because of their local definition via the Frobenius map. That is, if $\phi : \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}_K) \to \mathrm{Cl}_{\mathfrak{m}',\Sigma'}(\mathcal{O}_K)$ is the natural quotient map, then $\mathrm{Art}_{\ker\phi} = \mathrm{Art}_{\mathfrak{m}',\Sigma'}$.

6.3. **Proof of Theorem 1.1.** The main step in the proof is to identify that the map ψ introduced in Section 6.1 acts as contraction to $\mathcal{O}$ on the set of fractional ideals of $\mathcal{O}_K$ relatively prime to $(\mathfrak{m} : \mathcal{O}_K)$ (or equivalently, relatively prime to $\mathfrak{m}\mathcal{O}_K \cap \mathfrak{f}(\mathcal{O}_K)$).

Lemma 6.4. *For a fractional ideal $\mathfrak{a} \in \mathrm{J}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K)$ representing a class $[\mathfrak{a}] \in \mathrm{Cl}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K)$, the map $\psi : \mathrm{Cl}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K) \to \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ defined by eq.* (6.3) *may be explicitly written as $\psi([\mathfrak{a}]) = [\mathrm{con}(\mathfrak{a})]$.*

Proof. We apply Proposition 3.8 for the case $\mathcal{O} \subseteq \mathcal{O}_K$, taking $\mathfrak{m}' := (\mathfrak{m} : \mathcal{O}_K)$ and noting that $(\mathfrak{m} : \mathcal{O}_K) \subseteq \mathfrak{f}(\mathcal{O})$ (see Lemma 2.18). Proposition 3.8 constructed an isomorphism $\mathrm{con} : \mathrm{J}_{(\mathfrak{m}:\mathcal{O}_K)}(\mathcal{O}_K) \to \mathrm{J}_{(\mathfrak{m}:\mathcal{O}_K)}(\mathcal{O})$ and showed that its inverse map was $\mathrm{ext} : \mathrm{J}_{(\mathfrak{m}:\mathcal{O}_K)}(\mathcal{O}) \to \mathrm{J}_{(\mathfrak{m}:\mathcal{O}_K)}(\mathcal{O}_K)$. For a principal ideal $\mathfrak{a} \in \mathrm{P}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K)$ with $\mathfrak{a} = \alpha\mathcal{O}_K$, note that $\mathfrak{a} = \mathrm{ext}(\alpha\mathcal{O})$; thus, $\mathrm{con}(\mathfrak{a}) = \mathrm{con}(\mathrm{ext}(\alpha\mathcal{O})) = \alpha\mathcal{O}$. Thus, the composition

$$\mathrm{J}_{(\mathfrak{m}:\mathcal{O}_K)}(\mathcal{O}_K) \xrightarrow{\mathrm{con}} \mathrm{J}_{(\mathfrak{m}:\mathcal{O}_K)}(\mathcal{O}) \hookrightarrow \mathrm{J}_{\mathfrak{m}}(\mathcal{O}) \tag{6.6}$$

sends the subgroup $\mathrm{P}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K)$ to a subgroup of $\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})$, and thus defines a map

$$\widetilde{\psi} : \mathrm{Cl}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K) \to \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}). \tag{6.7}$$

To show that $\widetilde{\psi} = \psi$, it suffices to show that $\widetilde{\psi}$ makes the diagram in eq. (6.3) commute. To the left, for a pair $(\alpha, \varepsilon) \in (\mathcal{O}_K/((\mathfrak{m} : \mathcal{O}_K)))^\times \times \{\pm 1\}^{|\Sigma|}$, the square looks like

$$\begin{array}{ccc} (\alpha, \varepsilon) & \longmapsto & \{\beta\mathcal{O}_K : \beta \equiv \alpha \pmod{(\mathfrak{m} : \mathcal{O}_K)} \text{ and } \rho(\beta) = \varepsilon_\rho\} \\ \Big\downarrow & & \Big\downarrow \widetilde{\psi} \\ (\alpha \pmod{\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/((\mathfrak{m} : \mathcal{O}_K)))}, \varepsilon) & \longmapsto & \{\beta\mathcal{O} : \beta \equiv \alpha \pmod{\mathfrak{m}} \text{ and } \rho(\beta) = \varepsilon_\rho\}, \end{array} \tag{6.8}$$

and we observe that it commutes. On the right, $\widetilde{\psi}$ clearly does not change the class of $\mathfrak{a}$ in $\mathrm{Cl}(\mathcal{O}_K)$, so the right square commutes as well. So $\widetilde{\psi} = \psi$, and the lemma is proved. □

Proof of Theorem 1.1. Consider the map $\psi : \mathrm{Cl}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K) \to \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ defined by eq. (6.3), and let $J = \ker\psi$. By Theorem 6.2, $H^{\mathcal{O}}_{\mathfrak{m},\Sigma} := \left(H_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}\right)^{\mathrm{Art}(J)}$ is the unique abelian extension of K such that a prime $\mathfrak{p}$ of $\mathcal{O}_K$ splits completely in $H^{\mathcal{O}}_{\mathfrak{m},\Sigma}$ if and only if $[\mathfrak{p}]$ lies in J. But $[\mathfrak{p}] \in J$ if and only if $\psi([\mathfrak{p}]) = 0$, and by Lemma 6.4, $\psi([\mathfrak{p}]) = [\mathrm{con}(\mathfrak{p})] = [\mathfrak{p} \cap \mathcal{O}]$. (Since $\mathfrak{p}$ is a maximal ideal, also $\mathfrak{p} \cap \mathcal{O}$ is a maximal ideal by Lemma 3.2 (2).) □

6.4. **Proof of Theorem 1.2.** We prove a more general result.

Theorem 6.5. *For two orders $\mathcal{O} \subseteq \mathcal{O}'$ in a number field K and any ray class datum $(\mathcal{O}; \mathfrak{m}, \Sigma)$ for $\mathcal{O}$, there are inclusions of ray class fields $H^{\mathcal{O}'}_{\mathfrak{m}\mathcal{O}',\Sigma} \subseteq H^{\mathcal{O}}_{\mathfrak{m},\Sigma} \subseteq H^{\mathcal{O}'}_{(\mathfrak{m}:\mathcal{O}'),\Sigma}$.*

Proof. Consider the following (commutative) diagram, with the dotted lines denoting maps induced by the others. In this diagram, rows are exact, but the columns are *not* exact; all vertical maps are surjective.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \frac{(\mathcal{O}')^\times}{\mathrm{U}_{(\mathfrak{m}:\mathcal{O}'),\Sigma}(\mathcal{O}')} & \longrightarrow & (\mathcal{O}'/(\mathfrak{m}:\mathcal{O}'))^\times \times \{\pm 1\}^{|\Sigma|} & \longrightarrow & \mathrm{Cl}_{(\mathfrak{m}:\mathcal{O}'),\Sigma}(\mathcal{O}') & \longrightarrow & \mathrm{Cl}(\mathcal{O}') \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \vdots\,\psi & & \| \\
1 & \longrightarrow & \frac{(\mathcal{O}')^\times}{\mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O})} & \longrightarrow & \frac{(\mathcal{O}'/(\mathfrak{m}:\mathcal{O}'))^\times}{\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/(\mathfrak{m}:\mathcal{O}'))} \times \{\pm 1\}^{|\Sigma|} & \longrightarrow & \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) & \longrightarrow & \mathrm{Cl}(\mathcal{O}') \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \vdots\,\phi & & \| \\
1 & \longrightarrow & \frac{(\mathcal{O}')^\times}{\mathrm{U}_{\mathfrak{m}\mathcal{O}',\Sigma}(\mathcal{O}')} & \longrightarrow & (\mathcal{O}'/\mathfrak{m}\mathcal{O}')^\times \times \{\pm 1\}^{|\Sigma|} & \longrightarrow & \mathrm{Cl}_{\mathfrak{m}\mathcal{O}',\Sigma}(\mathcal{O}') & \longrightarrow & \mathrm{Cl}(\mathcal{O}') \longrightarrow 1
\end{array} \tag{6.9}$$

The horizontal rows are exact sequences from Theorem 5.4 with data as given in the following table.

Theorem 5.4	$(\mathcal{O}, \mathfrak{m}, \Sigma)$	$(\mathcal{O}', \mathfrak{m}', \Sigma')$	$\mathfrak{d}$
top row	$(\mathfrak{m} : \mathcal{O}'), \Sigma)$	$(\mathcal{O}', \mathcal{O}', \emptyset)$	$(\mathfrak{m} : \mathcal{O}')$
middle row	$(\mathcal{O}, \mathfrak{m}, \Sigma)$	$(\mathcal{O}', \mathcal{O}', \emptyset)$	$(\mathfrak{m} : \mathcal{O}')$
bottom row	$(\mathcal{O}', \mathfrak{m}\mathcal{O}', \Sigma)$	$(\mathcal{O}', \mathcal{O}', \emptyset)$	$\mathfrak{m}\mathcal{O}'$

In the second nontrivial column, we have used in all rows that $\mathrm{U}_{\mathcal{O}'}(\mathcal{O}'/\mathfrak{d}) = (\mathcal{O}'/\mathfrak{d})^\times$ and in the top and bottom rows row that $\mathrm{U}_{\mathfrak{d}}(\mathcal{O}/\mathfrak{d}) = \{1\}$.

The vertical maps in the first two nontrivial columns are given by modding out by everything that is 1 modulo $\mathfrak{m}$ (from the top row to the middle) and then by everything that is 1 modulo $\mathfrak{m}\mathcal{O}'$ (from the middle row to the bottom). These maps are well-defined because $(\mathfrak{m} : \mathcal{O}') \subseteq \mathfrak{m} \subseteq \mathfrak{m}\mathcal{O}'$. The commutativity of the leftmost two squares is thus clear. The commutativity of the diagram, excepting the dotted lines, follows by exactness because, on the longer horizontal rectangles, it simply encodes an equality between two zero maps.

The maps denoted by dotted lines are induced, so the whole diagram (6.9) commutes. The upper induced map ψ was described in Section 6.1. The lower induced map ϕ is equal to the map induced

by extension of ideals, as can be seen by commutativity of the diagram and comparison with the "change of order" exact sequence

$$1 \longrightarrow \frac{\mathrm{U}_{\mathfrak{m}\mathcal{O}',\Sigma}(\mathcal{O}')}{\mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O})} \longrightarrow \frac{\mathrm{U}_{\mathfrak{m}\mathcal{O}'}(\mathcal{O}'/(\mathfrak{m}:\mathcal{O}'))}{\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/(\mathfrak{m}:\mathcal{O}'))} \longrightarrow \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) \xrightarrow{\phi} \mathrm{Cl}_{\mathfrak{m}\mathcal{O}',\Sigma}(\mathcal{O}') \longrightarrow 1 \tag{6.10}$$

obtained from Theorem 5.4 (taking $(\mathcal{O},\mathfrak{m},\Sigma) := (\mathcal{O},\mathfrak{m},\Sigma)$, $(\mathcal{O}',\mathfrak{m}',\Sigma') := (\mathcal{O}',\mathfrak{m}\mathcal{O}',\Sigma)$, and $\mathfrak{d} := (\mathfrak{m}:\mathcal{O}')$).

Similarly, the composition $\phi\circ\psi$ fits into the "change of modulus" exact sequence

$$1 \longrightarrow \frac{\mathrm{U}_{\mathfrak{m}\mathcal{O}',\Sigma}(\mathcal{O}')}{\mathrm{U}_{(\mathfrak{m}:\mathcal{O}'),\Sigma}(\mathcal{O}')} \longrightarrow \mathrm{U}_{\mathfrak{m}\mathcal{O}'}(\mathcal{O}'/(\mathfrak{m}:\mathcal{O}')) \longrightarrow \mathrm{Cl}_{(\mathfrak{m}:\mathcal{O}'),\Sigma}(\mathcal{O}') \xrightarrow{\phi\circ\psi} \mathrm{Cl}_{\mathfrak{m}\mathcal{O}',\Sigma}(\mathcal{O}') \longrightarrow 1, \tag{6.11}$$

also a special case of Theorem 5.4 (where we take $(\mathcal{O},\mathfrak{m},\Sigma) := (\mathcal{O}',(\mathfrak{m}:\mathcal{O}'),\Sigma)$, $(\mathcal{O}',\mathfrak{m}',\Sigma') := (\mathcal{O}',\mathfrak{m}\mathcal{O}',\Sigma)$, and $\mathfrak{d} := (\mathfrak{m}:\mathcal{O}')$).

The diagram (6.9) establishes (from its third nontrivial column) the sequence of surjections

$$\mathrm{Cl}_{(\mathfrak{m}:\mathcal{O}'),\Sigma}(\mathcal{O}') \xrightarrow{\psi} \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) \xrightarrow{\phi} \mathrm{Cl}_{\mathfrak{m}\mathcal{O}',\Sigma}(\mathcal{O}').$$

Now by Theorem 6.2 (1), we have the tower of ray class fields of orders

$$\begin{array}{c} H^{\mathcal{O}'}_{(\mathfrak{m}:\mathcal{O}'),\Sigma} \\ \Big| \ker\psi \\ H^{\mathcal{O}}_{\mathfrak{m},\Sigma} \\ \Big| \ker\phi \\ H^{\mathcal{O}'}_{\mathfrak{m}\mathcal{O}',\Sigma} \\ \Big| \\ K \end{array} \tag{6.12}$$

with Galois groups as labelled, thus proving the theorem. □

Proof of Theorem 1.2. This is the special case $\mathcal{O}' = \mathcal{O}_K$ of Theorem 6.5. □

6.5. **Proof of Theorem 1.3.** We will now prove Theorem 1.3, giving a form of Artin reciprocity for a ray class group of an order. The result is obtained from the usual Artin reciprocity law together with properties of the map ψ in eq. (6.3) established earlier in this section.

Proof of Theorem 1.3. Let $H_1 = H^{\mathcal{O}_K}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}$, and let $\mathrm{Art} : \mathrm{Cl}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K) \to \mathrm{Gal}(H_1/K)$ be the (usual) Artin map. Let $\psi : \mathrm{Cl}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K) \to \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ be the map constructed in eq. (6.3). By Lemma 6.4, for any class $[\mathfrak{b}] \in \mathrm{Cl}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K)$, one has $\psi([\mathfrak{b}]) = [\mathrm{con}(\mathfrak{b})]$.

Let $H_0 = H^{\mathcal{O}}_{\mathfrak{m},\Sigma}$. By Definition 6.1 and the Galois correspondence it describes, there is an isomorphism $\mathrm{Art}_{\mathcal{O}}$ making the following diagram commute.

$$\begin{array}{ccc} \mathrm{Cl}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K) & \xrightarrow{\mathrm{Art}}_{\sim} & \mathrm{Gal}(H_1/K) \\ \big\downarrow{\scriptstyle \psi} & & \big\downarrow \\ \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) & \xrightarrow[\sim]{\mathrm{Art}_{\mathcal{O}}} & \mathrm{Gal}(H_0/K) \end{array} \tag{6.13}$$

To give an explicit formula for $\mathrm{Art}_{\mathcal{O}}$, consider any fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ relatively prime to $\mathfrak{f}(\mathcal{O}) \cap \mathfrak{m}$ (or, equivalently, relatively prime to $(\mathfrak{m} : \mathcal{O}_K)$). We compute $\mathrm{Art}_{\mathcal{O}}([\mathfrak{a}])$ by lifting $[\mathfrak{a}]$ to $\mathrm{Cl}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K)$ along ψ. The coprimality condition implies that $\mathrm{con}(\mathfrak{a}\mathcal{O}_K) = \mathrm{con}(\mathrm{ext}(\mathfrak{a})) = \mathfrak{a}$ (by Proposition 3.8), so $\psi([\mathfrak{a}\mathcal{O}_K]) = [\mathrm{con}(\mathrm{ext}(\mathfrak{a}))] = [\mathfrak{a}]$, that is, $[\mathfrak{a}\mathcal{O}_K]$ is a lift of $[\mathfrak{a}]$. Therefore eq. (6.13) gives

$$\mathrm{Art}_{\mathcal{O}}([\mathfrak{a}]) = \mathrm{Art}([\mathfrak{a}\mathcal{O}_K])|_{H_0}\,. \tag{6.14}$$

Now let $\mathfrak{p}$ be any prime ideal of $\mathcal{O}$ relatively prime to $\mathfrak{f}(\mathcal{O}) \cap \mathfrak{m}$, with residue field $\mathcal{O}/\mathfrak{p}$ having characteristic p. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_{H_0}$ lying over $\mathfrak{p}\mathcal{O}_K$. We claim that for all $\alpha \in \mathcal{O}_{H_0}$,

$$\mathrm{Art}_{\mathcal{O}}([\mathfrak{p}])(\alpha) \equiv \alpha^p \pmod{\mathfrak{P}}\,, \tag{6.15}$$

identifying $\mathrm{Art}_{\mathcal{O}}([\mathfrak{p}])$ as a Frobenius automorphism. To see this, let $\mathcal{P}$ be a prime ideal of $\mathcal{O}_{H_1}$ lying over $\mathfrak{P}$. By Artin reciprocity (part (2) of Theorem 6.2; see also Remark 6.3), for any $\alpha \in \mathcal{O}_{H_0}$,

$$\mathrm{Art}_{\mathcal{O}}([\mathfrak{p}])(\alpha) = \mathrm{Art}([\mathfrak{p}\mathcal{O}_K])|_{H_0}(\alpha) \tag{6.16}$$

Now the condition that $\mathfrak{p}$ is relatively prime to $\mathfrak{f}(\mathcal{O}) \cap \mathfrak{m}$ implies that $\mathfrak{p}\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$ by Lemma 3.2 and Proposition 3.8; in addition, $\mathfrak{P}$ and $\mathcal{P}$ are unramified over $\mathfrak{p}\mathcal{O}_K$ because H_0 and H_1 only have ramification over K at the primes dividing $\mathfrak{f}(\mathcal{O}) \cap \mathfrak{m}$ (that is, the primes dividing $(\mathfrak{m} : \mathcal{O}_K)$). Now for any $\beta \in \mathcal{O}_{H_1}$ we have by definition

$$\mathrm{Art}([\mathfrak{p}\mathcal{O}_K])(\beta)) \equiv \beta^p \pmod{\mathcal{P}}\,. \tag{6.17}$$

Applying this congruence with $\beta = \alpha \in \mathcal{O}_{H_0}$, noting that $\mathcal{P} \cap \mathcal{O}_{H_0} = \mathfrak{P}$ and $\alpha^p \in \mathcal{O}_{H_0}$, we may conclude

$$\mathrm{Art}_{\mathcal{O}}([\mathfrak{p}])(\alpha) \equiv \alpha^p \pmod{\mathfrak{P}}\,,$$

proving the claim.

Finally we note that fractional ideals of $\mathcal{O}$ relatively prime to $\mathfrak{f}(\mathcal{O})\cap\mathfrak{m}$ factor into powers of prime ideals relatively prime to $\mathfrak{f}(\mathcal{O}) \cap \mathfrak{m}$, so that the map $\mathrm{Art}_{\mathcal{O}}$ is uniquely determined by eq. (6.15). □

7. Computations of ray class groups of orders

We calculate ray class groups of various orders, using the exact sequences for change of order and modulus. Let $\mathcal{O}$ be an order in a number field K, and let $\rho_1, \ldots, \rho_r$ be the real embeddings of K. Consider a ray class modulus $(\mathfrak{m}, \Sigma)$ for an order $\mathcal{O}$, where $\mathfrak{m}$ is an integral $\mathcal{O}$-ideal and $\Sigma = \{\rho_{k_1}, \ldots, \rho_{k_\ell}\}$. In the following examples, we will abbreviate the pair $(\mathfrak{m}, \Sigma)$ by the formal product $\mathfrak{m}\infty_{k_1}\cdots\infty_{k_\ell}$. We will also denote principal ideals such as $\alpha\mathcal{O}$ by (α). We consider a

second K-order $\mathcal{O}'$ with $\mathcal{O} \subseteq \mathcal{O}'$ and a corresponding modulus $(\mathfrak{m}', \Sigma')$, requiring $\mathfrak{m} \subseteq \mathfrak{m}'$ and $\Sigma' \subseteq \Sigma$. We use the exact sequence of Theorem 5.4,

$$1 \to \frac{\mathrm{U}_{\mathfrak{m}',\Sigma'}(\mathcal{O}')}{\mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O})} \to \frac{\mathrm{U}_{\mathfrak{m}'}(\mathcal{O}'/(\mathfrak{m}:\mathcal{O}'))}{\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/(\mathfrak{m}:\mathcal{O}'))} \times \{\pm 1\}^{|\Sigma \setminus \Sigma'|} \to \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) \to \mathrm{Cl}_{\mathfrak{m}',\Sigma'}(\mathcal{O}') \to 1. \quad (7.1)$$

The following series of examples treats several different orders in the real quadratic field $K = \mathbb{Q}(\sqrt{2})$ and the computation of some of their ray class groups at moduli ramified at prime ideals lying over (7) and ∞. Taken together, the first three examples show that a ray class field of an order can be strictly larger than the compositum of the corresponding ray class field of the maximal order and the ring class field. Using Theorem 1.3, the class number calculations imply

$$H^{\mathbb{Z}[\sqrt{2}]}_{(7)\infty_2} \cdot H^{\mathbb{Z}[2\sqrt{2}]}_{(1)} \subsetneq H^{\mathbb{Z}[2\sqrt{2}]}_{(7)\infty_2}, \quad (7.2)$$

since $\left[H^{\mathbb{Z}[\sqrt{2}]}_{(7)\infty_2} H^{\mathbb{Z}[2\sqrt{2}]}_{(1)} : K\right] \leq \left[H^{\mathbb{Z}[\sqrt{2}]}_{(7)\infty_2} : K\right] \cdot \left[H^{\mathbb{Z}[2\sqrt{2}]}_{(1)} : K\right] = 6$ while $\left[H^{\mathbb{Z}[2\sqrt{2}]}_{(7)\infty_2} : K\right] = 12$. The final example is a calculation in a case where a ring class field is nontrivial.

7.1. **Example 1.** Take $\mathcal{O} = \mathcal{O}' = \mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$, $(\mathfrak{m}', \Sigma') = (\mathcal{O}_K, \emptyset) = (1)$, and $(\mathfrak{m}, \Sigma) = (7\mathcal{O}_K, \{\rho_2\}) = (7)\infty_2$. Then by eq. (7.1).

$$1 \to \frac{\mathbb{Z}[\sqrt{2}]^\times}{\mathrm{U}_{7\infty_2}\big(\mathbb{Z}[\sqrt{2}]\big)} \to \Big(\mathbb{Z}[\sqrt{2}]/(7)\Big)^\times \times \{\pm 1\} \to \mathrm{Cl}_{7\infty_2}\Big(\mathbb{Z}[\sqrt{2}]\Big) \to \mathrm{Cl}\Big(\mathbb{Z}[\sqrt{2}]\Big) \to 1. \quad (7.3)$$

The class group $\mathrm{Cl}\big(\mathbb{Z}[\sqrt{2}]\big) = 1$.. Thus, the ray class group $\mathrm{Cl}_{7,\infty_2}\big(\mathbb{Z}[\sqrt{2}]\big)$ is isomorphic to the previous term in the sequence modulo the image of global units. By the Chinese Remainder Theorem,

$$\Big(\mathbb{Z}[\sqrt{2}]/(7)\Big)^\times \cong \Big(\mathbb{Z}[\sqrt{2}]/(3+\sqrt{2})\Big)^\times \times \Big(\mathbb{Z}[\sqrt{2}]/(3-\sqrt{2})\Big)^\times \quad (7.4)$$

$$\cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}. \quad (7.5)$$

Moreover,

$$\frac{\mathbb{Z}[\sqrt{2}]^\times}{\mathrm{U}_{7\infty_2}\big(\mathbb{Z}[\sqrt{2}]\big)} = \frac{\langle -1, 1+\sqrt{2}\rangle}{\langle (1+\sqrt{2})^6\rangle} \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}. \quad (7.6)$$

Thus, we see that

$$\mathrm{Cl}_{(7)\infty_2}\Big(\mathbb{Z}[\sqrt{2}]\Big) \cong \mathbb{Z}/6\mathbb{Z}. \quad (7.7)$$

7.2. **Example 2.** Take $\mathcal{O} = \mathbb{Z}[2\sqrt{2}]$ and $\mathcal{O}' = \mathbb{Z}[\sqrt{2}]$, $(\mathfrak{m}', \Sigma') = (\mathcal{O}_K, \emptyset) = (1)$, and $(\mathfrak{m}, \Sigma) = (7\mathcal{O}, \infty_2) = (7)\infty_2$. Then eq. (7.1) gives

$$1 \to \frac{\mathbb{Z}[\sqrt{2}]^\times}{\mathrm{U}_{7\infty_2}\big(\mathbb{Z}[2\sqrt{2}]\big)} \to \frac{\left(\frac{\mathbb{Z}[\sqrt{2}]}{(14)}\right)^\times}{\mathrm{U}_7\Big(\frac{\mathbb{Z}[2\sqrt{2}]}{(14\mathbb{Z}+14\sqrt{2}\mathbb{Z})}\Big)} \times \{\pm 1\} \to \mathrm{Cl}_{(7),\infty_2}\Big(\mathbb{Z}[2\sqrt{2}]\Big) \to \mathrm{Cl}\Big(\mathbb{Z}[\sqrt{2}]\Big) \to 1. \quad (7.8)$$

As in the previous example, $\mathrm{Cl}\big(\mathbb{Z}[\sqrt{2}]\big) = 1$, so the ray class group $\mathrm{Cl}_{7\infty_2}\big(\mathbb{Z}[2\sqrt{2}]\big)$ is isomorphic to the previous term in the sequence modulo the image of global units. By the Chinese Remainder Theorem, we have

$$\Big(\mathbb{Z}[\sqrt{2}]/(14)\Big)^\times \cong \Big(\mathbb{Z}[\sqrt{2}]/(3+\sqrt{2})\Big)^\times \times \Big(\mathbb{Z}[\sqrt{2}]/(3-\sqrt{2})\Big)^\times \times \Big(\mathbb{Z}[\sqrt{2}]/(\sqrt{2})^2\Big)^\times \tag{7.9}$$

$$\cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}. \tag{7.10}$$

We also have

$$\mathrm{U}_7\Big(\mathbb{Z}[2\sqrt{2}]/(14\mathbb{Z} + 14\sqrt{2}\mathbb{Z})\Big) = 1 \tag{7.11}$$

and

$$\frac{\mathbb{Z}[\sqrt{2}]^\times}{\mathrm{U}_{7\infty_2}\big(\mathbb{Z}[2\sqrt{2}]\big)} = \frac{\langle -1, 1+\sqrt{2}\rangle}{\langle (1+\sqrt{2})^6\rangle} \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}. \tag{7.12}$$

We see that

$$\Big|\mathrm{Cl}_{7\infty_2}\Big(\mathbb{Z}[2\sqrt{2}]\Big)\Big| = 12, \tag{7.13}$$

With more careful accounting, we can obtain an isomorphism

$$\mathrm{Cl}_{7\infty_2}\Big(\mathbb{Z}[2\sqrt{2}]\Big) \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}. \tag{7.14}$$

7.3. **Example 3.** We compute $\mathrm{Cl}_{7\infty_2}\big(\mathbb{Z}[2\sqrt{2}]\big)$ a different way. Take $\mathcal{O} = \mathcal{O}' = \mathbb{Z}[2\sqrt{2}]$, $(\mathfrak{m}', \Sigma') = (1)$, and $(\mathfrak{m}, \Sigma) = (7)\infty_2$. Then

$$1 \to \frac{\mathbb{Z}[2\sqrt{2}]^\times}{\mathrm{U}_{7\infty_2}\big(\mathbb{Z}[2\sqrt{2}]\big)} \to \Big(\mathbb{Z}[2\sqrt{2}]/(7)\Big)^\times \times \{\pm 1\} \to \mathrm{Cl}_{7\infty_2}\Big(\mathbb{Z}[2\sqrt{2}]\Big) \to \mathrm{Cl}\Big(\mathbb{Z}[2\sqrt{2}]\Big) \to 1. \tag{7.15}$$

The ring class group $\mathrm{Cl}\big(\mathbb{Z}[2\sqrt{2}]\big) = 1$. By the Chinese Remainder Theorem,

$$\Big(\mathbb{Z}[2\sqrt{2}]/(7)\Big)^\times \cong \Big(\mathbb{Z}[2\sqrt{2}]/(1+2\sqrt{2})\Big)^\times \times \Big(\mathbb{Z}[2\sqrt{2}]/(1-2\sqrt{2})\Big)^\times \tag{7.16}$$

$$\cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}. \tag{7.17}$$

The quotient of global unit groups is

$$\frac{\mathbb{Z}[2\sqrt{2}]^\times}{\mathrm{U}_{7\infty_2}\big(\mathbb{Z}[2\sqrt{2}]\big)} = \frac{\langle -1, (1+\sqrt{2})^2\rangle}{\langle (1+\sqrt{2})^6\rangle} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}. \tag{7.18}$$

It follows that

$$\mathrm{Cl}_{7\infty_2}\Big(\mathbb{Z}[2\sqrt{2}]\Big) \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}. \tag{7.19}$$

7.4. **Example 4.** Take $\mathcal{O} = \mathcal{O}' = \mathbb{Z}[5\sqrt{2}]$, $(\mathfrak{m}', \Sigma') = (1)$, and $(\mathfrak{m}, \Sigma) = (7)\infty_2$. Then

$$1 \to \frac{\mathbb{Z}[5\sqrt{2}]^\times}{\mathrm{U}_{7\infty_2}\big(\mathbb{Z}[5\sqrt{2}]\big)} \to \Big(\mathbb{Z}[5\sqrt{2}]/(7)\Big)^\times \times \{\pm 1\} \to \mathrm{Cl}_{7\infty_2}\Big(\mathbb{Z}[5\sqrt{2}]\Big) \to \mathrm{Cl}\Big(\mathbb{Z}[5\sqrt{2}]\Big) \to 1. \tag{7.20}$$

In a similar method to the above examples (e.g., by another change of order calculation), we can compute

$$\mathrm{Cl}\Big(\mathbb{Z}[5\sqrt{2}]\Big) = \mathrm{Cl}_{(1)}\Big(\mathbb{Z}[5\sqrt{2}]\Big) \cong \mathbb{Z}/2\mathbb{Z}. \tag{7.21}$$

The ring class number is 2. As a consequence, by Theorem 1.3, the ring class field for $\mathbb{Z}[5\sqrt{2}]$ is a quadratic extension of K, so is a degree 4 extension of $\mathbb{Q}$. We also have

$$\Big(\mathbb{Z}[5\sqrt{2}]/(7)\Big)^{\times} \times \{\pm 1\} \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \tag{7.22}$$

$$\frac{\mathbb{Z}[5\sqrt{2}]^{\times}}{\mathrm{U}_{7\infty_2}\big(\mathbb{Z}[5\sqrt{2}]\big)} = \frac{\langle -1, (1+\sqrt{2})^3\rangle}{\langle (1+\sqrt{2})^6\rangle} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}. \tag{7.23}$$

We see that

$$\Big|\mathrm{Cl}_{7\infty_2}\Big(\mathbb{Z}[5\sqrt{2}]\Big)\Big| = \frac{(6\cdot 6\cdot 2)(2)}{2\cdot 2} = 36. \tag{7.24}$$

To determine the ray class group structure, it would be necessary to compute the maps in the exact sequence.

8. Concluding remarks

The main results of this paper assigned ray class fields to data associated to invertible ray class groups of orders. The main results concerned class fields described by splitting of primes in the invertible ray class groups of the orders. We now consider possible extensions of these results to parallel other results in class field theory of maximal orders.

There are several other aspects of class field theory, specified by the main theorems of class field theory as listed by Hasse [18], that might have analogues in the ray class field theory of orders.

(1) *Norms of ideals in orders.* The Takagi class field theory has an interpretation of ray class groups in which the kernels of some group maps involve groups generated by norms of ideals. There is a natural way to define norms of integral ideals $\mathfrak{a}$ in orders, as $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$. Norms of fractional ideals are discussed in Appendix B. One difficulty that arises is that norms of non-invertible ideals are not multiplicative, in general.

(2) *Zeta functions of orders.* We can associate zeta functions and L-functions to orders. There is a zeta function whose terms involve norms of invertible integral ideals of orders. There is another zeta function obtained by summing over norms of a larger set of ideals of an order, including non-invertible ideals. The uniqueness of primary decomposition (Proposition 2.2) implies that both of these zeta functions have Euler products; the latter one will have unusual factors at the finite set of maximal ideals of $\mathcal{O}$ that contain the conductor ideal $\mathfrak{f}(\mathcal{O})$. If we allow non-invertible ideals, then the ray class group is enlarged to become a *ray class monoid*. Several ray class monoid structures, which have nontrivial idempotents, are described in Appendix A. One can define L-functions of orders, associated to characters of ray class groups of orders. If one allows non-invertible ideals, then one can also allow characters of ray class monoids (see [9, 10, 19, 27–29]).

This paper expressed results using the framework classical algebraic number theory, using commutative ring theory. One can ask whether there might be an adelic treatment of ray class field theory for orders of a number fields. Certainly localization at each maximal ideal of the order is possible. There may however be difficulties in defining the adelic factors at the places dividing the conductor ideal of the order. It is an intreresting question what would replace the product formula for the elements of the field, given in terms of the primary decomposition of the order, since norms fail to be multiplicative in general.

Acknowledgments. The first author was partially supported by the University of Bristol, the Heilbronn Institute for Mathematical Research, and Purdue University, and he thanks Trevor Wooley for support and for helpful mathematical conversations. The second author was partially supported by NSF grant DMS-1701576.

APPENDIX A. RAY CLASS MONOIDS

In the definition of the ray class group, we considered only *invertible* ideals *coprime to the ray class modulus*. There are several ways to relax these conditions that give the structure of a monoid (semigroup with identity) containing the ray class group as a submonoid. In this section, we describe five different ray class monoids (including the ray class group itself); they will be denoted and named as follows.

Monoid	**Name**
$\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$	ray class group
$\mathrm{Clm}^{\flat}_{\mathfrak{m},\Sigma}(\mathcal{O})$	potentially-invertible ray class monoid
$\mathrm{Clm}_{\mathfrak{m},\Sigma}(\mathcal{O})$	non-invertible ray class monoid
$\overline{\mathrm{Clm}}^{*}_{\mathfrak{m},\Sigma}(\mathcal{O})$	non-coprime invertible ray class monoid
$\overline{\mathrm{Clm}}^{\flat}_{\mathfrak{m},\Sigma}(\mathcal{O})$	non-coprime potentially-invertible ray class monoid

These monoids are related by the following inclusions.

$$\begin{array}{ccccc} \overline{\mathrm{Clm}}^{*}_{\mathfrak{m},\Sigma}(\mathcal{O}) & \hookrightarrow & \overline{\mathrm{Clm}}^{\flat}_{\mathfrak{m},\Sigma}(\mathcal{O}) & & \\ \uparrow & & \uparrow & & \\ \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) & \hookrightarrow & \mathrm{Clm}^{\flat}_{\mathfrak{m},\Sigma}(\mathcal{O}) & \hookrightarrow & \mathrm{Clm}_{\mathfrak{m},\Sigma}(\mathcal{O}) \end{array} \tag{A.1}$$

Recall the definition of the ray class group:

$$\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) = \frac{\mathrm{J}_{\mathfrak{m}}(\mathcal{O})}{\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})}. \tag{A.2}$$

The easiest way to relax this definition is to remove the invertibility condition. For any order $\mathcal{O}$ in a number field K, recall that we've defined

$$\mathrm{J}(\mathcal{O}) := \{\text{nonzero fractional ideals of } \mathcal{O}\}, \text{ and} \tag{A.3}$$

$$\mathrm{J}_{\mathfrak{m}}(\mathcal{O}) := \{\text{nonzero fractional ideals of } \mathcal{O} \text{ coprime to } \mathfrak{m}\}. \tag{A.4}$$

This $\mathrm{J}(\mathcal{O})$ is a commutative monoid rather than a group. By modding out by the submonoid $\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})$, we obtain a quotient monoid.

Definition A.1. The *non-invertible ray class monoid* is defined to be

$$\mathrm{Clm}_{\mathfrak{m},\Sigma}(\mathcal{O}) = \frac{\mathrm{J}_{\mathfrak{m}}(\mathcal{O})}{\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})}. \tag{A.5}$$

Set $\mathrm{Clm}(\mathcal{O}) = \mathrm{Clm}_{\mathcal{O},\emptyset}(\mathcal{O})$.

The structure of $\mathrm{Clm}_{\mathfrak{m},\Sigma}(\mathcal{O})$, or even $\mathrm{Clm}(\mathcal{O})$, is difficult to describe in general. It may contain elements arising from ideals that are not invertible in any order, and such elements lead to pathological behavior (see Zanardo and Zannier [41]). However, there is a submonoid of "potentially invertible" ideals that is well-behaved and admits a decomposition into groups attached to intermediate orders.

Definition A.2. We say that an fractional ideal $\mathfrak{a} \in \mathrm{J}(\mathcal{O})$ is *potentially invertible* if $\mathfrak{a} \in \mathrm{J}^*(\mathcal{O}')$ for some order $\mathcal{O}'$ with $\mathcal{O} \subseteq \mathcal{O}' \subseteq \mathcal{O}_K$. Let

$$\mathrm{J}^\flat(\mathcal{O}) := \{\text{potentially inverible fractional ideals of } \mathcal{O}\}, \text{ and} \tag{A.6}$$

$$\mathrm{J}^\flat_{\mathfrak{m}}(\mathcal{O}) := \{\text{potentially invertible fractional ideals of } \mathcal{O} \text{ coprime to } \mathfrak{m}\}. \tag{A.7}$$

The *potentially-invertible ray class monoid* is defined to be

$$\mathrm{Clm}^\flat_{\mathfrak{m},\Sigma}(\mathcal{O}) = \frac{\mathrm{J}^\flat_{\mathfrak{m}}(\mathcal{O})}{\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})}. \tag{A.8}$$

Set $\mathrm{Clm}^\flat(\mathcal{O}) = \mathrm{Clm}^\flat_{\mathcal{O},\emptyset}(\mathcal{O})$.

To express the niceness of the structure of the potentially invertible ray class monoid, we introduce some terminology. The following definition is paraphrased from [17].

Definition A.3. Let M be a commutative semigroup, and let $\mathrm{Id}(M) = \{e \in M : e^2 = e\}$. For each $e \in \mathrm{Id}(M)$, let $M_e = \{x \in M : xe = x \text{ and } xy = e \text{ for some } y \in M\}$. (It is straightforward to check that each M_e is a group and that the M_e are disjoint.) Then, M is called a *Clifford semigroup* (also called a completely regular inverse semigroup) if

$$M = \bigsqcup_{e \in \mathrm{Id}(M)} M_e. \tag{A.9}$$

If in addition M has a (global) identity element, it is called a *Clifford monoid*.

Proposition A.4. *The potentially-invertible ray class monoid* $\mathrm{Clm}^\flat_{\mathfrak{m},\Sigma}(\mathcal{O})$ *has the structure of a Clifford monoid. Precisely,*

$$\mathrm{Clm}^\flat_{\mathfrak{m},\Sigma}(\mathcal{O}) \cong \bigsqcup_{\mathcal{O} \subseteq \mathcal{O}' \subseteq \mathcal{O}_K} \frac{\mathrm{J}^*_{\mathfrak{m}\mathcal{O}'}(\mathcal{O}')}{\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})\mathcal{O}'}, \tag{A.10}$$

where multiplication of $[\mathfrak{a}] \in \frac{\mathrm{J}^*_{\mathfrak{m}\mathcal{O}'}(\mathcal{O}')}{\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})\mathcal{O}'}$ *and* $[\mathfrak{b}] \in \frac{\mathrm{J}^*_{\mathfrak{m}\mathcal{O}''}(\mathcal{O}'')}{\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})\mathcal{O}''}$ *is given by* $[\mathfrak{a}][\mathfrak{b}] = [\mathfrak{a}\mathfrak{b}\mathcal{O}'''] = [\mathfrak{a}\mathcal{O}'''][\mathfrak{b}\mathcal{O}'''] \text{ in } \frac{\mathrm{J}^*_{\mathfrak{m}\mathcal{O}'''}(\mathcal{O}''')}{\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})\mathcal{O}'''}$*, with* $\mathcal{O}''' = \mathcal{O}'\mathcal{O}''$*. In particular, if* $\mathfrak{m} = \mathcal{O}$*, then*

$$\mathrm{Clm}^\flat_{\mathcal{O},\Sigma}(\mathcal{O}) \cong \bigsqcup_{\mathcal{O}\subseteq\mathcal{O}'\subseteq\mathcal{O}_K} \mathrm{Cl}_{\mathcal{O}',\Sigma}(\mathcal{O}'). \tag{A.11}$$

Proof. Let $M = \mathrm{Clm}^\flat_{\mathfrak{m},\Sigma}(\mathcal{O})$. Suppose $[\mathfrak{e}] \in \mathrm{Id}(M)$, using the notation from Definition A.3. Since $\mathfrak{e}$ is potentially invertible, there is some order $\mathcal{O}'$ with $\mathcal{O} \subseteq \mathcal{O}' \subseteq \mathcal{O}_K$ such that $\mathfrak{e}$ is an invertible $\mathcal{O}'$-ideal, and there is some $\mathcal{O}'$-ideal $\mathfrak{d}$ such that $\mathfrak{e}\mathfrak{d} = \mathcal{O}'$. Thus, $\mathfrak{e} = \mathfrak{e}\mathcal{O}' = \mathfrak{e}^2\mathfrak{d} = \mathfrak{e}\mathfrak{d} = \mathcal{O}'$. So

$$\mathrm{Id}(M) = \{\text{orders } \mathcal{O}' \subseteq K : \mathcal{O} \subseteq \mathcal{O}' \subseteq \mathcal{O}_K\}. \tag{A.12}$$

Moreover,

$$\begin{aligned} M_{\mathcal{O}'} &= \{[\mathfrak{a}] \in M : \mathfrak{a}\mathcal{O}' = \mathfrak{a} \text{ and } \mathfrak{a}\mathfrak{b} = \mathcal{O}' \text{ for some } \mathfrak{b} \in M\} && \text{(A.13)}\\ &= \{[\mathfrak{a}] \in M : \mathfrak{a} \text{ is an invertible } \mathcal{O}'\text{-ideal}\} && \text{(A.14)}\\ &= \frac{\mathrm{J}_{\mathfrak{m}}(\mathcal{O}) \cap \mathrm{J}^*(\mathcal{O}')}{\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})\mathcal{O}'} && \text{(A.15)}\\ &= \frac{\mathrm{J}^*_{\mathfrak{m}\mathcal{O}'}(\mathcal{O}')}{\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})\mathcal{O}'}. && \text{(A.16)} \end{aligned}$$

By the definition of the potentially-invertible ray class monoid, every element is in some $M_{\mathcal{O}'}$, so eq. (A.10) holds.

Finally, in the case $\mathfrak{m} = \mathcal{O}$, we have $\mathrm{P}_{\mathcal{O},\Sigma}(\mathcal{O})\mathcal{O}' = \mathrm{P}_{\mathcal{O}',\Sigma}(\mathcal{O}')$ because the congruence condition holds trivially. Hence, we obtain eq. (A.11). □

The order product $\mathcal{O}'\mathcal{O}''$, defined like an ideal product and used in the above proposition, is the smallest order containing $\mathcal{O}'$ and $\mathcal{O}''$. In many familiar cases, such as real quadratic orders, it is equal to the lattice sum $\mathcal{O}' + \mathcal{O}''$. It is clear that $\mathcal{O}' + \mathcal{O}'' \subseteq \mathcal{O}'\mathcal{O}''$. However, the following example shows that $\mathcal{O}' + \mathcal{O}''$ is not always an order and may be strictly smaller than $\mathcal{O}'\mathcal{O}''$.

Example A.5. Let $K = \mathbb{Q}(2^{1/7})$, and consider the following two orders in K.

$$\mathcal{O}' = \mathbb{Z}[2^{2/7}] = \mathbb{Z} + 2^{2/7}\mathbb{Z} + 2^{4/7}\mathbb{Z} + 2^{6/7}\mathbb{Z} + 2^{8/7}\mathbb{Z} + 2^{10/7}\mathbb{Z} + 2^{12/7}\mathbb{Z}; \tag{A.17}$$

$$\mathcal{O}'' = \mathbb{Z}[2^{3/7}] = \mathbb{Z} + 2^{9/7}\mathbb{Z} + 2^{18/7}\mathbb{Z} + 2^{6/7}\mathbb{Z} + 2^{15/7}\mathbb{Z} + 2^{3/7}\mathbb{Z} + 2^{12/7}\mathbb{Z}. \tag{A.18}$$

Then, the lattice sum of these orders is

$$\mathcal{O}' + \mathcal{O}'' = \mathbb{Z} + 2^{2/7}\mathbb{Z} + 2^{4/7}\mathbb{Z} + 2^{6/7}\mathbb{Z} + 2^{8/7}\mathbb{Z} + 2^{3/7}\mathbb{Z} + 2^{12/7}\mathbb{Z}. \tag{A.19}$$

In particular, $2^{2/7}, 2^{3/7} \in \mathcal{O}' + \mathcal{O}''$, but their product $2^{5/7} \notin \mathcal{O}' + \mathcal{O}''$. So $\mathcal{O}' + \mathcal{O}''$ is not an order. The product of orders is equal to

$$\mathcal{O}'\mathcal{O}'' = \mathbb{Z} + 2^{2/7}\mathbb{Z} + 2^{4/7}\mathbb{Z} + 2^{6/7}\mathbb{Z} + 2^{8/7}\mathbb{Z} + 2^{3/7}\mathbb{Z} + 2^{5/7}\mathbb{Z}. \tag{A.20}$$

Removing the coprimality conditions is more delicate than removing the invertibility conditions. The monoid $\frac{\mathrm{J}^*(\mathcal{O})}{\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})}$ is infinite for $\mathfrak{m} \neq \mathcal{O}$ and is not the monoid we want. It becomes more apparent how to remove the coprimality conditions in a sensible way by first rewriting the ray class group (and the potentially invertible ray class monoid) in terms of integral ideals.

Proposition A.6. *The ray class group and the potentially-invertible ray class monoid may be written as quotient monoids of integral ideals, as follows:*

$$\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) \cong \frac{\mathrm{I}^*_{\mathfrak{m}}(\mathcal{O})}{\sim_{\mathfrak{m},\Sigma}} \text{ and} \tag{A.21}$$

$$\mathrm{Clm}^{\flat}_{\mathfrak{m},\Sigma}(\mathcal{O}) \cong \frac{\mathrm{I}^{\flat}_{\mathfrak{m}}(\mathcal{O})}{\sim_{\mathfrak{m},\Sigma}}, \tag{A.22}$$

where

$$\mathfrak{a} \sim_{\mathfrak{m},\Sigma} \mathfrak{b} \iff \begin{array}{c} \exists \mathfrak{c} \in \mathrm{J}^*_{\mathfrak{m}}(\mathcal{O}) \text{ and } \alpha, \beta \in \mathcal{O}[S_{\mathfrak{m}}^{-1}] \text{ such that } \mathfrak{c}\mathfrak{a} = \alpha\mathcal{O}', \mathfrak{c}\mathfrak{b} = \beta\mathcal{O}', \\ \mathcal{O}' \text{ a } K\text{-order, } \alpha \equiv \beta \pmod{\mathfrak{m}}, \mathrm{sgn}(\rho(\alpha)) = \mathrm{sgn}(\rho(\beta)) \text{ for all } \rho \in \Sigma. \end{array} \tag{A.23}$$

Proof. Consider the map $\psi : \mathrm{I}^*_{\mathfrak{m}}(\mathcal{O}) \to \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ given as the composition of the inclusion map of integral ideals into fractional ideals and the quotient map to the ray class group:

$$\mathrm{I}^*_{\mathfrak{m}}(\mathcal{O}) \hookrightarrow \mathrm{J}^*_{\mathfrak{m}}(\mathcal{O}) \twoheadrightarrow \frac{\mathrm{J}^*_{\mathfrak{m}}(\mathcal{O})}{\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})} = \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}). \tag{A.24}$$

If $\mathfrak{d} = \mathfrak{a}\mathfrak{b}^{-1} \in \mathrm{J}^*_{\mathfrak{m}}(\mathcal{O})$ for $\mathfrak{a}, \mathfrak{b} \in \mathrm{I}^*_{\mathfrak{m}}(\mathcal{O})$, then there exists some nonzero $\beta \in \mathfrak{b}$ such that $\beta \equiv 1 \pmod{\mathfrak{m}}$ and $\rho(\beta) > 0$ for $\rho \in \Sigma$, so $\beta\mathfrak{d} \in \mathrm{I}^*_{\mathfrak{m}}(\mathcal{O})$ and $\beta\mathcal{O} \in \mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})$. Thus, every ray ideal class in $\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ is represented by an integral ideal, so the map ψ is surjective.

Suppose $\mathfrak{a}, \mathfrak{b} \in \mathrm{I}^*_{\mathfrak{m}}(\mathcal{O})$; we will show that $\psi(\mathfrak{a}) = \psi(\mathfrak{b})$ if and only if $\mathfrak{a} \sim_{\mathfrak{m},\Sigma} \mathfrak{b}$. Note that the order $\mathcal{O}'$ appearing in the definition of $\sim_{\mathfrak{m},\Sigma}$ is necessarily equal to the multiplier ring of both $\mathfrak{a}$ and $\mathfrak{b}$; therefore, in the case when $\mathfrak{a}, \mathfrak{b} \in \mathrm{I}^*_{\mathfrak{m}}(\mathcal{O})$, we have $\mathcal{O}' = \mathcal{O}$.

First, suppose $\psi(\mathfrak{a}) = \psi(\mathfrak{b})$. Then, $\mathfrak{a}\mathfrak{b}^{-1} = \mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})$, so there exists $\gamma \equiv 1 \pmod{\mathfrak{m}}$, $\rho(\gamma) > 0$ for all $\rho \in \Sigma$, such that $\mathfrak{a} = \gamma\mathfrak{b}$. Let $\mathfrak{c} = \alpha\mathfrak{a}^{-1}$ for some $\alpha \in \mathfrak{a} \cap \delta\mathcal{O}$. Then, $\mathfrak{c}\mathfrak{a} = \alpha\mathcal{O}$ and $\mathfrak{c}\mathfrak{b} = \alpha\delta^{-1}\mathcal{O}$, α and $\alpha\delta^{-1}$ are both in $\mathcal{O} \subseteq \mathcal{O}[S_{\mathfrak{m}}^{-1}]$, $\alpha \equiv \alpha\delta^{-1} \pmod{\mathfrak{m}}$, and $\mathrm{sgn}(\rho(\alpha)) = \mathrm{sgn}(\rho(\delta^{-1}\alpha)) > 0$ for all $\rho \in \Sigma$. So $\mathfrak{a} \sim_{\mathfrak{m},\Sigma} \mathfrak{b}$.

Conversely, suppose $\mathfrak{a} \sim_{\mathfrak{m},\Sigma} \mathfrak{b}$. Then, there exists $\mathfrak{c} \in \mathrm{J}^*_{\mathfrak{m}}(\mathcal{O})$ and $\alpha, \beta \in \mathcal{O}[S_{\mathfrak{m}}^{-1}]$ such that $\mathfrak{c}\mathfrak{a} = \alpha\mathcal{O}'$ and $\mathfrak{c}\mathfrak{b} = \beta\mathcal{O}'$, with $\alpha \equiv \beta \pmod{\mathfrak{m}}$ and $\mathrm{sgn}(\rho(\alpha)) = \mathrm{sgn}(\rho(\beta))$ for all $\rho \in \Sigma$. It follows that $\mathfrak{a}\mathfrak{b}^{-1} = \alpha\beta^{-1}\mathcal{O}$ and $\alpha\beta^{-1}\mathcal{O} \in \mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})$. Thus, $\psi(\mathfrak{a}) = \psi(\mathfrak{b})$.

We have thus proven the proposition in the case of the ray class group. In the case of the potentially invertible ray class monoid, the result follows from the result for the ray class group along with Proposition A.4. □

Definition A.7. We define the sets $\overline{\mathrm{J}}^*_{\mathfrak{m}}(\mathcal{O})$ (resp. $\overline{\mathrm{J}}^\flat_{\mathfrak{m}}(\mathcal{O})$) of *semilocally integral (at* $\mathfrak{m}$*)* ideals that are invertible and potentially invertible, respectively.

$$\overline{\mathrm{J}}^*_{\mathfrak{m}}(\mathcal{O}) = \{\mathfrak{a} \in \mathrm{J}^*(\mathcal{O}) : \mathfrak{a}\mathcal{O}[S_{\mathfrak{m}}^{-1}] \subseteq \mathcal{O}[S_{\mathfrak{m}}^{-1}]\}. \tag{A.25}$$

$$\overline{\mathrm{J}}^\flat_{\mathfrak{m}}(\mathcal{O}) = \{\mathfrak{a} \in \mathrm{J}^\flat(\mathcal{O}) : \mathfrak{a}\mathcal{O}[S_{\mathfrak{m}}^{-1}] \subseteq \mathcal{O}[S_{\mathfrak{m}}^{-1}]\}. \tag{A.26}$$

In both cases, the condition that $\mathfrak{a}\mathcal{O}[S_{\mathfrak{m}}^{-1}] \subseteq \mathcal{O}[S_{\mathfrak{m}}^{-1}]$ is equivalent to the condition that $\mathfrak{a}\mathcal{O}_{\mathfrak{p}} \subseteq \mathcal{O}_{\mathfrak{p}}$ for all nonzero prime ideals $\mathfrak{p} \subseteq \mathfrak{m}$; we call this condition *semilocal integrality at* $\mathfrak{m}$.

Crucially, ideals that are semilocally integral at $\mathfrak{m}$ need not be coprime to $\mathfrak{m}$; using ideals that are not coprime to $\mathfrak{m}$ will allow us to define a ray class monoid encoding ray class data from both $\mathfrak{m}$ and its proper divisors.

Definition A.8. Consider the equivalence relation $\sim_{\mathfrak{m},\Sigma}$ on $\overline{\mathrm{J}}^\flat_{\mathfrak{m}}(\mathcal{O})$ defined by

$$\mathfrak{a} \sim_{\mathfrak{m},\Sigma} \mathfrak{b} \iff \begin{array}{c} \exists \mathfrak{c} \in \mathrm{J}^*_{\mathfrak{m}}(\mathcal{O}) \text{ and } \alpha, \beta \in \mathcal{O}[S_{\mathfrak{m}}^{-1}] \text{ such that } \mathfrak{c}\mathfrak{a} = \alpha\mathcal{O}', \mathfrak{c}\mathfrak{b} = \beta\mathcal{O}', \\ \mathcal{O}' \text{ a } K\text{-order}, \alpha \equiv \beta \pmod{\mathfrak{m}}, \operatorname{sgn}(\rho(\alpha)) = \operatorname{sgn}(\rho(\beta)) \text{ for all } \rho \in \Sigma. \end{array} \tag{A.27}$$

The *non-coprime invertible ray class monoid* is

$$\overline{\mathrm{Clm}}^*_{\mathfrak{m},\Sigma}(\mathcal{O}) = \frac{\overline{\mathrm{J}}^*_{\mathfrak{m}}(\mathcal{O})}{\sim_{\mathfrak{m},\Sigma}}. \tag{A.28}$$

The *non-coprime principally-invertible ray class monoid* is

$$\overline{\mathrm{Clm}}^\flat_{\mathfrak{m},\Sigma}(\mathcal{O}) = \frac{\overline{\mathrm{J}}^\flat_{\mathfrak{m}}(\mathcal{O})}{\sim_{\mathfrak{m},\Sigma}}. \tag{A.29}$$

The monoid $\overline{\mathrm{Clm}}^*_{\mathfrak{m},\Sigma}(\mathcal{O})$ is not generally a Clifford monoid (and, therefore, neither is the larger $\overline{\mathrm{Clm}}^\flat_{\mathfrak{m},\Sigma}(\mathcal{O})$).

Example A.9. If $\mathfrak{m} = \pi^2\mathcal{O}$ for a principal prime ideal $\pi\mathcal{O}$, then the only idempotents in $M = \overline{\mathrm{Clm}}^*_{\mathfrak{m},\Sigma}(\mathcal{O})$ are $[\mathcal{O}]$ and $[\pi^2\mathcal{O}]$, and $[\pi\mathcal{O}] \notin M_e$ for any idempotent e. Thus, M is not a Clifford monoid.

A simple case of this phenomenon is the case $\mathcal{O} = \mathbb{Z}$ and $\mathfrak{m} = p^2\mathbb{Z}$, in which case $M \cong (\mathbb{Z}/p^2\mathbb{Z}, \cdot)$.

To facilitate describing the structure of the monoid $\overline{\mathrm{Clm}}^*_{\mathfrak{m},\Sigma}(\mathcal{O})$, we define a notion of an exact sequence of commutative monoids. There is no standard definition of such (see the discussion in [36]); we adopt a definition suited for our application. As in an exact sequence of abelian groups, we want the fibers of the latter map to be cosets of the image of the former; to guarantee this property, we impose it directly, because it is not sufficient to say that the image of the former map is the kernel of the latter.

Definition A.10. A sequence

$$\cdots \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to \cdots \tag{A.30}$$

of commutative monoids with homomorphisms between them is *exact at* B if every nonempty preimage of an element C under β is a coset of an image of α; that is, if for all $c \in C$, either $\beta^{-1}(c) = \emptyset$, or there exists $b \in B$ such that

$$b\alpha(A) = \beta^{-1}(c). \tag{A.31}$$

A sequence that is exact at all objects with an in-arrow and out-arrow is simply called *exact*.

It should be possible to give analogues of the exact sequence in Theorem 5.4 for ray class monoids. For now, we focus on "resolving" the map from $\overline{\mathrm{Clm}}^*_{\mathfrak{m},\Sigma}(\mathcal{O})$ to $\mathrm{Cl}(\mathcal{O})$ in order to understand the structure of $\overline{\mathrm{Clm}}^*_{\mathfrak{m},\Sigma}(\mathcal{O})$.

Proposition A.11. *Let $\phi : \overline{\mathrm{Clm}}^*_{\mathfrak{m},\Sigma}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O})$ be the map given by $\phi([\mathfrak{b}]) = [\mathfrak{b}]$. Then, there is an exact sequence of monoids*

$$(\mathcal{O}/\mathfrak{m}, \cdot) \times \{\pm 1\}^{\Sigma} \to \overline{\mathrm{Clm}}^*_{\mathfrak{m},\Sigma}(\mathcal{O}) \xrightarrow{\phi} \mathrm{Cl}(\mathcal{O}) \to 1. \tag{A.32}$$

Proof. Exactness at $\mathrm{Cl}(\mathcal{O})$ is equivalent to the surjectivity of ϕ. By Proposition A.6, every class in $\mathrm{Cl}(\mathcal{O})$ is represented by some invertible integral ideal $\mathfrak{b} \in \mathrm{I}^*(\mathcal{O})$, and $\mathrm{I}^*(\mathcal{O}) \subseteq \overline{\mathrm{J}}^*_{\mathfrak{m}}(\mathcal{O})$, so ϕ is surjective.

Define the map $\psi : (\mathcal{O}/\mathfrak{m}, \cdot) \times \{\pm 1\}^{\Sigma} \to \overline{\mathrm{Clm}}^*_{\mathfrak{m},\Sigma}(\mathcal{O})$ by

$$\psi(\overline{\alpha}, \epsilon) = [\alpha\mathcal{O}] \text{ where } \alpha \equiv \overline{\alpha} \pmod{\mathfrak{m}} \text{ and } \mathrm{sgn}(\rho(\alpha)) = \epsilon_\rho. \tag{A.33}$$

This map is well-defined because:

(i) For any pair $(\overline{\alpha}, \epsilon)$, the set $(\overline{\alpha} + \mathfrak{m}) \cap \{\alpha \in \mathcal{O} : \mathrm{sgn}(\rho(\alpha)) = \epsilon_\rho\} \neq \emptyset$.

(ii) If $\alpha_1, \alpha_2 \in \mathcal{O}\backslash\{0\}$, $\alpha_1 \equiv \alpha_2 \pmod{\mathfrak{m}}$, and $\mathrm{sgn}(\rho(\alpha_1)) = \mathrm{sgn}(\rho(\alpha_2))$, then $[\alpha_1\mathcal{O}] = [\alpha_2\mathcal{O}]$ in $\overline{\mathrm{Clm}}^*_{\mathfrak{m},\Sigma}(\mathcal{O})$.

To prove exactness at $\overline{\mathrm{Clm}}^*_{\mathfrak{m},\Sigma}(\mathcal{O})$, consider a class $\mathfrak{B} \in \mathrm{Cl}(\mathcal{O})$. By Lemma 4.12, we may write $\mathfrak{B} = [\mathfrak{b}]$ for some $\mathfrak{b} \in \mathrm{J}^*_{\mathfrak{m}}(\mathcal{O})$. Clearly $\phi([\alpha\mathfrak{b}]) = \mathfrak{B}$ for any $\alpha \in \mathcal{O}[S_{\mathfrak{m}}^{-1}] \setminus \{0\}$, so $\{[\alpha\mathfrak{b}] : \alpha \in \mathcal{O}[S_{\mathfrak{m}}^{-1}] \setminus \{0\}\} \subseteq \phi^{-1}(\mathfrak{B})$. On the other hand, suppose $\mathfrak{a} \in \overline{\mathrm{J}}^*_{\mathfrak{m}}(\mathcal{O})$ such that $\phi([\mathfrak{a}]) = \mathfrak{B}$. Then $\mathfrak{a}$ is equivalent to $\mathfrak{b}$ in $\mathrm{Cl}(\mathcal{O})$, so $\mathfrak{a} = \alpha\mathfrak{b}$ for some $\alpha \in K^\times$. Moreover, $\alpha\mathcal{O} = \mathfrak{a}\mathfrak{b}^{-1} \in \overline{\mathrm{J}}^*_{\mathfrak{m}}(\mathcal{O})$, that is, $\alpha\mathcal{O}$ is semilocally integral at $\mathfrak{m}$, so $\alpha \in \mathcal{O}[S_{\mathfrak{m}}^{-1}]\setminus\{0\}$. Therefore, $\{[\alpha\mathfrak{b}] : \alpha \in \mathcal{O}[S_{\mathfrak{m}}^{-1}]\setminus\{0\}\} = \phi^{-1}(\mathfrak{B})$. The left-hand set is the same as $[\mathfrak{b}]\phi\big((\mathcal{O}/\mathfrak{m}, \cdot) \times \{\pm 1\}^{\Sigma}\big)$, so we have proven that the sequence is exact at $\overline{\mathrm{Clm}}^*_{\mathfrak{m},\Sigma}(\mathcal{O})$. □

The exact sequence in Proposition A.11 is related to the ray class group by the following commutative diagram, where in both rows the image of the first map consists of the classes of principal ideals.

$$\begin{array}{ccccccc} (\mathcal{O}/\mathfrak{m})^\times \times \{\pm 1\}^{\Sigma} & \longrightarrow & \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) & \longrightarrow & \mathrm{Cl}(\mathcal{O}) & \to & 1 \\ \big\downarrow & & \big\downarrow & & \big\| & & \\ (\mathcal{O}/\mathfrak{m}, \cdot) \times \{\pm 1\}^{\Sigma} & \longrightarrow & \overline{\mathrm{Clm}}^*_{\mathfrak{m},\Sigma}(\mathcal{O}) & \longrightarrow & \mathrm{Cl}(\mathcal{O}) & \to & 1 \end{array} \tag{A.34}$$

We conclude by noting that the potentially invertible ray class monoid is the same as the ray class monoid in the quadratic case.

Proposition A.12. *If $\mathcal{O}$ is an order in a quadratic field, then* $\mathrm{Clm}_{\mathfrak{m},\Sigma}(\mathcal{O}) \cong \mathrm{Clm}^{\flat}_{\mathfrak{m},\Sigma}(\mathcal{O})$.

Proof. This proposition follows from the fact that every ideal in a quadratic order is an invertible ideal of its multiplier ring, hence potentially invertible. That fact is given as [13, Prop. 1.4.1] (and indeed follows directly from Proposition 2.22 by taking $n = 2$). □

Appendix B. Norms of ideals in orders

In this appendix, let K be a number field and $\mathcal{O}$ an order in K. We give a criterion for multiplicativity of (absolute) norms of integral ideals of an order to hold; it does not hold in general. We use this criterion to extend the notion of norm of an integral ideal of $\mathcal{O}$ to norm of a fractional ideal of $\mathcal{O}$. We discuss the effect of change of order on norms of fractional ideals.

Definition B.1. Let $\mathfrak{a}$ be an integral $\mathcal{O}$-ideal. If $\mathfrak{a}$ is nonzero, define the *norm* of $\mathfrak{a}$ to be $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{a}) = [\mathcal{O} : \mathfrak{a}]$, where $[\mathcal{O} : \mathfrak{a}] = |\mathcal{O}/\mathfrak{a}|$ is the index of $\mathfrak{a}$ in $\mathcal{O}$ as an abelian group. Define $\mathrm{Nm}_{\mathcal{O}}(0) = 0$.

For invertible ideals $\mathfrak{a}, \mathfrak{b}$ the norm is multiplicative on products: $\mathrm{Nm}(\mathfrak{ab}) = \mathrm{Nm}_{\mathcal{O}}(\mathfrak{a})\,\mathrm{Nm}_{\mathcal{O}}(\mathfrak{b})$. The norm need not be multiplicative on non-invertible ideals, and there are orders $\mathcal{O}$ having instances of both strict submultiplicativity $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{ab}) < \mathrm{Nm}_{\mathcal{O}}(\mathfrak{a})\,\mathrm{Nm}_{\mathcal{O}}(\mathfrak{b})$ and strict supermultiplicativity $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{ab}) > \mathrm{Nm}_{\mathcal{O}}(\mathfrak{a})\,\mathrm{Nm}_{\mathcal{O}}(\mathfrak{b})$ of noninvertible ideals; see [26, Example 3.4].

The following proposition shows that the norm of the product of two ideals is multiplicative if one of them is invertible.

Proposition B.2. *Let $\mathfrak{a} \in \mathrm{I}^*(\mathcal{O})$ and $\mathfrak{b} \in \mathrm{I}(\mathcal{O})$ (so $\mathfrak{a}$ is invertible, whereas $\mathfrak{b}$ may or may not be invertible). Then,* $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{ab}) = \mathrm{Nm}_{\mathcal{O}}(\mathfrak{a})\,\mathrm{Nm}_{\mathcal{O}}(\mathfrak{b})$.

Proof. If $\mathfrak{b} = 0$, then $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{ab}) = 0 = \mathrm{Nm}_{\mathcal{O}}(\mathfrak{a})\,\mathrm{Nm}_{\mathcal{O}}(\mathfrak{b})$. Assume from now on that $\mathfrak{b} \neq 0$.

The norm of $\mathfrak{ab}$ and the norm of $\mathfrak{a}$ are related by the following equation:

$$\mathrm{Nm}_{\mathcal{O}}(\mathfrak{ab}) = [\mathcal{O} : \mathfrak{ab}] = [\mathcal{O} : \mathfrak{a}][\mathfrak{a} : \mathfrak{ab}] = \mathrm{Nm}_{\mathcal{O}}(\mathfrak{a})[\mathfrak{a} : \mathfrak{ab}]. \tag{B.1}$$

Let $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ be the set of maximal ideals of $\mathcal{O}$ containing $\mathfrak{ab}$. Using primary decomposition (Proposition 2.2), we may write

$$\mathfrak{a} = \bigcap_{j=1}^{k} \mathfrak{q}_j = \prod_{j=1}^{k} \mathfrak{q}_j, \qquad\qquad \mathfrak{b} = \bigcap_{j=1}^{k} \mathfrak{r}_j = \prod_{j=1}^{k} \mathfrak{r}_j, \tag{B.2}$$

where $\mathfrak{q}_j$ and $\mathfrak{r}_j$ are either primary ideals having radical $\mathfrak{p}_j$, or else the equal to unit ideal $\mathcal{O}$. Locally, $\mathfrak{a}\mathcal{O}_{\mathfrak{p}_j} = \mathfrak{q}_j\mathcal{O}_{\mathfrak{p}_j}$ and $\mathfrak{b}\mathcal{O}_{\mathfrak{p}_j} = \mathfrak{r}_j\mathcal{O}_{\mathfrak{p}_j}$. Moreover, by Proposition 4.6, $\mathfrak{a}$ is locally principal, so we may write $\mathfrak{a}\mathcal{O}_{\mathfrak{p}_j} = \alpha_j\mathcal{O}_{\mathfrak{p}_j}$ for $1 \leq j \leq k$. Choose some $\alpha \in \mathcal{O}$ such that $\alpha \equiv \alpha_j \pmod{\mathfrak{q}_j\mathfrak{r}_j}$ for $1 \leq j \leq k$. Define an additive group homomorphism (indeed, an isomorphism of $\mathcal{O}$-modules)

$$\phi : \mathcal{O} \to \mathfrak{a}/\mathfrak{ab} \tag{B.3}$$

by $\phi(x) = \alpha x + \mathfrak{ab}$.

We first show that ϕ is surjective. Consider $y \in \mathfrak{a}$. Locally in $\mathcal{O}_{\mathfrak{p}_j}$, write $y = \alpha_j x_j$ for some $x_j \in \mathcal{O}_{\mathfrak{p}_j}$. Choose some $x \in \mathcal{O}$ such that $x \equiv x_j \pmod{\mathfrak{q}_j\mathfrak{r}_j}$ for $1 \le j \le k$. Thus, $y \equiv \alpha x \pmod{\mathfrak{q}_j\mathfrak{r}_j}$ for $1 \le j \le k$, so

$$y - \alpha x \in \bigcap_{j=1}^{k} \mathfrak{q}_j\mathfrak{r}_j = \prod_{j=1}^{k} \mathfrak{q}_j\mathfrak{r}_j = \mathfrak{ab}. \tag{B.4}$$

That is, $\phi(x) = y + \mathfrak{ab}$.

We now compute the kernel of ϕ. We have $\phi(x) = 0$ if and only if $\alpha x \in \mathfrak{ab}$. Clearly $\alpha x \in \mathfrak{ab}$ whenever $x \in \mathfrak{b}$. Conversely, suppose $\alpha x \in \mathfrak{ab}$. Then, in the local ring $\mathcal{O}_{\mathfrak{p}_j}$, $\alpha x \in \alpha\beta\mathcal{O}_{\mathfrak{p}_j} = \alpha_j\mathfrak{r}_j\mathcal{O}_{\mathfrak{p}_j}$. Also, $\alpha - \alpha_j \in \mathfrak{q}_j\mathfrak{r}_j\mathcal{O}_{\mathfrak{p}_j} = \alpha_j\mathfrak{r}_j\mathcal{O}_{\mathfrak{p}_j}$, and thus $\alpha_j x = \alpha x - (\alpha - \alpha_j)x \in \alpha_j\mathfrak{r}_j\mathcal{O}_{\mathfrak{p}_j}$. Dividing, $x \in \mathfrak{r}_j\mathcal{O}_{\mathfrak{p}_j}$, so $x \in \mathfrak{r}_j$ (because $x \in \mathcal{O}$). Thus,

$$x \in \bigcap_{j=1}^{k} \mathfrak{r}_j = \mathfrak{b}. \tag{B.5}$$

So $\ker \phi = \mathfrak{b}$.

By the first isomorphism theorem, there is an isomorphism of abelian groups (indeed, of $\mathcal{O}$-modules)

$$\mathcal{O}/\mathfrak{b} \cong \mathfrak{a}/\mathfrak{ab}. \tag{B.6}$$

Equating the sizes of the two abelian groups, $[\mathfrak{a} : \mathfrak{ab}] = [\mathcal{O} : \mathfrak{b}] = \mathrm{Nm}_{\mathcal{O}}(\mathfrak{b})$. Substituting into eq. (B.1), $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{ab}) = \mathrm{Nm}_{\mathcal{O}}(\mathfrak{a})\,\mathrm{Nm}_{\mathcal{O}}(\mathfrak{b})$. □

Proposition B.2 will justify an extension of the norm to fractional ideals.

Definition B.3. Let $\mathfrak{d} \in \mathrm{J}(\mathcal{O})$, and write $\mathfrak{d} = (\mathfrak{a} : \mathfrak{b}) = \mathfrak{a}\mathfrak{b}^{-1}$ for some $\mathfrak{a} \in \mathrm{I}(\mathcal{O})$ and $\mathfrak{b} \in \mathrm{I}^*(\mathcal{O})$. Define $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{d}) = \frac{\mathrm{Nm}_{\mathcal{O}}(\mathfrak{a})}{\mathrm{Nm}_{\mathcal{O}}(\mathfrak{b})}$.

Proposition B.4. *The norm of a fractional ideal as in Definition B.3 is well-defined. If* $\mathfrak{c} \in \mathrm{J}^*(\mathcal{O})$ *and* $\mathfrak{d} \in \mathrm{J}(\mathcal{O})$*, then* $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{cd}) = \mathrm{Nm}_{\mathcal{O}}(\mathfrak{c})\,\mathrm{Nm}_{\mathcal{O}}(\mathfrak{d})$.

Proof. If $\mathfrak{d} \in \mathrm{J}(\mathcal{O})$ and $\mathfrak{d} = \mathfrak{a}_1\mathfrak{b}_1^{-1} = \mathfrak{a}_2\mathfrak{b}_2^{-1}$ for some $\mathfrak{a}_1, \mathfrak{a}_2 \in \mathrm{I}(\mathcal{O})$ and $\mathfrak{b}_1, \mathfrak{b}_2 \in \mathrm{I}^*(\mathcal{O})$, then $\mathfrak{a}_1\mathfrak{b}_2 = \mathfrak{a}_2\mathfrak{b}_1$, so $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{a}_1)\,\mathrm{Nm}_{\mathcal{O}}(\mathfrak{b}_2) = \mathrm{Nm}_{\mathcal{O}}(\mathfrak{a}_2)\,\mathrm{Nm}_{\mathcal{O}}(\mathfrak{b}_1)$ by Proposition B.2. Thus, $\frac{\mathrm{Nm}_{\mathcal{O}}(\mathfrak{a}_1)}{\mathrm{Nm}_{\mathcal{O}}(\mathfrak{b}_1)} = \frac{\mathrm{Nm}_{\mathcal{O}}(\mathfrak{a}_2)}{\mathrm{Nm}_{\mathcal{O}}(\mathfrak{b}_2)}$, so $\mathrm{Nm}(\mathfrak{d})$ is well-defined.

Now, consider $\mathfrak{c} \in \mathrm{J}^*(\mathcal{O})$ and $\mathfrak{d} \in \mathrm{J}(\mathcal{O})$. Write $\mathfrak{c} = \mathfrak{a}_1\mathfrak{b}_1^{-1}$ and $\mathfrak{d} = \mathfrak{a}_2\mathfrak{b}_2^{-1}$ for $\mathfrak{a}_1, \mathfrak{b}_1, \mathfrak{b}_2 \in \mathrm{J}^*(\mathcal{O})$ and $\mathfrak{a}_2 \in \mathrm{J}(\mathcal{O})$. Then, $\mathfrak{cd} = (\mathfrak{a}_1\mathfrak{a}_2)(\mathfrak{b}_1\mathfrak{b}_2)^{-1}$, so

$$\mathrm{Nm}_{\mathcal{O}}(\mathfrak{cd}) = \frac{\mathrm{Nm}_{\mathcal{O}}(\mathfrak{a}_1\mathfrak{a}_2)}{\mathrm{Nm}_{\mathcal{O}}(\mathfrak{b}_1\mathfrak{b}_2)} = \frac{\mathrm{Nm}_{\mathcal{O}}(\mathfrak{a}_1)\,\mathrm{Nm}_{\mathcal{O}}(\mathfrak{a}_2)}{\mathrm{Nm}_{\mathcal{O}}(\mathfrak{b}_1)\,\mathrm{Nm}_{\mathcal{O}}(\mathfrak{b}_2)} = \mathrm{Nm}_{\mathcal{O}}(\mathfrak{c})\,\mathrm{Nm}_{\mathcal{O}}(\mathfrak{d}), \tag{B.7}$$

using Proposition B.2 and Definition B.3. □

Proposition B.5. *Suppose* $\mathcal{O} \subseteq \mathcal{O}'$ *for another order* $\mathcal{O}'$ *in* K*, and let* ext *be the extension map from fractional ideals on* $\mathcal{O}$ *to fractional ideal on* $\mathcal{O}'$*. If* $\mathfrak{c} \in \mathrm{J}^*(\mathcal{O})$*, then* $\mathrm{Nm}_{\mathcal{O}'}(\mathrm{ext}(\mathfrak{c})) = \mathrm{Nm}_{\mathcal{O}}(\mathfrak{c})$.

Proof. By the multiplicativity property of the norm proven in Proposition B.4 and the fact that extension preserves invertibility, it suffices to prove the claim for integral ideals; without loss of generality, assume $\mathfrak{c}$ is integral.

Write $\mathrm{ext}(\mathfrak{c}) = \mathfrak{c}\mathcal{O}'$. We evaluate $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{c}\mathcal{O}')$ in two different ways. Firstly,

$$\mathrm{Nm}_{\mathcal{O}}(\mathfrak{c}\mathcal{O}') = \mathrm{Nm}_{\mathcal{O}}(\mathfrak{c})\,\mathrm{Nm}_{\mathcal{O}}(\mathcal{O}') \text{ by Proposition B.2.} \tag{B.8}$$

Secondly, by definition of the norm,

$$\mathrm{Nm}_{\mathcal{O}}(\mathfrak{c}\mathcal{O}') = [\mathcal{O} : \mathfrak{c}\mathcal{O}'] = [\mathcal{O} : \mathcal{O}'][\mathcal{O}' : \mathfrak{c}\mathcal{O}'] = \mathrm{Nm}_{\mathcal{O}}(\mathcal{O}')\,\mathrm{Nm}_{\mathcal{O}'}(\mathfrak{c}\mathcal{O}'). \tag{B.9}$$

So $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{c})\,\mathrm{Nm}_{\mathcal{O}}(\mathcal{O}') = \mathrm{Nm}_{\mathcal{O}}(\mathcal{O}')\,\mathrm{Nm}_{\mathcal{O}'}(\mathfrak{c}\mathcal{O}')$, so $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{c}) = \mathrm{Nm}_{\mathcal{O}'}(\mathfrak{c}\mathcal{O}') = \mathrm{Nm}_{\mathcal{O}'}(\mathrm{ext}(\mathfrak{c}))$. □

REFERENCES

[1] M. Appleby, S. Flammia, and G. Kopp. A constructive approach to Zauner's conjecture via the Stark conjectures. In preparation (2022+).

[2] M. Appleby, S. Flammia, G. McConnell and J. Yard. Generating ray class fields of real quadratic fields by complex equiangular lines. Acta Arith. **192** (2020), no. 3, 211–233.

[3] M. Appleby, S. Flammia, G. McConnell and J. Yard. SICs and algebraic number theory. Found. Phys. **47** (2017), no. 8, 1042–1059. 1-18.

[4] M. Atiyah and I. MacDonald. *Introduction to Commutative Algebra*. Addison-Wesley: Reading, MA 1989.

[5] E. Bayer-Fluchtiger, Ideal lattices. In *A panorama of number theory or the view from Baker's garden (Zürich 1999))*, 168–184. Cambridge University Press: Cambridge, 2002.

[6] O. Beckwith and G. S. Kopp. Gauss composition with level structure. In preparation (2022+).

[7] M. Bhargava. Higher composition laws II: On cubic analogues of Gauss composition. Ann. of Math. **159**, no. 2 (2004), 865–886.

[8] G. Bruckner. Characterisierung der galoisschen Zahlkörper, deren zerlegte Primzahlen durch binäre quadratische Formen gegeben sind. Math. Nachr. **32** (1966), 317–326.

[9] A. H. Clifford and G. B. Preston, *The algebraic theory of semigroups, Vol. I.* Math. Surveys, no. 7, American Math. Society: Providence, RI 1961.

[10] A. H. Clifford and G. B. Preston, *The algebraic theory of semigroups, Vol. II.* Math. Surveys, no. 7, American Math. Society: Providence, RI 1967.

[11] H. Cohn. *Introduction to the Construction of Class Fields*. Corrected reprint of the 1985 original. Dover Publications: New York 1994.

[12] D. Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication* (second edition). Pure and Applied Mathematics. John Wiley & Sons, Inc., Hoboken, NJ 2013.

[13] E. C. Dade, O. Taussky and H. Zassenhaus. On the theory of orders, in particular on the semigroup of ideal classes and genera of an order in an algebraic number field. Math. Ann. **148** (1962), 31–64.

[14] H. Darmon, A. Pozzi, and J. Vonk. The values of the Dedekind-Rademacher cocycle at real multiplication points. arXiv preprint arXiv:2103.02490 (2021).

[15] I. S. Eum, J. K. Koo and D. H. Shin. Binary quadratic forms and ray class groups. Proc. Roy. Soc. of Edinburgh Sect. A **150** (2020), no. 2, 695–720.

[16] R. Fueter. Abelsche Gleichungen in quadratisch-imaginären Zahlkörpern. Math. Ann. **75** (1914), 177–255.

[17] F. Halter-Koch. Clifford semigroups of ideals in monoids and domains. Forum Math. **21** (2009), no. 6, 1001–1020.

[18] H. Hasse. History of class field theory. In *Algebraic Number Theory: Proceedings of the instructional conference held at the University of Sussex, Brighton, September 1–7, 1965*. Edited by J. W. S. Cassels and A. Fröhlich. Academic Press: London and New York 1967.

[19] P. Hill. Characters of commutative semigroups. J. Algebra **5** (1967), no. 1, 16–24.

[20] M. Katsurada. The establishment of the Takagi-Artin class field theory. In *The Intersection of History and Mathematics*, Science Networks: Historical Studies Vol. 15, 109–128. (S. Chikhara, S. Mitsuo, J. W. Dauben, eds.) Birkhäuser: Boston 1995.

[21] G. Koda. Representation of the norm of ideals by quadratic forms with congruence conditions. SUT J. Math. **56** (2020), no. 1, 21–37.
[22] G. S. Kopp. SIC-POVMs and the Stark conjectures. Int. Math. Res. Not. IMRN **2021** (2021), no. 18, 13812–13838.
[23] G. S. Kopp. Stark class invariants as limits of a ratio of q-Pochhammer symbols. In preparation (2022+).
[24] G. S. Kopp and J. C. Lagarias. SICs and orders of real quadratic fields. In preparation (2022+).
[25] C. Lv and Y. Deng. On orders in number fields: Picard groups, ring class fields and applications. Science China Mathematics **58** (2015), no. 8, 1627–1638.
[26] S. Marseglia. Super-multiplicativity of ideal norms in number fields. Acta Arithmetica **193** (2020), 75–93.
[27] A. M. Masuda, L. Quoos, B. Steinberg. Character theory of monoids over an arbitrary field. J. Algebra **431** (2015), 107–126.
[28] D. B. McAlister. Characters on commutative semigroups. Q. J. Math. **19** (1968), 141–157.
[29] D. B. McAlister. Characters of finite semigroups. J. Algebra **22** (1972), no. 1, 183–200.
[30] J. Neukirch. *Algebraic Number Theory*. Translated from German by N. Schappacher. Grundlehren Math. Wiss. **322**. Springer: Berlin 2013.
[31] N. Schappacher. On the history of Hilbert's twelfth problem: A comedy of errors. In *Matériaux pour l'histoire des mathématiques au XXe siècle (Nice 1996)*, 243–273. Sémin. Congr. **3**, Soc. Math. France, Paris, 1998.
[32] P. Stevenhagen. Generalized unramified class field theory. Math. Inst., Univ. Amersterdam, Report 85–13, 1985.
[33] P. Stevenhagen. Unramified class field theory for orders. Trans. Amer. Math. Soc. **311** (1989), no. 2, 483–500.
[34] P. Stevenhagen. The arithmetic of number rings. In *Algorithmic Number Theory* 209–266, MSRI Publications **44**, Amer. Math. Soc., 2008.
[35] T. Takagi. Über eine Theorie des relativ-Abel'schen Zahlkörpers. J. Coll. Sci. imp. Univ. Tokyo **41** (1920), no. 9, 1–133.
[36] J. Voight. Exact sequence of monoids. MathOverflow. URL (2011): `https://mathoverflow.net/questions/83080/exact-sequence-of-monoids`.
[37] H. Weber. *Elliptische Funktionen und algebraische Zahlen*. Braunschweig: Vieweg 1894. Second Edition: 1898. (Reprint: Chelsea: New York.)
[38] H. Weber. *Lehrbuch der Algebra II*. Braunschweig: Viehweg 1896, Second Edition: 1899. (Reprint: Chelsea, New York.)
[39] H. Weber. Über Zahlengruppen in algebraischen Zahlkörpern, I, II, III. Math. Ann. **48** (1897), 433–473; **49** (1897), 83–100; **50** (1898), 1–26.
[40] H. Weber. *Lehrbuch der Algebra III*. Braunschweig: Viehweg 1908. (Reprint: Chelsea, New York.)
[41] P. Zanardo and U. Zannier. The class semigroup of orders in number fields. Math. Proc. Camb. Phil. Soc. **115** (1994), no. 3, 379–391.
[42] G. Zauner. *Quantendesigns: Grundzüge einer nichtkommutativen Designtheorie*. PhD thesis, University of Vienna, 1999.
[43] G. Zauner. Quantum designs: Foundations of a noncommutative design theory. Int. J. Quantum Inf. **9** (2011), no. 1, 445–507.

DEPARTMENT OF MATHEMATICS, LOUISIANA STATE UNIVERSITY, BATON ROUGE, LA, USA
Email address: `kopp@math.lsu.edu`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MICHIGAN, ANN ARBOR, MI, USA
Email address: `lagarias@umich.edu`