

COMPUTING THE IDEAL CLASS MONOID OF AN ORDER

STEFANO MARSEGLIA

ABSTRACT. There are well known algorithms to compute the class group of the maximal order \mathcal{O}_K of a number field K and the group of invertible ideal classes of a non-maximal order R . In this paper we explain how to compute also the isomorphism classes of non-invertible ideals of an order R in a finite product of number fields K . In particular we also extend the above-mentioned algorithms to this more general setting. As an application, we use a generalization of a theorem of Latimer and MacDuffee to produce algorithms that return representatives of all conjugacy classes of integral matrices with given characteristic polynomial (satisfying certain assumptions) and solve the conjugacy problem for such matrices.

1. INTRODUCTION

Let K be a number field and R an order in K . There are well known algorithms to compute the ideal class group $\text{Pic}(R)$ when R is the ring of integers \mathcal{O}_K of K , also known as the maximal order, see for example [Coh93]. This information can be used to efficiently compute the group $\text{Pic}(R)$ of invertible ideal classes of a non-maximal order R , as is explained in [KP05].

On the other hand not much is known about non-invertible ideals and, in particular, it is not known how to compute the monoid of all ideal classes of R , which we will denote $\text{ICM}(R)$. In the literature one can find results about the local isomorphism classes of ideals. More precisely, one studies the genus of an ideal, which is its isomorphism class after localizing at a rational prime p , or its weak equivalence class, which is its isomorphism class after localizing at a prime ideal \mathfrak{p} of R . For the notion of genus we refer to [Rei70] and [Rei03], while for results about the weak equivalence classes we cite [DTZ62]. It is important to mention that these two apparently different notions are actually equivalent, as pointed out in [LW85, Section 5].

In the present paper we exhibit:

- an algorithm to compute the monoid $\text{ICM}(R)$ of isomorphism classes of fractional ideals of an order R in a finite product of number fields K , see Theorem 4.6, Proposition 5.1 and the algorithms in Section 6, and
- a bijection between the set of conjugacy classes of integral matrices with given square-free minimal polynomial m and characteristic polynomial c and the set of R -isomorphism classes of \mathbb{Z} -lattices in a certain \mathbb{Q} -algebra, where R is an order in a certain product of number fields, see Theorem 8.1. Under certain assumptions on the polynomials c and m , we can reduce such a description to an ideal class monoid computation and hence solve the conjugacy problem and produce representatives of each conjugacy class, see Corollary 8.2.

Theorem 8.1 is a generalization of the main result of [LM33] where the case when c is square-free is analyzed. Their theorem was then reproved with a different method under the extra assumption that c is irreducible in [Tau49]. The author recently discovered that Theorem 8.1 has independently been proved in [Hus16] in greater generality. Moreover, a new algorithm to test whether two rational matrices are conjugate over \mathbb{Z} is given in [EHO19]. This algorithm works in more generality than ours at the cost of being slower.

The present paper is structured as follows. In Section 2 we recall the definitions of an order R and a fractional ideal in a product of number fields K and some basic results, which are well known in the case that K is a number field. In Section 3 we introduce isomorphisms of fractional ideals, and the monoid that the corresponding classes form, called the ideal class monoid $\text{ICM}(R)$. Since it is hard to compute $\text{ICM}(R)$ directly, in Section 4 we relax the notion of isomorphism to a local one, called weak equivalence. We explain

2010 *Mathematics Subject Classification.* 11R54 11Y40 (primary), 11C20 15B36 (secondary).

This is the accepted version of the following article: *Marseglia, Stefano; Computing the ideal class monoid of an order.* *J. Lond. Math. Soc. (2)* 101 (2020), no. 3, 984-1007, which has been published in final form at <http://dx.doi.org/10.1112/jlms.12294>

how to effectively check whether two fractional ideals are weakly equivalent and how to algorithmically reconstruct $\text{ICM}(R)$ once we have computed $\text{Pic}(S)$, for every over-order S of R , and the monoid of weak equivalence classes $\mathcal{W}(R)$. In Section 5 we explain a concrete way to compute representatives of the weak equivalence class monoid $\mathcal{W}(R)$. In Section 6 we give the pseudo-code of the algorithms described in the previous sections and discuss the running time and the bottlenecks. In Section 7 we present some concrete calculations of ideal class monoids. Finally, in Section 8 we present our results about computing conjugacy classes of integral matrices and compare the running times of our algorithm and the algorithm proposed in [EHO19], see Example 8.4. Observe that Corollary 8.2 gives a solution to [EHO19, Problem 7.7] for matrices satisfying the appropriate hypotheses.

The algorithms have been implemented in Magma [BCP97] and the code is available at <https://github.com/stmar89/AbVarFq>.

Another application, namely computing isomorphism classes of abelian varieties defined over a finite field belonging to an isogeny class determined by a square-free Weil polynomial, is discussed in [Mar18b].

Acknowledgments. The author would like to thank Jonas Bergström for helpful discussions and Rachel Newton, Christophe Ritzenthaler, Peter Stevenhagen and Marco Streng for comments on a previous version of the paper, which is part of the author's Ph.D thesis [Mar18a]. The author wishes to thank Jürgen Klüners for pointing out the reference [Hus16]. We thank Bettina Eick, Tommy Hofmann and Eamonn O'Brien for allowing us to read an early version of their article [EHO19]. We are grateful to the anonymous referee of the *Journal of London Mathematical Society* for reading the paper carefully and providing thoughtful comments.

2. ORDERS

In what follows, the word ring will mean commutative ring with unit. An *order* is a reduced ring R , which is free and finitely generated as a \mathbb{Z} -module. Let K be the total quotient ring of an order R , that is, the localization of R at the multiplicative set of non-zero-divisors. Then K is an étale algebra over \mathbb{Q} with $R \otimes_{\mathbb{Z}} \mathbb{Q} = K$, and in particular K is a finite product of number fields, say $K = K_1 \times \dots \times K_r$. The set of orders in K contains a maximal element with respect to the inclusion relation. This order, denoted \mathcal{O}_K , is the integral closure of \mathbb{Z} in K and it is usually referred to as the *maximal order* or the *ring of integers* of K . Note that $\mathcal{O}_K = \mathcal{O}_{K_1} \times \dots \times \mathcal{O}_{K_r}$, where \mathcal{O}_{K_i} is the maximal order of K_i . Indeed, \mathcal{O}_K contains $\prod_i \mathcal{O}_{K_i}$, so \mathcal{O}_K is a product of orders S_i in K_i and by maximality it follows that $S_i = \mathcal{O}_{K_i}$. There are well known algorithms to compute each \mathcal{O}_{K_i} , see for example [Coh93, Chapter 6], and in what follows we will assume that we can compute \mathcal{O}_K .

From now on R will be an order in K . A finitely generated sub- R -module I of K is called a *fractional R -ideal* if $I \otimes_{\mathbb{Z}} \mathbb{Q} = K$. Such an I is a finitely generated free \mathbb{Z} -module of the same rank as R , and so we can find $x_1, \dots, x_n \in K$, where $n = \sum_{i=1}^r [K_i : \mathbb{Q}]$, such that

$$I = x_1\mathbb{Z} \oplus \dots \oplus x_n\mathbb{Z}.$$

In particular, if $I \subseteq R$ then the quotient R/I is finite. We denote by $\mathcal{I}(R)$ the set of all fractional ideals of R . Observe that for every fractional R -ideal I , there exists a non-zero-divisor $x \in K$ such that xI is an ideal of R . Moreover, every ideal of R containing a non-zero-divisor is a fractional R -ideal. The fractional R -ideals that are rings are called *over-orders* of R . Since \mathcal{O}_K and R have the same rank as free abelian groups, the quotient \mathcal{O}_K/R is finite and thus there are only finitely many over-orders of R .

Given two fractional R -ideals I and J , the product IJ , the sum $I+J$, the intersection $I \cap J$, and the ideal quotient

$$(I : J) = \{x \in K : xJ \subseteq I\}$$

are fractional R -ideals. In particular, ideal multiplication induces on $\mathcal{I}(R)$ the structure of a commutative monoid with unit element R . A useful property of the ideal quotient is the following lemma, whose proof we leave to the reader.

Lemma 2.1. *Let I, J, L be fractional R -ideals, then*

$$((I : J) : L) = (I : JL).$$

If I is a fractional R -ideal then $(I : I)$ is a sub-ring of K containing R . Hence it is an over-order of R and, in particular, it is the biggest over-order of R for which I is a fractional ideal. It is called the *multiplicator ring* of I .

Lemma 2.2. *The over-orders of R are precisely the idempotents of $\mathcal{I}(R)$, that is, the fractional R -ideals S such that $SS = S$.*

Proof. Let S be an over-order of R . Then S is multiplicatively closed and contains 1, so $SS = S$. Conversely, let S be an idempotent fractional ideal of R . Let $T = (S : S)$ be the multiplicator ring of S . As $SS = S$ we have $S \subseteq T$ and hence S is a finitely generated idempotent T -ideal. By the determinant trick it must be generated by an idempotent element e of T . As S has full rank over \mathbb{Z} we must have $e = 1$, that is, $S = T$. In particular, S is an over-order of R . \square

We will denote by $\text{Tr}_{K/\mathbb{Q}}$, or simply Tr when no confusion can arise, the *trace form* on K , which associates to every $x \in K$ the trace of the matrix of the multiplication by x . For every fractional R -ideal I , we define the *trace dual ideal* as $I^t = \{x \in K : \text{Tr}(xI) \subseteq \mathbb{Z}\}$. Given a \mathbb{Z} -basis $\{x_i\}$ of I , we have $I^t = x_1^*\mathbb{Z} \oplus \dots \oplus x_n^*\mathbb{Z}$, where $\{x_j^*\}$ is the *trace dual basis*, which is characterized by $\text{Tr}(x_i x_j^*) = 1$ or 0 according to whether $i = j$ or $i \neq j$. Observe that I^t is a fractional R -ideal and that the map $x \mapsto \varphi_x$, where $\varphi_x(y) = \text{Tr}(xy)$ is an isomorphism from I^t to $\text{Hom}_{\mathbb{Z}}(I, \mathbb{Z})$. In the next lemma we will summarize some well known properties of the trace dual ideal.

Lemma 2.3. *Let R be an order in K , let I and J be two fractional R -ideals and let x be in K^\times . Then the following holds:*

- $(I^t)^t = I$,
- $I \subset J \iff J^t \subset I^t$,
- $(I \cap J)^t = I^t + J^t$,
- $(xI)^t = \frac{1}{x}I^t$,
- $(I : J) = (I^t J)^t$,
- $(I : J) = (J^t : I^t)$,
- $S = (I : I) \iff II^t = S^t$.

Let \mathfrak{p} be a prime ideal of R which is also a fractional R -ideal. Since the integral domain R/\mathfrak{p} is finite, we see that \mathfrak{p} is a maximal ideal. Conversely, if \mathfrak{m} is a maximal ideal of R then it contains the prime p which is the characteristic of the field R/\mathfrak{m} , and hence \mathfrak{m} is a fractional R -ideal. We will refer to the maximal ideals of R as the *primes* of R . Since for any fractional R -ideal I contained in R the quotient R/I is finite, we deduce that there exists only a finite number of primes of R containing I .

A fractional R -ideal I is said to be *invertible* if $IJ = R$, for some fractional R -ideal J . Observe that if such a J exists then $J = (R : I)$.

Remark 2.4. *Note that we could equivalently say that an R -ideal I is invertible if and only if there exists an R -ideal J and a non-zero-divisor d such that $IJ = dR$. This characterization allows us to talk about invertible ideals in any ring.*

Lemma 2.5. *Let I be an invertible fractional R -ideal. Then R is the multiplicator ring of I .*

Proof. Put $S = (I : I)$. Since I is an R -module we have $R \subseteq S$ and using $I = SI$ we deduce that

$$R = I(R : I) = SI(R : I) = SR = S.$$

\square

Remark 2.6. *Let I be a fractional R -ideal and let S an over-order of R . In view of Lemma 2.5, the expression “ I is invertible as fractional S -ideal” implies that S is the multiplicator ring of I .*

The following lemmas are useful for understanding how invertible ideals behave with respect to localizations at primes.

Lemma 2.7. [Kap49, Theorem 12.3] *Let T be a Noetherian ring. Then T is a principal ideal ring if and only if every maximal ideal is principal.*

Lemma 2.8. [Gil92, Proposition 7.4] *Let T be a ring with finitely many maximal ideals and let I be a T -ideal. Then I is invertible in T if and only if I is principal and generated by a non-zero-divisor.*

It is not difficult to prove the following.

Lemma 2.9. *Let I be a fractional R -ideal. Then I is invertible if and only if $I_{\mathfrak{p}}$ is principal for every prime \mathfrak{p} of R .*

From the previous lemmas it is easy to deduce the following result.

Corollary 2.10. *Let \mathfrak{p} be a prime of R . Then \mathfrak{p} is invertible if and only if $R_{\mathfrak{p}}$ is a principal ideal ring.*

Observe that \mathcal{O}_K is the only order in K whose fractional ideals are all invertible. We introduce now some classes of orders which are particularly well behaved in terms of invertibility of ideals.

Proposition 2.11. [BL94, Proposition 2.7] *Let R be an order with trace dual R^t . The following are equivalent:*

- (a) *for every fractional R -ideal I , we have $(R : (R : I)) = I$;*
- (b) *for every fractional R -ideal I , we have $(I : I) = R$ if and only if I is invertible;*
- (c) *R^t is invertible in R .*

An order satisfying one of the equivalent conditions of Proposition 2.11 is called *Gorenstein*. This definition is equivalent to the usual one, see [Bas63, Theorem 6.3]. Observe that \mathcal{O}_K is Gorenstein, but there are Gorenstein orders which are not maximal. One class of examples of Gorenstein orders are the *monogenic* orders, which are of the form $\mathbb{Z}[x]/(f)$, where f is a monic polynomial with integer coefficients and non-zero discriminant.

Corollary 2.12. [BL94, Example 2.8] *Monogenic orders are Gorenstein.*

An order R is called a *Bass* order if every over-order of R is Gorenstein, or equivalently, if the R -module \mathcal{O}_K/R is cyclic, that is, if $\mathcal{O}_K = R + xR$ for some $x \in \mathcal{O}_K$. For a proof and other equivalent characterizations, see for example [LW85, Theorem 2.1] and Proposition 3.7. Observe that every order in a quadratic number field is a Bass order.

3. IDEAL CLASSES

Recall that for an order R in K we denote by $\mathcal{I}(R)$ the commutative monoid of fractional R -ideals.

Definition 3.1. *Let R be an order in K . The ideal class monoid of R is*

$$\text{ICM}(R) = \mathcal{I}(R) / \simeq,$$

where $I \simeq J$ if and only if I and J are isomorphic as R -modules. We will denote the ideal class of I with $\{I\}$.

The name is justified by the fact that $\text{ICM}(R)$ inherits the commutative monoid structure of $\mathcal{I}(R)$, as will become evident with Corollary 3.4.

Lemma 3.2. *Let R be an order in K . Consider an R -module morphism $\varphi : I \rightarrow J$, where I and J are two fractional R -ideals, then φ is a multiplication by some $\alpha \in K$.*

The previous lemma, whose proof is left to the reader, directly implies the following two Corollaries.

Corollary 3.3. *Let I and J be two fractional R -ideals. Then we have a natural identification*

$$\text{Hom}_R(I, J) = (J : I).$$

In particular, if \mathfrak{p} is a prime of R then every $R_{\mathfrak{p}}$ -linear morphism $\varphi : I_{\mathfrak{p}} \rightarrow J_{\mathfrak{p}}$ is a multiplication by some α in the total quotient ring of $R_{\mathfrak{p}}$.

Corollary 3.4. *Two fractional R -ideals I and J are isomorphic if and only if there exists an $\alpha \in K^{\times}$ such that $I = \alpha J$.*

The group $\mathcal{P}(R)$ of principal fractional R -ideals acts by multiplication on $\mathcal{I}(R)$ and we have that

$$\mathrm{ICM}(R) = \mathcal{I}(R) / \mathcal{P}(R).$$

Observe that every fractional ideal in $\mathcal{P}(R)$ is invertible (as a fractional R -ideal), so we can consider the quotient of invertible fractional R -ideals by $\mathcal{P}(R)$, which will inherit a group structure.

Definition 3.5. *Let R be an order in K . The Picard group of R is*

$$\mathrm{Pic}(R) = \{\text{invertible } I \in \mathcal{I}(R)\} / \mathcal{P}(R).$$

Since being invertible is a property of the ideal class, we can conclude that $\mathrm{Pic}(R) \subseteq \mathrm{ICM}(R)$. Observe that equality holds if and only if $R = \mathcal{O}_K$.

Since \mathcal{O}_K is a finite product of Dedekind domains, we have that every ideal can be written in a unique way as a product of prime ideals, see for example [Rei03, Theorem 22.24]. For every invertible fractional ideals of non-maximal prime order R , we can find an isomorphic one, say I , which is coprime with the conductor $\mathfrak{f} = (R : \mathcal{O}_K)$. This implies that $I\mathcal{O}_K \cap R = I$ and hence it follows that I admits a factorization into a product of primes of R . But this is not true if we look at non-invertible ideals.

It is easy to show that the multiplier ring is an invariant of the ideal class.

Lemma 3.6. *Let R be an order in K . If two fractional R -ideals I and J are isomorphic then they have the same multiplier ring.*

It follows that

$$(1) \quad \mathrm{ICM}(R) \supseteq \bigsqcup \mathrm{Pic}(S)$$

where the disjoint union is taken over the set of over-orders S of R .

Recall that a commutative monoid is called *Clifford* if it is a disjoint union of groups. For other equivalent definitions of a commutative Clifford monoid see [ZZ94, Section 1] or [Hel40, Chapter IV].

Proposition 3.7. *The following are equivalent:*

- (a) R is Bass,
- (b) the inclusion in (1) is an equality,
- (c) $\mathrm{ICM}(R)$ is Clifford.

Proof. (a) \Rightarrow (b): If R is Bass then every over-order is Gorenstein and in particular every fractional R -ideal I is invertible in its own multiplier ring S . This means that $\{I\}$ is in $\mathrm{Pic}(S)$ and (b) holds.

(b) \Rightarrow (c): This is obvious.

(c) \Rightarrow (a): Write $\mathrm{ICM}(R) = \bigsqcup_e G_e$, where e runs over the set of idempotent elements of $\mathrm{ICM}(R)$, and G_e denotes the group with unit e . Let J be a fractional R -ideal representing e . Then there exists $x \in K^\times$ such that $xJ^2 = J$. Put $S = xJ$. Then

$$S^2 = x^2 J^2 = x(xJ^2) = xJ = S.$$

Note that S is another representative of the class e and by Lemma 2.2 it is an over-order of R . Now let T be any over-order of R . We want to show that T^t is invertible in T . Say that the class representing T^t lies in G_e where $e = \{S\}$. Then T^t is invertible in S and, since the multiplier ring of T^t is T , by Lemma 2.5, we have that $S = T$. \square

Remark 3.8. *If $K = K_1 \times \dots \times K_r$, with K_i number fields, then $\mathcal{O}_K = \prod_i \mathcal{O}_{K_i}$ and*

$$\mathrm{Pic}(\mathcal{O}_K) = \mathrm{Pic}(\mathcal{O}_{K_1}) \times \dots \times \mathrm{Pic}(\mathcal{O}_{K_r}).$$

There are well known algorithms to compute each $\mathrm{Pic}(\mathcal{O}_{K_i})$, see [Ste08]. Note that if S is an over-order of R , then the extension map $I \mapsto IS$ induces a surjective group homomorphism $\mathrm{Pic}(R) \twoheadrightarrow \mathrm{Pic}(S)$, see for example [DTZ62, Corollary 2.1.11]. In particular, if $S = \mathcal{O}_K$ we have an exact sequence

$$(2) \quad 0 \rightarrow R^\times \rightarrow \mathcal{O}_K^\times \rightarrow \frac{(\mathcal{O}_K/\mathfrak{f})^\times}{(R/\mathfrak{f})^\times} \rightarrow \mathrm{Pic}(R) \rightarrow \mathrm{Pic}(\mathcal{O}_K) \rightarrow 0,$$

where \mathfrak{f} is the conductor of R . The exactness of (2) is classical for the case when $r = 1$, that is, when K is a number field. A proof for the case $r > 1$ can be found in [JP16]. The results contained in [KP05] describe how to compute the middle term of (2) in the case $r = 1$ and they can be extended word-by-word to the general case. Since $\mathcal{O}_K^\times = \prod_i \mathcal{O}_{K_i}^\times$ and there are well known algorithms to compute each $\mathcal{O}_{K_i}^\times$, we deduce that we can effectively compute $\text{Pic}(R)$ and R^\times .

4. WEAK EQUIVALENCE CLASSES

The following result was proved in [DTZ62] in the particular case of an integral domain. We include a proof for completeness.

Proposition 4.1. *Let I and J be two fractional R -ideals. The following are equivalent:*

- (a) $I_{\mathfrak{p}}$ and $J_{\mathfrak{p}}$ are isomorphic for every prime \mathfrak{p} of R ;
- (b) $1 \in (I : J)(J : I)$;
- (c) I and J have the same multiplier ring, say S , and there exists an invertible fractional S -ideal L such that $I = LJ$.

Proof. (a) \Rightarrow (b): Let \mathfrak{p} be a prime of R . By Corollary 3.3 there exists a non-zero-divisor x in the total quotient ring of $R_{\mathfrak{p}}$ such that $I_{\mathfrak{p}} = xJ_{\mathfrak{p}}$, which in turn implies that

$$(I_{\mathfrak{p}} : J_{\mathfrak{p}}) = (xJ_{\mathfrak{p}} : J_{\mathfrak{p}}) = x(J_{\mathfrak{p}} : J_{\mathfrak{p}}) \quad \text{and} \quad (J_{\mathfrak{p}} : I_{\mathfrak{p}}) = (J_{\mathfrak{p}} : xJ_{\mathfrak{p}}) = \frac{1}{x}(J_{\mathfrak{p}} : J_{\mathfrak{p}}).$$

Therefore

$$((I : J)(J : I))_{\mathfrak{p}} = (I_{\mathfrak{p}} : J_{\mathfrak{p}})(J_{\mathfrak{p}} : I_{\mathfrak{p}}) = x(J_{\mathfrak{p}} : J_{\mathfrak{p}}) \frac{1}{x}(J_{\mathfrak{p}} : J_{\mathfrak{p}}) = (J_{\mathfrak{p}} : J_{\mathfrak{p}}),$$

which clearly contains 1. Hence, the natural inclusion $(J : I)(I : J) \subseteq (J : J)$ is locally surjective at \mathfrak{p} . Since the choice of \mathfrak{p} was arbitrary we conclude that $(J : I)(I : J) = (J : J)$ and in particular that $1 \in (J : I)(I : J)$.

(b) \Rightarrow (c): By definition of quotient ideal we have that $(I : J)(J : I) \subseteq (I : I)$ and that $(I : J)(J : I) \subseteq (J : J)$. Since $(I : J)(J : I)$ has a structure of both $(I : I)$ and $(J : J)$ -module and contains 1, it follows that

$$(I : I) = (I : J)(J : I) = (J : J),$$

that is, I and J have the same multiplier ring and $(I : J)$ and $(J : I)$ are inverse to each other. The following inclusions

$$I = I(I : I) = I(I : J)(J : I) \subseteq J(I : J) \subseteq I$$

are therefore equalities and in particular $I = LJ$ for $L = (I : J)$.

(c) \Rightarrow (a): Let L' be any invertible ideal in R such that $L'S = L$. Note that such an L' exists since the extension map $\text{Pic}(R) \rightarrow \text{Pic}(S)$ is surjective, as we explain in Remark 3.8. The localization $L'_{\mathfrak{p}}$ at any prime \mathfrak{p} of R is principal by Lemma 2.8, say $L'_{\mathfrak{p}} = xR_{\mathfrak{p}}$. Then $I_{\mathfrak{p}} = xJ_{\mathfrak{p}}$ and hence $I_{\mathfrak{p}} \simeq J_{\mathfrak{p}}$. \square

Definition 4.2. *If two fractional R -ideals I and J satisfy the equivalent conditions of Proposition 4.1 we say that they are weakly equivalent. Denote by $\mathcal{W}(R)$ the set of weak equivalence classes and by $[I]$ the weak equivalence class of a fractional R -ideal I . Given any over-order S of R let $\mathcal{W}_S(R)$ be the subset of $\mathcal{W}(R)$ consisting of the weak equivalence classes $[I]$ such that $(I : I) = S$.*

Note that $\mathcal{W}(R)$ inherits the structure of a commutative monoid from $\mathcal{I}(R)$. Consider the partition

$$\mathcal{W}(R) = \bigsqcup \mathcal{W}_S(R),$$

where the disjoint union is taken over all the over-orders S of R . By Proposition 4.1.(b) an ideal is invertible if and only if it is weakly equivalent to its multiplier ring and hence we have that $\mathcal{W}_S(R) = \{[S]\}$ if and only if S is Gorenstein.

Remark 4.3. *Let p be a rational prime number and put $R_{(p)} = R \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$. Similarly, for fractional R -ideals I and J , put $I_{(p)} := I \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ and $J_{(p)} := J \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$. The ideals I and J are said to belong to the same genus if and only if $I_{(p)}$ and $J_{(p)}$ are isomorphic as $R_{(p)}$ -modules for every rational prime p . Note that $R_{(p)}$ is a semi-local ring and hence by Lemma 2.8 fractional ideals are invertible if and only if they are principal and generated by a non-zero-divisor. An easy modification of the proof of Proposition 4.1 shows that I and*

I and J are weakly equivalent if and only if they belong to the same genus. This equivalence was already noticed in [LW85, Section 5]. The notion of genus is classical and it has been widely studied in the literature, see for example [Rei03, Section 7] and [Rei70, Section 6]. For example, it is known that I and J are in the same genus if and only if they are isomorphic after tensoring with the p -adic completion \mathbb{Z}_p , which in turn holds if and only if the quotients $I/p^k I$ and $J/p^k J$ are isomorphic for an integer k , that only depends on $R_{(p)}$. We prefer to work with the notion of weak equivalence introduced above, since part (b) of Proposition 4.1 implies that checking whether two ideals are weakly equivalent can be performed in polynomial time.

Corollary 4.4. *Let I and J be fractional ideals. Then*

$$\{I\} = \{J\} \iff \{I^t\} = \{J^t\}$$

and

$$[I] = [J] \iff [I^t] = [J^t].$$

Proof. Note that $I = xJ$ if and only if $I^t = (1/x)J^t$, which gives the first equivalence. The second equivalence follows from the equality $(I : J)(J : I) = (J^t : I^t)(I^t : J^t)$ and part (b) of Proposition 4.1. \square

Note that two invertible fractional R -ideals I and J are isomorphic if and only if IJ^{-1} is a principal fractional R -ideal. Since being weakly equivalent is a necessary condition for being isomorphic, we can also reduce the isomorphism problem between non-invertible ideals to a principal ideal problem.

Corollary 4.5. *Let I and J be two weakly equivalent fractional R -ideals, and let S be their multiplier ring. Then*

$$I = (I : J)J,$$

and $(I : J)$ is an invertible fractional S -ideal. In particular, $I \simeq J$ if and only if $(I : J)$ is a principal fractional S -ideal.

Proof. Let S be the multiplier ring of I and J . If I and J are weakly equivalent, we show in the proof of Proposition 4.1 that $(I : J)$ is an invertible fractional S -ideal and $I = (I : J)J$. In particular, if $(I : J)$ is a principal fractional S -ideal, then I and J are isomorphic.

Conversely, if $I = xJ$ for some $x \in K^\times$ then

$$(I : J) = (xJ : J) = x(J : J) = xS,$$

which concludes the proof. \square

Finally, knowing the weak equivalence classes allows us to reconstruct the isomorphism classes. Let S be an over-order of R and define

$$\text{ICM}_S(R) = \{\{I\} \in \text{ICM}(R) \text{ s.t. } (I : I) = S\},$$

so that we get

$$\text{ICM}(R) = \bigsqcup \text{ICM}_S(R),$$

where the disjoint union is taken over all the over-orders S of R .

Theorem 4.6. *Let R be an order in K . For every over-order S of R , the action of $\text{Pic}(S)$ on $\text{ICM}_S(R)$ induced by ideal multiplication is free and*

$$\mathcal{W}_S(R) = \text{ICM}_S(R) / \text{Pic}(S).$$

More concretely, if

$$\mathcal{W}_S(R) = \{[I_1], \dots, [I_r]\} \quad \text{and} \quad \text{Pic}(S) = \{\{J_1\}, \dots, \{J_s\}\},$$

with the I_i 's pairwise not weakly equivalent and the J_j 's pairwise not isomorphic then

$$\text{ICM}_S(R) = \{\{I_i J_j\} : 1 \leq i \leq r, 1 \leq j \leq s\}$$

and the fractional ideals $I_i J_j$ are pairwise not isomorphic.

Proof. Let I be a fractional R -ideal with multiplier ring S . Then $[I] = [I_i]$ for some i , that is, there exists an invertible fractional S -ideal J such that $I = I_i J$. Let j be the index such that $\{J\} = \{J_j\}$. It follows that $\{I\} = \{I_i J_j\}$. It remains to prove that if $\{I_i J_j\} = \{I_k J_h\}$, that is, $I_i J_j = x I_k J_h$ for some $x \in K^\times$, then $i = k$ and $j = h$. Multiplying by $(S : J_j)$ on both sides, we get by Proposition 4.1.(c) that I_i is weakly equivalent to I_k , that is, $i = k$. To conclude, it is enough to prove that if $I = IJ$ with I and J both having multiplier ring S and J invertible, then $J = S$. We will prove that this is true locally at every prime of S . Since J is invertible, we have by Lemma 2.8 that $J_{\mathfrak{p}} = y S_{\mathfrak{p}}$ for some non-zero-divisor y . Hence it follows that

$$I_{\mathfrak{p}} = y S_{\mathfrak{p}} I_{\mathfrak{p}} = y I_{\mathfrak{p}}$$

which implies that both y and $1/y$ are in $(I_{\mathfrak{p}} : I_{\mathfrak{p}}) = S_{\mathfrak{p}}$. Therefore we again have $J_{\mathfrak{p}} = S_{\mathfrak{p}}$. \square

Remark 4.7. *Fixing the multiplier ring is a key point in using the previous proposition. Let $R = \mathbb{Z}[\alpha]$, where α is a root of $f(x) = x^2 - 8x - 8$. Note that $\mathcal{O}_K = \mathbb{Z}[\alpha/2]$ and $[\mathcal{O}_K : R] = 2$. Consider the invertible R -ideal $\mathfrak{p} = (3, \alpha - 1)$ and the conductor $\mathfrak{f} = (2, \alpha)$ of R . It is easy to verify that $\text{Pic}(\mathcal{O}_K)$ is trivial, while $\text{Pic}(R) \simeq \mathbb{Z}/2\mathbb{Z}$ with generator the ideal class of \mathfrak{p} . It follows that the product $\mathfrak{f}\mathfrak{p}$ is isomorphic to \mathfrak{f} and, in particular, that the action of $\text{Pic}(R)$ on the whole $\text{ICM}(R)$ is not free.*

Using Theorem 4.6 we can compute the ideal class monoid of an order R if we know all its over-orders, their Picard groups and the weak equivalence class monoid. For the first issue, by Lemma 2.2, it is enough to look at the idempotent R -modules of the finite quotient \mathcal{O}_K/R . In the end of Section 3 we discussed how to compute the Picard group of a possibly non-maximal order. Finally, in the next section we will describe how to compute $\mathcal{W}(R)$. See Section 6 for the corresponding algorithms.

5. COMPUTING THE WEAK EQUIVALENCE CLASS MONOID

The following results are inspired by [DTZ62] where the authors produce similar results in the particular case of an integral domain. Let R be an order in K . Recall that we can partition $\mathcal{W}(R)$ as the disjoint union of $\mathcal{W}_S(R)$ where S runs through the set of over-orders of R . We will now describe a method to compute $\mathcal{W}_S(R)$. Observe that when S is not Gorenstein there are always at least two distinct classes in $\mathcal{W}_S(R)$, namely $[S]$ and $[S^t]$.

Proposition 5.1. *Let T be any over-order of S such that $S^t T$ is invertible as a fractional T -ideal. Let \mathfrak{f} be an ideal contained in S such that $T \subseteq (\mathfrak{f} : \mathfrak{f})$. Then every class in $\mathcal{W}_S(R)$ has a representative I satisfying $\mathfrak{f} \subseteq I \subseteq T$.*

Proof. Let I' be any fractional ideal with $(I' : I') = S$. By Lemma 2.3 we have that $I'(I')^t T = S^t T$ and hence it follows that $I' T$ is an invertible fractional T -ideal. Let J be a representative of the pre-image under the surjective map $\text{Pic}(S) \rightarrow \text{Pic}(T)$ of the class of $(T : I' T)$ and put $I = I' J$. Note that $[I'] = [I]$ in $\mathcal{W}_S(R)$ and that $I T = T$, which implies that $I \subseteq T$.

On the other hand, as $\mathfrak{f} T = \mathfrak{f}$ we get that

$$\mathfrak{f} I = \mathfrak{f} T I = \mathfrak{f} T = \mathfrak{f},$$

and, since $\mathfrak{f} \subseteq (I : I)$, we obtain that $\mathfrak{f} = \mathfrak{f} I \subseteq I$, and we can conclude that $\mathfrak{f} \subseteq I \subseteq T$. \square

The previous proposition tells us that in order to compute the representatives of $\mathcal{W}_S(R)$ we can look at the sub- S -modules of the finite quotient T/\mathfrak{f} . One possible choice is to take $T = \mathcal{O}_K$ and $\mathfrak{f} = (S : \mathcal{O}_K)$, but to gain in efficiency we want to keep the quotient as small as possible. The natural choice is to take as T the smallest over-order of S with $S^t T$ invertible (as a fractional T -ideal) and as \mathfrak{f} , the colon ideal $(S : T)$, which is the biggest fractional T -ideal in S .

Remark 5.2. *Given orders $S \subseteq T$, let $\mathfrak{f} = (S : T)$. If S is Gorenstein then by Lemma 2.1 and Proposition 2.11 it follows that*

$$(\mathfrak{f} : \mathfrak{f}) = (S : T(S : T)) = (S : (S : T)) = T.$$

If S is not Gorenstein then the multiplier ring of \mathfrak{f} might still be equal to T . This for example must be the case when $T = \mathcal{O}_K$. The multiplier ring of \mathfrak{f} can also be strictly bigger than T , as Example 5.3 shows. If

we assume that $S^t T$ is invertible in T , as required in Proposition 5.1, then $(\mathfrak{f} : \mathfrak{f}) = T$, because $\mathfrak{f} = (S^t T)^t$ and a fractional ideal has the same multiplier ring as its trace dual.

Example 5.3. Let $f = x^6 - 4x^5 + 11x^4 - 24x^3 + 55x^2 - 100x + 125$. Observe that $f = f_1 f_2 f_3$ where $f_1 = x^2 - 4x + 5$, $f_2 = x^2 - 2x + 5$ and $f_3 = x^2 + 2x + 5$. Put $K = \mathbb{Q}[x]/(f)$ and $K_i = \mathbb{Q}[x]/(f_i)$ for $i = 1, 2, 3$. We identify $K = K_1 \times K_2 \times K_3$ and, for $i = 1, 2, 3$, we denote by e_i and α_i the elements $1 \bmod f_i$ and $x \bmod f_i$, respectively. Consider the orders

$$S = e_1 \mathbb{Z} \oplus \alpha_1 \mathbb{Z} \oplus 2e_2 \mathbb{Z} \oplus \left(\frac{1}{2}e_2 + \frac{1}{2}\alpha_2 \right) \mathbb{Z} \oplus (e_2 + e_3) \mathbb{Z} \oplus (e_2 + \alpha_3) \mathbb{Z}$$

and

$$T = e_1 \mathbb{Z} \oplus \alpha_1 \mathbb{Z} \oplus e_2 \mathbb{Z} \oplus \left(\frac{1}{2}e_2 + \frac{1}{2}\alpha_2 \right) \mathbb{Z} \oplus e_3 \mathbb{Z} \oplus \alpha_3 \mathbb{Z}.$$

Then $S \subseteq T$ with index 2 and the multiplier ring of $\mathfrak{f} = (S : T)$ is the maximal order

$$\mathcal{O}_K = e_1 \mathbb{Z} \oplus \alpha_1 \mathbb{Z} \oplus e_2 \mathbb{Z} \oplus \left(\frac{1}{2}e_2 + \frac{1}{2}\alpha_2 \right) \mathbb{Z} \oplus e_3 \mathbb{Z} \oplus \left(\frac{1}{2}e_3 + \frac{1}{2}\alpha_3 \right) \mathbb{Z}$$

and it is easy to check that $[\mathcal{O}_K : T] = 2$.

Remark 5.4. Let I' be a fractional R -ideal. As in the proof of Proposition 5.1, let J be a representative of the pre-image under the extension map $\text{Pic}(R) \rightarrow \text{Pic}(\mathcal{O}_K)$ of $\{(\mathcal{O}_K : I' \mathcal{O}_K)\}$ and put $I = I' J$. Then $[I] = [I']$ and $I \mathcal{O}_K = \mathcal{O}_K$ which implies

$$\mathfrak{f} \subseteq I \subseteq \mathcal{O}_K,$$

where \mathfrak{f} is the conductor of R , that is, $\mathfrak{f} = (R : \mathcal{O}_K)$. So if the quotient $\mathcal{O}_K/\mathfrak{f}$ is not too big we can look directly at its sub- R -modules in order to get all representatives of the classes of $\mathcal{W}(R)$. One can also obtain all the over-orders of R by computing the multiplier rings of the representatives of $\mathcal{W}(R)$.

Let T be an over-order of S such that $S^t T$ is an invertible fractional T -ideal. Choose primes $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ of S and positive integers e_1, \dots, e_r such that $T \subseteq (\mathfrak{f} : \mathfrak{f})$, where

$$\mathfrak{f} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

Note that such \mathfrak{f} satisfies the hypothesis of Proposition 5.1 and, moreover, $\mathfrak{f} \subset (S : T)$, since $(S : T)$ contains all fractional T -ideals contained in S . It follows that the primes \mathfrak{p}_i must be non-invertible.

By the Chinese Remainder Theorem there is a ring isomorphism

$$\frac{S}{\mathfrak{f}} \simeq \frac{S}{\mathfrak{p}_1^{e_1}} \times \cdots \times \frac{S}{\mathfrak{p}_r^{e_r}},$$

which, after taking the tensor product with T , becomes

$$(3) \quad \frac{T}{\mathfrak{f}} \simeq \frac{T}{\mathfrak{p}_1^{e_1} T} \times \cdots \times \frac{T}{\mathfrak{p}_r^{e_r} T}.$$

Observe that the isomorphism (3) is compatible with ideal multiplication and hence it respects weak equivalences. In particular, we can compute $\mathcal{W}_{S_{\mathfrak{p}_i}}(S_{\mathfrak{p}_i})$ by looking at the sub- S -modules of the ‘‘local’’ quotient $T/\mathfrak{p}_i^{e_i} T$ up to weak equivalence. Then we can ‘‘patch’’ them together via the isomorphism (3) and hence reconstruct all the representatives of $\mathcal{W}_S(R)$. If $r > 1$ this tells us that we can split the computation of $\mathcal{W}_S(R)$ and hence potentially obtain a more efficient algorithm. The next two remarks will tell us that we can further improve the algorithm by ignoring or reducing some factors in (3) if the corresponding primes \mathfrak{p}_i satisfy certain conditions.

Remark 5.5. Let \mathfrak{p}_i be one the primes appearing in (3). If the S/\mathfrak{p}_i -vector space $S^t/\mathfrak{p}_i S^t$ is one-dimensional, then by Nakayama’s lemma we have that S^t is locally principal at \mathfrak{p}_i . It follows that each fractional ideal I with multiplier ring S , that is, $II^t = S^t$, will be locally invertible at \mathfrak{p}_i , or, in other words, $\mathcal{W}_{S_{\mathfrak{p}_i}}(S_{\mathfrak{p}_i})$ is trivial.

Remark 5.6. Let \mathfrak{p} be one of the primes appearing in the decomposition (3). Observe that $T_{\mathfrak{p}}$ has only finitely many primes $\mathfrak{P}_1, \dots, \mathfrak{P}_m$, which are exactly the ones lying above \mathfrak{p} . Assume that $m < q$, where $q = \#(S/\mathfrak{p})$. Then by [DCD00, Lemma 4] for each ideal I of $S_{\mathfrak{p}}$ such that $IT_{\mathfrak{p}}$ is invertible there exists $x \in I$ such that $IT_{\mathfrak{p}} = xT_{\mathfrak{p}}$. This implies that

$$S_{\mathfrak{p}} \subseteq \frac{1}{x}I \subseteq \frac{1}{x}IT_{\mathfrak{p}} = T_{\mathfrak{p}}.$$

This means that, if we also assume that S^tT is invertible in T , we can find all the classes of $\mathcal{W}_{S_{\mathfrak{p}}}(S_{\mathfrak{p}})$ in the quotient $T_{\mathfrak{p}}/S_{\mathfrak{p}}$ and this quotient might be smaller than $T/\mathfrak{p}_i^{e_i}T$.

6. ALGORITHMS

In this section we present the pseudo-code for the algorithms described in the previous sections. The implementation in Magma [BCP97] is available at <https://github.com/stmar89/AbVarFq>. We will use without mentioning well known algorithms for abelian groups, which can all be found in [Coh93, Section 2.4].

Algorithm 1: Computing over-orders of a given order

Input: An order R in a \mathbb{Q} -étale algebra K ;
Output: A list \mathcal{L}^o containing the over-orders of R ;
 Compute the maximal order \mathcal{O}_K of K ;
 Compute the quotient as abelian groups $q : \mathcal{O}_K \twoheadrightarrow Q := \mathcal{O}_K/R$;
 Initialize an empty list \mathcal{L}^o ;
for each $H' \trianglelefteq Q$ **do**
 | Put $S := \langle q^{-1}(H') \rangle_R$;
 | **if** $SS = S$ **and** $S \notin \mathcal{L}^o$ **then**
 | | Append S to \mathcal{L}^o ;
 | **end**
end
return \mathcal{L}^o ;

Theorem 6.1. *Algorithm 1 is correct.*

Proof. This follows from the fact that the over-orders of R are precisely the idempotent fractional R -ideals contained in \mathcal{O}_K and containing R , as shown in Lemma 2.2. \square

A new and much more efficient version of Algorithm 1 is described in [HS19].

Algorithm 2: Returns whether two fractional R -ideals I and J are weakly equivalent

Input: Two fractional R -ideals I and J ;
Output: Whether I and J are weakly equivalent;
if $1 \in (I : J)(J : I)$ **then**
 | **return** *true*;
else
 | **return** *false*;
end

Theorem 6.2. *Algorithm 2 is correct.*

Proof. It follows by Proposition 4.1. \square

Algorithm 3: Computing representatives of the classes in $\mathcal{W}_S(R)$ for an order S

Input: An order S in a \mathbb{Q} -étale algebra K ;

Output: A list \mathcal{L}^w of the representatives of the weak equivalence classes of ideals with endomorphism ring S , that is $\mathcal{W}_S(R)$;

Compute the trace dual ideal S^t ;

Initialize an empty list \mathcal{L}^w ;

if $1 \in S^t(S : S^t)$ **then**

 Append S to \mathcal{L}^w ;

else

 Find an over-order T of S such that $1 \in S^tT(T : S^tT)$; // use Algorithm 1

 Put $f := (S : T)$;

 Consider the quotient $q := T \rightarrow Q := T/f$;

for each $H' \trianglelefteq Q$ **do**

 Put $I := \langle q^{-1}(H') \rangle_S$;

if there is no $J \in \mathcal{L}^w$ weakly eq. to I **then** // use Algorithm 2

 Append I to \mathcal{L}^w ;

end

end

end

return \mathcal{L}^w ;

Theorem 6.3. *Algorithm 3 is correct.*

Proof. The correctness of the algorithm follows from Propositions 4.1 and 5.1. □

Algorithm 4: Computing representatives of the classes in $\text{ICM}(R)$ for an order R

Input: An order R in a \mathbb{Q} -étale algebra K ;

Output: A list \mathcal{L}^{iso} of the representatives of the isomorphism classes of ideals, that is $\text{ICM}(R)$;

Compute the over-orders \mathcal{L}^o of R ; // use Algorithm 1

Initialize the empty list \mathcal{L}^{iso} ;

for each S in \mathcal{L}^o **do**

 Compute a list \mathcal{L}_S^w of representatives of $\mathcal{W}_S(R)$; // use Algorithm 3

 Compute a list \mathcal{L}_S^i of representatives of $\text{Pic}(S)$;

for each I in \mathcal{L}_S^w and each J in \mathcal{L}_S^i **do**

 Append IJ to \mathcal{L}^{iso} ;

end

end

return \mathcal{L}^{iso} ;

Theorem 6.4. *Algorithm 4 is correct.*

Proof. This follows from Theorem 4.6. □

Algorithm 5: Returns whether two fractional R -ideals I and J are isomorphic and if so it returns an element $\alpha \in K$ such that $\alpha I = J$

Input: Two fractional R -ideals I and J ;
Output: Whether I and J are isomorphic and if so it returns an element $\alpha \in K$ such that $\alpha I = J$;
if I and J are weakly equivalent **then** // use Algorithm 2
 Compute $C = (J : I)$;
 Compute $S = (I : I)$;
 if C is a principal S -ideal **then**
 Compute α such that $\alpha S = C$;
 return (*true*, α);
 end
end
return *false*;

Theorem 6.5. *Algorithm 5 is correct.*

Proof. This follows from Corollary 4.5. □

Algorithm 6: Returns the representative of the isomorphism class of a given fractional R -ideal

Input: a list \mathcal{L}^{iso} of representatives of $ICM(R)$ and a fractional R -ideal I ;
Output: a pair (I_0, α) , consisting of a fractional R -ideal I_0 from the list \mathcal{L}^{iso} and an element $\alpha \in K^\times$ such that $\alpha I = I_0$;
Put $\mathcal{L}_I = \{J \in \mathcal{L}^{iso} : J \text{ is weakly eq. to } I\}$; // use Algorithm 2
Scan \mathcal{L}_I for I_0 such that $\alpha I = I_0$, for some $\alpha \in K^\times$; // use Algorithm 5
return (I_0, α) ;

Theorem 6.6. *Algorithm 6 is correct.*

Proof. The algorithm terminates because \mathcal{L}_I contains by construction a fractional R -ideal isomorphic to I . □

Remark 6.7. *If the list \mathcal{L}^{iso} is computed using Algorithm 4 and in the process one stores the lists \mathcal{L}_S^w and \mathcal{L}_S^i then Algorithm 6 could be modified as follows. Firstly, one computes the multiplier ring S of I , then one finds a representative I_w of the weak equivalence of I in \mathcal{L}_S^w using Algorithm 2 and then one finds a representative I_i of the class of $(I : I_w)$ in \mathcal{L}_S^i either by solving the corresponding DLP in $\text{Pic}(S)$ or by using Algorithm 5. Finally the representative I_0 of the class of I in \mathcal{L}^{iso} is given by $I_w I_i$.*

Remark 6.8. *Given I and J in \mathcal{L}^{iso} one can use Algorithm 6 (or the variation in Remark 6.7) to compute the representative in \mathcal{L}^{iso} of the product IJ . This means that we can build a multiplication table of the commutative monoid $ICM(R)$.*

Remark 6.9. *Algorithm 1 requires the enumeration of the subgroups of the finite quotient \mathcal{O}_K/R which is a very costly computation. Since the number of subgroups that give rise to over-orders of R is much smaller than the total number, there is a big room for improvement. A new and efficient solution is provided in [HS19]. Similar considerations are valid also for the computations of the weak equivalence classes in Algorithm 3. In particular these two algorithms constitute the major bottlenecks of the computation of $ICM(R)$ in Algorithm 4. Algorithm 2 is efficient because it involves only the computations of ideal quotients, product of fractional ideals and testing inclusion. The most expensive operation in Algorithms 5 and 6 is testing whether a fractional ideal is principal and producing a generator.*

7. EXAMPLES

The examples contained in this section were computed with Magma [BCP97]. The implementation of the algorithms from Section 6 can be found at <https://github.com/stmar89/AbVarFq>.

Example 7.1. Let $f = x^3 + 31x^2 + 43x + 77$ and let α be a root of f . Consider the monogenic order defined by f , say $E = S_1 = \mathbb{Z}[\alpha]$. There are 15 over-orders of E . The maximal order is $\mathcal{O} = S_{15} = \mathbb{Z} \oplus \frac{\alpha+5}{8}\mathbb{Z} \oplus \frac{\alpha^2+2\alpha+49}{64}\mathbb{Z}$. Observe that $[\mathcal{O} : E] = 512$, so the only singular prime is 2. In Figure 1 and Table 1 we describe the over-orders with the weak equivalence classes and Picard groups.

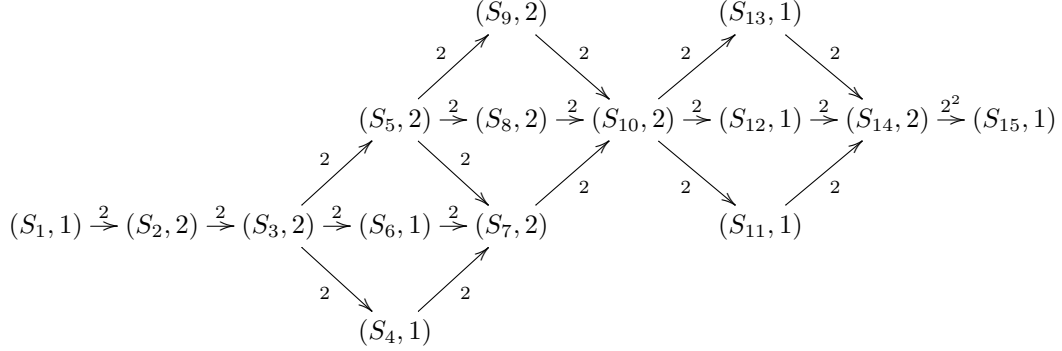


Figure 1. This is the lattice of inclusions of the over-orders of S_1 from Example 7.1. Each vertex is labeled as $(S_i, \#\mathcal{W}_{S_i}(S_1))$. The edges are marked by the index of the corresponding inclusion.

i	\mathbb{Z} -basis of S_i	$[\mathcal{O} : S_i]$	$\text{Pic}(S_i)$
1	$1, \alpha, \alpha^2$	512	$\mathbb{Z}/4\mathbb{Z}$
2	$1, \alpha, \frac{\alpha^2+1}{2}$	256	$\mathbb{Z}/4\mathbb{Z}$
3	$1, \alpha, \frac{\alpha^2+2\alpha+1}{4}$	128	$\mathbb{Z}/4\mathbb{Z}$
4	$1, \alpha, \frac{\alpha^2+6\alpha+5}{8}$	64	$\mathbb{Z}/2\mathbb{Z}$
5	$1, \alpha, \frac{\alpha^2+2\alpha+1}{8}$	64	$\mathbb{Z}/4\mathbb{Z}$
6	$1, \frac{\alpha+1}{2}, \frac{\alpha^2+3}{4}$	64	$\mathbb{Z}/2\mathbb{Z}$
7	$1, \frac{\alpha+1}{2}, \frac{\alpha^2+2\alpha+1}{8}$	32	$\mathbb{Z}/2\mathbb{Z}$
8	$1, \alpha, \frac{\alpha^2+10\alpha+9}{16}$	32	$\mathbb{Z}/2\mathbb{Z}$
9	$1, \alpha, \frac{\alpha^2+2\alpha+1}{16}$	32	$\mathbb{Z}/4\mathbb{Z}$
10	$1, \frac{\alpha+1}{2}, \frac{\alpha^2+2\alpha+1}{16}$	16	$\mathbb{Z}/2\mathbb{Z}$
11	$1, \frac{\alpha+1}{2}, \frac{\alpha^2+2\alpha+17}{32}$	8	1
12	$1, \frac{\alpha+1}{2}, \frac{\alpha^2+10\alpha+25}{32}$	8	1
13	$1, \frac{\alpha+1}{4}, \frac{\alpha^2+2\alpha+1}{16}$	8	$\mathbb{Z}/2\mathbb{Z}$
14	$1, \frac{\alpha+1}{4}, \frac{\alpha^2+2\alpha+17}{32}$	4	1
15	$1, \frac{\alpha+5}{8}, \frac{\alpha^2+2\alpha+49}{64}$	1	1

Table 1. The over-orders of S_1 from Example 7.1

Among the over-orders of E , the orders $S_2, S_3, S_5, S_7, S_8, S_9, S_{10}, S_{14}$ are non-Gorenstein and there are no other non-invertible weak equivalence classes apart from S_i^t . This implies that $\#\mathcal{W}(E) = 23$ and, using the information about the Picard groups, we can deduce that $\#\text{ICM}(E) = 59$.

Example 7.2. Let $f = x^3 - 1000x^2 - 1000x - 1000$ and let α be a root of f . Consider the monogenic order defined by f , say $E = S_1 = \mathbb{Z}[\alpha]$. There are 16 over-orders of E . The maximal order is $\mathcal{O} = S_{16} = \mathbb{Z} \oplus \frac{\alpha}{10}\mathbb{Z} \oplus \frac{\alpha^2}{100}\mathbb{Z}$. Observe that $[\mathcal{O} : E] = 1000$, so the singular primes are 2 and 5. In Figure 2 and Table 2 we describe the over-orders with the weak equivalence classes and Picard groups.

Among the over-orders of E , the orders $S_2, S_4, S_6, S_7, S_9, S_{10}, S_{14}$ are non-Gorenstein, so we also have the weak equivalence classes corresponding to S_i^t , for $i = 2, 4, 6, 7, 9, 10, 14$. But unlike the previous example, there are two other weak equivalence classes, represented by the ideals $I = 50\mathbb{Z} \oplus 10\alpha\mathbb{Z} \oplus 5\alpha^2\mathbb{Z}$ and $J = 20\mathbb{Z} \oplus 10\alpha\mathbb{Z} \oplus 2\alpha^2\mathbb{Z}$, both with multiplier ring S_6 . This means that $\#\mathcal{W}(E) = 25$ and using the information about the Picard groups of the over-orders we can deduce that $\#\text{ICM}(E) = 69116$.

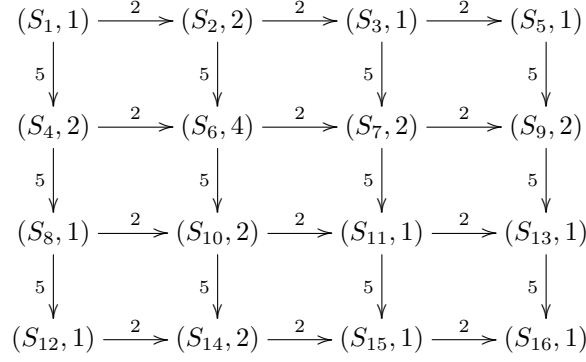


Figure 2. This is the lattice of inclusions of the over-orders of S_1 from Example 7.2. Each vertex is labeled as $(S_i, \# \mathcal{W}_{S_i}(S_1))$. The edges are marked by the index of the corresponding inclusion.

i	\mathbb{Z} -basis of S_i	$[\mathcal{O} : S_i]$	$\text{Pic}(S_i)$
1	$1, \alpha, \alpha^2$	1000	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8880\mathbb{Z}$
2	$1, \alpha, \frac{\alpha^2}{2}$	500	$\mathbb{Z}/8880\mathbb{Z}$
3	$1, \alpha, \frac{\alpha^2+2\alpha}{4}$	250	$\mathbb{Z}/8880\mathbb{Z}$
4	$1, \alpha, \frac{\alpha^2}{5}$	200	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/1776\mathbb{Z}$
5	$1, \frac{\alpha}{2}, \frac{\alpha^2}{4}$	125	$\mathbb{Z}/2960\mathbb{Z}$
6	$1, \alpha, \frac{\alpha^2}{10}$	100	$\mathbb{Z}/1776\mathbb{Z}$
7	$1, \alpha, \frac{\alpha^2+10\alpha}{20}$	50	$\mathbb{Z}/1776\mathbb{Z}$
8	$1, \alpha, \frac{\alpha^2+10\alpha}{25}$	40	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/444\mathbb{Z}$
9	$1, \frac{\alpha}{2}, \frac{\alpha^2}{20}$	25	$\mathbb{Z}/592\mathbb{Z}$
10	$1, \alpha, \frac{\alpha^2+10\alpha}{50}$	20	$\mathbb{Z}/444\mathbb{Z}$
11	$1, \alpha, \frac{\alpha^2+10\alpha}{100}$	10	$\mathbb{Z}/444\mathbb{Z}$
12	$1, \frac{\alpha}{5}, \frac{\alpha^2}{25}$	8	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/74\mathbb{Z}$
13	$1, \frac{\alpha}{2}, \frac{\alpha^2+10\alpha}{100}$	5	$\mathbb{Z}/148\mathbb{Z}$
14	$1, \frac{\alpha}{5}, \frac{\alpha^2}{50}$	4	$\mathbb{Z}/74\mathbb{Z}$
15	$1, \frac{\alpha}{5}, \frac{\alpha^2+10\alpha}{100}$	2	$\mathbb{Z}/74\mathbb{Z}$
16	$1, \frac{\alpha}{10}, \frac{\alpha^2}{100}$	1	$\mathbb{Z}/74\mathbb{Z}$

Table 2. The over-orders of S_1 from Example 7.2

Example 7.3. Consider the irreducible polynomials $f_1 = x^2 + 4x + 7$ and $f_2 = x^3 - 9x^2 - 3x - 1$ and define $f = f_1 f_2$. Put $K_1 = \mathbb{Q}[x]/(f_1)$, $K_2 = \mathbb{Q}[x]/(f_2)$ and $K = \mathbb{Q}[x]/(f) \simeq K_1 \times K_2$. For $i = 1, 2$ denote by R_i the monogenic order $\mathbb{Z}[x]/(f_i)$ and by \mathcal{O}_i the maximal order of K_i . Similarly, let R be the monogenic order $\mathbb{Z}[x]/(f)$ and \mathcal{O} the maximal order of K . It is easy to verify that $[\mathcal{O}_i : R_i] = 2$ for both $i = 1$ and $i = 2$. Therefore, for both $i = 1$ and $i = 2$, the only over-order of R_i is \mathcal{O}_i and hence R_i is a Bass order. In particular, it follows that

$$\text{ICM}(R_i) = \text{Pic}(R_i) \sqcup \text{Pic}(\mathcal{O}_i).$$

We can check that $\text{Pic}(R_1)$ is trivial and hence \mathcal{O}_1 is a principal ideal domain, since the extension map $I \mapsto I\mathcal{O}_1$ induces a surjective group homomorphism from $\text{Pic}(R_1)$ to $\text{Pic}(\mathcal{O}_1)$, see Remark 3.8. We deduce that

$$\text{ICM}(R_1) = \{\{R_1\}, \{\mathcal{O}_1\}\}.$$

On the other hand, $\text{Pic}(R_2)$ and $\text{Pic}(\mathcal{O}_2)$ are both isomorphic to $\mathbb{Z}/3\mathbb{Z}$ and generated respectively by $I = (69R_2 + (28 + \alpha_2 + \alpha_2^2)R_2)$ and $J = I\mathcal{O}_2$, where $\alpha_2 = x \bmod f_2$. It follows that

$$\text{ICM}(R_2) = \{\{R_2\}, \{I\}, \{I^2\}, \{\mathcal{O}_2\}, \{J\}, \{J^2\}\}.$$

The situation for R is much more complicated, as Figure 3 shows.

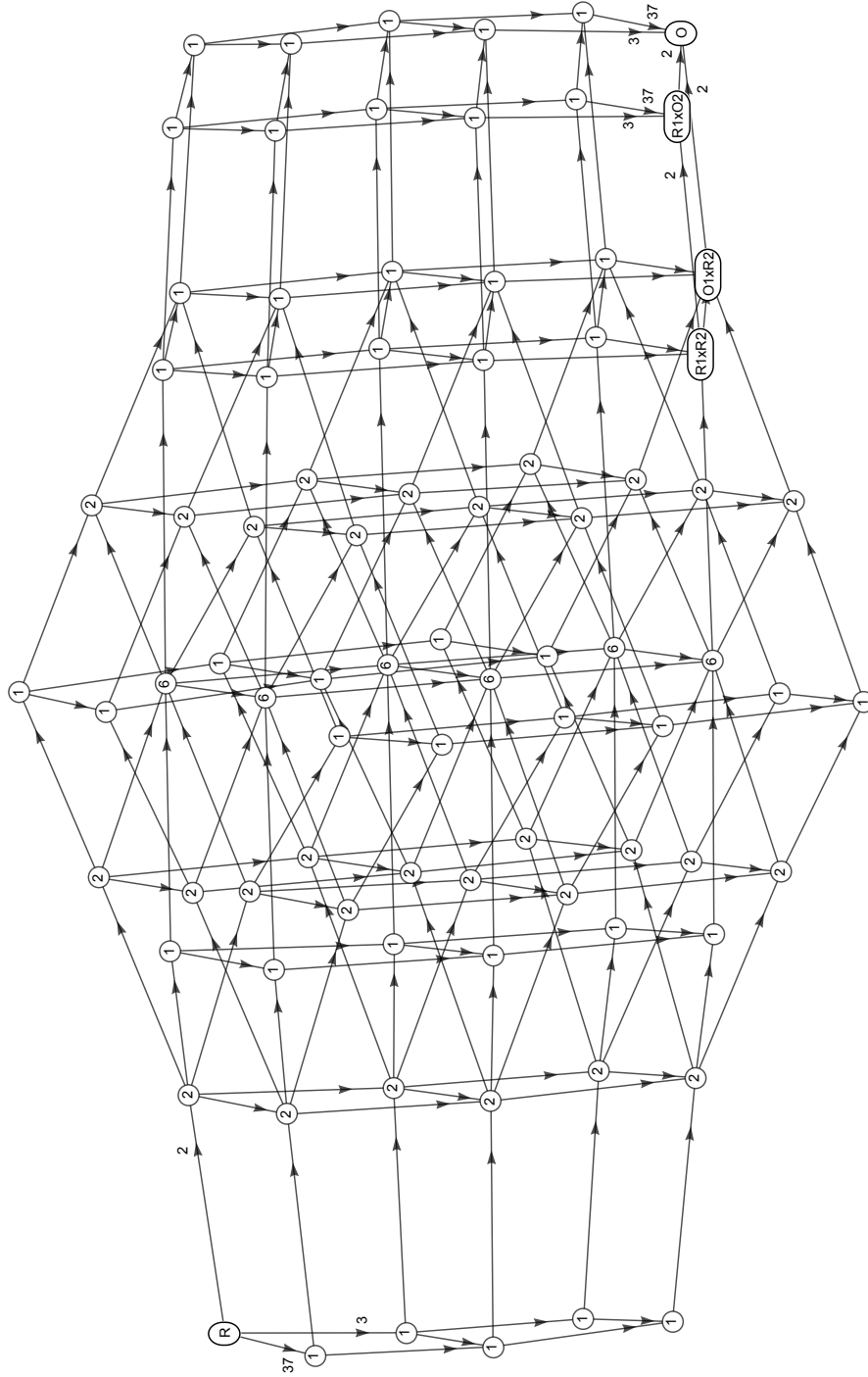


Figure 3. The lattice of inclusions of the over-orders in Example 7.3. The vertex corresponding to an order S is labelled by the size of $\mathcal{W}_S(R)$ except for the orders R , $R_1 \times R_2$, $\mathcal{O}_1 \times R_2$, $R_1 \times \mathcal{O}_2$ and \mathcal{O} (which are all Gorenstein). The horizontal (resp. vertical, diagonal) edges correspond to inclusions of index 2 (resp 3, 37). We have labeled some of them at top-left and bottom-right corners for clarity.

First of all, R is not a product of orders of K_1 and K_2 and it can be computed that the index of R in the maximal order $\mathcal{O} \simeq \mathcal{O}_1 \times \mathcal{O}_2$ is $21312 = 2^6 3^2 37$. We computed that R has 84 over-orders of which only 48 are Gorenstein and hence R is not Bass. We ran our algorithm for the ideal class monoid and we found that $\#\text{ICM}(R) = 852$.

8. CONJUGACY CLASSES OF INTEGRAL MATRICES

Recall that two $N \times N$ matrices A and B with entries in \mathbb{Z} are *conjugate* if there exists $O \in \text{GL}_N(\mathbb{Z})$ such that $OAO^{-1} = B$. If this is the case, then A and B have the same minimal polynomial m and the same characteristic polynomial c . The converse is not true in general. We will write $[A]_{\sim_{\mathbb{Z}}}$ for the conjugacy class of the matrix A . In what follows we will describe how to compute representatives of the conjugacy classes when the minimal polynomial is square-free. Our result is a generalization of [LM33], where the authors treat the case $m = c$, which was then re-proved with a different method in [Tau49], with the extra assumption that $m = c$ is irreducible. Note that Theorem 8.1 has independently been proved in [Hus16, Theorem 1.4] in greater generality.

Let f_1, \dots, f_r be a collection of distinct irreducible monic polynomials with integer coefficients and let e_1, \dots, e_r be positive integers such that $m = \prod f_i$, $c = \prod f_i^{e_i}$. Put $N = \deg(c)$ and denote by $\mathcal{M}_{m,c}(\mathbb{Z})$ the set of integral $N \times N$ matrices with minimal and characteristic polynomials m and c , respectively.

For every $i = 1, \dots, r$ put $K_i = \mathbb{Q}[x]/(f_i)$ and let Δ_i be the diagonal embedding of K_i into $K_i^{e_i}$. Define Δ as the product map $\prod_i \Delta_i$ with codomain $K = \prod_i K_i^{e_i}$. Observe that the order $R_0 = \mathbb{Z}[x]/(m)$ has total quotient ring the \mathbb{Q} -algebra $\prod_i K_i$. Denote with R the image of R_0 in K via Δ and put $\alpha = \Delta(x \bmod (m))$. Let $\mathcal{L}(R, K)$ be the set of full lattices in K which are R -modules and pick I in $\mathcal{L}(R, K)$. Fix a \mathbb{Z} -basis $\bar{w} = \{w_1, \dots, w_n\}$ of I . The R -linear endomorphism of I given by multiplication by α can be represented with respect to \bar{w} by an integral matrix $A = A(I, \bar{w})$ which lies in $\mathcal{M}_{m,c}(\mathbb{Z})$. Clearly this representation depends on the choice of the \mathbb{Z} -basis of I . If we change the \mathbb{Z} -basis of I by a matrix $O \in \text{GL}_N(\mathbb{Z})$ then the multiplication by α will be represented by $O^{-1}AO$. Hence we have a well defined map $I \rightarrow [A]_{\sim_{\mathbb{Z}}}$.

Theorem 8.1. *The association $\Phi : I \mapsto [A(I, \bar{w})]_{\sim_{\mathbb{Z}}}$ induces a bijection*

$$\begin{aligned} \tilde{\Phi} : \mathcal{L}(R, K) / \simeq_R &\longrightarrow \mathcal{M}_{m,c}(\mathbb{Z}) / \sim_{\mathbb{Z}}, \\ \{I\} &\longmapsto [A(I, \bar{w})]_{\sim_{\mathbb{Z}}} \end{aligned}$$

where \simeq_R denotes isomorphisms of R -modules.

Proof. First we prove that the map $\tilde{\Phi}$ is well defined, that is that if $\varphi : I \rightarrow J$ is an R -linear isomorphism then $\Phi(I) = \Phi(J)$. Let \bar{w} be a \mathbb{Z} -basis of I and $\varphi(\bar{w})$ the induced \mathbb{Z} -basis of J . Since φ is R -linear, we have that $A(I, \bar{w}) = A(J, \varphi(\bar{w}))$, which implies that $\Phi(I) = \Phi(J)$.

We now prove that $\tilde{\Phi}$ is injective. Let I and J be in $\mathcal{L}(R, K)$ and fix a \mathbb{Z} -basis, say

$$I = w_1\mathbb{Z} \oplus \dots \oplus w_N\mathbb{Z}$$

and

$$J = v_1\mathbb{Z} \oplus \dots \oplus v_N\mathbb{Z}.$$

Assume that $\Phi(I) = \Phi(J)$, that is $A(I, \bar{w}) = O^{-1}A(J, \bar{v})O$ for some $O \in \text{GL}_N(\mathbb{Z})$. By acting with O^{-1} on \bar{v} we find a new \mathbb{Z} -basis \bar{v}' for J such that $A(I, \bar{w}) = A(J, \bar{v}')$. Now the \mathbb{Z} -linear bijection $I \rightarrow J$ defined by $w_i \mapsto v'_i$ commutes with multiplication by α , since the matrices representing the operation with respect to \bar{w} and \bar{v}' are the same, and hence it is an R -linear isomorphism. Therefore $\{I\} = \{J\}$ and $\tilde{\Phi}$ is injective.

To conclude we need to prove that $\tilde{\Phi}$ is also surjective. We will do this by explicitly producing a map

$$\Psi : \mathcal{M}_{m,c}(\mathbb{Z}) \rightarrow \mathcal{L}(R, K) / \simeq_R$$

which descends to a section $\tilde{\Psi}$ of $\tilde{\Phi}$. Let A be a matrix in $\mathcal{M}_{m,c}(\mathbb{Z})$. Note that since m is square-free, A is semisimple. Denote the element $(x \bmod f_i)$ of K_i by α_i . Note that

$$\alpha = \underbrace{(\alpha_1, \dots, \alpha_1)}_{e_1 \text{ times}}, \dots, \underbrace{(\alpha_r, \dots, \alpha_r)}_{e_r \text{ times}}.$$

Let

$$(4) \quad v_{i,1}, \dots, v_{i,e_i} \in K_i^N$$

be a basis of the eigenspace corresponding to α_i , that is, linearly independent vectors such that

$$Av_{i,j_i} = \alpha_i v_{i,j_i}$$

for each $i = 1, \dots, r$ and $j_i = 1, \dots, e_i$. Let $E = e_1 + \dots + e_r$ and consider the $E \times N$ matrix whose rows are the vectors v_{i,j_i} and denote by w_k the k -th column, for $k = 1, \dots, N$. Observe that each w_k is an element of K and define

$$I = \langle w_1, \dots, w_N \rangle_{\mathbb{Z}} \subset K.$$

If $A = (a_{h,k})$ and $v_{i,j_i} = (v_{i,j_i}^{(1)}, \dots, v_{i,j_i}^{(N)})$ then

$$w_k = (v_{1,1}^{(k)}, \dots, v_{1,e_1}^{(k)}, \dots, v_{r,1}^{(k)}, \dots, v_{r,e_r}^{(k)})$$

and it follows that

$$(5) \quad \begin{aligned} \alpha w_k &= (\alpha_1 v_{1,1}^{(k)}, \dots, \alpha_1 v_{1,e_1}^{(k)}, \dots, \alpha_r v_{r,1}^{(k)}, \dots, \alpha_r v_{r,e_r}^{(k)}) \\ &= \left(\sum_{h=1}^N a_{k,h} v_{1,1}^{(h)}, \dots, \sum_{h=1}^N a_{k,h} v_{1,e_1}^{(h)}, \dots, \sum_{h=1}^N a_{k,h} v_{r,1}^{(h)}, \dots, \sum_{h=1}^N a_{k,h} v_{r,e_r}^{(h)} \right) \\ &= \sum_{h=1}^N a_{k,h} (v_{1,1}^{(h)}, \dots, v_{1,e_1}^{(h)}, \dots, v_{r,1}^{(h)}, \dots, v_{r,e_r}^{(h)}) \\ &= \sum_{h=1}^N a_{k,h} w_h \in I, \end{aligned}$$

which implies that I is closed under multiplication by α , and hence it is an R -module. Moreover, (5) means that the multiplication by α is represented by the matrix A with respect to the generators w_1, \dots, w_N . We prove now that I is a full lattice, or equivalently that the \mathbb{Q} -vector space $V = I \otimes_{\mathbb{Z}} \mathbb{Q}$ equals K . Note that A represents the \mathbb{Q} -linear map induced by multiplication by α on V . Since A is semisimple there is a decomposition

$$(6) \quad V = W_1 \oplus \dots \oplus W_r$$

into \mathbb{Q} -vector spaces which are stable under the action of α , and possibly after renumbering we can assume that $A|_{W_i}$ has minimal polynomial f_i and hence that W_i is a K_i -vector space. For each i , since the vectors $v_{i,1}, \dots, v_{i,e_i}$ are linearly independent over K_i , we see that W_i must have dimension e_i . This concludes the proof that $I \in \mathcal{L}(R, K)$.

Observe that the construction of I depends on the choice of eigenvectors in (4). A different choice is attained by the action of a block-diagonal matrix C in

$$\begin{pmatrix} \text{GL}_{e_1}(K_1) & 0 & \dots & 0 \\ 0 & \text{GL}_{e_2}(K_2) & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & \text{GL}_{e_r}(K_r) \end{pmatrix}$$

Observe that C induces an R -linear automorphism of K and hence its action on I will also be an R -isomorphic object of $\mathcal{L}(R, K)$. Hence we have a well defined map Ψ which associates $A \mapsto \{I\}$.

If instead of A we take a conjugate matrix B , it will reflect as taking an invertible \mathbb{Z} -linear combination of the eigenvectors in (4). Clearly this will not change the \mathbb{Z} -span that they generate, that is, the lattice I , and hence Ψ descends to a well defined map

$$\tilde{\Psi} : \mathcal{M}_{m,c}(\mathbb{Z}) / \sim_{\mathbb{Z}} \longrightarrow \mathcal{L}(R, K) / \simeq_R$$

which by construction is a section of $\tilde{\Phi}$. This implies that $\tilde{\Phi}$ is surjective and concludes the proof. \square

In general, the set of R -isomorphism classes in $\mathcal{L}(R, K)$ is hard to handle, but under certain assumptions we can reduce it to an ideal class monoid computation.

Corollary 8.2. *Let f be a square-free monic integral polynomial and put $R = \mathbb{Z}[x]/(f)$.*

(a) *There is a bijection*

$$\mathcal{M}_{f,f}(\mathbb{Z})/\sim_{\mathbb{Z}} \longleftrightarrow \text{ICM}(R).$$

(b) *Assume that R is a Bass order. Let N be a positive integer. We have a bijection*

$$\mathcal{M}_{f,f^N}(\mathbb{Z})/\sim_{\mathbb{Z}} \longleftrightarrow \mathcal{C}/\simeq_R,$$

where the objects of \mathcal{C} are R -modules of the form $I_1 \oplus \dots \oplus I_N$, with I_i fractional R -ideals satisfying $(I_i : I_i) \subseteq (I_{i+1} : I_{i+1})$, and two such modules $I_1 \oplus \dots \oplus I_N$ and $I'_1 \oplus \dots \oplus I'_N$ are isomorphic if and only if $(I_i : I_i) = (I'_i : I'_i)$ for every i and $\{I_1 \dots I_N\} = \{I'_1 \dots I'_N\}$ in $\text{ICM}(R)$.

Proof. Part (a) follows from the equality $\text{ICM}(R) = \mathcal{L}(R, R \otimes \mathbb{Q})/\simeq_R$ proved in Theorem 8.1 and part (b) is a direct consequence of the classification given in [LW85, Theorem 7.1]. \square

Observe that Corollary 8.2 provides an algorithm to check whether two matrices, with characteristic polynomial of the appropriate form, are conjugate over \mathbb{Z} . This problem is solved in greater generality by a new algorithm proposed in [EHO19]. In Example 8.4 and Table 3 we compare the running time with our algorithm for matrices with square-free characteristic polynomial.

Example 8.3. *Let $f = f_1 f_2$, K , α and R be defined as in Example 7.3. Put $\alpha_1 = x \bmod f_1$ and $\alpha_2 = x \bmod f_2$ so that $\alpha = (\alpha_1, \alpha_2)$. Furthermore denote by 1_1 and 1_2 the images of the unit elements of K_1 and K_2 respectively under the canonical isomorphism $K \simeq K_1 \times K_2$. Define*

$$\beta_1 = (1_1, 0), \quad \beta_2 = (\alpha_1, 0), \quad \beta_3 = (0, 1_2), \quad \beta_4 = (0, \alpha_2), \quad \beta_5 = (0, \alpha_2^2).$$

Observe that

$$\mathcal{A} = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4\}$$

and

$$\mathcal{B} = \{\beta_1, \beta_2, \beta_3, \beta_4, \beta_5\}$$

are two bases of K over \mathbb{Q} . Consider the ideal I given by

$$\begin{aligned} I = & \frac{1}{444} (-13 - 46\alpha - 138\alpha^2 - 50\alpha^3 + 7\alpha^4) \mathbb{Z} \oplus \frac{1}{222} (-9 - 29\alpha - 87\alpha^2 - 9\alpha^3 + 2\alpha^4) \mathbb{Z} \oplus \\ & \oplus \frac{1}{888} (883 - 12\alpha - 36\alpha^2 + 32\alpha^3 - 3\alpha^4) \mathbb{Z} \oplus \frac{1}{888} (57 + 1084\alpha + 588\alpha^2 + 168\alpha^3 - 25\alpha^4) \mathbb{Z} \oplus \\ & \oplus \frac{1}{444} (190 - 99\alpha - 75\alpha^2 + 5\alpha^3 + 3\alpha^4) \mathbb{Z}, \end{aligned}$$

or equivalently

$$I = -2\beta_1 \mathbb{Z} \oplus (\beta_1 + \beta_2) \mathbb{Z} \oplus \frac{1}{2}(5\beta_1 + \beta_2 + \beta_3) \mathbb{Z} \oplus \frac{1}{2}(5\beta_1 + \beta_2 + \beta_4) \mathbb{Z} \oplus \frac{1}{2}(3\beta_1 + \beta_2 + \beta_3 + \beta_5) \mathbb{Z}.$$

With respect to this \mathbb{Z} -basis of I , the multiplication by α is represented by the following integral matrix

$$A = \begin{pmatrix} -1 & 2 & 3 & 2 & 4 \\ -2 & -3 & 0 & 0 & -4 \\ 0 & 0 & 0 & -1 & -4 \\ 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 2 & 9 \end{pmatrix}.$$

Performing an LLL reduction of the \mathbb{Z} -basis of I , we get

$$\begin{aligned} I = & \frac{1}{2}(\beta_1 - \beta_2 + \beta_3 + \beta_5) \mathbb{Z} \oplus \frac{1}{2}(-\beta_1 - \beta_2 + 2\beta_3) \mathbb{Z} \oplus \frac{1}{2}(-\beta_1 + \beta_2 + \beta_3 + \beta_5) \mathbb{Z} \oplus \\ & \oplus \frac{1}{2}(\beta_1 + \beta_2 + 2\beta_3) \mathbb{Z} \oplus \frac{1}{2}(-\beta_1 - \beta_2 + 2\beta_4) \mathbb{Z} \end{aligned}$$

and with respect to this \mathbb{Z} -basis of I the multiplication by α is represented by

$$A' = \begin{pmatrix} 5 & 1 & 4 & -1 & 2 \\ -6 & -3 & 0 & 2 & -3 \\ 4 & -1 & 5 & 1 & 0 \\ 2 & 3 & -4 & -2 & 2 \\ 2 & 1 & 2 & 1 & 0 \end{pmatrix}.$$

We find that for

$$U = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ -1 & -1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix},$$

we have

$$A' = U^{-1}AU.$$

We now follow the proof of Theorem 8.1 and we construct the ideal associated to the matrix A . The eigenvectors corresponding to the eigenvalues α_1 and α_2 are respectively

$$\left(1_1, \frac{1}{2}(-\alpha_1 - 1_1), \frac{1}{4}(-\alpha_1 - 5 \cdot 1_1), \frac{1}{4}(-\alpha_1 - 5 \cdot 1_1), \frac{1}{4}(-\alpha_1 - 3 \cdot 1_1)\right)$$

and

$$\left(0, 0, 1, \alpha_2, \frac{1}{2}(\alpha_2^2 + 1_2)\right).$$

Hence we obtain

$$\begin{aligned} w_1 &= \beta_1, & w_2 &= -\frac{1}{2}(\beta_1 + \beta_2), & w_3 &= \frac{1}{4}(-5\beta_1 - \beta_2) + \beta_3, \\ w_4 &= \frac{1}{4}(-5\beta_1 - \beta_2) + \beta_4, & w_5 &= \frac{1}{4}(-3\beta_1 - \beta_2) + \frac{1}{2}(\beta_3 + \beta_5) \end{aligned}$$

and we put

$$J = \langle w_1, w_2, w_3, w_4, w_5 \rangle_{\mathbb{Z}}.$$

We find that I and J are isomorphic. More precisely, we have

$$(-2\beta_1 + 28\beta_4 - 3\beta_5)J = I.$$

Example 8.4. We compare the running time of our algorithm and the one in [EHO19] to test conjugacy of integral matrices with square-free characteristic polynomial. Table 3 contains the results of our computation on a Intel Xeon CPU E5-2697 v2 running at 2.70GHz. The entry of the k -th row and d -th column consists of the pair (t_1, t_2) , where t_1 and t_2 are the average running times of our algorithm and the one in [EHO19], respectively, on 100 pairs (M_1, M_2) of $d \times d$ integer matrices built using the following procedure. Pick a monic square-free polynomial $f \in \mathbb{Z}[x]$ with random coefficients with absolute value bounded by k and let C be companion matrix of f . Construct a random matrix R_1 in $\text{GL}_d(\mathbb{Z})$ by multiplying 10 matrices of the form $I_d + E$, where I_d is the identity in $\text{GL}_d(\mathbb{Z})$ and E has exactly one non-zero entry, which is off the diagonal and has absolute value at most k . Set $M_1 = R_1^{-1}CR_1$. Build M_2 in an analogous way. The characteristic polynomial of both M_1 and M_2 is f , so they correspond to fractional ideals of $\mathbb{Z}[x]/f$, see Corollary 8.2.(a).

	$d = 4$	$d = 6$	$d = 8$	$d = 10$
$k = 20$	(0.69, 1.2)	(1.5, 3.0)	(3.2, 9.6)	(7.7, 39.2)
$k = 40$	(0.75, 1.2)	(1.5, 5.2)	(3.6, 16.3)	(15.9, 125.0)
$k = 80$	(0.69, 1.6)	(1.9, 38.8)	(6.9, 80.9)	(74.6, 669.9)
$k = 160$	(0.69, 5.2)	(2.0, 104.9)	(26.2, 294.2)	(-, -)
$k = 320$	(0.75, 33.2)	(2.9, -)	(53.9, -)	(-, -)
$k = 640$	(0.81, 127.7)	(21.8, -)	(238.2, -)	(-, -)

Table 3. Running-time comparison, see Example 8.4.

Remark 8.5. *Corollary 8.2 allows us to produce representatives of the conjugacy classes of integral matrices with given characteristic polynomial (satisfying certain assumptions), solving [EHO19, Problem 7.7] for such characteristic polynomials. Moreover, it gives an answer to the conjugacy problem over the integers, that is to determine whether two integral matrices A and B with square-free characteristic polynomial are conjugate. This was already considered in [Gru80] where the author performs a series of reductions in order to translate the problem into an isomorphism test between fractional ideals of an integral domain. In this process the author has made a mistake, namely, the morphism (3) on page 107 is not a bijection, since the injective map from R to the product of the monogenic orders is not surjective in general, which could lead to a very different output as Example 7.3 shows.*

REFERENCES

- [Bas63] Hyman Bass, *On the ubiquity of Gorenstein rings*, Math. Z. **82** (1963), 8–28. MR 0153708 (27 #3669)
- [BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. MR MR1484478
- [BL94] J. Buchmann and H. W. Lenstra, Jr., *Approximating rings of integers in number fields*, J. Théor. Nombres Bordeaux **6** (1994), no. 2, 221–260. MR 1360644 (96m:11092)
- [Coh93] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR 1228206
- [DCD00] Ilaria Del Corso and Roberto Dvornicich, *Relations among discriminant, different, and conductor of an order*, J. Algebra **224** (2000), no. 1, 77–90. MR 1736694 (2000m:11114)
- [DTZ62] 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. MR 0140544 (25 #3962)
- [EHO19] Bettina Eick, Tommy Hofmann, and Eamonn O’Brien, *The conjugacy problem in $\mathbf{GL}(n, \mathbf{Z})$* , J. Lond. Math. Soc. (2) **00** (2019), 1–26.
- [Gil92] Robert Gilmer, *Multiplicative ideal theory*, Queen’s Papers in Pure and Applied Mathematics, vol. 90, Queen’s University, Kingston, ON, 1992, Corrected reprint of the 1972 edition. MR 1204267
- [Gru80] Fritz J. Grunewald, *Solution of the conjugacy problem in certain arithmetic groups*, Word problems, II (Conf. on Decision Problems in Algebra, Oxford, 1976), Stud. Logic Foundations Math., vol. 95, North-Holland, Amsterdam-New York, 1980, pp. 101–139. MR 579942
- [Hel40] Olaf Helmer, *Divisibility properties of integral functions*, Duke Math. J. **6** (1940), 345–356. MR 0001851
- [HS19] Tommy Hofmann and Carlo Sircana, *On the computation of overorders*, arXiv:1909.10860, 2019.
- [Hus16] David Husert, *Similarity of integer matrices*, University of Paderborn, 2016, PhD Thesis.
- [JP16] Bruce W. Jordan and Bjorn Poonen, *The analytic class number formula for orders in products of number fields*, arXiv:1604.04564v1, 2016.
- [Kap49] Irving Kaplansky, *Elementary divisors and modules*, Trans. Amer. Math. Soc. **66** (1949), 464–491. MR 0031470
- [KP05] Jürgen Klüners and Sebastian Pauli, *Computing residue class rings and Picard groups of orders*, J. Algebra **292** (2005), no. 1, 47–64. MR 2166795 (2006f:11142)
- [LM33] Claiborne G. Latimer and C. C. MacDuffee, *A correspondence between classes of ideals and classes of matrices*, Ann. of Math. (2) **34** (1933), no. 2, 313–316. MR 1503108
- [LW85] Lawrence S. Levy and Roger Wiegand, *Dedekind-like behavior of rings with 2-generated ideals*, J. Pure Appl. Algebra **37** (1985), no. 1, 41–58. MR 794792
- [Mar18a] Stefano Marseglia, *Computing abelian varieties over finite fields*, Stockholm University, 2018.
- [Mar18b] ———, *Computing isomorphism classes of square-free polarized abelian varieties over finite fields*, arXiv:1805.10223, 2018.
- [Rei70] Irving Reiner, *A survey of integral representation theory*, Bull. Amer. Math. Soc. **76** (1970), 159–227. MR 0254092
- [Rei03] ———, *Maximal orders*, London Mathematical Society Monographs. New Series, vol. 28, The Clarendon Press, Oxford University Press, Oxford, 2003. MR 1972204
- [Ste08] Peter Stevenhagen, *The arithmetic of number rings*, Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ., vol. 44, Cambridge Univ. Press, Cambridge, 2008, pp. 209–266. MR 2467548 (2009k:11213)
- [Tau49] Olga Taussky, *On a theorem of Latimer and MacDuffee*, Canadian J. Math. **1** (1949), 300–302. MR 0030491
- [ZZ94] P. Zanardo and U. Zannier, *The class semigroup of orders in number fields*, Math. Proc. Cambridge Philos. Soc. **115** (1994), no. 3, 379–391. MR 1269926 (95d:11159)

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET, SWEDEN

Current address: Mathematical Institute, Utrecht University, The Netherlands

E-mail address: s.marseglia@uu.nl