RAY CLASS GROUPS AND RAY CLASS FIELDS FOR ORDERS OF NUMBER FIELDS

GENE S. KOPP AND JEFFREY C. LAGARIAS

Abstract. This paper contributes to the theory of orders of number fields. This paper defines a notion of *ray class group* associated to an arbitrary order in a number field together with an arbitrary ray class modulus for that order (including Archimedean data), constructed using invertible fractional ideals of the order. It shows existence of *ray class fields* corresponding to the 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 ring class groups (resp., fields) of orders in the case of trivial modulus. The paper gives exact sequences 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 describe each ray class field of an order in terms of the splitting behavior of primes.

Contents

1. Introduction

This paper contributes to the theory of orders of number fields. An *order* $\mathcal{O}$ of an algebraic number field K is a subring of K containing 1 and having finite rank equal to $[K : \mathbb{Q}]$ as a $\mathbb{Z}$-module. Dedekind showed that the ring $\mathcal{O}_K$ of all algebraic integers in K is the maximal order, and all other orders $\mathcal{O}$ are of finite index in $\mathcal{O}_K$.

The object of this paper is to extend to general orders $\mathcal{O}$ the notions of ray class groups and ray class fields for the maximal order $\mathcal{O}_K$. A ray class group or field of an order is

Date: November 30, 2024.
2020 *Mathematics Subject Classification.* 11R37 (primary), 11R54 (secondary).
Key words and phrases. class field theory, orders of number fields, ray class fields, ring class fields.

specified by a *level datum* $\mathcal{L} = (\mathcal{O}; \mathfrak{m}, \Sigma)$ for the field K, in which $\mathcal{O}$ is an order of K, $\mathfrak{m}$ is an integral ideal of $\mathcal{O}$, and Σ is a set of real places of K. The pair $(\mathfrak{m}, \Sigma)$ is called a *modulus*.

Ray class groups are groups of ray classes, which are sets of fractional ideals satisfying congruence conditions modulo $\mathfrak{m}$ and sign conditions at the places in Σ. The set of ray classes modulo $(\mathfrak{m}, \Sigma)$ of a non-maximal order under ideal multiplication forms a monoid (semigroup with identity) rather than a group, because it includes non-invertible ideal classes. The set of invertible ray classes forms a group, the *ray class group* of the order.

A ray class field of an order is a certain abelian Galois extension of the number field K associated to a level datum $\mathcal{L} = (\mathcal{O}; \mathfrak{m}, \Sigma)$. The ray class fields of an order $\mathcal{O}$ form a "distinguished" class of abelian extensions of K, cofinal in the partially ordered set of abelian extensions of K, whose prime decomposition properties over K are described by the corresponding ray class group and by algebraic properties of the specific order $\mathcal{O}$ of K.

1.1. **Background.** The first complete version of class field theory for number fields was developed by Takagi [56] in 1920, building on work of Weber, Hilbert, Furtwängler, and Fueter; see [28, 30]. In Takagi's treatment, the ray class fields of a number field K are associated to ray class groups, which are defined as groups of fractional ideals modulo subgroups of principal ideals satisfying congruence and sign conditions.

The ray class fields of a number field K comprise an infinite set of finite abelian extensions of K that 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 attached to moduli $(\mathfrak{m}, \Sigma)$, where $\mathfrak{m}$ is an ideal of the ring of integers $\mathcal{O}_K$, and Σ is a subset of the real embeddings of K. The extension $H_{\mathfrak{m},\Sigma}/K$ is ramified at a subset of the primes diving $\mathfrak{m}$ and the infinite places in Σ. The ray class field attached to the modulus $(\mathcal{O}_K, \emptyset)$ is the *Hilbert class field*.

Associated to each non-maximal order $\mathcal{O}$ of K, there is a separate classical notion of a *ring class field* $H^{\mathcal{O}}$, associated to a *ring class group* $\mathrm{Cl}(\mathcal{O})$. 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 $\tau \in K$; see Schertz [49, Ch. 6]. 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}. The extension $H^{\mathcal{O}}/K$ is ramified at a subset of the primes dividing the conductor ideal $\mathfrak{f}(\mathcal{O}) = (\mathcal{O} : \mathcal{O}_K)$.

1.2. **Ray class groups for orders.** The first object of the paper is the definition of ray class groups for orders, made in terms of fractional ideals of the order, and the derivation of formulas for computing invariants of such ray class groups, allowing variation of both the order $\mathcal{O}$ and the ray class modulus $(\mathfrak{m}, \Sigma)$. Ray class groups for orders specialize to Takagi ray class groups (when $\mathcal{O} = \mathcal{O}_K$) and to ring class groups (when $(\mathfrak{m}, \Sigma) = (\mathcal{O}, \emptyset)$).

In order to define ray class groups, this paper first gives a detailed review of the properties of integral and fractional ideals of orders, emphasizing their differences from maximal orders, with examples. For integral ideals of non-maximal orders:

(1) Ideals do not always factor (uniquely or otherwise) into products of prime ideals.
(2) If an integral ideal $\mathfrak{a}$ divides $\mathfrak{b}$, then $\mathfrak{b} \subseteq \mathfrak{a}$, but the converse need not hold. "Greatest common divisor" and "least common multiple" of ideals are not well defined. However, the notion of *coprimality* of two integral ideals is well defined.
(3) Unique factorization of ideals is restored for the set of all integral ideals coprime to the *conductor ideal* $\mathfrak{f}(\mathcal{O})$ of the order, which is the set-theoretically largest ideal of $\mathcal{O}$ that is also an ideal of $\mathcal{O}_K$.

For fractional ideals of non-maximal orders:

(1) There exist non-invertible nonzero fractional ideals, so that nonzero fractional ideals under the ideal product operation form a monoid rather than a group.
(2) The monoid of nonzero fractional ideals $\mathrm{J}(\mathcal{O})$ for ideal product may contain non-integral fractional ideals $\mathfrak{a}$ having a power $\mathfrak{a}^k$ that is an integral ideal. The ideal $\mathfrak{a}^k$ may be $\mathcal{O}$, giving non-trivial torsion elements in the group of invertible fractional ideals $\mathrm{J}^*(\mathcal{O})$. (For the maximal order, $\mathrm{J}(\mathcal{O}) = \mathrm{J}^*(\mathcal{O})$ is a free abelian group.)
(3) There is a notion of *coprimality* of a fractional ideal and an integral ideal. When a ray class modulus $\mathfrak{m}$ contains the conductor ideal $\mathfrak{f}(\mathcal{O})$, then the set $\mathrm{J}_{\mathfrak{m}}(\mathcal{O})$ of fractional ideals coprime to $\mathfrak{m}$ is a free abelian group.

The paper also treats *extension* and *contraction* of integral and fractional ideals between one order $\mathcal{O}$ and a larger order $\mathcal{O}'$ of a fixed number field K. This treatment is intended to be more broadly useful beyond its application to ray class groups; see Section 1.6 for details.

The *ray class group* $\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ is a quotient group of the group $\mathrm{J}^*_{\mathfrak{m}}(\mathcal{O})$ of invertible fractional ideals coprime to the modulus $\mathfrak{m}$ by a suitable subgroup $\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})$ of principal ideals. The modulus $\mathfrak{m}$ may be any nonzero integral ideal—it is permitted to be non-invertible. For this reason, the paper necessarily studies the complexities and pitfalls of non-invertible ideals. More generally, there is a *ray class monoid* $\mathrm{Clm}_{\mathfrak{m},\Sigma}(\mathcal{O})$ under ideal product built from the monoid of fractional ideals $\mathrm{J}_{\mathfrak{m}}(\mathcal{O})$ coprime to $\mathfrak{m}$ by modding out by the action of the subgroup $\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})$. Its structure is not considered in this paper and will be treated separately in [34].

The main result of the paper for ray class groups $\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ is an exact sequence relating ray class groups of orders, in which both the order and the ideal modulus conditions can be simultaneously varied, given as Theorem 6.5. This exact sequence is obtained using extension and contraction maps relating integral ideals in two orders $\mathcal{O} \subseteq \mathcal{O}'$. The exact sequence also yields a formula for the cardinality of a ray class group of an order (Theorem 6.9).

1.3. **Ray class fields for orders and class field theory for orders.** The second object of the paper is to establish the existence of ray class fields of orders attached to ray class groups of orders. These are a distinguished set of abelian extensions of K, whose arithmetic of splitting of primes is described by the given ray class group of the order. We formulate three results which together comprise a ray class field theory for orders.

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 level 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, motivated by special values of modular functions. (See [64, p. 164], [28, p. 266], and [63].)

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 level 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 coprime to the quotient ideal $(\mathfrak{m} : \mathcal{O}_K)$ (as defined in (1.1)) 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 level 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 $(\mathcal{O}'; \mathfrak{m}', \Sigma')$.

To understand Theorem 1.1, it is helpful to compare the quotient ideal $(\mathfrak{m} : \mathcal{O}_K)$ to more familiar ideals. Note first that, given two orders $\mathcal{O} \subseteq \mathcal{O}'$, any (integral) $\mathcal{O}'$-ideal $\mathfrak{a}$ is automatically an $\mathcal{O}$-ideal. In particular, all $\mathcal{O}_K$-ideals are automatically $\mathcal{O}$-ideals for all orders $\mathcal{O}$ of K. Next, recall that, given two $\mathcal{O}$-ideals $\mathfrak{a}, \mathfrak{b}$, the *quotient ideal*

$$(\mathfrak{a} : \mathfrak{b}) := \{x \in K : x\mathfrak{b} \subseteq \mathfrak{a}\}. \tag{1.1}$$

The quotient ideal $(\mathfrak{a} : \mathfrak{b})$ is an $\mathcal{O}$-ideal, and if in addition $\mathfrak{b}$ is an $\mathcal{O}'$-ideal, then $(\mathfrak{a} : \mathfrak{b})$ will also be an $\mathcal{O}'$-ideal. Thus, given an $\mathcal{O}$-ideal $\mathfrak{m}$, the quotient ideal $(\mathfrak{m} : \mathcal{O}_K)$ will be an $\mathcal{O}_K$-ideal, which is the (set-theoretically) 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 $\mathfrak{f}(\mathcal{O}) = (\mathcal{O} : \mathcal{O}_K)$. The conductor ideal encodes information on all the non-invertible ideals in the order $\mathcal{O}$; see Lemma 2.13. It is the (set-theoretically) largest integral $\mathcal{O}$-ideal that is also an $\mathcal{O}_K$-ideal. It follows that for any integral $\mathcal{O}$-ideal $\mathfrak{m}$, we have $(\mathfrak{m} : \mathcal{O}_K) \subseteq \mathfrak{f}(\mathcal{O})$.

The ideal $(\mathfrak{m} : \mathcal{O}_K)$ satisfies the inclusions (all as $\mathcal{O}_K$-ideals)

$$\mathfrak{f}(\mathcal{O})\mathfrak{m} \subseteq (\mathfrak{m} : \mathcal{O}_K) \subseteq \mathfrak{f}(\mathcal{O}) \cap \mathfrak{m}\mathcal{O}_K; \tag{1.2}$$

these inclusions are proven in Lemma 3.9 (taking $\mathcal{O}' = \mathcal{O}_K$ in its statement). The three ideals in (1.2) have the same prime divisors in the maximal order $\mathcal{O}_K$: 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 second result locates the ray class field $H^{\mathcal{O}}_{\mathfrak{m},\Sigma}/K$ of an order $\mathcal{O}$ for the level 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 level datum $(\mathcal{O}; \mathfrak{m}, \Sigma)$, there are inclusions of ray class fields $H^{\mathcal{O}_K}_{\mathfrak{m}\mathcal{O}_K,\Sigma} \subseteq H^{\mathcal{O}}_{\mathfrak{m},\Sigma} \subseteq H^{\mathcal{O}_K}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}$.*

In the special case $\mathfrak{m} = \mathcal{O}$, we have $(\mathfrak{m} : \mathcal{O}_K) = \mathfrak{f}(\mathcal{O})$. 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 whose ramification over K occurs only at prime $\mathcal{O}_K$-ideals containing the conductor ideal $\mathfrak{f}(\mathcal{O})$.

It follows from Theorem 1.2 and (1.2), together with standard class field theory, that the set of all ray class fields of a fixed order $\mathcal{O}$ is cofinal in the set of all finite abelian extensions of K. Theorem 1.2 is obtained as a special case of a general result relating ray class fields of two given orders $\mathcal{O} \subseteq \mathcal{O}'$, given as Theorem 7.5.

The third result adapts Artin reciprocity to our setting to give a correspondence between class groups and Galois groups of class fields. The correspondence asserts that the ray class field $H^{\mathcal{O}}_{\mathfrak{m},\Sigma}$ of an order $\mathcal{O}$ is associated to an appropriate ray class group $\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ in such a way that a Galois correspondence holds: $\mathrm{Gal}(H^{\mathcal{O}}_{\mathfrak{m},\Sigma}/K) \cong \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ as abelian groups.

Theorem 1.3. *For an order $\mathcal{O}$ in a number field K and any level 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 coprime to $\mathfrak{f}(\mathcal{O}) \cap \mathfrak{m}$, having the property that*

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

where $\mathfrak{P}$ is any prime of $\mathcal{O}_{H_0}$ lying over $\mathfrak{p}\mathcal{O}_K$, and $q = p^j$ is the number of elements in the finite field $\mathcal{O}/\mathfrak{p}$. For any (not necessarily prime) ideal $\mathfrak{a}$ of $\mathcal{O}$ coprime 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* $H_1 = H^{\mathcal{O}_K}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}$ *being a (Takagi) ray class field for the maximal order* $\mathcal{O}_K$*, and* $H_0 \subseteq H_1$*.*

In Theorem 1.3, the set of prime ideals coprime to $\mathfrak{f}(\mathcal{O}) \cap \mathfrak{m}$ includes all but finitely many of the prime ideals of $\mathcal{O}$.

For the classical case of the maximal order $\mathcal{O}_K$, the Artin map $\mathrm{Art}(\cdot)$ on the right side of (1.3) is given in Neukirch [46, Ch. VI, Thm. 7.1] for any ray ideal $\mathfrak{m}$, in the case of $\Sigma = \Sigma_{\max}$, the set of all real places of K. Additionally, the special case $\mathfrak{m} = \mathcal{O}_K$ with $\Sigma = \Sigma_{\max}$ produces the *narrow Hilbert class field* (termed by Neukirch the *big Hilbert class field*) of K, denoted $H^{\mathcal{O}_K}_{\mathcal{O}_K,\Sigma_{\max}}$; compare [46, Ch. VI, Prop. 6.8]. The alternative choice of[1] the minimal set $\Sigma = \emptyset$ of real places produces the original (or *wide*) *Hilbert class field* (called by Neukirch the *small Hilbert class field*) of K, denoted $H^{\mathcal{O}_K}_{\mathcal{O}_K,\emptyset}$. The wide class field has Galois group isomorphic to the ideal class group of $\mathcal{O}_K$; see [46, Ch. VI, Prop. 6.9]. The difference between wide and narrow Hilbert class fields exhibits the role of the real places Σ in the level datum.

Our three main theorems do not provide an independent development of global class field theory; their proofs are completed using the existing global class field theory. Their contribution is to identify a new set of distinguished abelian extensions of K whose structure encodes properties of the arithmetic of the ray class groups attached to a fixed order $\mathcal{O}$ of K (rather than the maximal order).

The proofs of these these results proceed on the ray class group side. We identify the $\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ with a certain quotient group of a Takagi ray class group of the maximal order. The exact sequences in Theorem 6.5 are used. Our definition (Definition 7.1) of the ray class field associated to the level datum $(\mathcal{O}; \mathfrak{m}, \Sigma)$ is formulated using this identification. Theorem 1.1, Theorem 1.2 and Theorem 1.3 are then obtained via the main correspondence and existence theorems of global class field theory in a form given in Section 7.

1.4. **Applications.** The constructions in this paper are motivated by several mathematical phenomena involving ray class groups and ray class fields of orders that arise outside pure class field theory. We briefly describe three of them.

(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 and also suggest a geometric approach to explicit class field theory for real quadratic fields that fundamentally involves non-maximal orders. A SIC is a generalized quantum measurement (a *POVM*) with restrictive information-theoretic properties that make it optimal for certain protocols in quantum information processing. It is equivalent to a maximal set of d^2 complex lines in $\mathbb{C}^d$ that are "equiangular" with respect to the Hermitian inner product. SICs are known to exist in at least dimensions $d \leq 53$ and are conjectured by Zauner [66, 67] 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, 31]. The connection was originally discovered through numerical experimentation. Work by the current authors and others [1, 33] uses ray class groups and ray class fields of real quadratic orders in a conjectural framework for classifying SICs. That work also indicates SICs and generalized SICs may be used to study abelian extensions of real quadratic fields.

[1]Neukirch does not introduce the real place parameters Σ, and his definition [46, Ch. VI, Defn. 6.2] of ray class groups corresponds to the choice $\Sigma = \Sigma_{\max}$.

(2) Class field theory for imaginary quadratic orders arises naturally in the theory of complex multiplication (CM) for elliptic curves. In particular, if E is an elliptic curve with CM by $\mathcal{O}$ having a Weierstrass equation with coefficients in $\mathbb{Q}(j(E)) = H^{\mathcal{O}}_{\mathcal{O},\emptyset}$, then the n-torsion points of E have coordinates in the field $H^{\mathcal{O}}_{n\mathcal{O},\emptyset}$; see [8, Thm. 1.4]. A related construction describes *elliptic units* in abelian extensions of imaginary quadratic fields as special values of modular functions called *modular units* [35]; this construction also naturally extends to non-maximal orders.

Ray class fields of orders of higher degree arise in the study of higher-dimensional abelian varieties with CM. Pathologies of non-maximal orders of degree greater than 2, such as potentially being non-Gorenstein, create obstructions to proving theorems in CM theory [11].

(3) Ray class groups and ray class fields of orders appear naturally in approaches to Hilbert's 12th Problem for real quadratic and complex cubic fields. For example, when replacing the complex upper half plane by the p-adic Drinfeld upper half plane, as in the work of Darmon and Dasgupta on elliptic units for real quadratic fields [19] and the work of Darmon, Pozzi, and Vonk [20, 21] on rigid meromorphic cocycles, non-maximal orders arise in the study of "singular moduli" in the same way as they do in the classical theory of complex multiplication. Non-maximal orders are needed to describe arbitrary real multiplication (RM) values of rigid meromorphic cocycles. Complex meromorphic modular cocycles introduced by the first author [32] have RM values that are (essentially) the classical Archimedean Stark class invariants conjectured to be algebraic units by Stark in the real quadratic case. The RM values studied are naturally parameterized by elements of ray class groups (more generally, ray class monoids) of orders, and they are conjectured to lie in ray class fields of orders. We also expect the elliptic gamma functions connected by Bergeron, Charollois, and García to Stark units over complex cubic fields [7] to have special values parameterized by ray classes of general complex cubic orders, which generate ray class fields of those orders.

The treatment of integral and fractional ideals of orders, and extension and contraction maps, given in Sections 2 to 4, is intended to apply more broadly, outside its use in defining ray class groups of orders. The related concept of *ideal lattices* is foundational to various versions of lattice based-cryptography [39, 44, 45] and ring-based schemes proposed for homomorphic encryption [26, 38]. Ideal lattices are identified with ideals in polynomial rings $\mathbb{Z}[x]/(f(x))$, which for irreducible monic $f(x)$ correspond to ideals of the monogenic order $\mathcal{O} = \mathbb{Z}[\theta]$ generated by a root of f. An ideal lattice can be encoded as an integer matrix associated to an integral ideal of an order, as studied by Taussky [58–60]; see also Taussky's earlier work [57]. A number-theoretic perspective on ideal lattices is given by Bayer-Fluckiger [5,6].

1.5. **Prior work.** There has been an extensive algebraic study of the structure of orders of number fields, beginning with Dedekind [22] in 1877; see also [23]. Two general references are Stevenhagen [54] and Neukirch [46, Ch. 1, Sec. 12]. Neukirch views orders of number fields as number rings with "singularities" at the primes dividing the conductor ideal, by analogy with geometric interpretations of subrings of function fields (e.g., $F[t^2, t^3] \subseteq F(t)$ as the coordinate ring of the cuspidal cubic).

An important 1962 paper of Dade, Taussky, and Zassenhaus [18] presented fundamental results on the structure of invertible fractional ideals, class groups of orders, and the class

monoids obtained when including non-invertible ideals. They developed a structure theory for one-dimensional Noetherian domains [18, 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 [18, 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 $(:)$ is the ideal quotient as defined by (1.1); see [18, Prop. 1.10]. They note the set $\mathrm{J}(\mathcal{D})$ carries the structure of a semigroup under ideal multiplication. Dade, Taussky, and Zassenhaus define a $\mathcal{D}$-*order* to be any fractional ideal $\mathfrak{a}$ of $\mathcal{D}$ that is also an integral domain [18, 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 define *invertible fractional ideals* and characterize them using ideal quotient [18, Defn. (p. 41), Prop. 1.3.6].

Class field theory has gone through many versions. We use the version using ray classes, formulated in the work of Takagi, Hasse, and Artin. A useful treatment is given in Cohn [15]. An appendix of Cohn's book gives Emil Artin's 1932 lectures.

Computational class field theory, generally using ray classes, is especially important in applications (such as those mentioned in Section 1.4). Cohen and Stevenhagen have written a useful survey [14].

Ring class groups and ring class fields go back to fundamental work of Weber in 1897–1898 [63], motivated (in part) by complex multiplication; see his books [61, 62, 64]. The ring class groups associated to orders of imaginary quadratic fields appear in the theory of complex multiplication, because ideal classes of those orders are classified by homothety classes of lattices in $\mathbb{C}$ having a given endomorphism ring $\mathcal{O} \neq \mathbb{Z}$; see [17, Cor. 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 [17], as stated in [17, Thm. 9.2].

It is known that the compositum of all ring class fields of a field 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 [25, 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 [48, p. 258]. Moreover, Bruckner [9, Satz 8] showed for a quadratic field K that the compositum of ring class fields for K is the compositum of all Galois fields L containing K for which $\mathrm{Gal}(L/\mathbb{Q})$ is a generalized dihedral group. The case of imaginary quadratic fields is also treated in Cox [17, Thm. 9.18, Cor. 11.35].

In 2015, Lv and Deng [37] treated ring class fields for arbitrary orders in number fields in a classical setting, corresponding to the "unramified" case $(\mathcal{O}; \mathfrak{m}, \Sigma) = (\mathcal{O}; \mathcal{O}, \emptyset)$. (The term "unramified" here refers to the fact that the modulus is trivial; the ring class field usually is a ramified extension at the primes containing the conductor.) An extension to general number rings (allowing inversion of arbitrary sets of nonzero elements) was given in 2018 by Yi and Lv [65].

There was significant further work on of class field theory for orders in the general "ramified" case, in situations related to complex multiplication. In 1935, Söhngen [50] constructed a "class field theory for orders" for imaginary quadratic fields, with explicit generators given by special values of Weber functions, which is described in detail in the book

of Schertz [49, Ch. 3, Ch. 6.2]. The ray class field theory for imaginary quadratic orders has been applied to CM theory for elliptic curves; we mention Bourdon and Clark [8] and Lozano-Robledo [36, Sec. 3].

In another direction of generalization, in the late 1980's, Stevenhagen [51, 52] formulated an abstract development of *unramified class field theory for orders*, which extends beyond orders of number fields; see also [51]. 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 2001 Stevenhagen [53, Sec. 4] recast much of Söhngen's class field theory for imaginary quadratic orders into a profinite, idèlic framework.

Very recently Campagna and Pengo [10, Sec. 4] developed a class field theory for orders of general number fields using an idèlic framework. They define ray class fields of orders by specifying a particular idèlic unit group attached to a level datum $(\mathcal{O}; \mathfrak{m}, \emptyset)$, which defines the associated class field by the idelic main theorem of class field theory. They did not consider ray conditions at the Archimedean places, since their interest was CM fields. The PhD thesis of Pengo [47, Sec. 6] formulated an idèlic definition of ray class fields for orders in the general case.

1.6. **Contents of the paper.** This paper works in the classical framework of integral and fractional ideals. Schertz [49, p. 82] used the classical framework in treating the theory of complex multiplication "because the classical language marries well with singular values of elliptic and modular functions that are essentially dependent on ideals." These functions are used in explicit class field theory. The classical ideal viewpoint is appropriate also for formulating the structures of monoids of all ray classes, allowing non-invertible classes, which arise in applications [32, 34].

Section 2 gives an extensive treatment of integral ideals of an order, including invertible and non-invertible ideals, needed for the constructions of ray class groups and maps between them. It emphasizes the special features of non-maximal orders and contains many examples. This section is needed because many calculations and proofs in the paper use possibly non-invertible integral ideals, sometimes in semilocal rings obtained by inverting elements coprime to a single auxiliary ideal $\mathfrak{d}$. 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. The set of integral ideals of an order of a number field coprime to a modulus ideal $\mathfrak{m}$ forms a monoid under ideal multiplication.

Section 3 treats fractional ideals of an order and gives further examples of behavior special to non-maximal orders. The ideal quotient of two fractional ideals is always well-defined; however, not all fractional ideals are invertible. There exist invertible ideals that are torsion elements of the invertible ideal group. The monoid of all nonzero fractional ideals coprime to the conductor ideal of the order is a free abelian group.

Section 4 studies, inside a fixed number field K, the effect of change of order on the structure of ideals, via the contraction and extension maps on integral and fractional ideals. A detailed treatment is needed for showing good behavior away from the conductor ideal and for proving exact sequences of ray class groups in Section 6. A ring-theoretic subtlety is that the contraction map $\mathrm{con}(\mathfrak{a}) = \mathfrak{a} \cap \mathcal{O}$ is not a monoid homomorphism for integral ideals. We show the contraction map when restricted to integral ideals coprime to the (relative) conductor ideal $\mathfrak{f}_{\mathcal{O}'}(\mathcal{O})$ is a monoid homomorphism. Using this property, we are able to define a contraction map on fractional ideals coprime to $\mathfrak{f}(\mathcal{O})$, which is a homomorphism but no longer agrees with the formula $\mathrm{con}(\mathfrak{a}) = \mathfrak{a} \cap \mathcal{O}$.

Section 5 defines ray class groups of orders for a level datum $(\mathcal{O}; \mathfrak{m}, \Sigma)$. It relates such groups under extension and contraction of order. Lemma 5.12 is a key technical result, showing that ray class groups do not change when adding coprimality conditions to an auxiliary modulus $\mathfrak{d}$, permitting comparison of different orders and different moduli. Section 5.4 determines a surjective map from a general ray class group of an order to a particular ray class group of the maximal order.

Section 6 gives exact sequences relating ray class groups under change of order and change of modulus. It first analyzes the effect of change of order $\mathcal{O} \subseteq \mathcal{O}'$ on unit groups and principal ideal groups, in Proposition 6.4. The exact sequence of Theorem 6.5 in Section 6.2, which relates unit groups and class groups of different orders and moduli, is the main formula of this paper for applications. Section 6.3 gives a formula for a generalized class number, that is, the cardinality of a given ray class group of an order. This formula generalizes a formula in Neukirch [46, Thm. I. 12.12] in the ring class group case.

Section 7 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 7.1. The desired ray class field of the order is then identified as a subfield L of a Takagi ray class field H_1. It is defined as the fixed field $L = H_1^{\mathrm{Art}(\ker(\psi))}$ of the kernel of the map ψ in (7.1) acting via the Artin map. Section 7.2 recalls the main existence theorems of class field theory 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 7.3 proves Theorem 1.1 by identifying the map ψ in (7.1) with the contraction map between fractional ideals of the maximal order $\mathcal{O}_K$ and the given order $\mathcal{O}$. Section 7.4 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 7.5 proves Theorem 1.3.

Section 8 presents examples of ray class groups and ray class fields of quadratic orders.

Section 9 presents some remarks on extending results of the paper.

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

1.7. **Notation.**

- $\mathcal{O}$ = arbitrary order of a number field K.
- $\mathfrak{f}(\mathcal{O}) = (\mathcal{O} : \mathcal{O}) =$ conductor ideal of $\mathcal{O}$.
- $\mathcal{O}'$ = 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 $\mathfrak{a}$, which is an order $\mathcal{O}'$.
- $\mathrm{I}(\mathcal{O}) =$ 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 $\mathcal{O}$.
- $\mathfrak{m}$ = general integral $\mathcal{O}$-ideal; finite part of the ray class modulus.
- Σ = subset of the set of real embeddings of K; infinite part of the ray class modulus.
- $\mathrm{I}_{\mathfrak{m}}(\mathcal{O}) =$ monoid of integral ideals of $\mathcal{O}$ coprime 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 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 coprime to the (nonzero) integral ideal $\mathfrak{m}$ of $\mathcal{O}$.

- $\mathrm{J}^*_{\mathfrak{m}}(\mathcal{O})$ = group of invertible fractional ideals coprime 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 $\alpha\mathcal{O}$, with $\alpha \in K^\times$, $\alpha \equiv 1 \pmod{\mathfrak{m}}$, and $\rho(\alpha) > 0$ for $\rho \in \Sigma$.
- $\mathrm{P}^{\mathfrak{d}}_{\mathfrak{m},\Sigma}(\mathcal{O})$ = 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 coprime to a given integral ideal $\mathfrak{d}$ of $\mathcal{O}$.
- $\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ = ray class group of order $\mathcal{O}$ with modulus $(\mathfrak{m}, \Sigma)$.
- $\mathcal{L} := (\mathcal{O}; \mathfrak{m}, \Sigma)$ abbreviates a (ray class) level datum, where $\mathcal{O}$ is an order of a number field K, $\mathfrak{m}$ is an integral $\mathcal{O}$-ideal, and Σ is a subset of the real places of K.

2. Ideals of orders

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 coprime 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.

Non-maximal orders of a number field are never Dedekind domains; rather, they are one-dimensional Noetherian integral domains that are not regular rings. The ideal theory of non-maximal orders has notable differences from that of the maximal order. Not all integral ideals factor into prime ideals (uniquely or otherwise). There exist non-invertible integral ideals. "Greatest common divisor" and "least common multiple" of ideals are not well-defined, although there is a notion of *coprimality* of two ideals. The failure of unique factorization into prime ideals is restored on restricting to ideals coprime to the conductor ideal $\mathfrak{f}(\mathcal{O}) = (\mathcal{O} : \mathcal{O}_K)$. In addition, the monoid of invertible integral ideals need not be free.

In the rest of Section 2 and in Section 3, we state and prove required foundational results at varying levels of generality, always restricted to commutative rings with unity. In decreasing generality, these include integral domains, Noetherian integral domains, Noetherian integral domains of dimension one, and orders $\mathcal{O}$ of algebraic number fields.

Compared to more general integral domains, orders of a number field K have strong 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

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

and it is an order of K. The multiplier ring is the largest order (as a set) such that Λ is a fractional ideal of that order. 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 well-known finiteness of the class group $\mathrm{Cl}(\mathcal{O})$ of an order.

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

We start with a general integral domain $\mathcal{D}$. An *integral ideal* (or simply an *ideal* or *$\mathcal{D}$-ideal*) $\mathfrak{a}$ of $\mathcal{D}$ is an $\mathcal{D}$-submodule $\mathfrak{a} \subseteq \mathcal{D}$. The *$\mathcal{D}$-ideal product* $\mathfrak{a}\mathfrak{b}$ of two $\mathcal{D}$-ideals $\mathfrak{a}, \mathfrak{b}$ is the $\mathcal{D}$-ideal

$$\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cdot \mathfrak{b} = \left\{ \sum_j \alpha_j\beta_j : \alpha_j \in \mathfrak{a}, \beta_j \in \mathfrak{b} \right\}. \tag{2.1}$$

We let $\mathrm{I}(\mathcal{D})$ denote the set of integral ideals of an integral domain, which forms a monoid for the operation of $\mathcal{D}$-ideal product, with $\mathcal{D}$ as the identity. A $\mathcal{D}$-ideal $\mathfrak{p}$ is *prime* if $xy \in \mathfrak{p}$ implies $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$, and $\mathfrak{p} \neq \mathcal{D}$. Additionally, there is a notion of coprimality of $\mathcal{D}$-ideals.

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

If $\mathfrak{a}, \mathfrak{b}$ are both coprime to $\mathfrak{m}$, then their product $\mathfrak{ab}$ is coprime to $\mathfrak{m}$, because

$$\mathcal{D} = (\mathfrak{a} + \mathfrak{m})(\mathfrak{b} + \mathfrak{m}) = \mathfrak{ab} + \mathfrak{am} + \mathfrak{bm} + \mathfrak{mm} \subseteq \mathfrak{ab} + \mathfrak{m} \subseteq \mathcal{D}.$$

We now specialize $\mathcal{D}$ to be a Noetherian integral domain. Thus, all ideals of $\mathcal{D}$ are finitely generated.

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* [4, Ch. 4]. 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 is primary. (Indeed, any power of a primary ideal 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 one-dimensional Noetherian domains, stronger results hold. One-dimensional Noetherian domains are Noetherian domains for which all nonzero prime ideals are maximal. The class of one-dimensional Noetherian domains includes all orders of number fields and is closed under localization and under completion. For a one-dimensional Noetherian domain $\mathcal{D}$, primary decompositions of ideals exist and are unique. In addition, the primary decomposition given as an intersection of ideals coincides with its decomposition as a product of the same primary ideals. To state the result precisely, recall that the *radical* of an ideal is

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

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 $\mathfrak{p}$, or alternatively, that $\mathfrak{q}$ is $\mathfrak{p}$*-primary.*

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*

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

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*

$$\mathfrak{m} = \prod_i \mathfrak{q}_i. \tag{2.2}$$

Proof. This is [4, Prop. 9.1]. The last assertion (2.2) is established in its proof. □

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

A prime ideal $\mathfrak{p}$ is called *non-singular* 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 2.13. 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*

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

Necessarily $\mathcal{O} \subseteq \mathrm{ord}(\mathfrak{a}) \subseteq \mathcal{O}_K$. All orders $\mathcal{O}'$ between $\mathcal{O}$ and $\mathcal{O}_K$ occur this way; one may choose $\gamma \in K^\times$ so that $\mathfrak{a} = \gamma\mathcal{O}' \subseteq \mathcal{O}$, and $\mathfrak{a}$ is then an integral $\mathcal{O}$-ideal having $\mathrm{ord}(\mathfrak{a}) = \mathcal{O}'$.

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 $\mathfrak{ab} = \gamma\mathcal{O}$. Otherwise $\mathfrak{a}$ is *non-invertible*.

The invertibility property is preserved under $\mathcal{O}$-ideal product. If $\mathfrak{ac} = \lambda\mathcal{O}$ and $\mathfrak{bd} = \mu\mathcal{O}$, then $(\mathfrak{ac})(\mathfrak{bd}) = \lambda\mu\mathcal{O}$, so $\mathfrak{ab}$ is invertible. This statement also has a converse.

Lemma 2.4. *Let $\mathcal{O}$ be an order of a number field.*

(1) *If $\mathfrak{c}$ is an invertible integral $\mathcal{O}$-ideal, and $\mathfrak{c} = \mathfrak{ab}$ as $\mathcal{O}$-ideals, then both $\mathfrak{a}$ and $\mathfrak{b}$ are invertible $\mathcal{O}$-ideals.*

(2) *If $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ are $\mathcal{O}$-ideals (invertible or not) and $\mathrm{ord}(\mathfrak{c}) = \mathcal{O}$, then $\mathfrak{c} = \mathfrak{ab}$ implies $\mathrm{ord}(\mathfrak{a}) = \mathrm{ord}(\mathfrak{b}) = \mathcal{O}$. In particular, all invertible integral $\mathcal{O}$-ideals $\mathfrak{a}$ have $\mathrm{ord}(\mathfrak{a}) = \mathcal{O}$.*

Proof of (1). Given $\mathfrak{c} = \mathfrak{ab}$ is invertible, then there is an integral ideal $\mathfrak{d}$ with $\mathfrak{cd} = \gamma\mathcal{O}$. Now $\mathfrak{a}$ is invertible since $\mathfrak{a}(\mathfrak{bd}) = \mathfrak{cd} = \gamma\mathcal{O}$, and similarly for $\mathfrak{b}$. □

Proof of (2). Given $\mathfrak{c} = \mathfrak{ab}$, we have $\mathrm{ord}(\mathfrak{a}) \subseteq \mathrm{ord}(\mathfrak{ab}) = \mathrm{ord}(\mathfrak{c})$. Since $\mathcal{O} \subseteq \mathrm{ord}(\mathfrak{a}) \subseteq \mathrm{ord}(\mathfrak{c})$ and $\mathrm{ord}(\mathfrak{c}) = \mathcal{O}$ by hypothesis, we have $\mathrm{ord}(\mathfrak{a}) = \mathcal{O}$; similarly $\mathrm{ord}(\mathfrak{b}) = \mathcal{O}$. For invertible ideals we have $\mathfrak{ac} = \gamma\mathcal{O}$. Since $\mathrm{ord}(\gamma\mathcal{O}) = \mathcal{O}$, we deduce $\mathrm{ord}(\mathfrak{a}) = \mathcal{O}$. □

We let $\mathrm{I}^*(\mathcal{O})$ denote the monoid of invertible integral ideals under ideal multiplication. All nonzero principal ideals $\mathfrak{a} = \alpha\mathcal{O} \in \mathrm{I}^*(\mathcal{O})$, because $(\alpha\mathcal{O})(\mathcal{O}) = \alpha\mathcal{O}$.

Not all ideals of a general order $\mathcal{O}$ are invertible; a necessary condition for invertibility of an $\mathcal{O}$-ideal $\mathfrak{a}$ is that $\mathrm{ord}(\mathfrak{a}) = \mathcal{O}$, as given in Lemma 2.4(2). The next example shows this necessary condition is in general not sufficient.

Example 2.5. [Non-invertible ideal $\mathfrak{q}$ of $\mathcal{O}$ with $\mathrm{ord}(\mathfrak{q}) = \mathcal{O}$] (This phenomenon occurs only for number fields K with $[K : \mathbb{Q}] \geq 3$ having a non-Gorenstein order $\mathcal{O}$; see also [11].) Take $K = \mathbb{Q}(\sqrt[3]{2})$, and consider three orders of K with $\mathcal{O} \subsetneq \mathcal{O}' \subsetneq \mathcal{O}_K$ given by:

$$\mathcal{O} = \mathbb{Z}[2\sqrt[3]{2}, 2\sqrt[3]{4}] = \mathbb{Z} + 2\sqrt[3]{2}\mathbb{Z} + 2\sqrt[3]{4}\mathbb{Z};$$
$$\mathcal{O}' = \mathbb{Z}[\sqrt[3]{4}] = \mathbb{Z} + 2\sqrt[3]{2}\mathbb{Z} + \sqrt[3]{4}\mathbb{Z};$$
$$\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}] = \mathbb{Z} + \sqrt[3]{2}\mathbb{Z} + \sqrt[3]{4}\mathbb{Z}.$$

We set $\mathfrak{q} = 2\mathbb{Z} + 2\sqrt[3]{2}\mathbb{Z} + 4\sqrt[3]{4}\mathbb{Z}$ and note it is a $\mathcal{O}$-ideal of index 4 in $\mathcal{O}$, hence a primary ideal of $\mathcal{O}$. We show $\mathfrak{q}$ is not invertible as an $\mathcal{O}$-ideal by contradiction. If it were invertible, then $\mathfrak{q}^2$ would also be an invertible $\mathcal{O}$-ideal. Now $\mathfrak{q}^2 = 4\mathbb{Z} + 4\sqrt[3]{2}\mathbb{Z} + 4\sqrt[3]{4}\mathbb{Z} = 4\mathcal{O}_K$ has $\mathrm{ord}(\mathfrak{q}^2) = (\mathfrak{q}^2 : \mathfrak{q}^2) = \mathcal{O}_K$, so $\mathfrak{q}^2$ is not invertible for $\mathcal{O}$ by Lemma 2.4(2), a contradiction.

Secondly, $\mathfrak{q}$ has multiplier ring $\mathrm{ord}(\mathfrak{q}) = (\mathfrak{q} : \mathfrak{q}) = \mathcal{O}$. To see this, we observe that the only orders containing $\mathcal{O}$ are $\mathcal{O}'$ and $\mathcal{O}_K$. It suffices to show $\mathfrak{q}\mathcal{O}' \neq \mathfrak{q}$, which holds because $2 \in \mathfrak{q}$ and $\sqrt[3]{4} \in \mathcal{O}'$ have product $2\sqrt[3]{4} \notin \mathfrak{q}$. Thus, $\mathfrak{q}$ is not an $\mathcal{O}'$-ideal, hence $\mathrm{ord}(\mathfrak{q}) = \mathcal{O}$.

There is a factorization theory for invertible integral ideals based on a notion of irreducible integral ideal. In general this theory does not result in unique factorizations, nor are irreducible integral ideals always prime.

Definition 2.6 (Irreducible integral ideal)**.** An invertible 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, contradicting irreducibility.) 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 phenomena are illustrated by Example 2.8.

Example 2.7 (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 $\mathcal{O}_K$. 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 2.8 (Nonunique factorization of an invertible ideal into irreducible invertible factors)**.** Let $K = \mathbb{Q}(\sqrt{2})$ with $\mathcal{O}_K = \mathbb{Z}+\sqrt{2}\mathbb{Z}$, and let $\mathcal{O} = \mathbb{Z}+2\sqrt{2}\mathbb{Z}$. Then $\mathcal{O}$ does not contain the fundamental unit $\varepsilon = 1 + \sqrt{2}$, but does contain $\varepsilon^2 = 3 + 2\sqrt{2}$. Now the two $\mathcal{O}$-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 $\mathcal{O}$-ideals, hence invertible. They are both primary ideals associated to the prime ideal $\mathfrak{p} = 2\mathbb{Z}+2\sqrt{2}\mathbb{Z} = 2\mathcal{O}_K \subsetneq \mathcal{O}$, which is not invertible. The ideal $\mathfrak{p}$ has index 2 in $\mathcal{O}$. Therefore $\mathfrak{q}_1$ and $\mathfrak{q}_2$, which are each of index 4 in $\mathcal{O}$ and index 2 in $\mathfrak{p}$, must be irreducible. One has

$$(\mathfrak{q}_1)^2 = (\mathfrak{q}_2)^2 = 4\mathcal{O} = 4\mathbb{Z} + 8\sqrt{2}\mathbb{Z}.$$

Thus the invertible ideal $4\mathcal{O}$ 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 is an important invariant of the order that contains information on the non-invertible ideals of $\mathcal{O}$.

Definition 2.9. The absolute and relative conductor are defined as follows.

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

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

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

Example 2.10 (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
$$\mathcal{O}_{f^2\Delta} = \mathbb{Z}\left[\frac{f^2\Delta + \sqrt{f^2\Delta}}{2}\right] = \mathbb{Z} + f\frac{\Delta+\sqrt{\Delta}}{2}\mathbb{Z}$$
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 2.11 (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
$$\mathcal{O} = \mathbb{Z}[5\omega, 5i, 5\omega i] = \mathbb{Z} + 5\omega\mathbb{Z} + 5i\mathbb{Z} + 5\omega i\mathbb{Z} \text{ and}$$
$$\mathcal{O}' = \mathbb{Z}[\omega, 5i] = \mathbb{Z} + \omega\mathbb{Z} + 5i\mathbb{Z} + 5\omega i\mathbb{Z}.$$
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 2.12 (Noninvertible relative conductor)**.** We compute the relative conductor for orders $\mathcal{O}$ and $\mathcal{O}'$ in Example 2.11. 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. Therefore it is not invertible as an integral $\mathcal{O}$-ideal by Lemma 2.4(2).

The conductor determines all singular prime ideals.

Lemma 2.13. *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 not coprime to $\mathfrak{f}(\mathcal{O})$, that is, $\mathfrak{p} + \mathfrak{f}(\mathcal{O}) = \mathfrak{p}$. Equivalently, $\mathfrak{f}(\mathcal{O}) \subseteq \mathfrak{p}$.*
(2) *$\mathfrak{p}$ is a non-invertible prime ideal of $\mathcal{O}$.*
(3) *$\mathfrak{p}$ is a singular prime ideal of $\mathcal{O}$.*

Proof. For any prime ideal $\mathfrak{p}$ 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 coprime to $\mathfrak{f}(\mathcal{O})$ if and only if $\mathfrak{p} + \mathfrak{f}(\mathcal{O}) = \mathfrak{p}$.

Proof of (1) $\Leftrightarrow$ (2). The contrapositive of this assertion says: $\mathfrak{p}$ is an invertible prime ideal of $\mathcal{O}$ if and only if $\mathfrak{f}(\mathcal{O}) \not\subseteq \mathfrak{p}$. Since $\mathfrak{p}$ is maximal, the latter means $\mathfrak{p} + \mathfrak{f}(\mathcal{O}) = \mathcal{O}$, that is, $\mathfrak{p}$ is coprime to $\mathfrak{f}(\mathcal{O})$. The contrapositive is proved as [46, Ch. I, Prop. 12.10].

Proof of (2) $\Leftrightarrow$ (3). The contrapositive of the assertion says: $\mathfrak{p}$ is an invertible prime ideal of $\mathcal{O}$ if and only if $\mathfrak{p}$ is a non-singular 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 [46, Ch. I, Sec. 11, 12 and Lem. 12.4].) Equivalently, the localization $\mathcal{O}_{\mathfrak{p}}$ is a discrete valuation ring, so the set of all nonzero ideals in the local ring are powers of the maximal ideal $\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$, that is, $\mathfrak{p}$ is non-singular, as required. □

In the next example, the *norm* of an integral ideal $\mathfrak{a}$ of an order $\mathcal{O}$ is the index

$$\mathrm{Nm}_{\mathcal{O}}(\mathfrak{a}) := [\mathcal{O} : \mathfrak{a}]$$

with $\mathcal{O}$ and $\mathfrak{a}$ regarded as $\mathbb{Z}$-modules. This definition coincides with the usual definition of *norm* of an ideal for the maximal order. Norms are treated in Appendix A, where the definition of *norm* is extended to fractional ideals of an order.

Example 2.14 (Structure of primary ideals for $\mathfrak{p}$ containing $\mathfrak{f}(\mathcal{O})$; failure of gcd and lcm)**.** The set of primary ideals $\mathfrak{q}$ associated to a prime ideal $\mathfrak{p}$ containing the conductor ideal $\mathfrak{f}(\mathcal{O})$ can have a very complicated structure.

(1) The containment of ideals $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ does not always imply the divisibility of $\mathfrak{q}_1$ by $\mathfrak{q}_2$.
(2) For suitable pairs of primary ideal, non-existence of gcd and of lcm can occur.
(3) The ideal norm function may not multiplicative on primary ideals.

Let $K = \mathbb{Q}(i)$ with maximal order $\mathcal{O}_K = \mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z}$, and consider the order $\mathcal{O} = \mathbb{Z}[2i] = \mathbb{Z} + 2i\mathbb{Z}$ of index 2 in $\mathcal{O}_K$. The conductor ideal $\mathfrak{f}(\mathcal{O}) = 2\mathcal{O}_K = 2\mathbb{Z} + 2i\mathbb{Z}$ is a maximal ideal of $\mathcal{O}$, since it is of index 2 in $\mathcal{O}$. We consider the set $\mathcal{F}$ of all primary ideals associated to $\mathfrak{f}(\mathcal{O})$, and sort them by the size of their norm, which is always a power of 2. The unique element of norm 2 in $\mathcal{O}$ is $\mathfrak{Q}_2 := \mathfrak{f}(\mathcal{O})$. Since $\mathrm{ord}(\mathfrak{Q}_2) = \mathcal{O}_K$ is larger than $\mathcal{O}$, $\mathfrak{Q}_2$ is not invertible for $\mathcal{O}$ by Lemma 2.4(2).

There are two invertible ideals in $\mathcal{F}$ of norm 4, both principal:

$$\mathfrak{q}_4 := 2\mathcal{O} = 2\mathbb{Z} + 4i\mathbb{Z} \quad \text{and} \quad \mathfrak{q}_4' := 2i\mathcal{O} = 4\mathbb{Z} + 2i\mathbb{Z}.$$

There is also one non-invertible ideal of norm 4,

$$\mathfrak{Q}_4 := 2(1+i)\mathcal{O}_K = 4\mathbb{Z} + (2+2i)\mathbb{Z}.$$

Both $\mathfrak{q}_4$ and $\mathfrak{q}_4'$ are contained in $\mathfrak{Q}_2$, but they cannot be divisible by $\mathfrak{Q}_2$ because it is a non-invertible ideal, while all divisors of invertible ideals are invertible by Lemma 2.4(1). This illustrates (1).

Note that $\mathfrak{q}_4$ and $\mathfrak{q}_4'$ are irreducible integral ideals, as their only (integral ideal) common divisor is $\mathcal{O}$. However, they are not coprime integral ideals, since $\mathfrak{q}_4 + \mathfrak{q}_4' = \mathfrak{Q}_2$.

In addition $\mathfrak{Q}_4$ is an irreducible $\mathcal{O}$-integral ideal, because it is not divisible by $\mathfrak{Q}_2$ viewed as an $\mathcal{O}$-integral ideal. This holds since $(1+i)\mathcal{O}_K$ is not an integral $\mathcal{O}$-ideal, as it contains $1 + i \notin \mathbb{Z}[2i]$. ($\mathfrak{Q}_2$ is divisible by $(1+i)\mathcal{O}_K$ viewed as an $\mathcal{O}_K$-ideal.)

There is a single ideal in $\mathcal{F}$ of norm 8, which is $\mathfrak{Q}_8 := (\mathfrak{Q}_2)^2 = 4\mathcal{O}_K = 4\mathbb{Z} + 4i\mathbb{Z}$. It is a non-invertible ideal, since $\mathrm{ord}(\mathfrak{Q}_8) = \mathcal{O}_K$. Now $\mathfrak{Q}_8 = (\mathfrak{Q}_2)^2$, so we have

$$8 = \mathrm{Nm}_{\mathcal{O}}(\mathfrak{Q}_8) = \mathrm{Nm}_{\mathcal{O}}((\mathfrak{Q}_2)^2) > (\mathrm{Nm}_{\mathcal{O}}\,\mathfrak{Q}_2)^2 = 4.$$

This illustrates that the ideal norm on $\mathcal{O}$ is not always multiplicative, giving assertion (3).

We also note that $\mathfrak{q}_4\mathfrak{Q}_2 = \mathfrak{q}_4'\mathfrak{Q}_2 = \mathfrak{Q}_8$. The norms are multiplicative in this case, since $\mathfrak{q}_4$ is invertible; see Proposition A.2 in Appendix A.

We now study the primary ideals of norm 16 in $\mathcal{F}$. There are two invertible ideals:

$$\mathfrak{q}_{16} := 4\mathcal{O} = 4\mathbb{Z} + 8i\mathbb{Z} \quad \text{and} \quad \mathfrak{q}'_{16} := 4i\mathcal{O} = 8\mathbb{Z} + 4i\mathbb{Z}.$$

There is also a non-invertible ideal of norm 16,

$$\mathfrak{Q}_{16} := 4(1+i)\mathcal{O}_K = 8\mathbb{Z} + (4+4i)\mathbb{Z}.$$

As invertible ideals, $\mathfrak{q}_{16}$ and $\mathfrak{q}'_{16}$ cannot be divisible by $\mathfrak{Q}_2$, $\mathfrak{Q}_4$ or $\mathfrak{Q}_8$. We find that

$$\mathfrak{q}_{16} = (\mathfrak{q}_4)^2 = (\mathfrak{q}'_4)^2 \quad \text{and} \quad \mathfrak{q}'_{16} = \mathfrak{q}_4\mathfrak{q}'_4. \tag{2.3}$$

It follows that each of $\mathfrak{q}_{16}$ and $\mathfrak{q}'_{16}$ are contained in both $\mathfrak{q}_4$ and in $\mathfrak{q}'_4$. In the divisibility partial order, the factorization (2.3) shows that there are no intermediate elements of the partial order between $\mathfrak{q}_4$ (respectively, $\mathfrak{q}'_4$) and either $\mathfrak{q}_{16}$ or $\mathfrak{q}'_{16}$ (since $\mathfrak{q}_4$ and $\mathfrak{q}'_4$ are irreducible). Consequently, the lcm of $\mathfrak{q}_4$ and $\mathfrak{q}'_4$ is not well-defined, and the gcd of $\mathfrak{q}_{16}$ and $\mathfrak{q}'_{16}$ is not well defined. This illustrates (2).

The divisibility partial order relating these ideals is pictured in Figure 1.

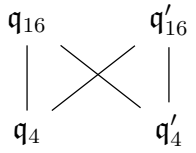

FIGURE 1. Hasse diagram for $\{\mathfrak{q}_4, \mathfrak{q}'_4, \mathfrak{q}_{16}, \mathfrak{q}'_{16}\}$.

Remark 2.15 (Structure of primary ideals for prime ideals $\mathfrak{p}$ not containing $\mathfrak{f}(\mathcal{O})$)**.** For prime ideals $\mathfrak{p}$ coprime to the conductor ideal $\mathfrak{f}(\mathcal{O})$, none of the pathologies (1)–(3) shown in Example 2.14 occur. The contrapositive of Lemma 2.13 shows that $\mathfrak{p}$ is an invertible ideal and is non-singular, that is, its complete set of $\mathfrak{p}$-primary ideals is $\{\mathfrak{p}^j : j \geq 1\}$. For $\mathfrak{p}$-primary ideals, containment is equivalent to divisibility, so gcd and lcm are well-defined. The $\mathcal{O}$-norms of $\mathfrak{p}$-primary ideals are multiplicative by Proposition A.2, because all $\mathfrak{p}^j$ are invertible.

2.4. **Monoids of integral ideals coprime to a fixed modulus $\mathfrak{m}$.** Recall that $\mathrm{I}(\mathcal{O})$ denotes the monoid of all integral ideals and $\mathrm{I}^*(\mathcal{O})$ the monoid of all invertible integral ideals. We introduce monoids of integral ideals and invertible integral ideals coprime to a fixed modulus $\mathfrak{m}$.

Definition 2.16 (Monoids of integral ideals coprime to $\mathfrak{m}$)**.** Given an integral ideal $\mathfrak{m}$ of an order $\mathcal{O}$ of a number field, let $\mathrm{I}_{\mathfrak{m}}(\mathcal{O})$ denote the set of $\mathfrak{m}$-*coprime integral ideals* of $\mathcal{O}$, and let $\mathrm{I}^*_{\mathfrak{m}}(\mathcal{O})$ denote the set of $\mathfrak{m}$-*coprime invertible integral ideals*. That is,

$$\mathrm{I}_{\mathfrak{m}}(\mathcal{O}) = \{\mathfrak{a} \in \mathrm{I}(\mathcal{O}) : \mathfrak{a} + \mathfrak{m} = \mathcal{O}\}, \qquad \text{and} \qquad \mathrm{I}^*_{\mathfrak{m}}(\mathcal{O}) = \{\mathfrak{a} \in \mathrm{I}^*(\mathcal{O}) : \mathfrak{a} + \mathfrak{m} = \mathcal{O}\}.$$

Lemma 2.17. *Let $\mathcal{O}$ be an order of a number field and $\mathfrak{m}$ an integral ideal of $\mathcal{O}$.*

(1) *The sets $\mathrm{I}_{\mathfrak{m}}(\mathcal{O})$ and $\mathrm{I}^*_{\mathfrak{m}}(\mathcal{O})$ are monoids for $\mathcal{O}$-ideal product.*
(2) *If $\mathfrak{m}, \mathfrak{m}'$ are ideals of $\mathcal{O}$ with $\mathfrak{m} \subseteq \mathfrak{m}'$, then $\mathrm{I}_{\mathfrak{m}}(\mathcal{O}) \subseteq \mathrm{I}_{\mathfrak{m}'}(\mathcal{O})$, and $\mathrm{I}^*_{\mathfrak{m}}(\mathcal{O}) \subseteq \mathrm{I}^*_{\mathfrak{m}'}(\mathcal{O})$.*

Proof of (1). We check that these sets are closed under $\mathcal{O}$-ideal product. If $\mathfrak{a} + \mathfrak{m} = \mathcal{O}$ and $\mathfrak{b} + \mathfrak{m} = \mathcal{O}$, then

$$\mathcal{O} = (\mathfrak{a} + \mathfrak{m})(\mathfrak{b} + \mathfrak{m}) = \mathfrak{a}\mathfrak{b} + (\mathfrak{a}\mathfrak{m} + \mathfrak{b}\mathfrak{m} + \mathfrak{m}\mathfrak{m}) = \mathfrak{a}\mathfrak{b} + \mathfrak{m}.$$

We noted earlier that invertibility of integral ideals is preserved under $\mathcal{O}$-ideal product. $\square$

Proof of (2). If $\mathfrak{a} + \mathfrak{m} = \mathcal{O}$ and $\mathfrak{m} \subseteq \mathfrak{m}'$, then $\mathfrak{a} + \mathfrak{m}' = \mathcal{O}$, since $\mathfrak{a} + \mathfrak{m} \subseteq \mathcal{O}$. □

The next result shows that for any $\mathfrak{m}$ contained in the conductor ideal, the associated monoid of integral ideals coprime to $\mathfrak{m}$ has unique factorization into prime ideals.

Proposition 2.18. *Let $\mathcal{O}$ be an order of a number field K, with $\mathfrak{f}(\mathcal{O})$ its absolute conductor ideal. Suppose the integral ideal $\mathfrak{m}$ has $\mathfrak{m} \subseteq \mathfrak{f}(\mathcal{O})$. Then, the following hold.*

1. *The monoid $\mathrm{I}_{\mathfrak{m}}^*(\mathcal{O})$ is a free abelian monoid whose set of generators is the set of prime ideals $\mathbb{P}(\mathfrak{m}) = \{\mathfrak{p} : \mathfrak{m} \not\subseteq \mathfrak{p},\ \mathfrak{p} \neq \{0\}\}$. All the prime ideals in $\mathbb{P}(\mathfrak{m})$ are non-singular, and all ideals $\mathfrak{a} \in \mathrm{I}_{\mathfrak{m}}^*(\mathcal{O})$ have unique prime factorization into nonnegative powers of prime ideals in $\mathbb{P}(\mathfrak{m})$.*
2. *The monoid $\mathrm{I}_{\mathfrak{m}}(\mathcal{O})$ of nonzero ideals coprime to $\mathfrak{m}$ and the monoid $\mathrm{I}_{\mathfrak{m}}^*(\mathcal{O})$ of invertible ideals coprime to $\mathfrak{m}$ coincide.*

Proof of (1). We suppose $\mathfrak{m} \subseteq \mathfrak{f}(\mathcal{O}) = (\mathcal{O} : \mathcal{O}_K)$. All ideals in $\mathrm{I}_{\mathfrak{m}}(\mathcal{O})$ are coprime to $\mathfrak{m}$, hence they are coprime to $\mathfrak{f}(\mathcal{O})$. But the prime ideals not coprime to $\mathfrak{f}(\mathcal{O})$ are exactly the singular prime ideals by Lemma 2.13(3). Thus $\mathbb{P}(\mathfrak{m})$ contains only non-singular prime ideals. Since coprimality to $\mathfrak{m}$ is preserved by ideal product, all products of a finite number of ideals drawn from $\mathbb{P}(\mathfrak{m})$ (allowing multiplicity) belong to $\mathrm{I}_{\mathfrak{m}}(\mathcal{O})$. This exhausts the allowed primary decompositions of elements of $\mathrm{I}(\mathcal{O})$, hence $\mathrm{I}(\mathcal{O})$ is a free abelian monoid. □

Proof of (2). The result follows (1) because all non-singular prime ideals of $\mathcal{O}$ are invertible, by Lemma 2.13. □

Remark 2.19. The conclusions of Proposition 2.18 need not hold for non-maximal orders when $\mathfrak{m} \not\subseteq \mathfrak{f}(\mathcal{O})$. The following examples take $\mathfrak{m} = \mathcal{O}$.

1. For some non-maximal orders $\mathcal{O}$, the monoid of all invertible integral ideals $\mathrm{I}^*(\mathcal{O}) = \mathrm{I}_{\mathcal{O}}^*(\mathcal{O})$ is not a free abelian monoid, because its irreducible elements may satisfy nontrivial relations. See Example 2.14, (2.3), where $\mathfrak{q}_4$ and $\mathfrak{q}_4'$ are distinct irreducible ideals, but $(\mathfrak{q}_4)^2 = (\mathfrak{q}_4')^2$.
2. For any non-maximal order, the monoid $\mathrm{I}(\mathcal{O}) = \mathrm{I}_{\mathcal{O}}(\mathcal{O})$ of all integral ideals contains noninvertible ideals. The conductor ideal has $\mathrm{ord}(\mathfrak{f}(\mathcal{O})) = \mathcal{O}_K \neq \mathcal{O}$, so is not invertible by Lemma 2.4(2).

3. Fractional ideals of orders

This section treats fractional ideals of Noetherian integral domains of dimension one, and in particular, orders of number fields.

The fractional ideal theory of non-maximal orders of number fields has some key differences from that of the maximal order. Not all fractional ideals are invertible, and the set of fractional ideals under ideal multiplication has the structure of a monoid (a semigroup with identity) that is not a group. The group of invertible fractional ideals need not be free; it may contain (a finite number of) torsion elements.

3.1. Fractional ideals for integral domains.

Following [18, Defn. 1.1.6], define fractional ideals for Noetherian integral domains.

Definition 3.1 (Fractional ideal)**.** A *fractional ideal* $\mathfrak{a}$ of a Noetherian integral domain $\mathcal{D}$ is a $\mathcal{D}$-submodule of its fraction field K with the property that $\lambda\mathfrak{a} \subseteq \mathcal{D}$ for some $\lambda \in K^\times$. (A *integral ideal* is a fractional ideal contained in $\mathcal{D}$.)

The set of fractional ideals of $\mathcal{D}$ has sum, product, intersection, and quotient operations. In particular, the *ideal product* operation $\cdot$ is defined as in (2.1). The *ideal quotient* (or *colon ideal*) operation $(\ :\ )$ is

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

As for integral ideals, we define the *multiplier ring* of a fractional ideal $\mathfrak{a}$ as $\mathrm{ord}(\mathfrak{a}) = (\mathfrak{a} : \mathfrak{a})$.

Proposition 3.2. *The set* $\mathrm{J}(\mathcal{D})$ *of all fractional ideals of a Noetherian integral domain* $\mathcal{D}$ *is closed under the four operations* $+$, $\cdot$, $\cap$, *and* $(\ :\ )$ *(addition, multiplication, intersection, and ideal quotient.)*

Proof. This is [18, Prop. 1.1.11]. □

The set of all fractional ideals of $\mathrm{J}(\mathcal{D})$ forms a monoid under the ideal product operation, with identity element $\mathcal{D}$.

We extend the notion of coprimality to that between a fractional ideal and an integral ideal; we do not define coprimality between two non-integral fractional ideals of $\mathcal{D}$.

Definition 3.3 (Coprimality of a fractional ideal and an integral ideal)**.** A fractional $\mathcal{D}$-ideal $\mathfrak{d}$ is *coprime* to an integral ideal $\mathfrak{c} \subseteq \mathcal{D}$ if it may be written as a quotient $\mathfrak{d} = (\mathfrak{a} : \mathfrak{b})$, where $\mathfrak{a}$ is an $\mathcal{D}$-integral ideal coprime to $\mathfrak{c}$, and $\mathfrak{b}$ is an invertible $\mathcal{D}$-integral ideal coprime to $\mathfrak{c}$.

In this definition, one cannot always choose $\mathfrak{a}, \mathfrak{b}$ to be coprime to each other, even when $\mathcal{D} = \mathcal{O}$ is an order of a number field; see Example 3.11. Nevertheless one may check that, if $\mathfrak{d}_1, \mathfrak{d}_2$ are coprime to $\mathfrak{c}$, then so is their ideal product $\mathfrak{d}_1\mathfrak{d}_2$.

Definition 3.4 (Invertible fractional ideal)**.** A fractional $\mathcal{D}$-ideal $\mathfrak{a}$ is *invertible* for $\mathcal{D}$ if there is another fractional ideal $\mathfrak{b}$ of $\mathcal{D}$ such that $\mathfrak{a}\mathfrak{b} = \mathcal{D}$. Otherwise it is *non-invertible* for $\mathcal{D}$.

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. There is a converse invertibility result for fractional ideals that extends Lemma 2.4 for integral ideals.

Lemma 3.5. *Let* $\mathcal{D}$ *be a Noetherian integral domain.*

(1) *If* $\mathfrak{c}$ *is an invertible fractional* $\mathcal{D}$*-ideal, and* $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ *with* $\mathfrak{a}, \mathfrak{b}$ *fractional* $\mathcal{D}$*-ideals, then* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are both invertible fractional* $\mathcal{D}$*-ideals.*

(2) *If* $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ *are all* $\mathcal{D}$*-fractional ideals (invertible or not) and* $\mathrm{ord}(\mathfrak{c}) = \mathcal{D}$*, then* $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ *implies* $\mathrm{ord}(\mathfrak{a}) = \mathrm{ord}(\mathfrak{b}) = \mathcal{D}$*. In particular all invertible fractional* $\mathcal{D}$*-ideals* $\mathfrak{a}$ *have* $\mathrm{ord}(\mathfrak{a}) = \mathcal{D}$*.*

Proof. The proof is identical to the proof of Lemma 2.4, replacing $\mathcal{O}$ by $\mathcal{D}$ and "integral" by "fractional." □

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 3.6. *Let* $\mathcal{D}$ *be a Noetherian integral domain, and let* $\mathfrak{a}$ *and* $\mathfrak{b}$ *be integral* $\mathcal{D}$*-ideals. If* $\mathfrak{b}$ *is invertible as a fractional ideal of* $\mathcal{D}$*, then the fractional ideal* $(\mathfrak{a} : \mathfrak{b}) = \mathfrak{a}\mathfrak{b}^{-1}$*.*

Proof. We first show $(\mathfrak{a} : \mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b}^{-1}$, or equivalently (since $\mathfrak{b}$ is invertible) 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, $cb \in \mathfrak{a}$.

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, $d\mathfrak{b} \subseteq \mathcal{D}$, so $ad\mathfrak{b} \subseteq a\mathcal{D} \subseteq \mathfrak{a}$. By definition of the quotient ideal, $ad \in (\mathfrak{a} : \mathfrak{b})$. □

Lemma 3.7. *Let $\mathcal{D}$ be a Noetherian integral domain.*

(1) *Any invertible fractional ideal $\mathfrak{a}$ of $\mathcal{D}$ with $\mathfrak{a} \subseteq \mathcal{D}$ is an invertible integral ideal, and conversely.*
(2) *If two integral ideals $\mathfrak{c}, \mathfrak{d}$ of $\mathcal{D}$ are coprime as integral ideals, then $\mathfrak{d}$, regarded as a fractional ideal, is coprime to $\mathfrak{c}$, and conversely.*

Proof of (1). Given an integral ideal $\mathfrak{a} \subseteq \mathcal{D}$ invertible as a fractional ideal, there is a fractional ideal $\mathfrak{c}$ such that $\mathfrak{ac} = \mathcal{D}$. There exists $\lambda \in \mathcal{D}$ so that $\lambda\mathfrak{c} \subseteq \mathcal{D}$ is an integral ideal, and $\mathfrak{a}(\lambda\mathfrak{c}) = \lambda\mathcal{D}$ certifies that $\mathfrak{a}$ is an invertible integral ideal.

Given an invertible integral ideal $\mathfrak{a}$, there is some integral ideal $\mathfrak{b}$ such that $\mathfrak{ab} = \gamma\mathcal{D}$ for a nonzero $\gamma \in \mathcal{D}$. Then $\mathfrak{a}(\gamma^{-1}\mathfrak{b}) = \mathcal{D}$ certifies $\mathfrak{a}$ is an invertible fractional ideal. □

Proof of (2). Suppose $\mathfrak{c}, \mathfrak{d}$ are integral ideals satisfying the coprimality condition $\mathfrak{c} + \mathfrak{d} = \mathcal{D}$. Viewing $\mathfrak{d}$ as a fractional ideal, the decomposition $\mathfrak{d} = (\mathfrak{d} : \mathcal{D})$ certifies the fractional ideal $\mathfrak{d}$ is coprime to $\mathfrak{c}$, since $\mathfrak{d}$ (on the right side of the decomposition) is by hypothesis coprime to $\mathfrak{c}$ as an integral ideal, and $\mathcal{D}$ is an invertible integral ideal coprime to $\mathfrak{c}$.

Conversely, we are given integral ideals $\mathfrak{c}, \mathfrak{d}$ for which $\mathfrak{d}$, regarded as a fractional ideal, is coprime to $\mathfrak{c}$. Then we have $\mathfrak{d} = (\mathfrak{a} : \mathfrak{b})$ for two integral ideals $\mathfrak{a}, \mathfrak{b}$ in which $\mathfrak{b}$ is invertible and $\mathfrak{c} + \mathfrak{a} = \mathfrak{c} + \mathfrak{b} = \mathcal{D}$. By Lemma 3.6, $\mathfrak{d} = \mathfrak{ab}^{-1}$. Thus, as fractional ideals, we have $\mathfrak{db} = \mathfrak{a}$, and $\mathfrak{a} \subseteq \mathfrak{d}$, since $\mathfrak{b}$ is an integral ideal. Now $\mathfrak{c} + \mathfrak{a} = \mathcal{D}$ means there exists $c \in \mathfrak{c}$ and $a \in \mathfrak{a}$ such that $c + a = 1$, and necessarily $a \in \mathfrak{d}$, so $\mathfrak{c} + \mathfrak{d} = \mathcal{D}$. □

Invertible fractional ideals are characterized by local data.

Proposition 3.8. *If $\mathcal{D}$ is any Noetherian 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 a special case of of [18, Cor. 2.1.7]. □

The next lemma collects basic properties of ideal quotients of fractional ideals and deduces the inclusions in (5), which justify (1.2), taking $\mathcal{D} = \mathcal{O}$ and $\mathcal{D}' = \mathcal{O}'$.

Lemma 3.9. *Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ be fractional ideals in a Noetherian 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 $\mathcal{D}$, and suppose $\mathcal{D} \subseteq \mathcal{D}'$ with $\mathcal{D}'$ a Noetherian integral domain that is also a fractional ideal of $\mathcal{D}$. Set $\mathfrak{f}_{\mathcal{D}'}(\mathcal{D}) = (\mathcal{D} : \mathcal{D}')$. Then

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

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

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

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

$$(\mathfrak{m} : \mathcal{D}') \subseteq (\mathfrak{m}\mathcal{D}' : \mathcal{D}'\mathcal{D}') = (\mathfrak{m}\mathcal{D}' : \mathcal{D}') = \mathfrak{m}\mathcal{D}',$$

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

3.2. **Fractional ideals for orders of number fields.** We specialize to the case of an order $\mathcal{O}$ of a number field K.

For the maximal order $\mathcal{O}_K$ (and more generally for Dedekind domains), the fractional ideal group $\mathrm{J}^*(\mathcal{O}_K)$ is a free abelian group. For non-maximal orders $\mathcal{O}$, $\mathrm{J}^*(\mathcal{O})$ may contain a (finite) nontrivial torsion subgroup; see Example 3.11.

Concerning coprimality, 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 $\mathcal{O}$.

Example 3.10 (Non-integral fractional ideals having an ideal power that is an integral ideal)**.** Consider the non-maximal order $\mathcal{O} = \mathbb{Z}[2i]$ of the Gaussian field $K = \mathbb{Q}(i)$, whose maximal order is $\mathcal{O}_K = \mathbb{Z}[i]$.

(1) The non-integral fractional ideal
$$\mathfrak{a} := (1+i)\mathcal{O} = 4\mathbb{Z} + (1+i)\mathbb{Z}$$
is a principal fractional ideal; hence, it is an invertible fractional ideal. It has ideal square $\mathfrak{a}^2 = 2i\mathcal{O} = \mathfrak{q}_4'$ (in the notation of Example 2.14), which is an integral ideal, shown to be irreducible in Example 2.14.

Thus the irreducible integral ideal $\mathfrak{q}_4'$ becomes a perfect square viewed in the group $\mathrm{J}^*(\mathcal{O})$ of invertible fractional ideals. In contrast, the irreducible integral ideal $\mathfrak{q}_4 = 2\mathcal{O}$ is not a perfect square in $\mathrm{J}^*(\mathcal{O})$.

(2) The non-integral fractional ideal
$$\mathfrak{b} := (1+i)\mathcal{O}_K = 2\mathbb{Z} + (1+i)\mathbb{Z}$$
is a non-invertible fractional $\mathcal{O}$-ideal. It has ideal square $\mathfrak{b}^2 = 2\mathcal{O}_K = \mathfrak{Q}_2$ (in the notation of Example 2.14), which is a non-invertible irreducible integral $\mathcal{O}$-ideal. The integral ideal $\mathfrak{Q}_2$ is the square of an element $\mathfrak{b}$ of the monoid $\mathrm{J}(\mathcal{O})$ of fractional ideals.

Example 3.11 (A finite order element of $\mathrm{J}^*(\mathcal{O})$)**.** Consider the order $\mathcal{O} = \mathbb{Z} + 2i\mathbb{Z}$, which is a suborder of $\mathcal{O}_K = \mathbb{Z} + i\mathbb{Z}$ in $K = \mathbb{Q}(i)$. Its conductor is $\mathfrak{f}(\mathcal{O}) = 2\mathcal{O}_K = 2\mathbb{Z} + 2i\mathbb{Z}$.

The $\mathcal{O}$-fractional ideal $\mathfrak{d} := i\mathcal{O} = 2\mathbb{Z} + i\mathbb{Z}$, is not an integral $\mathcal{O}$-ideal since $i \notin \mathcal{O}$. The ideal $\mathfrak{d}$ is a torsion element of $\mathrm{J}^*(\mathcal{O})$, with $\mathfrak{d}^2 = \mathcal{O}$. It is an invertible fractional ideal, and it is another example of a (non-integral) fractional ideal that has an ideal power that is an integral ideal.

Example 3.12 (An element of $\mathrm{J}^*(\mathcal{O})$ not a quotient of two coprime integral ideals)**.** We continue to consider the $\mathcal{O}$-fractional ideal $\mathfrak{d} = i\mathcal{O}$ for the non-maximal order $\mathcal{O} = \mathbb{Z} + 2i\mathbb{Z}$ of $K = \mathbb{Q}(i)$. It is expressible as a ratio $i\mathcal{O} = \mathfrak{a}\mathfrak{b}^{-1}$ of two invertible integral $\mathcal{O}$-ideals, taking $\mathfrak{a} = 2\mathcal{O}$ and $\mathfrak{b} = 2i\mathcal{O}$. But $\mathfrak{a} + \mathfrak{b} = 2\mathcal{O}_K$, so $\mathfrak{a}, \mathfrak{b}$ are not coprime integral ideals of $\mathcal{O}$.

In fact, $i\mathcal{O}$ cannot be expressed as a ratio of two coprime integral $\mathcal{O}$-ideals, which we now show by contrapositive. Suppose $i\mathcal{O} = \mathfrak{a}\mathfrak{b}^{-1}$ for integral $\mathcal{O}$-ideals $\mathfrak{a}$ and $\mathfrak{b}$, and multiply both sides by $\mathfrak{b}$ to obtain $i\mathfrak{b} = \mathfrak{a}$. Thus, $\mathfrak{a} = i\mathfrak{b} \subseteq i\mathcal{O}$, and $\mathfrak{a} \subseteq \mathcal{O}$, so $\mathfrak{a} \subseteq \mathcal{O} \cap i\mathcal{O} = (\mathbb{Z} + 2i\mathbb{Z}) \cap (2\mathbb{Z} + i\mathbb{Z}) = 2\mathcal{O}_K$. Similarly, $\mathfrak{b} = i\mathfrak{a} \subseteq i\mathcal{O}$ and $\mathfrak{b} \subseteq \mathcal{O}$, so $\mathfrak{b} \subseteq 2\mathcal{O}_K$. Thus, $\mathfrak{a} + \mathfrak{b} \subseteq 2\mathcal{O}_K$, so $\mathfrak{a}$ and $\mathfrak{b}$ cannot be coprime.

3.3. **Monoids of fractional ideals of orders coprime to a modulus $\mathfrak{m}$.** Recall that $\mathrm{J}(\mathcal{O})$ is the monoid of fractional ideals of the order $\mathcal{O}$, and $\mathrm{J}^*(\mathcal{O})$ is the group of invertible fractional ideals of $\mathcal{O}$. We have introduced a notion of $\mathfrak{m}$-coprimality for fractional ideals in Definition 3.3. We now define monoids of fractional ideals and groups of invertible fractional ideals coprime to a modulus $\mathfrak{m}$ which is an integral ideal.

Definition 3.13 (Monoids of fractional ideals coprime to $\mathfrak{m}$)**.** Given an integral ideal $\mathfrak{m}$ of an order $\mathcal{O}$ of a number field, let $\mathrm{J}_{\mathfrak{m}}(\mathcal{O})$ denote the set of $\mathfrak{m}$-*coprime fractional ideals* of $\mathcal{O}$,

$$\mathrm{J}_{\mathfrak{m}}(\mathcal{O}) = \{\mathfrak{a} \in \mathrm{J}(\mathcal{O}) : \mathfrak{a} \text{ is coprime to } \mathfrak{m}\}.$$

Let $\mathrm{J}^*_{\mathfrak{m}}(\mathcal{O})$ denote the set of $\mathfrak{m}$-*coprime invertible fractional ideals*,

$$\mathrm{J}^*_{\mathfrak{m}}(\mathcal{O}) = \{\mathfrak{a} \in \mathrm{J}^*(\mathcal{O}) : \mathfrak{a} \text{ is coprime to } \mathfrak{m}\}.$$

Lemma 3.14. *Let $\mathcal{O}$ be an order of a number field and $\mathfrak{m}$ an integral $\mathcal{O}$-ideal.*

(1) *The set $\mathrm{J}_{\mathfrak{m}}(\mathcal{O})$ of $\mathfrak{m}$-coprime fractional ideals is a monoid under $\mathcal{O}$-fractional ideal product.*
(2) *The set $\mathrm{J}^*_{\mathfrak{m}}(\mathcal{O})$ of $\mathfrak{m}$-coprime invertible fractional ideals is a group under $\mathcal{O}$-fractional ideal product.*
(3) *If $\mathfrak{m}, \mathfrak{m}'$ are ideals of $\mathcal{O}$ with $\mathfrak{m} \subseteq \mathfrak{m}'$, then $\mathrm{J}_{\mathfrak{m}}(\mathcal{O}) \subseteq \mathrm{J}_{\mathfrak{m}'}(\mathcal{O})$, and $\mathrm{J}^*_{\mathfrak{m}}(\mathcal{O}) \subseteq \mathrm{J}^*_{\mathfrak{m}'}(\mathcal{O})$.*

Proof of (1) and (2). Let $\mathfrak{c}_1, \mathfrak{c}_2 \in \mathrm{J}_{\mathfrak{m}}(\mathcal{O})$; we check that $\mathfrak{c}_1\mathfrak{c}_2 \in \mathrm{J}_{\mathfrak{m}}(\mathcal{O})$. Write $\mathfrak{c}_i = \mathfrak{a}_i\mathfrak{b}_i^{-1}$ for integral ideals $\mathfrak{a}_i, \mathfrak{b}_i$ coprime to $\mathfrak{m}$. Then $\mathfrak{c}_1\mathfrak{c}_2 = (\mathfrak{a}_1\mathfrak{a}_2)(\mathfrak{b}_1\mathfrak{b}_2)^{-1}$. The ideals $\mathfrak{a}_1\mathfrak{a}_2$ and $\mathfrak{b}_1\mathfrak{b}_2$ are coprime to $\mathfrak{m}$ by Lemma 2.17(1), so $\mathfrak{c}_1\mathfrak{c}_2 \in \mathrm{J}_{\mathfrak{m}}(\mathcal{O})$. Moreover, if $\mathfrak{c}_1$ and $\mathfrak{c}_2$ are invertible (that is, in $\mathrm{J}^*_{\mathfrak{m}}(\mathcal{O})$), then so is $\mathfrak{c}_1\mathfrak{c}_2$. Both $\mathrm{J}_{\mathfrak{m}}(\mathcal{O})$ and $\mathrm{J}^*_{\mathfrak{m}}(\mathcal{O})$ have identity element $\mathcal{O}$, and $\mathrm{J}^*_{\mathfrak{m}}(\mathcal{O})$ has inverses $(\mathfrak{a}\mathfrak{b}^{-1})^{-1} = \mathfrak{b}\mathfrak{a}^{-1}$. □

Proof of (3). The result is inherited from the inclusions in Lemma 2.17(2) applied to integral ideals $\mathfrak{a}, \mathfrak{b}$ defining an element $\mathfrak{c} = \mathfrak{a}\mathfrak{b}^{-1} \in \mathrm{J}_{\mathfrak{m}}(\mathcal{O})$. □

The next result shows that for all ideals $\mathfrak{m}$ contained in the conductor ideal, the associated monoid of integral ideals coprime to $\mathfrak{m}$ have unique factorization into prime ideals.

Proposition 3.15. *Let $\mathcal{O}$ be an order of a number field K. Suppose the integral ideal $\mathfrak{m}$ has $\mathfrak{m} \subseteq \mathfrak{f}(\mathcal{O})$. Then the following hold.*

(1) *The monoid $\mathrm{J}^*_{\mathfrak{m}}(\mathcal{O})$ of invertible fractional ideals is a free abelian group whose generators are the set of prime ideals $\mathbb{P}(\mathfrak{m}) = \{\mathfrak{p} : \mathfrak{m} \not\subseteq \mathfrak{p}, \mathfrak{p} \neq 0\}$. All of these prime ideals are non-singular. Ideals $\mathfrak{a} \in \mathrm{J}^*_{\mathfrak{m}}(\mathcal{O})$ have unique factorization into integral powers of the prime ideals in $\mathbb{P}(\mathfrak{m})$.*
(2) *The monoid $\mathrm{J}_{\mathfrak{m}}(\mathcal{O})$ of fractional ideals coprime to $\mathfrak{m}$ under ideal multiplication and the monoid $\mathrm{J}^*_{\mathfrak{m}}(\mathcal{O})$ of invertible fractional ideals coprime to $\mathfrak{m}$ coincide.*

Proof of (1). This result follows from the unique factorization property of Proposition 2.18(1) using the fact that all $\mathfrak{p} \in \mathbb{P}(\mathfrak{m})$ are invertible integral ideals, as shown in Proposition 2.18(2), hence invertible fractional ideals. □

Proof of (2). This follows from the fact that all non-singular prime $\mathcal{O}$-ideals are invertible. □

Remark 3.16. The conclusions of Proposition 3.15 for fractional ideals do not generally hold for $\mathfrak{m} \not\subseteq \mathfrak{f}(\mathcal{O})$, e.g., for $\mathfrak{m} = \mathcal{O}$ and $\mathcal{O}$ non-maximal.

(1) For some non-maximal orders $\mathcal{O}$, choosing $\mathfrak{m} = \mathcal{O}$, the monoid of all invertible fractional ideals $\mathrm{J}^*(\mathcal{O}) = \mathrm{J}^*_{\mathcal{O}}(\mathcal{O})$ is not a free abelian monoid, because it contains nontrivial torsion elements. See Example 3.11.
(2) For any non-maximal order $\mathcal{O}$, the monoid $\mathrm{J}(\mathcal{O}) = \mathrm{J}_{\mathcal{O}}(\mathcal{O})$ of all fractional ideals contains non-invertible ideals. The conductor ideal $\mathfrak{f}(\mathcal{O})$ is a noninvertible fractional ideal, because its non-invertibility as an integral ideal (by Lemma 2.13) implies the same as a fractional ideal by Lemma 3.7(1).

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

For two orders $\mathcal{O} \subseteq \mathcal{O}'$ having the same quotient field K, we consider the effect of natural maps sending (integral and fractional) $\mathcal{O}$-ideals to $\mathcal{O}'$-ideals, and vice versa.

Definition 4.1. 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 the integral $\mathcal{O}$-ideal of elements of $\mathfrak{a}'$ also in $\mathcal{O}$.

This is a special case of extension and contraction of ideals under ring homomorphism [4, p. 9]. In Section 4.1, we study the effect of ext and con on general integral ideals. In Section 4.2, we show these maps are bijective monoid homomorphisms when restricted to submonoids of integral ideals coprime to the relative conductor $f_{\mathcal{O}'}(\mathcal{O})$. In Section 4.3, we extend ext and con to bijective homomorphisms on groups of invertible fractional ideals coprime to $f_{\mathcal{O}'}(\mathcal{O})$.

4.1. 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 invertibility of ideals, and it preserves the property of being a principal ideal. The map ext may not be surjective; see Example 4.4.

The contraction map $\mathrm{con} : \mathrm{I}(\mathcal{O}') \to \mathrm{I}(\mathcal{O})$ 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 4.5. Contraction need not preserve invertibility of ideals nor the property of being a principal ideal; see Example 4.6. We will show in Section 4.2 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 4.2. *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 4.2, we will need a standard result in commutative algebra.

Lemma 4.3. *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,*

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

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

Proof. This is [4, Lem. 5.14]. □

Proof of Lemma 4.2(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 4.3, $\overline{\mathfrak{p}} = \mathrm{rad}(\mathcal{O}_K) = \mathcal{O}_K$. 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 $\mathrm{con}(\mathrm{ext}(\mathfrak{p})) = \mathfrak{p}$. □

Proof of Lemma 4.2(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. □

Proof of Lemma 4.2(3). By (1) we have $\mathrm{con}(\mathrm{ext}(\mathfrak{p})) = \mathfrak{p}$. Let $\mathfrak{p}'$ be 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. □

Proof of Lemma 4.2(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 4.4 below. □

Example 4.4. [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 $\mathcal{O} \subseteq \mathcal{O}'$. 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 4.3(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 the image of the map ext: Suppose it were, so $\mathfrak{p}' = \mathrm{ext}(\mathfrak{a})$ for some $\mathfrak{a} \in \mathrm{I}(\mathcal{O})$. Then, $\mathrm{ext}(\mathrm{con}(\mathrm{ext}(\mathfrak{a}))) = \mathrm{ext}(\mathfrak{a})$ by [4, Prop. I.17]. But

$$\mathrm{ext}(\mathrm{con}(\mathrm{ext}(\mathfrak{a}))) = \mathrm{ext}(\mathrm{con}(\mathfrak{p}')) = \mathrm{ext}(\mathfrak{p}) = \mathfrak{p},$$

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

Example 4.5. [The contraction map between ideal monoids $\mathrm{I}(\mathcal{O}')$ and $\mathrm{I}(\mathcal{O})$ need not be a monoid homomorphism.] As in Example 4.4, 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 $\mathcal{O} \subseteq \mathcal{O}'$. We consider $\mathrm{con} : \mathrm{I}(\mathcal{O}') \to \mathrm{I}(\mathcal{O})$. Also, as in Example 4.4, 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,

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

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

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

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

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

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

Example 4.6. [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 non-maximal order $\mathcal{O} = \mathbb{Z} + q\sqrt{-13}\mathbb{Z}$ where q is an odd inert prime (for example, $q = 5$). Recall from Example 2.7 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 $\mathrm{con} : \mathcal{O}_K \to \mathcal{O}$, we have

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

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 $\mathfrak{m}$ is not an invertible fractional $\mathcal{O}$-ideal hence also not a principal $\mathcal{O}$-ideal.

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.)

4.2. **Extension and contraction of integral ideals coprime to the relative conductor.** Extension and contraction operations behave well when restricted to integral ideals coprime to the relative conductor ideal.

Lemma 4.7. *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 coprimality of $\mathfrak{a}'$ to the relative conductor $\mathfrak{f} = \mathfrak{f}_{\mathcal{O}'}(\mathcal{O})$ we have

$$1 = a' + c' \tag{4.1}$$

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 (4.1) 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 $\mathfrak{a}'\mathfrak{f} \subseteq \mathfrak{f} \subseteq \mathcal{O}$ and $\mathfrak{a}'\mathfrak{f} \subseteq \mathfrak{a}'\mathcal{O}' = \mathfrak{a}'$. Now, given $b' \in \mathfrak{a}'$, we have from (4.1) that

$$b' = b'a + b'c'.$$

Now $b'a \in \mathrm{ext}(\mathrm{con}(\mathfrak{a}))$ since $b' \in \mathcal{O}$ and $a \in \mathrm{con}(\mathfrak{a})$, 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 that $\mathrm{ext}(\mathrm{con}(\mathfrak{a}')) = \mathfrak{a}'$.

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

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

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 $\mathrm{ext}(\mathfrak{ab}) = \mathrm{ext}(\mathfrak{a})\,\mathrm{ext}(\mathfrak{b})$. Because con defines an inverse to ext, it follows that con is also a homomorphism from $\mathrm{I}_{\mathfrak{f}}(\mathcal{O}')$ onto $\mathrm{I}_{\mathfrak{f}}(\mathcal{O})$. □

4.3. **Extension and contraction of fractional ideals coprime 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 4.8. *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*

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

are well-defined and are inverses of each other.

Remark 4.9. The extension map on fractional ideals $\mathfrak{a}$ coprime to $\mathfrak{f}_{\mathcal{O}'}(\mathcal{O})$ is $\mathrm{ext}(\mathfrak{a}) = \mathfrak{a}\mathcal{O}'$, as in the case for integral ideals in Definition 4.1(1). However, the contraction map on fractional ideals coprime to $\mathfrak{f}_{\mathcal{O}'}(\mathcal{O})$ requires a new definition different from Definition 4.1(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 coprime 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 4.8, 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 4.8. 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 $\mathfrak{m}' \subseteq \mathfrak{f}_{\mathcal{O}'}(\mathcal{O}) \subseteq \mathcal{O}$, hence $\mathfrak{m}'$ is integral as an $\mathcal{O}$-ideal by Lemma 3.7(1).

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 $\mathfrak{a}' \in \mathrm{I}_{\mathfrak{m}'}(\mathcal{O}')$, so $\mathfrak{a}' + \mathfrak{m}' = \mathcal{O}'$. 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 $\mathfrak{a} \in \mathrm{I}_{\mathfrak{m}'}(\mathcal{O})$, so $\mathfrak{a} + \mathfrak{m}' = \mathcal{O}$. Then, there exist $a \in \mathfrak{a}$ and $m \in \mathfrak{m}'$ with $a + m = 1$. Clearly, $a \in \mathrm{ext}(\mathfrak{a})$. Therefore, $\mathrm{ext}(\mathfrak{a})$ is coprime to $\mathfrak{m}'$ in $\mathcal{O}'$.

Now Lemma 4.7 asserts that $\mathrm{con}(\mathrm{ext}(\mathfrak{a})) = \mathfrak{a}$ and $\mathrm{ext}(\mathrm{con}(\mathfrak{a}')) = \mathfrak{a}'$ for all integral ideals in their respective domains. Because the domains and codomains of the maps above match on integral ideals, the isomorphisms given by Lemma 4.7 restricts to bijective isomorphisms $\mathrm{con} : \mathrm{I}_{\mathfrak{m}'}(\mathcal{O}') \to \mathrm{I}_{\mathfrak{m}'}(\mathcal{O})$ 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 any 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 $\mathfrak{d} = \mathfrak{a}\mathfrak{b}^{-1}$ by Lemma 3.6. We define $\mathrm{ext}(\mathfrak{d}) = \mathrm{ext}(\mathfrak{a})\,\mathrm{ext}(\mathfrak{b})^{-1}$; any group homomorphism extending ext must be defined thus. To show this definition is independent of the choice of 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 $\mathrm{con}(\mathfrak{a}'(\mathfrak{b}')^{-1}) = \mathrm{con}(\mathfrak{a}')\,\mathrm{con}(\mathfrak{b}')^{-1}$ for $\mathfrak{a}' \in \mathrm{I}_{\mathfrak{m}'}(\mathcal{O}')$ 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. □

5. 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 coprimality conditions to an arbitrary ideal $\mathfrak{d}$.

5.1. **Definition of ray class groups of orders.** Let $\mathcal{O}$ be an order of a number field K.

Definition 5.1. 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 with level datum $(\mathcal{O}; \mathfrak{m}, \Sigma)$, one needs to talk about modular congruences between non-integral elements of K. This requires a bit of care, given in the following definition.

Definition 5.2. Given $\alpha, \beta \in K$, we say $\alpha \equiv_{\mathcal{O}} \beta \pmod{\mathfrak{m}}$ (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 5.6.)

Definition 5.3 (Principal ray ideal group)**.** 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* $(\mathfrak{m}, \Sigma)$, denoted $\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})$, by:

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

Definition 5.4. The *ray class group* of $\mathcal{O}$ modulo $(\mathfrak{m}, \Sigma)$ is

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

That is,

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

This definition of the ray class group for an order $\mathcal{O}$ parallels the definition of the ray class group for the maximal order. To make the definition flexible, we will show in Section 5.3 that one may add auxiliary congruence conditions without changing the group, for example, requiring coprimality to the conductor ideal $\mathfrak{f}(\mathcal{O})$.

Definition 5.5. The *(wide) ring class group* (or *Picard group*) $\mathrm{Cl}(\mathcal{O})$ of an order $\mathcal{O}$ is the special case of modulus $(\mathcal{O}, \emptyset)$, so that

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

One can show this definition of ring class group (and the corresponding ring class field described by splitting of degree one prime ideals) is consistent with the classical definitions in the case of quadratic fields, as given in [16, pp. 114–115] and [17, pp. 162–163].

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

We introduce a notation for localization of rings, for later use.

Definition 5.6. 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,

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

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.)

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 termed the *localization away from* $\mathfrak{p}$.

The localization of an R-modules M may be defined by the extension of scalars $M[S_I^{-1}] := M \otimes_R R[S_I^{-1}]$ (or by an equivalent direct construction given in [4, Ch. 3]). We use the notation $M_{\mathfrak{p}} := M[S_{\mathfrak{p}}^{-1}] = M \otimes_R R_{\mathfrak{p}}$ for the localization of an $\mathcal{O}$-module M away from a prime ideal $\mathfrak{p}$. In the cases we consider, the natural map $M \to M_{\mathfrak{p}}$ is injective, so we will drop the tensor product notation, simply writing $M[S_{\mathfrak{p}}^{-1}] = MR_{\mathfrak{p}} = R_{\mathfrak{p}}M$.

The following proposition recalls a basic fact from commutative algebra: Fractional ideal containment (and more generally, injectivity of module maps) is a local property.

Proposition 5.7. *For any commutative ring R and a map of R-modules $\phi : M \to N$, the following are equivalent:*

(1) *ϕ is injective.*
(2) *The induced map $\phi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective for every prime ideal $\mathfrak{p}$ of R.*
(3) *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 $\mathfrak{a}, \mathfrak{b} \in \mathrm{J}(\mathcal{O})$,

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

Proof. The statement for R-modules is [4, Prop. 3.9]. The statement for fractional $\mathcal{O}$-ideals follows by taking $\phi : \mathfrak{a} \to \mathfrak{b}$ to be the inclusion map. □

We next recall a sharpening of Proposition 3.8, valid for orders of number fields.

Proposition 5.8. *Let $\mathcal{O}$ be an order in a number field K. Invertible fractional ideals of $\mathcal{O}$ are locally principal: If $\mathfrak{a} \in \mathrm{J}^*(\mathcal{O})$, then $\mathfrak{a}_{\mathfrak{p}} = \mathfrak{a}\mathcal{O}_p$ is a principal ideal of $\mathcal{O}_{\mathfrak{p}}$. Moreover, the correspondence $\mathfrak{a} \mapsto (\mathfrak{a}_{\mathfrak{p}}) := (\mathfrak{a}\mathcal{O}_{\mathfrak{p}})$ defines an isomorphism*

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

where $\mathfrak{p}$ varies over the nonzero prime ideals of $\mathcal{O}$, and $\mathrm{P}(\mathcal{O}_{\mathfrak{p}}) = \{\alpha\mathcal{O}_{\mathfrak{p}} : \alpha \in K_{\mathfrak{p}}\}$ is the group of nonzero principal fractional ideals of $\mathcal{O}_{\mathfrak{p}}$ in its quotient field $K_{\mathfrak{p}}$.

Proof. This is [46, Ch. I, Prop. 12.6] and is also proved in [55, Thm. 2.14]. □

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

(1) *One has $\{\mathfrak{p} : \mathfrak{p}$ a prime $\mathcal{O}$-ideal with $\mathfrak{m}_1 \subseteq \mathfrak{p}\} \subseteq \{\mathfrak{p} : \mathfrak{p}$ a prime $\mathcal{O}$-ideal with $\mathfrak{m}_2 \subseteq \mathfrak{p}\}$ if and only if $\mathrm{I}_{\mathfrak{m}_2}(\mathcal{O}) \subseteq \mathrm{I}_{\mathfrak{m}_1}(\mathcal{O})$.*
(2) *If $\mathrm{I}_{\mathfrak{m}_2}(\mathcal{O}) \subseteq \mathrm{I}_{\mathfrak{m}_1}(\mathcal{O})$, then $\mathrm{J}^*_{\mathfrak{m}_2}(\mathcal{O}) \subseteq \mathrm{J}^*_{\mathfrak{m}_1}(\mathcal{O})$.*
(3) *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 (1) (by proving the contrapositive). To prove the "only if" direction of (1), suppose

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

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

$$\begin{aligned}
\mathfrak{b} + \mathfrak{m}_2 = \mathcal{O} &\implies \mathfrak{b}\mathcal{O}_{\mathfrak{p}_j} + \mathfrak{m}_2\mathcal{O}_{\mathfrak{p}_j} = \mathcal{O}_{\mathfrak{p}_j} \text{ for } 1 \le j \le m \\
&\implies \mathfrak{b}\mathcal{O}_{\mathfrak{p}_j} = \mathcal{O}_{\mathfrak{p}_j} \text{ for } 1 \le j \le m, \text{ because } \mathfrak{m}_2\mathcal{O}_{\mathfrak{p}_j} \subseteq \mathfrak{p}_j\mathcal{O}_{\mathfrak{p}_j} \\
&\qquad \text{and } \mathfrak{p}_j\mathcal{O}_{\mathfrak{p}_j} \text{ is the unique maximal ideal of } \mathcal{O}_{\mathfrak{p}_j} \\
&\implies \mathfrak{b}\mathcal{O}_{\mathfrak{p}} + \mathfrak{m}_1\mathcal{O}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}} \text{ for all nonzero prime } \mathcal{O}\text{-ideals } \mathfrak{p}, \\
&\qquad \text{because } \mathfrak{m}_1\mathcal{O}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}} \text{ for } \mathfrak{p} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\} \\
&\implies \mathfrak{b} + \mathfrak{m}_1 = \mathcal{O} \text{ by Proposition 5.7.}
\end{aligned}$$

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

To prove (2), 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, $\mathrm{I}_{\mathfrak{m}_2}(\mathcal{O}) \subseteq \mathrm{I}_{\mathfrak{m}_1}(\mathcal{O}) \implies \mathrm{I}^*_{\mathfrak{m}_2}(\mathcal{O}) \subseteq \mathrm{I}^*_{\mathfrak{m}_1}(\mathcal{O}) \implies \mathrm{J}^*_{\mathfrak{m}_2}(\mathcal{O}) \subseteq \mathrm{J}^*_{\mathfrak{m}_1}(\mathcal{O})$.

To prove (3), consider a nonzero $\mathcal{O}$-ideal $\mathfrak{m}$. Let $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ be the set of all prime ideals containing $\mathfrak{m}$. For each j with $1 \le j \le m$, choose some nonzero element $\mu_j \in \mathfrak{m}\mathcal{O}_{\mathfrak{p}_j}$. By Proposition 5.8, 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

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

Thus, by (1), 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 (2), $\mathrm{J}^*_{\mathfrak{m}}(\mathcal{O}) = \mathrm{J}^*_{\widetilde{\mathfrak{m}}}(\mathcal{O})$. □

5.3. **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 the fractional ideal group to fractional ideals coprime to some ideal $\mathfrak{d}$, and restricting the principal ideals similarly, yields the same group. In this subsection we show this is true for arbitrary orders.

Being able to impose an auxiliary coprimality condition to some ideal $\mathfrak{d}$ on the fractional ideal groups, done in Lemma 5.12, makes possible the comparison of ray class groups for different orders and different ray class moduli, particularly the comparison of arbitrary ray class groups with certain ray class groups of the maximal order.

Definition 5.10 (Principal ray ideal group coprime to $\mathfrak{d}$)**.** Given an integral $\mathcal{O}$-ideal $\mathfrak{d}$, the group of *principal ray ideals (modulo $\mathfrak{m}$) coprime to $\mathfrak{d}$*, denoted $\mathrm{P}^{\mathfrak{d}}_{\mathfrak{m},\Sigma}(\mathcal{O})$, is given by:

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

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

Lemma 5.11. *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 5.2). 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 $\mathfrak{d} = \mathcal{O}$. □

The following key lemma is the most technically tricky result in this paper.

Lemma 5.12. *For any nonzero ideals $\mathfrak{d} \subseteq \mathfrak{m} \subseteq \mathcal{O}$ and any set Σ of real places of K (possibly empty),*

$$\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) = \frac{\mathrm{J}^*_{\mathfrak{d}}(\mathcal{O})}{\mathrm{P}^{\mathfrak{d}}_{\mathfrak{m},\Sigma}(\mathcal{O})}. \tag{5.1}$$

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

$$\phi : \mathrm{J}^*_{\mathfrak{d}}(\mathcal{O}) \to \frac{\mathrm{J}^*_{\mathfrak{m}}(\mathcal{O})}{\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})} = \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}). \tag{5.2}$$

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 (5.1), it suffices to prove that ϕ is surjective.

Given $\mathfrak{b} \in \mathrm{J}^*_{\mathfrak{m}}(\mathcal{O})$, to show surjectivity we must find some $\beta\mathcal{O} \in \mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})$ (equivalently, $\beta^{-1}\mathcal{O} \in \mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})$) such that $\mathfrak{a} = \beta^{-1}\mathfrak{b} \in \mathrm{J}^*_{\mathfrak{d}}(\mathcal{O})$. To construct a suitable element β, the argument will move to the maximal order $\mathcal{O}_K$ and then back to $\mathcal{O}$.

For the integral ideal $\mathfrak{m}$, by Lemma 5.9(3), 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 identical to the set of nonzero prime ideals with $\mathfrak{m} \subseteq \mathfrak{q}_j$. By Proposition 5.8, the invertible fractional ideals $\widetilde{\mathfrak{m}}, \mathfrak{b}$ are locally principal: For each nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$,

(1) $\widetilde{\mathfrak{m}}\mathcal{O}_{\mathfrak{p}} = \mu_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}$ for some $\mu_{\mathfrak{p}} \in K^\times$, and we may choose $\mu_{\mathfrak{p}} = 1$ whenever $\mathfrak{p} \notin \{\mathfrak{q}_1, \dots, \mathfrak{q}_n\}$;
(2) $\mathfrak{b}\mathcal{O}_{\mathfrak{p}} = \beta_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}$ for some $\beta_{\mathfrak{p}} \in K^\times$, and we may choose $\beta_{\mathfrak{p}} = 1$ whenever $\mathfrak{b} \not\subseteq \mathfrak{p}$.

The finite set of prime ideals $\mathfrak{p}$ with $\mathfrak{b} \not\subseteq \mathfrak{p}$ is a union of two subsets:

(1) a subset (possibly empty) of the set of prime ideals $\{\mathfrak{p}_i : 1 \le i \le m\}$ having $\mathfrak{d} \subseteq \mathfrak{p}_i$ and $\mathfrak{m} \not\subseteq \mathfrak{p}_i$;
(2) a set (possibly empty) of prime ideals $\{\mathfrak{r}_k : 1 \le j \le \ell\}$ having $\mathfrak{d} \not\subseteq \mathfrak{r}_k$.

(Note that the prime ideals $\mathfrak{p}_i$, $\mathfrak{q}_j$, $\mathfrak{r}_k$ need not be invertible.)

The condition that $\mathfrak{b}+\mathfrak{m} = \mathcal{O}$ is equivalent to the condition that $\mathfrak{b} \notin \mathfrak{q}_j$ for $1 \le j \le n$, and, in turn, to the condition that $\mathfrak{b} + \widetilde{\mathfrak{m}} = \mathcal{O}$. Additionally, it follows that the sets $\{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}$, $\{\mathfrak{q}_1, \dots, \mathfrak{q}_n\}$, and $\{\mathfrak{r}_1, \dots, \mathfrak{r}_\ell\}$ are all disjoint.

To show surjectivity (5.2) our object is to multiply $\mathfrak{b}$ by an element in $\mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})$ to force an additional coprimality condition with respect to the prime ideals $\{\mathfrak{p}_1, \cdots \mathfrak{p}_m\}$ without changing its behavior locally at the prime ideals $\mathfrak{q}_i$. The set of primes $\{\mathfrak{r}_1, \dots, \mathfrak{r}_\ell\}$, being disjoint from both the set of $\mathfrak{p}_i$ and the set of $\mathfrak{q}_j$, play no role in the following argument.

We now move to the maximal order $\mathcal{O}_K$. For $1 \le i \le m$, write $\mathfrak{p}_i = \mathrm{con}(\mathfrak{p}'_i)$ for some nonzero prime ideal $\mathfrak{p}'_i$ of $\mathcal{O}_K$; this is possible by Lemma 4.2. 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 $\mathfrak{p}'_i, \mathfrak{q}'_j$ are all

distinct, because the primes $\mathfrak{p}_i, \mathfrak{q}_j$ 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,

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

where $\overline{\mathcal{O}}_\mathfrak{p}$ is the integral closure of $\mathcal{O}_\mathfrak{p}$ in its fraction field $K_\mathfrak{p} = K$. 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 [46, Thm. 3.4], we can find $\beta \in K$ such that

(1) $|\beta - \beta_{\mathfrak{p}_i}|_{v_i} < |\beta|_{v_i}$ for $1 \le i \le m$,

(2) $|\beta - 1|_{w_j} \le \left|\tilde{f}_{\mathfrak{q}_j}\mu_{\mathfrak{q}_j}\right|_{w_j}^{-1}$ for $1 \le j \le n$, and

(3) $\rho(\beta) > 0$ for $\rho \in \Sigma$, via the Archimedean bound $|\beta - 1|_\rho < 1$.

We now define the invertible fractional $\mathcal{O}$-ideal $\mathfrak{a}$ by $\mathfrak{a} := \beta^{-1}\mathfrak{b}$.

We have $\mathfrak{a}\mathcal{O}_\mathfrak{p} = \beta^{-1}\beta_\mathfrak{p}\mathcal{O}_\mathfrak{p}$ for all prime $\mathcal{O}$-ideals $\mathfrak{p}$. By (1), for $1 \le i \le m$, $|\beta^{-1}\beta_{\mathfrak{p}_i} - 1|_{v_i} < 1$, so in particular, $\beta^{-1}\beta_{\mathfrak{p}_i}$ is a unit in $\mathcal{O}_{\mathfrak{p}'_i} = \overline{\mathcal{O}}_{\mathfrak{p}_i}$. But $\overline{\mathcal{O}}_{\mathfrak{p}_i}^\times \cap \mathcal{O}_{\mathfrak{p}_i} = \mathcal{O}_{\mathfrak{p}_i}^\times$, so $\beta^{-1}\beta_{\mathfrak{p}_i}$ is a unit in $\mathcal{O}_{\mathfrak{p}_i}$, and thus $\mathfrak{a}\mathcal{O}_{\mathfrak{p}_i} = \mathcal{O}_{\mathfrak{p}_i}$. 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 $1 \le j \le n$, $|\beta^{-1} - 1|_{w_j} \le \left|\tilde{f}_{\mathfrak{q}_j}\mu_{\mathfrak{q}_j}\right|_{w_j}^{-1}$ 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

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

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, $\beta^{-1} \equiv 1 \pmod{\mathfrak{m}}$, since $\widetilde{\mathfrak{m}} \subseteq \mathfrak{m}$. Combining this congruence with the positivity condition (3), we have $\mathfrak{a}\mathfrak{b}^{-1} = \beta^{-1}\mathcal{O} \in \mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O}_K)$. □

5.4. **Effect of change of order and modulus on ray class groups of orders.** While it is clear that Lemma 5.12 implies the existence of surjective change-of-modulus maps $\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) \to \mathrm{Cl}_{\mathfrak{m}',\Sigma'}(\mathcal{O})$ whenever $\mathfrak{m} \subseteq \mathfrak{m}'$ and $\Sigma \supseteq \Sigma'$, it is also true (but not immediately obvious) that one can change the order $\mathcal{O}$. For orders $\mathcal{O} \subseteq \mathcal{O}'$, the change-of-order map between ray class groups is induced by the extension map $\mathrm{ext} : \mathrm{J}^*(\mathcal{O}) \to \mathrm{J}^*(\mathcal{O}')$ on fractional ideals. We thus call it the *induced extension map* $\overline{\mathrm{ext}}$.

We show that the induced extension map is well-defined and surjective. This result will be applied and refined in Proposition 6.6 to explicitly describe the kernel of $\overline{\mathrm{ext}}$.

Lemma 5.13. *Let K be a number field, and consider level data $\mathcal{L} = (\mathcal{O}; \mathfrak{m}, \Sigma)$ and $\mathcal{L}' = (\mathcal{O}'; \mathfrak{m}', \Sigma')$ for K such that $\mathcal{O} \subseteq \mathcal{O}'$, $\mathfrak{m}\mathcal{O}' \subseteq \mathfrak{m}'$, and $\Sigma \supseteq \Sigma'$. There exists a unique homomorphism*

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

satisfying $\overline{\mathrm{ext}}([\mathfrak{a}]) = [\mathrm{ext}(\mathfrak{a})]$ for $\mathfrak{a} \in \mathrm{J}^*_\mathfrak{m}(\mathcal{O})$, and this map is surjective. For another level datum $\mathcal{L}'' = (\mathcal{O}'', \mathfrak{m}'', \Sigma'')$ for K such that $\mathcal{O}' \subseteq \mathcal{O}''$, $\mathfrak{m}'\mathcal{O}'' \subseteq \mathfrak{m}''$, and $\Sigma' \supseteq \Sigma''$, the compatibility relation $\overline{\mathrm{ext}}^{\mathcal{L}''}_{\mathcal{L}'} \circ \overline{\mathrm{ext}}^{\mathcal{L}'}_{\mathcal{L}} = \overline{\mathrm{ext}}^{\mathcal{L}''}_{\mathcal{L}}$ holds.

Proof. Uniqueness follows from the formula $\overline{\mathrm{ext}}([\mathfrak{a}]) = [\mathrm{ext}(\mathfrak{a})]$, provided that this formula defines a well-defined homomorphism.

To see that $\overline{\mathrm{ext}}$ is a well-defined, 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 $\mathrm{P}_{\mathfrak{m}',\Sigma'}(\mathcal{O}')$. So consider an ideal $\mathfrak{b} \in \mathrm{P}_{\mathfrak{m},\Sigma}(\mathcal{O})$. Then $\mathfrak{b} = b\mathcal{O}$ for some $b \in K$, $b - 1 \in \mathfrak{m}\mathcal{O}[S_{\mathfrak{m}}^{-1}]$, and $\rho(b) > 0$ for $\rho \in \Sigma$. Since $\mathfrak{m}\mathcal{O}[S_{\mathfrak{m}}^{-1}] \subseteq \mathfrak{m}\mathcal{O}'[S_{\mathfrak{m}}^{-1}] \subseteq \mathfrak{m}'\mathcal{O}'[S_{\mathfrak{m}'}^{-1}]$, we have $b - 1 \in \mathfrak{m}'\mathcal{O}'[S_{\mathfrak{m}'}^{-1}]$, that is, $b \equiv 1 \pmod{\mathfrak{m}'}$. Additionally, since $\Sigma \supseteq \Sigma'$, we have $\rho(b) > 0$ for $\rho \in \Sigma'$. Thus, $\mathrm{ext}(\mathfrak{b}) \in \mathrm{P}_{\mathfrak{m}',\Sigma'}(\mathcal{O}')$.

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 $\mathfrak{f}$. (For example, take $\mathfrak{d} = (\mathfrak{m} : \mathcal{O}')$.) Using Lemma 5.12, under the inclusion map on ideals, we have

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

To see that the map $\overline{\mathrm{ext}}$ is surjective, let $A \in \mathrm{Cl}_{\mathfrak{m}',\Sigma'}(\mathcal{O}')$, and let $\mathfrak{a} \in \mathrm{J}^*_{\mathfrak{d}}(\mathcal{O}')$ 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 4.7, so $\overline{\mathrm{ext}}([\mathrm{con}(\mathfrak{a})]) = [\mathfrak{a}] = A$.

The compatibility relation $\overline{\mathrm{ext}}^{\mathcal{L}''}_{\mathcal{L}'} \circ \overline{\mathrm{ext}}^{\mathcal{L}'}_{\mathcal{L}} = \overline{\mathrm{ext}}^{\mathcal{L}''}_{\mathcal{L}}$ is a direct consequence of the formula $\overline{\mathrm{ext}}([\mathfrak{a}]) = [\mathrm{ext}(\mathfrak{a})]$. □

6. Exact sequences for ray class groups of orders

In this section, we compare ray class groups for pairs of level data for the same field. So as to have a convenient shorthand to indicate which pairs of level data are comparable, we introduce a partial order on level data.

Definition 6.1. Let $\mathcal{L} = (\mathcal{O}; \mathfrak{m}, \Sigma)$ and $\mathcal{L}' = (\mathcal{O}'; \mathfrak{m}', \Sigma')$ be level data for the same number field K. (That is, $\mathcal{O}, \mathcal{O}'$ are K-orders, $\mathfrak{m}$ is an integral $\mathcal{O}$-ideal, $\mathfrak{m}'$ is an integral $\mathcal{O}'$-ideal, and $\Sigma, \Sigma' \subseteq \{\text{embeddings } K \hookrightarrow \mathbb{R}\}$.) We say that

$$\mathcal{L} \leq \mathcal{L}'$$

if and only if

$$\mathcal{O} \subseteq \mathcal{O}',\ \mathfrak{m}\mathcal{O}' \subseteq \mathfrak{m}',\ \text{and } \Sigma \supseteq \Sigma'.$$

When $\mathcal{L} \leq \mathcal{L}'$, the induced extension map $\overline{\mathrm{ext}}^{\mathcal{L}'}_{\mathcal{L}}$ is shown in Lemma 5.13 to be a surjective group homomorphism from $\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ to $\mathrm{Cl}_{\mathfrak{m}',\Sigma'}(\mathcal{O}')$. In this section, we completely describe the kernel of $\overline{\mathrm{ext}}$ in terms of local and global unit groups.

6.1. 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 6.2. For a commutative ring with unity R and an ideal I of R, define the group

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

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

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

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 6.3. *For any level datum $(\mathcal{O}; \mathfrak{m}, \Sigma)$, we have an exact sequence*

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

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

Proof. By definition,

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

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,

$$\begin{aligned}\ker(\phi) &= \{\alpha \in \mathcal{O}[S_{\mathfrak{d}}^{-1}] : \alpha\mathcal{O} = \mathcal{O},\ \alpha \equiv 1 \pmod{\mathfrak{m}},\ \rho(\alpha) > 0 \text{ for all } \rho \in \Sigma\} \\ &= \mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O}).\end{aligned}$$

The proposition follows. □

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

Proposition 6.4. *Let K be a number field, and consider level data $\mathcal{L} = (\mathcal{O}; \mathfrak{m}, \Sigma)$ and $\mathcal{L}' = (\mathcal{O}'; \mathfrak{m}', \Sigma')$ for K such that $\mathcal{L} \le \mathcal{L}'$. Let $\mathfrak{d}$ be any $\mathcal{O}'$-ideal such that $\mathfrak{d} \subseteq (\mathfrak{m} : \mathcal{O}')$. Then we have a short exact sequence of the form*

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

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 6.3, we have short exact sequences

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

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

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

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 induce compatible isomorphisms

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

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

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

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 $\operatorname{sign}(\rho(\widetilde{u}+\lambda)) = \varepsilon_\rho$ 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

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

by $\overline{\phi}(u) := \phi(u) \pmod{\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/\mathfrak{d}) \times \{\pm 1\}^{E\setminus\Sigma}}$; $\overline{\phi}$ is surjective because ϕ is. Furthermore, we compute the kernel of $\overline{\phi}$ as follows.

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

We already knew that $\operatorname{sign}(\rho(u)) = 1$ 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.

$$\begin{aligned}
&\iota'^{-1}\left(u \pmod{\mathfrak{d}\mathcal{O}'[S_{\mathfrak{d}}^{-1}]}\right) \in \mathrm{U}_{\mathfrak{m}}(\mathcal{O}/\mathfrak{d}) \\
&\quad\iff u \pmod{\mathfrak{d}\mathcal{O}'[S_{\mathfrak{d}}^{-1}]} \in \iota'(\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/\mathfrak{d})) = \iota(\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/\mathfrak{d})) = \mathrm{U}_{\mathfrak{m}}\left(\mathcal{O}[S_{\mathfrak{d}}^{-1}]/\mathfrak{d}\mathcal{O}[S_{\mathfrak{d}}^{-1}]\right) \\
&\quad\iff u \equiv 1 \pmod{\mathfrak{m}\mathcal{O}[S_{\mathfrak{d}}^{-1}]}.
\end{aligned}$$

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

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

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

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

proving the proposition. □

6.2. **Exact sequences relating ray class groups of varying orders.** We relate class groups of varying orders and moduli; the formula (6.1) is important for applications. The following results generalize results presented in [46, Ch. 1, Sec. 10] corresponding to the special case $\mathcal{L} = (\mathcal{O}; \mathcal{O}, \emptyset)$, $\mathcal{L}' = (\mathcal{O}_K; \mathcal{O}_K, \emptyset)$. More loosely speaking, they generalize results presented in [16, Sec. 7.2] corresponding to the special case $\mathcal{L} = (\mathcal{O}_K; \mathfrak{m}, \Sigma)$, $\mathcal{L}' = (\mathcal{O}_K; \mathcal{O}_K, \emptyset)$.

Theorem 6.5. *Let K be a number field, and consider level data $\mathcal{L} = (\mathcal{O}; \mathfrak{m}, \Sigma)$ and $\mathcal{L}' = (\mathcal{O}'; \mathfrak{m}', \Sigma')$ for K such that $\mathcal{L} \le \mathcal{L}'$ in the sense of Definition 6.1. 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 6.2, we have the following exact sequence.*

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

To prove this result, we use the following proposition.

Proposition 6.6. *Let K be a number field, and consider level data $\mathcal{L} = (\mathcal{O}; \mathfrak{m}, \Sigma)$ and $\mathcal{L}' = (\mathcal{O}'; \mathfrak{m}', \Sigma')$ for K such that $\mathcal{L} \le \mathcal{L}'$. Let $\mathfrak{d}$ be any $\mathcal{O}'$-ideal such that $\mathfrak{d} \subseteq (\mathfrak{m} : \mathcal{O}')$. Then we have an exact sequence of the form*

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

Proof. The extension map $\overline{\text{ext}} : \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) \to \mathrm{Cl}_{\mathfrak{m}',\Sigma'}(\mathcal{O}')$ is surjective by Lemma 5.13, 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 5.12,

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

The kernel of the extension map is

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

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 4.8, 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

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

Moreover,

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

The proposition follows. □

We now prove the main exact sequence.

Proof of Theorem 6.5. The result follows by gluing together the two short exact sequences in Proposition 6.4 and Proposition 6.6. □

We also give the specialization of Theorem 6.5 to $\mathcal{L} = (\mathcal{O}; \mathfrak{m}, \Sigma)$ and $\mathcal{L}' = (\mathcal{O}; \mathcal{O}, \emptyset)$. This case will be important for the application to SIC-POVMs [1, 33].

Corollary 6.7. *Let K be a number field and $\mathcal{O}$ an order of K. Let $\mathfrak{m}$ be an ideal of $\mathcal{O}$ and $\Sigma \subseteq \{$embeddings $K \hookrightarrow \mathbb{R}\}$. With the* U*-groups defined as in Definition 6.2, we have the following exact sequence.*

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

In particular, the kernel

$$\ker(\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) \twoheadrightarrow \mathrm{Cl}(\mathcal{O})) \cong \frac{(\mathcal{O}/\mathfrak{m})^\times \times \{\pm 1\}^{|\Sigma|}}{\mathrm{im}(\mathcal{O}^\times)},$$

where $\mathrm{im}(\mathcal{O}^\times)$ *is the image of global units under the map* $\varepsilon \mapsto (\overline{\varepsilon}, (\mathrm{sgn}(\rho(\varepsilon)))_{\rho\in\Sigma})$.

Proof. Take ray class level data $\mathcal{L} = (\mathcal{O}; \mathfrak{m}, \Sigma)$ and $\mathcal{L}' = (\mathcal{O}; \mathcal{O}, \emptyset)$, and choose $\mathfrak{d} = \mathfrak{m}$ in Theorem 6.5. All the hypotheses are satisfied, noting $\mathfrak{d} = \mathfrak{m} = (\mathfrak{m} : \mathcal{O})$. The terms in the exact sequence simplify, with $\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/\mathfrak{m}) = \mathrm{U}_{\mathfrak{d}}(\mathcal{O}/\mathfrak{d})$ being the trivial group, $\mathrm{U}_{\mathcal{O}}(\mathcal{O}/\mathfrak{d}) = (\mathcal{O}/\mathfrak{m})^\times$, and $\mathrm{U}_{\mathcal{O},\emptyset}(\mathcal{O}) = \mathcal{O}^\times$. □

Remark 6.8. Corollary 6.7 parallels a result of Campagna and Pengo [10, Thm. 4.6] for their idèlic formulation of class field theory for orders. The kernel $\ker(\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) \twoheadrightarrow \mathrm{Cl}(\mathcal{O}))$ is isomorphic to the Galois group $\mathrm{Gal}\big(H^{\mathcal{O}}_{\mathfrak{m},\Sigma}/H^{\mathcal{O}}\big)$ by Theorem 1.3, so Corollary 6.7 describes the structure of this Galois group. More generally, Theorem 6.5 describes the structure of the Galois group $\mathrm{Gal}\big(H^{\mathcal{O}}_{\mathfrak{m},\Sigma}/H^{\mathcal{O}'}_{\mathfrak{m}',\Sigma'}\big)$.

6.3. **Cardinality of ray class groups of orders.** The following result gives a formula for the "class number" of the ray class group with level datum $(\mathcal{O}; \mathfrak{m}, \Sigma)$. It generalizes a formula given by Neukirch [46, Thm. I.12.12] for the cardinality of the Picard group of an order (corresponding to level datum $(\mathcal{O}; \mathcal{O}, \emptyset)$) as well as a formula given by Cohn [16, Thm. 7.2.7] for the "unit ray class number" (corresponding to level datum $(\mathcal{O}_K; \mathfrak{m}, \Sigma)$).

Theorem 6.9. *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 level 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

$$\#\,\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) = \frac{h_K}{[\mathcal{O}_K^\times : \mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O})]} \cdot \frac{2^{|\Sigma|}\#(\mathcal{O}_K/(\mathfrak{m} : \mathcal{O}_K))^\times}{\#\,\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/(\mathfrak{m} : \mathcal{O}_K))} \tag{6.2}$$

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

$$\mathrm{rank}(\mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O})) = \mathrm{rank}(\mathcal{O}_K^\times) = r + s - 1. \tag{6.3}$$

Proof. We specialize the short exact sequence in Theorem 6.5, given $\mathfrak{m} \subseteq \mathcal{O}$, for the level data $\mathcal{L} = (\mathcal{O}; \mathfrak{m}, \Sigma)$ and $\mathcal{L}' = (\mathcal{O}_K; \mathcal{O}_K, \emptyset)$. We choose $\mathfrak{d} = (\mathfrak{m} : \mathcal{O}_K)$. All the hypotheses of Theorem 6.5 are satisfied, since $\mathfrak{m}\mathcal{O}_K \subseteq \mathcal{O}_K = \mathfrak{m}'$, and we obtain

$$1 \to \frac{\mathcal{O}_K^\times}{\mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O})} \to \frac{(\mathcal{O}_K/(\mathfrak{m} : \mathcal{O}_K))^\times}{\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/(\mathfrak{m} : \mathcal{O}_K))} \times \{\pm 1\}^{|\Sigma|} \to \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_K) \to 1. \tag{6.4}$$

The second nontrivial term in this exact sequence is clearly 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 finite. Equation (6.3) follows from the finiteness of the first term and 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 and solving for $\#\,\mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ yields (6.2). □

6.4. **Ring class groups of orders.** Theorem 6.5 allows us to express the (wide) ring class group $\mathrm{Cl}(\mathcal{O}) = \mathrm{Cl}_{\mathcal{O},\emptyset}(\mathcal{O})$ of an order $\mathcal{O}$, as defined in Definition 5.5, as a quotient of the Takagi ray class group $\mathrm{Cl}_{\mathfrak{f}}(\mathcal{O}_k) = \mathrm{Cl}_{\mathfrak{f}(\mathcal{O}),\emptyset}(\mathcal{O}_K)$ (of the maximal order) for the conductor ideal $\mathfrak{f}(\mathcal{O})$, permitting us to quantify the difference between them.

To understand the structure of the (wide) ring class group $\mathrm{Cl}(\mathcal{O})$, take $\mathcal{L} = (\mathcal{O}; \mathcal{O}, \emptyset)$ and $\mathcal{L}' = (\mathcal{O}_K; \mathcal{O}_K, \emptyset)$. Now choose $\mathfrak{d} = \mathfrak{f} = \mathfrak{f}(\mathcal{O})$. In particular, since $\mathfrak{d} = (\mathcal{O} : \mathcal{O}_K)$, this is the case already used in (6.4) with the further specialization $(\mathfrak{m}, \Sigma) = (\mathcal{O}, \emptyset)$. Theorem 6.5 applies to give the exact sequence

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

For the Takagi ray class group, choose instead $\mathcal{L} = (\mathcal{O}_K; \mathfrak{f}(\mathcal{O}), \emptyset)$ and $\mathcal{L}' = (\mathcal{O}_K; \mathcal{O}_K, \emptyset)$. Again set $\mathfrak{d} = \mathfrak{f} = \mathfrak{f}(\mathcal{O})$, and note $\mathfrak{d} \subseteq (\mathfrak{f}(\mathcal{O}) : \mathcal{O}_K) = \mathfrak{f}(\mathcal{O})$. Note that the unit group $\mathrm{U}_{\mathfrak{f}}(\mathcal{O}_K/\mathfrak{f}) = \{1\}$, so we obtain the exact sequence

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

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.

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

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

7. Ray class fields of orders

In this section, we define and prove existence of class fields associated to the ray class groups of Section 5. As usual, we fix a number field K. We will attach a ray class field $H^{\mathcal{O}}_{\mathfrak{m},\Sigma}$ to the level datum $\mathcal{L} = (\mathcal{O}; \mathfrak{m}, \Sigma)$ for K; this field will be an abelian extension of K.

7.1. **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 level datum $(\mathcal{O}; \mathfrak{m}, \Sigma)$, and we also consider the level 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 7.2(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 level datum $(\mathcal{O}; \mathfrak{m}, \Sigma)$ for the order $\mathcal{O}$.

To construct ψ, we start from the exact sequence from Theorem 6.5 for $\mathcal{L} = (\mathcal{O}; \mathfrak{m}, \Sigma)$ and $\mathcal{L}' = (\mathcal{O}_K; \mathcal{O}_K, \emptyset)$ with and $\mathfrak{d} := (\mathfrak{m} : \mathcal{O}_K)$. It is

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

since $\mathrm{U}_{\mathfrak{m}'}(\mathcal{O}'/\mathfrak{d}) = (\mathcal{O}_K/(\mathfrak{m} : \mathcal{O}_K))^\times$. Consider also a second exact sequence given by Theorem 6.5, taking $\mathcal{L} = (\mathcal{O}_K; (\mathfrak{m} : \mathcal{O}_K), \Sigma)$, $\mathcal{L}' = (\mathcal{O}_K; \mathcal{O}_K, \emptyset)$, and $\mathfrak{d} = (\mathfrak{m} : \mathcal{O}_K)$. In this exact 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

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

As in Section 6.3, 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.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \frac{\mathcal{O}_K^\times}{\mathrm{U}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K)} & \longrightarrow & (\mathcal{O}_K/(\mathfrak{m}:\mathcal{O}_K))^\times \times \{\pm 1\}^{|\Sigma|} & \longrightarrow & \mathrm{Cl}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K) & \longrightarrow & \mathrm{Cl}(\mathcal{O}_K) \longrightarrow 1 \\ & & \downarrow \kappa & & \downarrow \pi & & \vdots\, \psi & & \| \mathrm{id} \\ 1 & \longrightarrow & \frac{\mathcal{O}_K^\times}{\mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O})} & \longrightarrow & \frac{(\mathcal{O}_K/(\mathfrak{m}:\mathcal{O}_K))^\times}{\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/(\mathfrak{m}:\mathcal{O}_K))} \times \{\pm 1\}^{|\Sigma|} & \longrightarrow & \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) & \longrightarrow & \mathrm{Cl}(\mathcal{O}_K) \longrightarrow 1 \end{array} \tag{7.1}$$

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 7.1. The *ray class field of the order $\mathcal{O}$ with modulus $(\mathfrak{m}, \Sigma)$* is the subfield $H^{\mathcal{O}}_{\mathfrak{m},\Sigma}$ of the Takagi ray class field $H^{\mathcal{O}_K}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}$ associated to $J(\mathcal{O}; \mathfrak{m}, \Sigma) := \ker \psi$ in (7.1) 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 $H^{\mathcal{O}}_{\mathfrak{m},\Sigma}$ 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 $\rho \in \Sigma$.

7.2. **The classical existence theorem.** We state the classical existence theorem of class field theory, called the Weber–Hilbert–Artin–Takagi [WHAT] correspondence by Cohn [16, Chap. 7], in our notation.

Theorem 7.2 (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 the 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 $\mathfrak{m}$.)*
   (a) *If $J_1 \subseteq J_2$, then $L_{J_2} \subseteq L_{J_1}$.*
   (b) *For $J = \{\mathcal{I}\}$, where $\mathcal{I} = [\mathcal{O}_K]$ is the principal ray class modulo $(\mathfrak{m}, \Sigma)$, the field $L = L_{\{\mathcal{I}\}} = H^{\mathcal{O}_K}_{\mathfrak{m},\Sigma}$ is 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 $\mathcal{O}_K$ (coprime 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 $[\mathfrak{a}]$ coprime 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 $\mathrm{Art}(J) \subseteq \mathrm{Gal}(L/K)$; that is,*

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

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* $\sigma_p(x) \equiv x^q \pmod{\mathfrak{P}}$ *for all* $x \in \mathcal{O}_L$*, where* $q = p^j$ *is the number of elements in the finite field* $\mathcal{O}_K/\mathfrak{p}$*.*

Proof. This statement (1) is extracted from [16, Thm. 7.4.1], whereas (2) follows from [16, Thm. 7.4.2]. See also [27, Thm. 6.6.8] for (1) and [27, Thm. and Defn. 6.6.2] for (2). □

Remark 7.3. 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 7.2, one can also define an Artin isomorphism Art_J making the diagram

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

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 $\mathrm{Art}_{\ker\phi} = \mathrm{Art}_{\mathfrak{m}',\Sigma'}$.

7.3. **Proof of Theorem 1.1.** The main step in the proof is to identify the map ψ introduced in Section 7.1 with contraction to $\mathcal{O}$ on the set of fractional ideals of $\mathcal{O}_K$ coprime to $(\mathfrak{m} : \mathcal{O}_K)$ (or equivalently, coprime to $\mathfrak{m}\mathcal{O}_K \cap \mathfrak{f}(\mathcal{O}_K)$).

Lemma 7.4. *For a class* $[\mathfrak{a}] \in \mathrm{Cl}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K)$ *represented by some* $\mathfrak{a} \in \mathrm{J}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K)$*, the map* $\psi : \mathrm{Cl}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K) \to \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O})$ *defined by* (7.1) *may be explicitly written* $\psi([\mathfrak{a}]) = [\mathrm{con}(\mathfrak{a})]$*.*

Proof. We apply Proposition 4.8 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 3.9. Proposition 4.8 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

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

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

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

To show that $\widetilde{\psi} = \psi$, it suffices to show that $\widetilde{\psi}$ makes the diagram in (7.1) commute. On 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

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

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 (7.1), and let $J = \ker\psi$. By Theorem 7.2, $H^{\mathcal{O}}_{\mathfrak{m},\Sigma} := \left(H_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}\right)^{\mathrm{Art}(J)}$ 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 7.4, $\psi([\mathfrak{p}]) = [\mathrm{con}(\mathfrak{p})] = [\mathfrak{p} \cap \mathcal{O}]$. (Since $\mathfrak{p}$ is a maximal ideal, $\mathfrak{p} \cap \mathcal{O}$ is also a maximal ideal by Lemma 4.2(2).) □

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

Theorem 7.5. *For two orders $\mathcal{O} \subseteq \mathcal{O}'$ in a number field K and any level datum $(\mathcal{O}; \mathfrak{m}, \Sigma)$, 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.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \frac{(\mathcal{O}')^\times}{\mathrm{U}_{(\mathfrak{m}:\mathcal{O}'),\Sigma}(\mathcal{O}')} & \longrightarrow & (\mathcal{O}'/(\mathfrak{m}:\mathcal{O}'))^\times \times \{\pm 1\}^{|\Sigma|} & \longrightarrow & \mathrm{Cl}_{(\mathfrak{m}:\mathcal{O}'),\Sigma}(\mathcal{O}') & \longrightarrow & \mathrm{Cl}(\mathcal{O}') \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \vdots\,\psi & & \| \\
1 & \longrightarrow & \frac{(\mathcal{O}')^\times}{\mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O})} & \longrightarrow & \frac{(\mathcal{O}'/(\mathfrak{m}:\mathcal{O}'))^\times}{\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/(\mathfrak{m}:\mathcal{O}'))} \times \{\pm 1\}^{|\Sigma|} & \longrightarrow & \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) & \longrightarrow & \mathrm{Cl}(\mathcal{O}') \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \vdots\,\phi & & \| \\
1 & \longrightarrow & \frac{(\mathcal{O}')^\times}{\mathrm{U}_{\mathfrak{m}\mathcal{O}',\Sigma}(\mathcal{O}')} & \longrightarrow & (\mathcal{O}'/\mathfrak{m}\mathcal{O}')^\times \times \{\pm 1\}^{|\Sigma|} & \longrightarrow & \mathrm{Cl}_{\mathfrak{m}\mathcal{O}',\Sigma}(\mathcal{O}') & \longrightarrow & \mathrm{Cl}(\mathcal{O}') \longrightarrow 1
\end{array} \tag{7.2}$$

The horizontal rows are exact sequences from Theorem 6.5 with data given in the following table.

Theorem 6.5	$\mathcal{L} = (\mathcal{O}; \mathfrak{m}, \Sigma)$	$\mathcal{L}' = (\mathcal{O}'; \mathfrak{m}', \Sigma')$	$\mathfrak{d}$
top row	$(\mathcal{O}'; (\mathfrak{m} : \mathcal{O}'), \Sigma)$	$(\mathcal{O}'; \mathcal{O}', \emptyset)$	$(\mathfrak{m} : \mathcal{O}')$
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 quotienting 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 (7.2) commutes. The upper induced map ψ was described in Section 7.1. 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

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

obtained from Theorem 6.5 (taking $\mathcal{L} = (\mathcal{O}; \mathfrak{m}, \Sigma)$, $\mathcal{L}' = (\mathcal{O}'; \mathfrak{m}\mathcal{O}', \Sigma)$, and $\mathfrak{d} := (\mathfrak{m} : \mathcal{O}')$).

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

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

also a special case of Theorem 6.5 (where we take $\mathcal{L} = (\mathcal{O}', (\mathfrak{m}:\mathcal{O}'), \Sigma)$, $\mathcal{L}' = (\mathcal{O}', \mathfrak{m}\mathcal{O}', \Sigma)$, and $\mathfrak{d} := (\mathfrak{m}:\mathcal{O}')$).

The diagram (7.2) establishes (from its third nontrivial column) the sequence of surjections

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

Now by Theorem 7.2(1), we have the tower of ray class fields of orders

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

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

Proof of Theorem 1.2. This is the special case $\mathcal{O}' = \mathcal{O}_K$ of Theorem 7.5. □

7.5. **Proof of Theorem 1.3.** We now prove Theorem 1.3, giving a form of Artin reciprocity for a ray class group and ray class field of an order. The result is obtained from the usual Artin reciprocity law together with properties of the map ψ in (7.1) 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 (7.1). By Lemma 7.4, 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 7.1 and the Galois correspondence it describes, there is an isomorphism $\mathrm{Art}_{\mathcal{O}}$ making the following diagram commute.

$$\begin{array}{ccc} \mathrm{Cl}_{(\mathfrak{m}:\mathcal{O}_K),\Sigma}(\mathcal{O}_K) & \xrightarrow{\mathrm{Art}}_{\sim} & \mathrm{Gal}(H_1/K) \\ \Big\downarrow \psi & & \Big\downarrow \\ \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) & \xrightarrow[\sim]{\mathrm{Art}_{\mathcal{O}}} & \mathrm{Gal}(H_0/K) \end{array} \tag{7.3}$$

To give an explicit formula for $\mathrm{Art}_{\mathcal{O}}$, consider any fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ coprime to $\mathfrak{f}(\mathcal{O}) \cap \mathfrak{m}$ (or, equivalently, coprime 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 4.8), 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 (7.3) gives

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

Now let $\mathfrak{p}$ be any prime ideal of $\mathcal{O}$ coprime 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 $\alpha \in \mathcal{O}_{H_0}$,

$$\mathrm{Art}_{\mathcal{O}}([\mathfrak{p}])(\alpha) \equiv \alpha^q \pmod{\mathfrak{P}}, \tag{7.4}$$

where $q = p^j$ is the number of elements in $\mathcal{O}/\mathfrak{p}$, 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 7.2; see also Remark 7.3), for any $\alpha \in \mathcal{O}_{H_0}$,

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

Now the condition that $\mathfrak{p}$ is coprime 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 4.2 and Proposition 4.8; 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

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

where q' is the number of elements in $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$. We have $q' = q$ since the hypotheses guarantee that $\mathcal{O}/\mathfrak{p} \cong \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$. Applying this congruence with $\beta = \alpha \in \mathcal{O}_{H_0}$, noting that $\mathcal{P} \cap \mathcal{O}_{H_0} = \mathfrak{P}$ and $\alpha^q \in \mathcal{O}_{H_0}$, we may conclude

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

proving the claim.

Finally we note that by Proposition 2.18 and Lemma 3.6, fractional ideals of $\mathcal{O}$ coprime to $\mathfrak{f}(\mathcal{O}) \cap \mathfrak{m}$ factor into powers of prime ideals coprime to $\mathfrak{f}(\mathcal{O}) \cap \mathfrak{m}$, so the map $\mathrm{Art}_{\mathcal{O}}$ is uniquely determined by (7.4). □

8. Computations of ray class groups of orders

To illustrate how to compute with the exact sequence for change of order and modulus, we calculate several ray class groups of orders. 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 apply Theorem 6.5 with $\mathcal{L} = (\mathcal{O}; \mathfrak{m}, \Sigma)$ and $\mathcal{L}' = (\mathcal{O}'; \mathfrak{m}', \Sigma')$, and make the choice $\mathfrak{d} = (\mathfrak{m} : \mathcal{O}')$, to obtain the exact sequence

$$1 \to \frac{\mathrm{U}_{\mathfrak{m}',\Sigma'}(\mathcal{O}')}{\mathrm{U}_{\mathfrak{m},\Sigma}(\mathcal{O})} \to \frac{\mathrm{U}_{\mathfrak{m}'}(\mathcal{O}'/(\mathfrak{m} : \mathcal{O}'))}{\mathrm{U}_{\mathfrak{m}}(\mathcal{O}/(\mathfrak{m} : \mathcal{O}'))} \times \{\pm 1\}^{|\Sigma \setminus \Sigma'|} \to \mathrm{Cl}_{\mathfrak{m},\Sigma}(\mathcal{O}) \to \mathrm{Cl}_{\mathfrak{m}',\Sigma'}(\mathcal{O}') \to 1. \tag{8.1}$$

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 ∞ of $\mathbb{Z}$. We let ∞_1, ∞_2 denote the real embeddings $\rho_i : \mathbb{Q}(\sqrt{2}) \to \mathbb{R}$ defined by $\rho_1(\sqrt{2}) = \sqrt{2}$ and $\rho_2(\sqrt{2}) = -\sqrt{2}$, respectively.

The first three examples taken together give information on the corresponding ray class fields. They 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 with the ring class field. Using Theorem 1.3, the class number calculations imply

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

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

8.1. **Example 1.** Take level data $\mathcal{L} = \big(\mathbb{Z}[\sqrt{2}]; 7\mathbb{Z}[\sqrt{2}], \{\rho_2\}\big) = \big(\mathbb{Z}[\sqrt{2}]; (7)\infty_2\big)$ and $\mathcal{L}' = \big(\mathbb{Z}[\sqrt{2}]; \mathbb{Z}[\sqrt{2}], \emptyset\big) = \big(\mathbb{Z}[\sqrt{2}]; (1)\big)$. Then by (8.1),

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

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,

$$\begin{aligned}\Big(\mathbb{Z}[\sqrt{2}]/(7)\Big)^\times &\cong \Big(\mathbb{Z}[\sqrt{2}]/(3+\sqrt{2})\Big)^\times \times \Big(\mathbb{Z}[\sqrt{2}]/(3-\sqrt{2})\Big)^\times \\ &\cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}.\end{aligned}$$

Moreover,

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

Thus, we see that

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

8.2. **Example 2.** Take $\mathcal{L} = \big(\mathbb{Z}[2\sqrt{2}]; 7\mathbb{Z}[2\sqrt{2}], \{\rho_2\}\big) = \big(\mathbb{Z}[2\sqrt{2}]; (7)\infty_2\big)$ and, as above, take $\mathcal{L}' = \big(\mathbb{Z}[\sqrt{2}]; \mathbb{Z}[\sqrt{2}], \emptyset\big) = \big(\mathbb{Z}[\sqrt{2}]; (1)\big)$. Then (8.1) gives

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

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

$$\begin{aligned}\Big(\mathbb{Z}[\sqrt{2}]/(14)\Big)^\times &\cong \Big(\mathbb{Z}[\sqrt{2}]/(3+\sqrt{2})\Big)^\times \times \Big(\mathbb{Z}[\sqrt{2}]/(3-\sqrt{2})\Big)^\times \times \Big(\mathbb{Z}[\sqrt{2}]/(\sqrt{2})^2\Big)^\times \\ &\cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.\end{aligned}$$

We also have

$$\mathrm{U}_{(7)}\Big(\mathbb{Z}[2\sqrt{2}]/(14\mathbb{Z}+14\sqrt{2}\mathbb{Z})\Big) = 1$$

and

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

We see that

$$\left|\mathrm{Cl}_{(7)\infty_2}\Big(\mathbb{Z}[2\sqrt{2}]\Big)\right| = 12.$$

With more careful accounting, we can obtain an isomorphism

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

8.3. **Example 3.** We compute the same group $\mathrm{Cl}_{(7)\infty_2}\big(\mathbb{Z}[2\sqrt{2}]\big)$ a different way. Take $\mathcal{L} = \big(\mathbb{Z}[2\sqrt{2}]; (7)\infty_2\big)$ as above, but instead take $\mathcal{L}' = \big(\mathbb{Z}[2\sqrt{2}]; (1)\big)$. Then (8.1) gives

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

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

$$\begin{aligned}\Big(\mathbb{Z}[2\sqrt{2}]/(7)\Big)^\times &\cong \Big(\mathbb{Z}[2\sqrt{2}]/(1+2\sqrt{2})\Big)^\times \times \Big(\mathbb{Z}[2\sqrt{2}]/(1-2\sqrt{2})\Big)^\times \\ &\cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}.\end{aligned}$$

The quotient of global unit groups is

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

It follows that

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

8.4. **Example 4.** Take $\mathcal{L} = \big(\mathbb{Z}[5\sqrt{2}]; (7)\infty_2\big)$ and $\mathcal{L}' = \big(\mathbb{Z}[5\sqrt{2}]; (1)\big)$. Then (8.1) gives

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

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

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

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 it is a degree 4 extension of $\mathbb{Q}$. We also have

$$\begin{aligned}\Big(\mathbb{Z}[5\sqrt{2}]/(7)\Big)^\times \times \{\pm 1\} &\cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}; \\ \frac{\mathbb{Z}[5\sqrt{2}]^\times}{\mathrm{U}_{(7)\infty_2}\big(\mathbb{Z}[5\sqrt{2}]\big)} &= \frac{\langle -1, (1+\sqrt{2})^3\rangle}{\langle (1+\sqrt{2})^6\rangle} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.\end{aligned}$$

We see that

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

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

9. Concluding remarks

The main results of this paper assigned ray class fields to invertible ray class groups of orders defined for level data specifying an order and a modulus (an ideal and a set of real places). The constructed class fields were characterized in terms of splitting conditions on their prime ideals.

There are several other aspects of class field theory, specified by the main theorems of class field theory listed by Hasse [28], 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 A. One subtlety that arises is that norms of non-invertible ideals are in general not multiplicative.

(2) *Zeta functions of orders.* Zeta functions played an important role in the historical development of class field theory. 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 $\mathfrak{f}(\mathcal{O})$.

(3) *Ray class monoids and L-functions.* If we allow non-invertible ideals, then the ray class group is enlarged to become a *ray class monoid*. We treat aspects of the structure of ray class monoids of orders in [34]. Additionally one can define L-functions associated to characters of ray class groups of orders. If one allows non-invertible ideals, then one can also allow new L-functions using characters of ray class monoids. See [12, 13, 29, 41–43] for the character theory of monoids and semigroups.

There is a development of class field theory for orders inside an idèlic framework formulated by Pengo [47] and detailed by Campagna and Pengo [10, Sec. 4] (see in particular their Defn. 4.1). It remains to relate that idèlic definition to the ray class group defined in Definition 7.1 of this paper. The equivalence of the two notions of class fields of orders (in the case of no ramification at infinity considered by Campagna and Pengo) has not been definitively established (but see Remark 6.8).

Acknowledgments. The authors thank Pete L. Clark, Francesco Campagna and Riccardo Pengo, and John Voight for helpful comments and references. The first author was partially supported by the NSF grant DMS-2302514 and by University of Bristol, the Heilbronn Institute for Mathematical Research, and Purdue University. He thanks Trevor Wooley for support and for helpful mathematical conversations. The second author was partially supported by NSF grant DMS-1701576.

Appendix A. Norms of ideals in orders of number fields

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 A.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: $\mathrm{Nm}(\mathfrak{ab}) = \mathrm{Nm}_{\mathcal{O}}(\mathfrak{a})\,\mathrm{Nm}_{\mathcal{O}}(\mathfrak{b})$. The following proposition shows the stronger result that the norm of the product of two integral ideals is multiplicative whenever one of them is invertible.

Proposition A.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:

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

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

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

where $\mathfrak{q}_j$ and $\mathfrak{r}_j$ are separately either primary ideals having radical $\mathfrak{p}_j$, or else equal to the 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 since $\mathfrak{a}$ is invertible, by Proposition 5.8 it 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 $1 \leq j \leq k$. These conditions imply $\alpha \in \mathfrak{a}$, Define an additive group homomorphism (indeed, an isomorphism of $\mathcal{O}$-modules)

$$\phi : \mathcal{O} \to \mathfrak{a}/\mathfrak{ab}$$

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 $1 \leq j \leq k$. Thus, $y \equiv \alpha x \pmod{\mathfrak{q}_j\mathfrak{r}_j}$ for $1 \leq j \leq k$, so

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

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

We now compute the kernel of ϕ. We have $\phi(x) = 0$ if and only if $\alpha x \in \mathfrak{ab}$. Now $\alpha \in \mathfrak{a}$, so $\alpha x \in \mathfrak{ab}$ whenever $x \in \mathfrak{b}$. Conversely, suppose $\alpha x \in \mathfrak{ab}$. Then, in the local ring $\mathcal{O}_{\mathfrak{p}_j}$, we have $\alpha x \in \mathfrak{ab}\mathcal{O}_{\mathfrak{p}_j} = \alpha_j\mathfrak{r}_j\mathcal{O}_{\mathfrak{p}_j}$. 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,

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

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

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

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

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

The norm also enjoys a multiplicativity property for coprime ideals, allowing the norm to be calculated from its values on primary ideals.

Proposition A.3. *If $\mathfrak{a}, \mathfrak{b}$ are coprime integral $\mathcal{O}$-ideals, then $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{ab}) = \mathrm{Nm}_{\mathcal{O}}(\mathfrak{a})\,\mathrm{Nm}_{\mathcal{O}}(\mathfrak{b})$. In particular, if $\mathfrak{m}$ is any nonzero integral $\mathcal{O}$-ideal with primary decomposition*

$$\mathfrak{m} = \bigcap_{i=1}^{n} \mathfrak{q}_i = \prod_{i=1}^{n} \mathfrak{q}_i,$$

then its norm is given by $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{m}) = \prod_{i=1}^{n} \mathrm{Nm}_{\mathcal{O}}(\mathfrak{q}_i)$.

Proof. When $\mathfrak{a}$ or $\mathfrak{b}$ is zero, $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{ab}) = 0 = \mathrm{Nm}_{\mathcal{O}}(\mathfrak{a})\,\mathrm{Nm}_{\mathcal{O}}(\mathfrak{b})$. Otherwise, $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$, and by the Chinese Remainder Theorem [24, Ch. 7, Thm. 17],

$$\mathcal{O}/(\mathfrak{ab}) = \mathcal{O}/(\mathfrak{a} \cap \mathfrak{b}) \cong \mathcal{O}/\mathfrak{a} \oplus \mathcal{O}/\mathfrak{b},$$

so $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{ab}) = |\mathcal{O}/(\mathfrak{ab})| = |\mathcal{O}/\mathfrak{a}| \cdot |\mathcal{O}/\mathfrak{b}| = \mathrm{Nm}_{\mathcal{O}}(\mathfrak{a})\,\mathrm{Nm}_{\mathcal{O}}(\mathfrak{b})$.

Primary ideals associated to different maximal ideals are coprime, so the norm of an nonzero integral $\mathcal{O}$-ideal is the product of the norms of its primary constituents. □

The norm need not be multiplicative if both ideals $\mathfrak{a}$, $\mathfrak{b}$ are non-invertible and non-coprime. Marseglia [40] observed in a single order $\mathcal{O}$ 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 $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{ab}) > \mathrm{Nm}_{\mathcal{O}}(\mathfrak{a})\,\mathrm{Nm}_{\mathcal{O}}(\mathfrak{b})$.

Example A.4 (Super-multiplicativity and sub-multiplicativity of norms)**.** The multiplicativity condition $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{ab}) = \mathrm{Nm}_{\mathcal{O}}(\mathfrak{a})\,\mathrm{Nm}_{\mathcal{O}}(\mathfrak{b})$ for $\mathfrak{a}, \mathfrak{b} \in \mathrm{I}(\mathcal{O})$ can only fail when both $\mathfrak{a}$ and $\mathfrak{b}$ are not invertible. In particular, neither $\mathfrak{a}$ nor $\mathfrak{b}$ can be coprime to the conductor $\mathfrak{f}(\mathcal{O})$.

(1) An example of strict super-multiplicativity of norms was given in Example 2.14. It showed in $\mathcal{O} = \mathbb{Z}[2i]$ having conductor ideal $\mathfrak{O}_2 = 2\mathcal{O}_K$, where $\mathcal{O}_K = \mathbb{Z}[i]$, that:

$$8 = \mathrm{Nm}_{\mathcal{O}}((\mathfrak{O}_2)^2) > (\mathrm{Nm}_{\mathcal{O}}(\mathfrak{O}_2))^2 = 4.$$

(2) An example of strict sub-multiplicativity of norms are given by Marseglia [40, Ex. 3.4]. The example takes $K = \mathbb{Q}(\alpha)$, where α is a root of a monic irreducible polynomial of degree 4 with integer coefficients, such as $x^4 - x - 1$. Consider the order

$$\mathcal{O} := \mathbb{Z} + p\mathbb{Z}[\alpha] = \mathbb{Z} + p\alpha\mathbb{Z} + p\alpha^2\mathbb{Z} + p\alpha^3\mathbb{Z},$$

where $p \geq 5$ is a rational prime number. Then the lattices

$$\mathfrak{a} := p\mathbb{Z} + p\alpha\mathbb{Z} + p^2\alpha^2\mathbb{Z} + p^2\alpha^3\mathbb{Z} \text{ and}$$
$$\mathfrak{b} := p\mathbb{Z} + p^2\alpha\mathbb{Z} + p\alpha^2\mathbb{Z} + p^2\alpha^3\mathbb{Z}.$$

are $\mathcal{O}$-ideals, and

$$\mathfrak{ab} = p^2\mathbb{Z} + p^2\alpha\mathbb{Z} + p^2\alpha^2\mathbb{Z} + p^2\alpha^3\mathbb{Z}.$$

We have

$$p^5 = \mathrm{Nm}_{\mathcal{O}}(\mathfrak{ab}) < \mathrm{Nm}_{\mathcal{O}}(\mathfrak{a})\,\mathrm{Nm}_{\mathcal{O}}(\mathfrak{b}) = p^3 \cdot p^3 = p^6.$$

Marseglia gave an example of strict super-multiplicativity in this order $\mathcal{O}$ as well.

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

Definition A.5. 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 $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{d}) = \frac{\mathrm{Nm}_{\mathcal{O}}(\mathfrak{a})}{\mathrm{Nm}_{\mathcal{O}}(\mathfrak{b})}$. (The next proposition shows this norm is well-defined.)

Proposition A.6. *The norm of a fractional ideal $\mathfrak{d}$ in Definition A.5 is well-defined. If $\mathfrak{d} \subseteq \mathcal{O}$, then its fractional ideal norm agrees with its integral ideal norm. If $\mathfrak{c} \in \mathrm{J}^*(\mathcal{O})$ and $\mathfrak{d} \in \mathrm{J}(\mathcal{O})$, then* $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{c}\mathfrak{d}) = \mathrm{Nm}_{\mathcal{O}}(\mathfrak{c})\,\mathrm{Nm}_{\mathcal{O}}(\mathfrak{d})$.

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 A.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.

In the case $\mathfrak{d} \subseteq \mathcal{O}$, we may choose $\mathfrak{a}_1 = \mathfrak{d}$ and $\mathfrak{b}_1 = \mathcal{O}$, so the integral ideal norm agrees with the fractional ideal norm.

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, $\mathfrak{c}\mathfrak{d} = (\mathfrak{a}_1\mathfrak{a}_2)(\mathfrak{b}_1\mathfrak{b}_2)^{-1}$, so

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

using Proposition A.2 and Definition A.5. □

Example A.7 (Behavior of norms of non-integral fractional ideals having an ideal power that is an integral ideal)**.** Consider the non-maximal order $\mathcal{O} = \mathbb{Z}[2i]$ of the Gaussian field $K = \mathbb{Q}(i)$, with maximal order $\mathcal{O}_K = \mathbb{Z}[i]$.

(1) The (non-integral) fractional $\mathcal{O}$-ideal

$$\mathfrak{r}_1 := (1+i)\mathcal{O} = 4\mathbb{Z} + (1+i)\mathbb{Z},$$

is a principal fractional $\mathcal{O}$-ideal, hence it is an invertible fractional $\mathcal{O}$-ideal. Here $\mathfrak{r}_1 = \mathfrak{c}\mathfrak{d}^{-1}$ where $\mathfrak{c} = 2(1+i)\mathcal{O}$ and $\mathfrak{d} = 2\mathcal{O}$ are invertible integral $\mathcal{O}$-ideals, from which we may compute $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{r}_1) = 2$.

Recall from Example 3.10 that $\mathfrak{r}_1$ has ideal square $\mathfrak{r}_1^2 = 2i\mathcal{O} = \mathfrak{q}_4'$, which was shown to be an irreducible integral $\mathcal{O}$-ideal in Example 2.14, having $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{q}_4') = 4$. The fractional $\mathcal{O}$-ideal $\mathfrak{r}_1$ then has fractional $\mathcal{O}$-ideal norm $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{r}_1) = 2$.

The equality $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{r}_1^2) = (\mathrm{Nm}_{\mathcal{O}}(\mathfrak{r}_1))^2 = 4$ is consistent with Proposition A.6, since $\mathfrak{r}_1$ is an invertible ideal.

(2) The (non-integral) fractional $\mathcal{O}$-ideal

$$\mathfrak{r}_2 := (1+i)\mathcal{O}_K = 2\mathbb{Z} + (1+i)\mathbb{Z},$$

is a non-invertible fractional $\mathcal{O}$-ideal. Viewed as a fractional $\mathcal{O}$-ideal, $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{r}_2) = 2$, using $\mathfrak{r}_2 = \mathfrak{c}_2(\mathfrak{d}_2)^{-1}$ with $\mathfrak{c}_2 = 2(1+i)\mathcal{O}_K$ and $\mathfrak{d}_2 = 2\mathcal{O}$. Next we have

$$(\mathfrak{r}_2)^2 = 2\mathcal{O}_K = \mathfrak{Q}_2,$$

and $\mathfrak{r}_2^2$ is a non-invertible $\mathcal{O}$-ideal since it is an $\mathcal{O}_K$-ideal. We have $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{Q}_2) = 2$. Consequently,

$$2 = \mathrm{Nm}_{\mathcal{O}}(\mathfrak{r}_2^2) \neq (\mathrm{Nm}_{\mathcal{O}}(\mathfrak{r}_2))^2 = 4,$$

showing that the hypothesis of $\mathcal{O}$-invertibility of at least one of $\mathfrak{c}$ and $\mathfrak{d}$ cannot be relaxed in Proposition A.6.

(3) The (non-integral) fractional $\mathcal{O}$-ideal

$$\mathfrak{r}_3 := i\mathcal{O} = 2\mathbb{Z} + i\mathbb{Z}$$

is an invertible fractional $\mathcal{O}$-ideal and it has square $(\mathfrak{r}_3)^2 = \mathcal{O}$, which is an invertible integral $\mathcal{O}$-ideal. In this case, $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{r}_3) = 1$.

The final proposition shows that norms of invertible fractional $\mathcal{O}$-ideals are preserved under extension.

Proposition A.8. *Suppose $\mathcal{O} \subseteq \mathcal{O}'$ for K-orders, and let* ext *be the extension map from fractional ideals on $\mathcal{O}$ to fractional ideals 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 definition $\mathrm{ext}(\mathfrak{c}) = \mathfrak{c}\mathcal{O}'$, and we wish to show

$$\mathrm{Nm}_{\mathcal{O}'}(\mathfrak{c}\mathcal{O}') = \mathrm{Nm}_{\mathcal{O}}(\mathfrak{c}).$$

Pick a positive integer $d \in \mathbb{N}$ so that $d(\mathcal{O}' + \mathfrak{c}\mathcal{O}') \subseteq \mathcal{O}$; it follows that $d\mathcal{O}' \subseteq \mathcal{O}$ and $d\mathfrak{c}\mathcal{O}' \subseteq \mathcal{O}$. Let n be the degree of the field extension $K/\mathbb{Q}$. Then $d\mathcal{O}'$ is an integral $\mathcal{O}'$-ideal with

$$\mathrm{Nm}_{\mathcal{O}'}(d\mathcal{O}') = [\mathcal{O}' : d\mathcal{O}'] = d^n.$$

Since $d\mathcal{O}'$ is an invertible $\mathcal{O}'$-ideal, Proposition A.6 for $\mathcal{O}'$-ideals gives

$$\mathrm{Nm}_{\mathcal{O}'}(d\mathfrak{c}\mathcal{O}') = \mathrm{Nm}_{\mathcal{O}'}((d\mathcal{O}')(\mathfrak{c}\mathcal{O}')) = \mathrm{Nm}_{\mathcal{O}'}(d\mathcal{O}')\,\mathrm{Nm}_{\mathcal{O}'}(\mathfrak{c}\mathcal{O}').$$

Since $d\mathfrak{c}\mathcal{O}'$ is an integral $\mathcal{O}'$-ideal (because it is contained in $\mathcal{O}$),

$$\mathrm{Nm}_{\mathcal{O}'}(d\mathfrak{c}\mathcal{O}') = [\mathcal{O}' : d\mathfrak{c}\mathcal{O}'].$$

We have $d\mathfrak{c}\mathcal{O}' \subseteq \mathcal{O} \subseteq \mathcal{O}'$, so the following index relations on $\mathbb{Z}$-modules hold:

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

Combining the four calculations thus far, in reverse order, we obtain

$$[\mathcal{O}' : \mathcal{O}]\,\mathrm{Nm}_{\mathcal{O}}(d\mathfrak{c}\mathcal{O}') = d^n\,\mathrm{Nm}_{\mathcal{O}'}(\mathfrak{c}\mathcal{O}'). \tag{A.2}$$

Since $\mathfrak{c}$ is an invertible $\mathcal{O}$-ideal, Proposition A.6 for $\mathcal{O}$-ideals gives

$$\mathrm{Nm}_{\mathcal{O}}(d\mathfrak{c}\mathcal{O}') = \mathrm{Nm}_{\mathcal{O}}((d\mathcal{O}')\mathfrak{c}) = \mathrm{Nm}_{\mathcal{O}}(\mathfrak{c})\,\mathrm{Nm}_{\mathcal{O}}(d\mathcal{O}').$$

Since $d\mathcal{O}' \subseteq \mathcal{O} \subseteq \mathcal{O}'$, a $\mathbb{Z}$-module index calculation yields

$$\mathrm{Nm}_{\mathcal{O}}(d\mathcal{O}') = [\mathcal{O} : d\mathcal{O}'] = \frac{[\mathcal{O}' : d\mathcal{O}']}{[\mathcal{O}' : \mathcal{O}]} = \frac{d^n}{[\mathcal{O}' : \mathcal{O}]}.$$

Combining the calculations in the previous two lines gives

$$\mathrm{Nm}_{\mathcal{O}}(d\mathfrak{c}\mathcal{O}') = \mathrm{Nm}_{\mathcal{O}}(\mathfrak{c})\,\frac{d^n}{[\mathcal{O}' : \mathcal{O}]} = \frac{d^n\,\mathrm{Nm}_{\mathcal{O}}(\mathfrak{c})}{[\mathcal{O}' : \mathcal{O}]}. \tag{A.3}$$

Substituting the right-hand side of (A.3) for $\mathrm{Nm}_{\mathcal{O}}(d\mathfrak{c}\mathcal{O}')$ into (A.2) yields

$$[\mathcal{O}' : \mathcal{O}]\,\frac{d^n\,\mathrm{Nm}_{\mathcal{O}}(\mathfrak{c})}{[\mathcal{O}' : \mathcal{O}]} = d^n\,\mathrm{Nm}_{\mathcal{O}'}(\mathfrak{c}\mathcal{O}'),$$

which simplifies to $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{c}) = \mathrm{Nm}_{\mathcal{O}'}(\mathfrak{c}\mathcal{O}')$. □

Example A.9 (Change of norm under extension for non-invertible ideals)**.** The norm of a non-invertible $\mathcal{O}$-ideal may change under extension. For any non-maximal order $\mathcal{O}$ the (absolute) conductor ideal $\mathfrak{f}(\mathcal{O}) = \mathfrak{f}_{\mathcal{O}_K}(\mathcal{O})$ is non-invertible integral $\mathcal{O}$-ideal that is an $\mathcal{O}_K$-ideal, whose norm will always increase under extension to $\mathcal{O}_K$. We have $\mathrm{ext}(\mathfrak{f}(\mathcal{O})) = \mathfrak{f}(\mathcal{O})$, and $\mathrm{Nm}_{\mathcal{O}}(\mathfrak{f}(\mathcal{O})) = [\mathcal{O} : \mathfrak{f}(\mathcal{O})]$, while

$$\mathrm{Nm}_{\mathcal{O}_K}(\mathfrak{f}(\mathcal{O})) = [\mathcal{O}_K : \mathfrak{f}(\mathcal{O})] = [\mathcal{O}_K : \mathcal{O}][\mathcal{O} : \mathfrak{f}(\mathcal{O})] = [\mathcal{O}_K : \mathcal{O}]\,\mathrm{Nm}_{\mathcal{O}}(\mathfrak{f}(\mathcal{O})).$$

The usefulness of Proposition A.8 is that it applies to invertible fractional ideals $\mathfrak{c}$ that are not coprime to the relative conductor ideal $\mathfrak{f}_{\mathcal{O}'}(\mathcal{O})$. For the non-maximal order $\mathcal{O} = \mathbb{Z}[2i]$ of the Gaussian field $K = \mathbb{Q}(i)$, treated in Example A.7, the ideal $\mathfrak{r}_1 := (1+i)\mathcal{O} = 4\mathbb{Z}+(1+i)\mathbb{Z}$ is a principal fractional $\mathcal{O}$-ideal so is $\mathcal{O}$-invertible. It is not coprime to the conductor ideal $\mathfrak{f}(\mathcal{O}) = \mathfrak{f}_{\mathcal{O}_K}(\mathcal{O}) = 2\mathcal{O}_K$. Noting that $\mathfrak{r}_1\mathcal{O}_K = (1+i)\mathcal{O}_K$, it follows that $\mathrm{Nm}_{\mathcal{O}_K}(\mathfrak{r}_1\mathcal{O}_K) = \mathrm{Nm}_{\mathcal{O}}(\mathfrak{r}_1) = 2$, consistent with Proposition A.8.

References

[1] M. Appleby, S. Flammia, and G. Kopp. A constructive approach to Zauner's conjecture via the Stark conjectures. In preparation (2024+).

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

[3] 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.

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

[5] E. Bayer-Fluckiger. Lattices and number fields. In *Algebraic geometry: Hirzebruch 70 (Warsaw 1998)*, 69–84, Contemp.Math. 241, Amer. Math. Soc. Providence, RI 1999.

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

[7] N. Bergeron, P. Charollois, and L. García Elliptic units for complex cubic fields. Preprint arXiv:2311.04110 (2023).

[8] A. Bourdon and P. L. Clark. Torsion points and Galois representations on CM elliptic curves. Pacific J. Math. **305** (2020), no. 1, 43–88.

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

[10] F. Campagna and R. Pengo. Entanglement in the family of division fields of elliptic curves with complex multiplication. Pacific J. Math. **317** (2022), no. 1, 21–66.

[11] P. L. Clark. Gorenstein endomorphism rings of abelian varieties. Preprint.

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

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

[14] H. Cohen and P. Stevenhagen. Computational class field theory. In *Surveys in algorithmic number theory*, J. P. Buhler and P. Stevenhagen, Math. Sci. Res. Inst. Publ. **44**, pp. 497–534. Cambridge University Press: New York 2008.

[15] H. Cohn. *A Classical Invitation to Algebraic Numbers and Class Fields*. With two appendices by O. Taussky. Springer: New York 1978.

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

[17] 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.

[18] 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.

[19] H. Darmon and S. Dasgupta. Elliptic units for real quadratic fields. Ann. of Math. (2) **163** (2006), no. 1, 301–346.
[20] H. Darmon, A. Pozzi, and J. Vonk. The values of the Dedekind–Rademacher cocycle at real multiplication points. J. Eur. Math. Soc. (JEMS) **26** (2024), no. 10, 3987–4032.
[21] H. Darmon and J. Vonk. Singular moduli for real quadratic fields: a rigid analytic approach. Duke Math. J. **170** (2021), no. 1, 23–93.
[22] R. Dedekind. Über die Anzahl der Ideal-Klassen in den verschiedenen Ordnungen eines endlichen Körpers. Festschrift der Technischen Hochschule in Braunschweig zur Säkularfeier des Geburtstages von C. F. Gauss, Branschweig 1877, 1–55. [In R. Dedekind, *Gesammelte Mathematische Werke* (ed. R. Fricke, E. Noether, Ö. Ore), Band I, pp. 105–157, Vieweg & Sohn., Braunschweig 1930.]
[23] R. Dedekind. Über die Theorie der ganzen algebraische Zahlen. Supplement XI von Dirichlets Vorlesungen über Zahlentheorie, 4. Aufl. 434–657. [In R. Dedekind, *Gesammelte Mathematische Werke* (ed. R. Fricke, E. Noether, Ö. Ore), Band III, pp. 1-222. Vieweg & Sohn., Braunschweig 1930.]
[24] D. S. Dummit and R. M. Foote. *Abstract Algebra* (Third Edition). John Wiley & Sons, Inc., Hoboken 2004.
[25] R. Fueter. Abelsche Gleichungen in quadratisch-imaginären Zahlkörpern. Math. Ann. **75** (1914), 177–255.
[26] C. Gentry. Fully homomorphic encryption using ideal lattices. Proc. 41st ACM Symposium on Theory of Computing (STOC), pp. 169–178, ACM, New York 2009.
[27] F. Halter-Koch. *Class Field Theory and L Functions: Foundations and Main Results.* CRC Press: Boca Raton, FL 2022.
[28] 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.
[29] P. Hill. Characters of commutative semigroups. J. Algebra **5** (1967), no. 1, 16–24.
[30] M. Katsuya 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.
[31] G. S. Kopp. SIC-POVMs and the Stark conjectures. Int. Math. Res. Not. IMRN **2021** (2021), no. 18, 13812–13838.
[32] G. S. Kopp. Stark class invariants as limits of a ratio of q-Pochhammer symbols. Preprint arXiv:2411.06763 (2024).
[33] G. S. Kopp and J. C. Lagarias. SICs and orders of real quadratic fields. Preprint arXiv:2407.08048 (2024).
[34] G. S. Kopp and J. C. Lagarias. Ray class monoids for orders of number fields. In preparation (2024+).
[35] D. S. Kubert and S. Lang. *Modular Units.* Grundlehren der Mathematischen Wissenschaften Vol. 244. Springer-Verlag: New York and Berlin, 1981.
[36] A. Lozano-Robledo. Galois representations attached to elliptic curves with complex multiplication. Algebra and Number Theory, **16** (2022), no. 4, 777-837.
[37] 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.
[38] V. Lyubashevsky, C. Peikert, O. Regev. A toolkit for ring-LWE-cryptography. EUROCRYPT 2013, 35–54. Lecture Notes In Comput. Sci., 7881, Springer 2013.
[39] V. Lyubashevsky, C. Peikert, O. Regev. On ideal lattices and learning with errors over rings. J. ACM **60** (2013), 1–35.
[40] S. Marseglia. Super-multiplicativity of ideal norms in number fields. Acta Arithmetica **193** (2020), 75–93.
[41] A. M. Masuda, L. Quoos, B. Steinberg. Character theory of monoids over an arbitrary field. J. Algebra **431** (2015), 107–126.
[42] D. B. McAlister. Characters on commutative semigroups. Q. J. Math. **19** (1968), 141–157.
[43] D. B. McAlister. Characters of finite semigroups. J. Algebra **22** (1972), no. 1, 183–200.
[44] D. Micciancio. Generalized compact knapsacks, cyclic lattices and efficient one-way functions. Computational complexity **16** (2007), 365–411.

[45] D. Micciancio and O. Regev. Lattice-based cryptography. In: *Post-Quantum Cryptography* (B. J. Bernstein, J. Buchmann, and E. Dahmen, eds.), pp. 147–191, Springer: New York 2009.
[46] J. Neukirch. *Algebraic Number Theory*. Translated from German by N. Schappacher. Grundlehren Math. Wiss. **322**. Springer: Berlin 2013.
[47] R. Pengo. *Mahler measures, special values of L-functions and complex multiplication*. Ph.D. thesis, København Universiteit, 2020.
[48] 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.
[49] R. Schertz. *Complex multiplication*. New Mathematical Monographs **15**, Cambridge University Press, 2010.
[50] H. Söhngen. Zur complexen Multiplikation. Math. Ann. **111** (1935), no. 1, 302–328.
[51] P. Stevenhagen. Generalized unramified class field theory. Math. Inst., Univ. Amersterdam, Report 85–13, 1985.
[52] P. Stevenhagen. Unramified class field theory for orders. Trans. Amer. Math. Soc. **311** (1989), no. 2, 483–500.
[53] P. Stevenhagen. Hilbert's 12th problem, complex multiplication and Shimura reciprocity. In *Class Field Theory: Its centenary and prospect*, pp. 161–176, Adv. Stud. Pure Math. **30**, Math. Soc. Japan, Tokyo, 2001.
[54] P. Stevenhagen. The arithmetic of number rings. In *Algorithmic Number Theory*, pp. 209–266, MSRI Publications **44**, Amer. Math. Soc., 2008.
[55] P. Stevenhagen. *Number Rings*. University of Leiden 2019, 91pp.
[56] T. Takagi. Über eine Theorie des relativ-Abel'schen Zahlkörpers. J. Coll. Sci. imp. Univ. Tokyo **41** (1920), no. 9, 1–133.
[57] O. Taussky. On a theorem of Latimer and MacDuffee. Canadian J. Math. **1** (1949), 300–302.
[58] O. Taussky. Ideal Matrices I. Archiv der Math. **13** (1962), 275–282.
[59] O. Taussky. Ideal Matrices II. Math. Annalen **150** (1963), 218–225.
[60] O. Taussky. Introduction into connections between algebraic number theory and integral matrices. Appendix (pp. 305–326) in: H. Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields*, Springer-Verlag, New York 198.
[61] H. Weber. *Elliptische Funktionen und algebraische Zahlen*. Braunschweig: Vieweg 1894. Second Edition: 1898. (Reprint: Chelsea: New York.)
[62] H. Weber. *Lehrbuch der Algebra II*. Braunschweig: Viehweg 1896, Second Edition: 1899. (Reprint: Chelsea, New York.)
[63] H. Weber. Über Zahlengruppen in algebraischen Zahlkörpern, I, II, III. Math. Ann. **48** (1897), 433–473; **49** (1897), 83–100; **50** (1898), 1–26.
[64] H. Weber. *Lehrbuch der Algebra III*. Braunschweig: Viehweg 1908. (Reprint: Chelsea, New York.)
[65] H. Yi and C. Lv. On ring class fields of number rings. Preprint arXiv:1810.04810 (2018).
[66] G. Zauner. *Quantendesigns: Grundzüge einer nichtkommutativen Designtheorie*. PhD thesis, University of Vienna, 1999.
[67] 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