Conjugacy of Integral Matrices over Algebraic Extensions

Rebecca Afandi

Abstract

We consider conjugacy of integral matrices by elements in $\text{GL}_n(R)$ for certain rings $R$ with subring $\mathbb{Z}$. We note that a Hasse principal does not hold in the context of matrix conjugacy because matrices which are $\text{GL}_n(\mathbb{Z}_p)$-conjugate for all $p$ are not necessarily $\text{GL}_n(\mathbb{Z})$-conjugate. By a theorem of Guralnick, we know that integral $n \times n$ matrices are $\text{GL}_n(\mathbb{Z}_p)$-conjugate for all primes $p$ if and only if they are conjugate by an element in $\text{GL}_n(E)$ for some algebraic integral extension $E$ of $\mathbb{Z}$. We study the problem of finding this extension $E$. Since a result by Latimer and MacDuffee for describing $\mathbb{Z}$-conjugacy can be generalized to the context of $R$-conjugacy for $R$ any integral domain, we can adapt an existing algorithm for $\mathbb{Z}$-conjugacy to a new context. We also offer a method for finding $E$ which makes use of the principal ideal theorems of class field theory. We illustrate our method in several examples.

1 Introduction

For a field $F$, the theory of conjugacy of matrices in $F^{n \times n}$ by elements in the general linear group, $\text{GL}_n(F)$, is classical and well-developed. We enter into an area of ongoing research if we work over a ring rather than a field. For a ring $R$, we say that matrices $A, B \in R^{n \times n}$ are $R$-conjugate or conjugate over $R$ to mean that they are conjugate by an element in the general linear group, $\text{GL}_n(R)$, i.e., there exists $C \in \text{GL}_n(R)$ with $C^{-1}AC = B$. We denote the equivalence relation given by $R$-conjugacy by $\sim_R$. The restriction that the determinant of the conjugating matrix need be a unit in $R$ results in a more nuanced situation in which many open problems emerge.

In this paper, we consider $R$-conjugacy of integral matrices for $R$ a number of rings, including the ring $\mathbb{Z}$, algebraic extensions of $\mathbb{Z}$ (we will denote these by $E$), the ring $\mathbb{Z}_p$ of $p$-adic integers for a prime $p$, and $\mathbb{Z}(p)$, the localization of $\mathbb{Z}$ at a prime $p$. Guralnick [Gur80] showed that $\mathbb{Z}_p$-conjugacy of integral matrices implies conjugacy of those matrices over $\mathbb{Z}(p)$ (we provide some details of Guralnick’s argument in Remark 2.2). Since $\mathbb{Z}_p$-conjugacy and $\mathbb{Z}(p)$-conjugacy are equivalent, we will more often refer to $\mathbb{Z}_p$-conjugacy for ease of notation. Unless specified otherwise, we use $R$ to denote any of the aforementioned rings.

Much progress has been made in understanding $\mathbb{Z}$-conjugacy. Grunewald [Gru80, Thm. A] proved that there exists an algorithm for determining whether integral matrices are $\mathbb{Z}$-conjugate. Grunewald’s idea for an algorithm relies on isomorphism-testing of certain modules, however, he did not offer practical means of constructing all the necessary submodules. Eick, Hofmann, and O’Brien [EHO19] successfully applied Grunewald’s ideas and implemented an algorithm for $\mathbb{Z}$-conjugacy.

If we restrict ourselves to integral matrices with a square-free characteristic polynomial, there is an interesting theoretical result which relates the theory of $\mathbb{Z}$-conjugacy to equivalence of certain number theoretic objects. We will mainly be concerned with this case, so we set the following notation.

For square-free $f \in \mathbb{Z}[x]$ of degree $n$, we let $\mathcal{M}_f$ denote the set defined by

$$\mathcal{M}_f = \{ A \in \mathbb{Z}^{n \times n} : \det(xI - A) = f \}.$$
Note that every matrix in \( \mathcal{M}_f \) has the same rational canonical form, the companion matrix of \( f \). Thus, the set \( \mathcal{M}_f \) gives a single \( \mathbb{Q} \)-conjugacy class which we may partition further into \( \mathbb{Z} \)-conjugacy classes.

Supposing that \( f = \prod_{i=1}^{r} f_i \) is square-free and each \( f_i \) is an irreducible factor with root \( \alpha_i \), one of the landmark results of the theory of \( \mathbb{Z} \)-conjugacy is the LM correspondence \( \text{[LM33]} \), which states that \( \mathbb{Z} \)-conjugacy classes of matrices within \( \mathcal{M}_f \) correspond to certain fractional ideal classes in \( K := \prod_{i=1}^{r} \mathbb{Q}(\alpha_i) \). Taussky \( \text{[Tau49]} \) and Marseglia \( \text{[Mar20]} \) made the theoretical LM correspondence more concrete by providing bijections in the case that \( f \) is irreducible and square-free, respectively. Marseglia used this bijection to implement an algorithm in Magma \( \text{[BCP97]} \) which gives the \( \mathbb{Z} \)-conjugacy classes of matrices within \( \mathcal{M}_f \) for \( f \) square-free.

A class of integral matrices which is of particular relevance in this paper are those which are \( \mathbb{Z}_p \)-conjugate for all primes \( p \); we say that such matrices are **locally conjugate**. A special case of a theorem of Guralnick \( \text{[Gur80] Thm. 7} \) states that integral matrices are locally conjugate if and only if they are conjugate over an algebraic integral extension of \( \mathbb{Z} \). Note that this means that for integral matrices to be \( \mathbb{R} \)-conjugate for any of the rings of concern to us, we must first have that they are \( \mathbb{Q} \)-conjugate. We may therefore express \( \mathbb{R} \)-conjugacy classes as a partition of \( \mathcal{M}_f \).

Guralnick’s theorem motivates the main problem of this paper.

**Problem 1.1. The conjugacy extension problem**

Let \( f \in \mathbb{Z}[x] \) be square-free. For locally conjugate integral matrices \( A \) and \( B \) in \( \mathcal{M}_f \), find an algebraic extension \( E \) of \( \mathbb{Z} \) such that \( A \) and \( B \) are \( E \)-conjugate.

Before discussing our approach to attacking Problem 1.1, we give a preliminary result regarding \( \mathbb{Z}_p \) conjugacy.

**Theorem 1.2.** Let \( f \in \mathbb{Z}[x] \) which is square-free of degree \( n \), and take \( A, B \in \mathcal{M}_f \). For any prime \( p \) which does not divide the discriminant, \( \text{disc}(f) \), the matrices \( A \) and \( B \) are in the same \( \text{GL}_n(\mathbb{Z}_p) \)-conjugacy class.

The previous theorem tells us that to determine whether matrices are locally conjugate, one need only test for \( \mathbb{Z}_p \)-conjugacy for finitely many primes \( p \).

In Section 3.1, we note that the LM correspondence can be generalized to the context of conjugacy over an integral domain. Since the rings \( R \) we consider in this paper are integral domains with \( \mathbb{Z} \) as a subring, there is a nice relationship between the original and generalized bijections. If the \( \mathbb{Z} \)-conjugacy class of a matrix \( A \) corresponds to the fractional ideal class of \( I \), then the \( \mathbb{R} \)-conjugacy class of \( A \) corresponds to the fractional ideal class of \( R \otimes I \). Since a fractional ideal is a free \( \mathbb{Z} \)-module, the tensor product essentially extends scalars to \( R \). If \( f \) factors into the product \( \prod_{i=1}^{r} f_i \) of irreducible factors over \( R[x] \), we also identify \( R \otimes I \) as being contained within the direct \( \prod_{i=1}^{r} \text{Frac}(R)(\alpha_i) \) by considering \( \alpha \) as the tuple \( (\alpha_1, ..., \alpha_r) \) of the roots of the irreducible factors.

Since the LM correspondences for \( \mathbb{R} \)-conjugacy and \( \mathbb{Z} \)-conjugacy can be related via the tensor product, we can adapt an algorithm in \( \text{[Mar20]} \) which tests for \( \mathbb{Z} \)-conjugacy to obtain Algorithm 3.2 which tests for \( \mathbb{R} \)-conjugacy of integral matrices. We implemented this algorithm in Magma in the case that \( R = \mathcal{O}_F \) for a number field \( F \) and for matrices with characteristic polynomial which is irreducible in \( R[x] \).

The algorithm determines whether a given pair of matrices are \( \mathbb{R} \)-conjugate by determining whether a particular ideal is principal after extension of scalars to \( R \). Because of this, it is natural to make use of the principal ideal theorems of class field theory. For instance, for a number field \( K \), all fractional \( \mathcal{O}_K \)-ideals are principal in the ring of integers of the Hilbert class field of \( K \).
This leads us to a natural question: “Does the choice of $E = \mathcal{O}_{K_1}$ for $K := \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$ solve the conjugacy extension problem for matrices in $\mathcal{M}_f$?” We show in Example 3.4 that the answer to this question is ‘No’. This is because when $f$ has multiple irreducible factors in $R[x]$, the elements of $R \otimes I$ are tuples with number of components equaling the number of irreducible factors of $f$. For a fractional ideal $I$, it is not straightforward to test whether $R \otimes I$ is principal unless we are in the case that $f$ is irreducible in $R[x]$.

We offer a method for trying to solve the conjugacy extension problem which entails finding whether proper subfields of class fields satisfy certain criteria (see Test 3.9 in Section 3.3.1 for details). If such a subfield can be found in a particular example, then its ring of integers gives a solution to the conjugacy extension problem in that instance. We successfully carry out Test 3.9 to find an extension $E$ such that matrices in all locally conjugate matrices in $\mathcal{M}_f$ are $E$-conjugate in several examples with irreducible characteristic polynomial.

Acknowledgements

The author’s work has been supported in part by NSF Grant DMS-1720146, which is gratefully acknowledged.

2 Preliminaries

Before discussing our contributions to addressing the conjugacy extension problem, we discuss what is known about $\mathbb{Z}$-conjugacy. We also provide some results on $\mathbb{Z}_p$ conjugacy, including our proof of Theorem 1.2.

2.1 Conjugacy over $\mathbb{Z}$

A fundamental result of the study of $\mathbb{Z}$-conjugacy is a correspondence in [LM33], which we will refer to as the LM correspondence. This correspondence states that the $\mathbb{Z}$-conjugacy classes of matrices in $\mathcal{M}_f$ with $f$ square-free are in bijection with classes of certain fractional ideal classes which are associated to $f$ [LM33].

The LM correspondence was made more explicit in [Tau49] in associating the $\mathbb{Z}$-conjugacy class of a matrix $A$ with irreducible characteristic polynomial with the class of a fractional ideal with $\mathbb{Z}$-basis comprised of the components of an eigenvector of $A$ [Tau49].

More recently, Marseglia generalized the bijection in [Tau49] to the case that $f$ has multiple irreducible factors [Mar20]. Actually, the bijection defined in [Mar20, Thm. 8.1] relates matrices with a given square-free minimal polynomial to objects which generalize fractional ideals. We only consider the bijection restricted to the case of square-free characteristic polynomial so that the matrices correspond to fractional ideals, which can be computed using the algorithm in [Mar20]. We now state the LM correspondence in terms of Marseglia’s formulation.

**Theorem 2.1.** (LM correspondence) [LM33], [Mar20]. Let $f = \prod_{i=1}^{r} f_i$ be a square-free polynomial in $\mathbb{Z}[x]$ and let $\alpha = (\alpha_1, ..., \alpha_k)$ where $\alpha_i$ denotes a root of the irreducible factor $f_i$. The $\mathbb{Z}$-conjugacy classes within $\mathcal{M}_f$ are in bijection with the fractional $\mathbb{Z}[\alpha]$-ideal classes.

Following [Mar20], we now discuss what is meant by a fractional $\mathbb{Z}[\alpha]$-ideal when $\alpha$ denotes a $k$-tuple. If $\alpha = (\alpha_1, .., \alpha_k)$ as in Theorem 2.1 then we use $\mathbb{Z}[\alpha]$ to denote the ring

$\mathbb{Z}[(\alpha_1, .., \alpha_k)] = \{(p(\alpha_1), .., p(\alpha_k)) : p \in \mathbb{Z}[x]\}$.

3
The definition of a fractional $\mathbb{Z}[\alpha]$-ideal in this context is a generalization of the usual notion; a fractional $\mathbb{Z}[\alpha]$-ideal is defined to be a $\mathbb{Z}[\alpha]$-submodule of $\prod_{i=1}^r \mathbb{Q}(\alpha_i)$ which is also a free $\mathbb{Z}$-module of degree $n = \deg(f)$.

Equivalence of $\mathbb{Z}[\alpha]$-ideals is given by $\mathbb{Z}[\alpha]$-module isomorphism, which is also the same as scaling by a non-zero-divisor of $\prod_{i=1}^r \mathbb{Q}(\alpha_i)$.

We denote the set of fractional $\mathbb{Z}[\alpha]$-ideal classes by $\mathcal{I}_{\mathbb{Z}[\alpha]}$. Consider the map $\psi$ from the proof of [Mar20, Thm. 8.1]

$$\psi : \mathcal{M}_f \to \mathcal{I}_{\mathbb{Z}[\alpha]} / \cong_{\mathbb{Z}[\alpha]}$$

$$A \mapsto [I]$$

where $I$ is defined in the following way. For $i = 1, \ldots, k$, let $(v_{i1}, \ldots, v_{in})^t$ be an eigenvector of $A$ with eigenvalue $\alpha_i$ and

$$I = (v_{i1}, \ldots, v_{ki})\mathbb{Z} \oplus \ldots \oplus (v_{i1}, \ldots, v_{kn})\mathbb{Z}.$$

Note that $A$ is the multiplication-by-$\alpha$ map on $I$ with respect to the $\mathbb{Z}$-basis

$$\{(v_{i1}, v_{ki}), \ldots, (v_{i1}, v_{kn})\}.$$

From $\psi$, we obtain the induced map on $\mathbb{Z}$-conjugacy classes:

$$\tilde{\psi} : \mathcal{M}_f / \cong_{\mathbb{Z}} \to \mathcal{I}_{\mathbb{Z}[\alpha]} / \cong_{\mathbb{Z}[\alpha]}$$

$$[A] \mapsto [\psi(A)].$$

For a given square-free polynomial $f$ in $\mathbb{Z}[x]$, Marseglia gives an algorithm to compute all of the fractional $\mathbb{Z}[\alpha]$-ideal classes [Mar20]. This is a new contribution since it was previously only known how to compute the invertible $\mathbb{Z}[\alpha]$-ideal classes (previous methods are given in [Coh13], [KP05]). Together with the previously discussed bijection, this algorithm can be used to compute a list of representatives of the $\mathbb{Z}$-conjugacy classes within $\mathcal{M}_f$.

Eick, Hofmann, and O’Brien [EHO19] provide an algorithm for testing whether two matrices are $\mathbb{Z}$-conjugate, even if their minimal polynomial is not square-free. This algorithm relies on isomorphism-testing of certain modules and is motivated by the work of Grunewald in [Gru80].

While the algorithm in [EHO19] deals with a more general class of matrices, Marseglia’s algorithm ran faster in several examples (as recorded in Table 3 of [Mar20]). Difficulties in efficiently running the algorithm in [EHO19] may arise in computing the class group or in testing for isomorphism among a very large number of modules [EHO19]. Even the algorithm in [Mar20] appears to take exponential time in $n$, the degree of the characteristic polynomial. This is because Marseglia’s algorithm entails testing whether a particular fractional ideal is principal, and this is thought to be no easier than computing the class group [KV10]. The most efficient known algorithm is the probabilistic algorithm by Buchmann [Buc88], which is known to have exponential run time in $n$ [KV10].

With so much recent progress made in understanding $\mathbb{Z}$-conjugacy, we next shift our focus to $\mathbb{Z}_p$-conjugacy, and eventually to conjugacy over integral extensions of $\mathbb{Z}$.

### 2.2 Conjugacy over $\mathbb{Z}_p$

For a prime $p$, we consider conjugacy of integral matrices by elements in $\text{GL}_n(\mathbb{Z}_p)$. This allows us to make some important observations before delving into our discussion of Problem 1.1.
Remark 2.2. We follow Guralnick’s [Gur80] argument to show that $\mathbb{Z}_p$-conjugacy implies conjugacy over $\mathbb{Z}(p)$. If matrices $A, B \in \mathbb{Z}^{n \times n}$ are conjugate by an element in $\text{GL}_n(\mathbb{Z}_p)$, then $A$ and $B$ are $\text{GL}_n(\mathbb{Z}/p^{k}\mathbb{Z})$-conjugate for all $k \geq 1$. By the Artin-Rees Lemma, there is a natural number $k'$ such that the $\mathbb{Z}$-linear map $T(X) := AX - XB$ satisfies the inclusion $p^{k'}\mathbb{Z}^n \cap \text{Im}(T) \subseteq p\text{Im}(T)$. The solution $X$ to $AX = XB$ modulo $p^{k'}$ may be lifted to $X'$, a matrix in $\text{GL}_n(\mathbb{Z}(p))$ which conjugates $A$ to $B$ (see [Gur80], Theorem 4).

We now provide a proof for Theorem 1.2.

Proof: In the following, we will denote the image of a matrix $A$ modulo $p$ by $A(p)$.

Let $p$ be a prime with $p \nmid \text{disc}(f)$. Since $f$ modulo $p$ is square-free, there is a single $\mathbb{F}_p$-conjugacy class, containing $A(p)$ and $B(p)$. Let $C \in \text{GL}_n(\mathbb{F}_p)$ be a matrix which conjugates $A$ to $B$. We show that $C$ may be lifted to a conjugating matrix in $\text{GL}_n(\mathbb{Z}_p)$.

Consider the $\mathbb{Z}$-linear map $T(X) := AX - XB$. Note that $T(C) \equiv 0$ modulo $p$.

We wish to show that $p\mathbb{Z}^n \cap \text{Im}(T) \subseteq p\text{Im}(T)$. This is the inclusion following from the Artin-Rees Lemma with $k' = 1$. Working with suitable bases for the domain and codomain of $T$, we may express $T$ by a matrix, $S$, in its Smith normal form. Since $f$ is square-free, the rank $r$ of $S$ is $r = n^2 - n$. Since also $f$ is square-free modulo $p$, the matrix $S(p)$ also has rank $r$.

Letting $s_1, \ldots, s_r$ denote the non-zero diagonal entries of $S$, we see that

$$p\mathbb{Z}^n \cap \text{Im}(T) = (p\mathbb{Z} \times \ldots \times p\mathbb{Z}) \cap (s_1\mathbb{Z} \times \ldots \times s_r\mathbb{Z})$$

$$= \text{LCM}(p, s_1)\mathbb{Z} \times \ldots \times \text{LCM}(p, s_r)\mathbb{Z}$$

$$= \text{LCM}(s_1, \ldots, s_r)\mathbb{Z} \times \ldots \times \text{LCM}(s_1, \ldots, s_r)\mathbb{Z}$$

$$= \text{Im}(T).$$

By the previous inclusion, we have $T(C) = pT(D) = T(pD)$ for some $D \in \mathbb{Z}^n$. From this, we obtain $T(C - pD) = T(C) - T(pD) = 0$ and $\text{det}(C - pD) \equiv \text{det}(C)$, which is non-zero modulo $p$. Thus, $C' := C - pD$ is an element in $\text{GL}_n(\mathbb{Z}(p))$ which conjugates $A$ to $B$.

We ask whether a local-global principle holds in the context of matrix conjugacy. In other words, we ask whether locally conjugate matrices are conjugate over $\mathbb{Z}$.

This question is answered affirmatively in [Neb19] for adjacency matrices of Paley and Peisert graphs. In general, however, locally conjugate matrices need not be $\mathbb{Z}$-conjugate. We use the LM correspondence to obtain an example which demonstrates this.

Example 2.3. Let $f = x^2 + 5$ and denote a root of $f$ by $\alpha$. The number field $K = \mathbb{Q}(\alpha)$ has class number 2, and $\mathcal{O}_K = \mathbb{Z}[\alpha]$. A representative of the non-principal fractional ideal class is $I = 2\mathbb{Z} \oplus (1 + \alpha)\mathbb{Z}$. The trivial ideal class has representative $\mathbb{Z}[\alpha]$.

Computing the multiplication-by-$\alpha$ matrices with respect to the $\mathbb{Z}$-bases of each of the ideal class representatives, we find that the matrices $A = \begin{pmatrix} 0 & 1 \\ -5 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix}$ are representatives of the two distinct $\mathbb{Z}$-conjugacy classes within $\mathcal{M}_f$.

Note that $\text{disc}(f) = -2^2 \cdot 5$. We can easily verify that $A$ and $B$ are $\mathbb{Z}_p$-conjugate for $p = 2$ and $p = 5$, which is enough to determine that $A$ and $B$ are locally conjugate by Theorem 2.1.
While locally conjugate matrices are not necessarily \( Z \)-conjugate, a theorem of Guralnick tells us of what can be concluded about such matrices \( [\text{Gur80}] \).

**Theorem 2.4.** (\([\text{Gur80}], \text{Case of Thm. 7}\)) Integral matrices are locally conjugate if and only if they are conjugate over an algebraic integral extension of \( Z \).

The proof of Theorem 2.4 is based on an existence theorem in \([\text{Dad63}]\), which asserts that for a primitive, homogeneous form, there is an algebraic extension of \( Z \) over which the form realizes a unit. Dade provides a method for finding such an extension, though there is no bound on the degree of the output, as noted in \([\text{Wat63}]\).

This leads us to the main problem we address in this paper, the conjugacy extension problem.

### 3 The conjugacy extension problem

For the remainder of the paper, we discuss our contributions to Problem 1.1, the conjugacy extension problem.

In Section 3.1, we describe how the LM correspondence can be generalized to the context of conjugacy over an integral domain. This can then be used to adapt Marseglia’s algorithm to an algorithm which tests for \( R \)-conjugacy of integral matrices.

In Section 3.2, we introduce how class fields may be used to generate reasonable candidates for the extension \( E \) which solves Problem 1.1. Class fields offer an alternative method to Dade’s method in \([\text{Dad63}]\) for finding such an extension. We will first introduce a special case of the class field method in Section 3.2.2 and then provide it in full generality in Section 3.3.1. A nice feature of our method is that it is motivated by the theory of \( R \)-conjugacy of integral matrices in that it makes use of the generalized LM correspondence.

#### 3.1 Generalizing to an integral domain

The LM correspondence given by Theorem 2.1 may be generalized to describe conjugacy over any integral domain. Estes and Guralnick \([\text{EG84}]\) give a theoretical proof showing that, for irreducible \( f \), the LM correspondence holds over an integral domain for matrices in \( M_f \). The result in \([\text{EG84}]\) may be generalized to the case that \( f \) is square-free with multiple irreducible factors (the details of this generalization are found in \([\text{Afa21}]\)).

More concretely, one can see that LM correspondence holds over an integral domain by adapting the bijection \( \psi \) from \([\text{Mar20}]\). Since there is an embedding of \( Z \) in each of the rings \( R \) we consider in this paper, we may describe the \( R \)-conjugacy classes of matrices in \( M_f \) as being in correspondence with \( R[\alpha] \)-module isomorphism classes in \( R \otimes_Z \mathcal{I}_{\mathcal{Z}[\alpha]} := \{ R \otimes I : I \in \mathcal{I}_{\mathcal{Z}[\alpha]} \} \). For a fractional \( \mathcal{Z}[\alpha] \)-ideal, \( I = \oplus v_i Z \), we have \( R \otimes I = \oplus v_i R \). Suppose that in expressing \( I \) as \( I = \oplus v_i Z \), each \( v_i \) is an integral polynomial in \( \alpha \) (we may make this assumption about the \( v_i \) since we may clear denominators of the \( Z \)-basis of a fractional ideal to obtain an equivalent fractional ideal). Recall the point that when we express \( R \otimes I \) as having \( R \)-basis element \( v_i \), we mean the same polynomial in \( \alpha \), but where \( \alpha \) denotes the tuple of roots of \( f \) in \( R[x] \).

We make the connection between the the original and generalized LM bijections more explicit. To distinguish the type of conjugacy class to which we are referring, we denote the \( R \)-conjugacy class of \( A \) by \( [A]_R \). If \( \tilde{\psi}([A]_Z) = [I] \), then one may define the generalized correspondence by:

\[
\tilde{\psi}_R : M_f/R \to R \otimes \mathcal{I}_{\mathcal{Z}[\alpha]}/\sim_{R[\alpha]}
\]

\[
[A]_R \mapsto [R \otimes Z I].
\]
Since the LM correspondence generalizes in this straightforward way, we may also easily adapt Marseglia’s algorithm in [Mar20] to testing whether integral matrices are \( R \)-conjugate for \( R \) an integral domain with subring \( \mathbb{Z} \).

Before giving this modified algorithm, we need a definition.

**Definition 3.1.** [Mar20] For \( I \), a \( \mathbb{Z}[\alpha] \)-ideal in \( K \), the **multicaptor ring of \( I \)** is given by the colon ideal of \( I \) with itself: \( (I : I) := \{ x \in \mathcal{O}_K : xI \subseteq I \} \). Letting \( \hat{I} = R \otimes I \), the multicaptor ring of \( \hat{I} \) is \( (\hat{I} : \hat{I}) := \{ x \in R \otimes \mathcal{O}_K : x\hat{I} \subseteq \hat{I} \} = R \otimes (I : I) \). Note that \((\hat{I} : \hat{I})\) is the largest subring \( \mathcal{O} \) of \( R \otimes \mathcal{O}_K \) containing \( R[\alpha] \) such that \( \hat{I} \) is an \( \mathcal{O} \)-module.

**Algorithm 3.2.** \( R \)-Conjugacy of Integral Matrices (Adaptation of Algorithm in [Mar20])

**Input:** Integral matrices \( A, B \in \mathcal{M}_f \) for \( f \) square-free and an integral domain \( R \) containing \( \mathbb{Z} \). Still let \( \alpha \) denote the \( k \)-tuple of roots of the irreducible factors of \( f \) in \( R[x] \). Let \( K = \prod_{i=1}^n \text{Frac}(R)(\alpha_i) \).

**Output:** If \( A \sim_R B \), returns ‘Yes’ and the conjugating matrix in \( \text{GL}_n(R) \). Otherwise, returns ‘No’.

**Step 1)** Compute fractional \( R[\alpha] \)-ideals \( \hat{I} \) and \( \hat{J} \) corresponding to \( A \) and \( B \). If \( \tilde{\psi}([A]_\mathbb{Z}) = [I] \) and \( \tilde{\psi}([B]_\mathbb{Z}) = [J] \), then the \( R \)-conjugacy classes of \( A \) and \( B \) correspond to the fractional \( R[\alpha] \)-ideal classes of \( \hat{I} = R \otimes \mathbb{Z} \hat{I} \) and \( \hat{J} = R \otimes \mathbb{Z} \hat{J} \), respectively.

**Step 2)** Compute \((\hat{I} : \hat{I})\) and \((\hat{J} : \hat{J})\). If \((\hat{I} : \hat{I}) \neq (\hat{J} : \hat{J})\), then \( \hat{I} \) is not in the same class as \( \hat{J} \), and so \( A \) and \( B \) are not \( R \)-conjugate. Output ‘No’ and terminate. Otherwise, set \( \mathcal{O} = (\hat{I} : I) = (\hat{J} : J) \) and proceed to Step 3).

**Step 3)** Test if \((\hat{I} : \hat{J})\mathcal{O} \) is principal. If not, the fractional ideals \( \hat{I} \) and \( \hat{J} \) are not equivalent and so \( A \sim_R B \). Output ‘No’ and terminate. Otherwise, there is a \( \gamma \in K \) such that \((\hat{I} : \hat{J}) = (\gamma)\), meaning that \( \hat{I} = \gamma \hat{J} \) and \( A \sim_R B \). To compute the conjugating matrix, proceed to Step 4).

**Step 4)** Suppose that \( \hat{I} = \oplus v_i R \) and \( \hat{J} = \oplus \gamma v_i R \) (we are expressing each of the fractional ideals with respect to an \( R \)-basis so that \( A(v_1, \ldots, v_n)^t = \alpha(v_1, \ldots, v_n)^t \) and \( B(w_1, \ldots, w_n)^t = \alpha(w_1, \ldots, w_n)^t \)). Compute the change of basis matrix, call it \( C \), between \( \{v_1, \ldots, v_n\} \) and \( \{\gamma w_1, \ldots, \gamma w_n\} \). Since \( C \) gives the change of basis for two \( R \)-bases of \( \hat{I} \), the determinant of \( C \) is a unit in \( R \), and \( C \) conjugates \( A \) to \( B \). Return ‘Yes’ and the matrix \( C \). Terminate.

In the context of Problem 1.1 we begin by assuming that we our input matrices \( A \) and \( B \) are locally conjugate. If \( I \) and \( J \) correspond to \([A]_\mathbb{Z}\) and \([B]_\mathbb{Z}\) respectively, then the generalized LM correspondence tells us that \( \mathbb{Z}_p \otimes I \cong \mathbb{Z}_p \otimes J \) as \( \mathbb{Z}_p[\alpha] \)-modules for any prime \( p \). Using more classical language, we say \( I \) and \( J \) are in the same genus (in the sense of [Rei76, Ch.6]). Is is known that \( I \) and \( J \) are in the same genus if and only if \((I : I) = (J : J)\) (see Proposition 4.1 and Remark 4.3 of [Mar20]). Then in Step 2) of Algorithm 3.2 we will have \((I : I) = R \otimes (I : I) = R \otimes (J : J) = (J : J)\). While this equality is ensured for locally conjugate matrices, we still compute \( \mathcal{O} \) since it is needed for Step 3).
3.1.1 Implementation of the algorithm

We implemented Algorithm 3.2 in Magma [BCP97] in the case that $R$ is the ring of integers of a number field and the input matrices are in $M_f$ with $f$ irreducible in $R[x]$. To carry out Step 3. of the algorithm, we use the `IsPrincipal` function in Magma, which in the case of more than one irreducible factor, can only test for principality of fractional ideals in an étale $\mathbb{Q}$-algebra. If $R \supseteq \mathbb{Z}$ and we wish to work with $R[\alpha]$-ideals within the $\text{Frac}(R)$-algebra $\prod_{i=1}^{r} \text{Frac}(R)(\alpha_i)$, the IsPrincipal function only applies in the case that $r = 1$.

In the next section, we will consider whether the principal ideal theorems of class field theory can be applied to solving Problem 1.1. We will see that care must be taken, as complications arise when $f$ is not irreducible. In most of our examples, we choose an algebraic extension of $\mathbb{Z}$ so that the characteristic polynomial of our matrices remains irreducible in the extension. This restriction allows us to make use of our implementation.

3.2 Hilbert class fields

As noted in Algorithm 3.2, integral matrices are conjugate over an algebraic extension $R$ of $\mathbb{Z}$ if a particular fractional $\mathbb{Z}[\alpha]$-ideal is principal after extending scalars to $R$. For this reason, it is natural to ask whether matrices are conjugate over class fields, which come equipped with principal ideal theorems. In this section, we discuss the Hilbert class field of a number field.

We refer to [Chi08] for the following definitions and properties of class field theory.

**Definition 3.3.** The Hilbert class field of a number field $K$ is the maximal abelian unramified extension of $K$. We will denote the Hilbert class field of $K$ by $K_1$ (we denote the Hilbert class field this way in order to be consistent with the conventional notation for ray class fields, as we will see in Section 3.3).

It is known that $[K_1 : K] = h_K$, the class number of $K$. We consider Hilbert class fields due to the following property.

**Property 3.4.** For $K$ a number field with Hilbert class field $K_1$, every fractional $\mathcal{O}_K$-ideal is principal in $\mathcal{O}_{K_1}$.

It is important to note that Property 3.4 holds for fractional $\mathcal{O}_K$-ideals in the classical sense, i.e., fractional ideals which are submodules of a number field, but not necessarily for ideals within a product of number fields. We therefore restrict ourselves to the case of matrices in $M_f$ with $f$ irreducible.

Let $\alpha$ denote a root of the irreducible polynomial $f$. Then conjugacy of matrices in $M_f$ coincides with equivalence of fractional $\mathbb{Z}[\alpha]$-ideals in $K := \mathbb{Q}(\alpha)$. Let $R = \mathcal{O}_{K_1}$. Since $\alpha \in \mathcal{O}_{K_1}$, the polynomial $f$ factors further in $R$. Then extending scalars of the fractional ideals of concern to $R$ yields fractional $R[\alpha]$-ideals whose elements have multiple components. Property 3.4 of Hilbert class fields may not be helpful in this context since principality in each component does not imply principality of the object as a whole. As mentioned previously, the Magma function IsPrincipal does not apply to these fractional ideals, so computations for determining principality must be done manually.

3.2.1 Example

The next example demonstrates the subtlety that occurs when working with fractional ideals defined within a product of number fields.

**Example 3.5.** Let $f = x^2 + 5$ and $K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$. It is known that $h_K = 2$, and $I = 2\mathbb{Z} \oplus (1 + \alpha)\mathbb{Z}$ is a fractional ideal which is not principal. From the trivial fractional ideal $\mathbb{Z}[\alpha]$, we obtain via
the LM correspondence the transpose of the companion matrix of \( f \). Set \( A = \begin{pmatrix} 0 & 1 \\ -5 & 0 \end{pmatrix} \). The matrix 
\[
B = \begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix}
\]
corresponds to \( I \). Then we may choose \( A \) and \( B \) as representatives of the two \( \mathbb{Z} \)-conjugacy classes within \( \mathcal{M}_f \).

In this example, the full ring of integers of \( K \) is \( \mathbb{Z}[\alpha] \). This ensures that any fractional \( \mathbb{Z}[\alpha] \)-ideal has multiplier ring \( \mathbb{Z}[\alpha] \). Since the multiplier ring of \( I \) and \( \mathbb{Z}[\alpha] \) coincide, these fractional ideals are in the same genus, meaning that \( A \) and \( B \) are locally conjugate matrices.

One can calculate that the Hilbert class field of \( K \) is given by \( K_1 = \mathbb{Q}(\beta) \cong \mathbb{Q}[x]/(x^4+12x^2+16) \). Letting \( R = \mathcal{O}_{K_1} \), we consider \( R \)-conjugacy of \( A \) and \( B \). Since \( f \) factors as \( f = (x-\alpha)(x+\alpha) \) in \( R[x] \), the \( R[\alpha] \)-ideal of concern is \( R \otimes I = (2,2)R \oplus (1+\alpha,1-\alpha)R \). This \( R[\alpha] \)-ideal is not principal, meaning that the matrices \( A \) and \( B \) are not \( R \)-conjugate. This shows that the ring of integers of the Hilbert class field of \( \mathbb{Q}[x]/(f) \) does not automatically solve Problem 3.4 for locally conjugate matrices in \( \mathcal{M}_f \).

We will now provide the details for showing that the fractional \( R[\alpha] \)-ideal \( R \otimes I \) from the previous example is not principal. We let \( \overline{\alpha} = (\alpha,-\alpha) \). For any polynomial \( p \) in \( \alpha \), we use the notation \( \overline{p} \) to indicate the same polynomial evaluated in \( \overline{\alpha} \). For \( r \in R \), we have \( \overline{r} = (r,r) \).

We must determine whether
\[
R \otimes I = \overline{\mathcal{O}} \oplus (1+\alpha)R = (2,2)R \oplus (1+\alpha,1-\alpha)R
\]
has a generator \((\gamma_1,\gamma_2) \in K_1 \times K_1 \). If such a generator exists, then there is a change of \( R \)-basis between \([\overline{\alpha},1+\alpha] \) and \(( (\gamma_1,\gamma_2), (\gamma_1\alpha,-\gamma_2\alpha) ) \). Finding whether \( R \otimes I \) is principal is equivalent to determining whether there are \( \overline{\tau}_i = (r_i,r_i) \in R \) with
\[
\begin{align*}
2r_1 + (1+\alpha)r_2 &= \gamma_1 \\
2r_1 + (1-\alpha)r_2 &= \gamma_2 \\
2r_3 + (1+\alpha)r_4 &= \gamma_1\alpha \\
2r_3 + (1-\alpha)r_4 &= -\gamma_2\alpha
\end{align*}
\]
and \( r_1r_4 - r_2r_3 \in R^\times \). Isolating each component, we are searching for a solution \( r_i \) to
\[
\begin{align*}
2r_1 + (1+\alpha)r_2 &= \gamma_1 \\
2r_1 + (1-\alpha)r_2 &= \gamma_2 \\
2r_3 + (1+\alpha)r_4 &= \gamma_1\alpha \\
2r_3 + (1-\alpha)r_4 &= -\gamma_2\alpha
\end{align*}
\]
(1)

When we consider the principality of \( R \otimes I \), it will be useful to work with a \( \mathbb{Z} \)-basis \( \mathcal{B} \) of \( R \). Letting \( \beta \), a root of \( x^4+12x^2+16 \), denote a primitive element of \( K_1 \), we work with the \( \mathbb{Z} \)-basis \( \mathcal{B} = \{ 1, \beta, \beta^2, \beta^3 \} \) of \( R \). Denote the \( i \)-th basis element of \( \mathcal{B} \) by \( \mathcal{B}_i \).

We know that \( I_1 := 2R \oplus (1+\alpha)R \) and \( I_2 := 2R \oplus (1-\alpha)R \) are principal by Property 3.4. In fact, both \( I_1 \) and \( I_2 \) have a shared generator, call it \( \gamma \). If \( R \otimes I = (\gamma_1,\gamma_2) \), then we must have \( \gamma_1 = \gamma u_1 \) and \( \gamma_2 = \gamma u_2 \) for \( u_i \in R^\times \). Multiplying through the equations in (1) by \( u_i^{-1} \), we see that we are seeking a unit \( u \) of \( R \) so that
\[
\begin{align*}
2r_1 + (1+\alpha)r_2 &= \gamma \\
2r_1 + (1-\alpha)r_2 &= \gamma u \\
2r_3 + (1+\alpha)r_4 &= \gamma \alpha \\
2r_3 + (1-\alpha)r_4 &= -\gamma u\alpha
\end{align*}
\]
has a solution \( r_i \) with \( r_1r_4 - r_2r_3 \) a unit.

We rewrite this system in terms of the basis \( \mathcal{B} \). For \( x \in K_1 \), let \( M_x \) denote the multiplication-by-\( x \) matrix on \( R \) with respect to \( \mathcal{B} \). For any element \( y \in K_1 \), let \( \mathcal{Y} \) denote the coefficient vector of \( y \) in terms of \( \mathcal{B} \). Also let \( \overline{\mathcal{Y}}_i = (\overline{r_{i1}},...,\overline{r_{i4}}) \) denote the the vector of indeterminates.
Then if we seek a solution to
\[ 2r_1 + (1 + \alpha)r_2 = \gamma \]
\[ 2r_1 + (1 - \alpha)r_2 = \gamma u, \]
we can translate this to solving
\[
\begin{pmatrix}
M_2 & M_{1+\alpha} \\
M_2 & M_{1-\alpha}
\end{pmatrix}
\begin{pmatrix}
\mathbf{r}_1 \\
\mathbf{r}_2
\end{pmatrix}^t = \gamma
\]
for \( \mathbf{r}_1, \mathbf{r}_2 \in \mathbb{Z}^4 \). Such a solution must satisfy the difference of the equations
\[
\begin{pmatrix}
0_{4 \times 4} & M_{2\alpha}
\end{pmatrix}
\begin{pmatrix}
\mathbf{r}_1 \\
\mathbf{r}_2
\end{pmatrix}^t = M_\gamma(1 - u).
\]
We examine solutions to (2) using the Smith normal form of \( \begin{pmatrix}
0_{4 \times 4} & M_{2\alpha}
\end{pmatrix} \). There are matrices \( P \in \text{GL}_4(\mathbb{Z}) \) and \( Q \in \text{GL}_8(\mathbb{Z}) \) with
\[
P \begin{pmatrix}
0_{4 \times 4} & M_{2\alpha}
\end{pmatrix} Q = S
\]
where
\[
S = \begin{pmatrix}
2 & 2 \\
10 & 10
\end{pmatrix}
\]
\[
\begin{pmatrix}
0_{4 \times 4}
\end{pmatrix}
\]
An integral solution to (2) is
\[
Q \left( P M_\gamma(1 - u) \right) (\mathbf{r}_1 | \mathbf{r}_2)^t = M_\gamma(1 - u).
\]
We examine solutions to (2) using the Smith normal form of \( \begin{pmatrix}
0_{4 \times 4} & M_{2\alpha}
\end{pmatrix} \). There are matrices \( P \in \text{GL}_4(\mathbb{Z}) \) and \( Q \in \text{GL}_8(\mathbb{Z}) \) with \( P \begin{pmatrix}
0_{4 \times 4} & M_{2\alpha}
\end{pmatrix} Q = S \) where
\[
S = \begin{pmatrix}
2 & 2 \\
10 & 10
\end{pmatrix}
\]
\[
\begin{pmatrix}
0_{4 \times 4}
\end{pmatrix}
\]
An integral solution to (2) is
\[
Q \left( P M_\gamma(1 - u) \right) (\mathbf{r}_1 | \mathbf{r}_2)^t = M_\gamma(1 - u).
\]
We examine solutions to (2) using the Smith normal form of \( \begin{pmatrix}
0_{4 \times 4} & M_{2\alpha}
\end{pmatrix} \). There are matrices \( P \in \text{GL}_4(\mathbb{Z}) \) and \( Q \in \text{GL}_8(\mathbb{Z}) \) with \( P \begin{pmatrix}
0_{4 \times 4} & M_{2\alpha}
\end{pmatrix} Q = S \) where
\[
S = \begin{pmatrix}
2 & 2 \\
10 & 10
\end{pmatrix}
\]
\[
\begin{pmatrix}
0_{4 \times 4}
\end{pmatrix}
\]
An integral solution to (2) is
\[
Q \left( P M_\gamma(1 - u) \right) (\mathbf{r}_1 | \mathbf{r}_2)^t = M_\gamma(1 - u).
\]
We examine solutions to (2) using the Smith normal form of \( \begin{pmatrix}
0_{4 \times 4} & M_{2\alpha}
\end{pmatrix} \). There are matrices \( P \in \text{GL}_4(\mathbb{Z}) \) and \( Q \in \text{GL}_8(\mathbb{Z}) \) with \( P \begin{pmatrix}
0_{4 \times 4} & M_{2\alpha}
\end{pmatrix} Q = S \) where
\[
S = \begin{pmatrix}
2 & 2 \\
10 & 10
\end{pmatrix}
\]
\[
\begin{pmatrix}
0_{4 \times 4}
\end{pmatrix}
\]
An integral solution to (2) is
\[
Q \left( P M_\gamma(1 - u) \right) (\mathbf{r}_1 | \mathbf{r}_2)^t = M_\gamma(1 - u).
\]
We examine solutions to (2) using the Smith normal form of \( \begin{pmatrix}
0_{4 \times 4} & M_{2\alpha}
\end{pmatrix} \). There are matrices \( P \in \text{GL}_4(\mathbb{Z}) \) and \( Q \in \text{GL}_8(\mathbb{Z}) \) with \( P \begin{pmatrix}
0_{4 \times 4} & M_{2\alpha}
\end{pmatrix} Q = S \) where
\[
S = \begin{pmatrix}
2 & 2 \\
10 & 10
\end{pmatrix}
\]
\[
\begin{pmatrix}
0_{4 \times 4}
\end{pmatrix}
\]
An integral solution to (2) is
\[
Q \left( P M_\gamma(1 - u) \right) (\mathbf{r}_1 | \mathbf{r}_2)^t = M_\gamma(1 - u).
\]
We examine solutions to (2) using the Smith normal form of \( \begin{pmatrix}
0_{4 \times 4} & M_{2\alpha}
\end{pmatrix} \). There are matrices \( P \in \text{GL}_4(\mathbb{Z}) \) and \( Q \in \text{GL}_8(\mathbb{Z}) \) with \( P \begin{pmatrix}
0_{4 \times 4} & M_{2\alpha}
\end{pmatrix} Q = S \) where
\[
S = \begin{pmatrix}
2 & 2 \\
10 & 10
\end{pmatrix}
\]
\[
\begin{pmatrix}
0_{4 \times 4}
\end{pmatrix}
\]
Using the Smith normal form of \((0_{4 \times 4} \begin{vmatrix} M_{2\alpha} \end{vmatrix})\) once again, we find that \(PM_2(2\alpha)\) is not divisible by \((2, 2, 10, 10)^t\), meaning that there is no solution to (3).

We have shown that there is no \(u \in \mathbb{R}^4\) so that the system

\[
\begin{align*}
2r_1 + (1 + \alpha)r_2 &= \gamma \\
2r_1 + (1 - \alpha)r_2 &= \gamma u \\
2r_3 + (1 + \alpha)r_4 &= \gamma \alpha \\
2r_3 + (1 - \alpha)r_4 &= -\gamma u \alpha
\end{align*}
\]

has a solution. Thus, we have shown that \(R \otimes I\) is not principal and, consequently, that \(A\) and \(B\) are not conjugate over the ring of integers of \(K_1\).

### 3.2.2 Subfields of the Hilbert class field

As this example shows, testing whether \(R \otimes I\) is principal when \(f\) is not irreducible in \(R[x]\) can be involved, so we restrict our focus to algebraic extensions \(R\) of \(\mathbb{Z}\) such that \(f\) remains irreducible in \(R[x]\). While \(\mathcal{O}_{K_1}\) does not satisfy this criterion, we can still consider proper subfields of the Hilbert class field. This leads us to the following test for searching for a solution to Problem 1.1.

#### Test 3.6. Subfields of \(K_1\)

Suppose we begin with \(f\) irreducible in \(\mathbb{Z}[x]\) and locally conjugate matrices \(A, B \in \mathcal{M}_f\). Let \(I\) and \(J\) correspond via the LM correspondence to \(A\) and \(B\), respectively. Since the matrices are locally conjugate, we know that \((I : I) = (J : J)\). Let \(\mathcal{O}\) denote the shared multiplicator ring of \(I\) and \(J\). Let \(K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)\) and let \(K_1\) denote the Hilbert class field of \(K\).

We search through subfields of \(K_1\) and search for a subfield \(F\) satisfying the following criteria:

1. \(f\) is irreducible in \(\mathcal{O}_F[x]\).
2. \(\mathcal{O}_F \otimes (I : J)\mathcal{O}\) is principal

If \(F\) satisfies the above criteria, then \(\mathcal{O}_F\) is a solution to Problem 1.1 for \(A\) and \(B\).

This method of searching through the subfields of the Hilbert class field was successful in several examples. The following is a table indicating how often it worked for a particular sample of real quadratic fields, which we obtained from the LMFDB [LID].

In the first column, we list the irreducible quadratic polynomial \(f\). For the sample of number fields \(K := \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)\) represented in the following table, we have that the ring of integers equals \(\mathbb{Z}[\alpha]\). Then the only possible multiplicator ring is \(\mathbb{Z}[\alpha]\), meaning that all matrices in \(\mathcal{M}_f\) are locally conjugate. The fact that \(\mathcal{O}_K = \mathbb{Z}[\alpha]\) also implies that \(I_{\mathbb{Z}[\alpha]}\) is simply the ideal class group. The third column in the table gives the class number of \(K\).

All the ideal class groups represented in the table are cyclic, and the fourth column lists a matrix \(A\) which is chosen to correspond to a generator of the class group. Then \(A\) is not \(\mathbb{Z}\)-conjugate to the companion matrix of \(f\). The last column records whether Test 3.6 successfully yields a subfield \(F\) of the Hilbert class field satisfying the criteria. If so, the polynomial defining \(F\) over \(\mathbb{Q}\) is listed or ‘Yes’ is listed if the polynomial is
too lengthy to display. If no suitable subfield of $K_1$ was found, we list ‘No’. Note that we did not usually check for conjugacy for fields in which $f$ factored further due to the difficulty of testing for principality of fractional ideals.

Table 1: We use Test 3.6 for $M_f$ with $f$ defining a real quadratic field $K$. The discriminant of the fields $K$ in the table range from from 1 to 100 if $h_K = 2$ and from 1 to 500 if $h_K = 3$ or $h_K = 4$.

| $f$         | disc($f$) | $h_K$ | $A$       | Test 3.6 successful? |
|-------------|-----------|-------|-----------|----------------------|
| $x^2 - 10$  | $2^3 \cdot 5$ | 2     | $\begin{pmatrix} -1 & 3 \\ 3 & 1 \end{pmatrix}$ | $x^2 - 2$ |
| $x^2 - 15$  | $2^2 \cdot 3 \cdot 5$ | 2     | $\begin{pmatrix} -1 & 2 \\ 7 & 1 \end{pmatrix}$ | $x^2 + 2x - 11$ |
| $x^2 - x - 16$ | $5 \cdot 13$ | 2     | $\begin{pmatrix} 0 & 2 \\ 8 & 1 \end{pmatrix}$ | $x^2 - 52$ |
| $x^2 - x - 21$ | $5 \cdot 17$ | 2     | $\begin{pmatrix} 0 & 3 \\ 7 & 1 \end{pmatrix}$ | $x^2 - 2205$ |
| $x^2 - x - 57$ | 229       | 3     | $\begin{pmatrix} -2 & 3 \\ 17 & 3 \end{pmatrix}$ | $x^3 + 957x^2 + 206910x - 3157132$ |
| $x^2 - x - 64$ | 257       | 3     | $\begin{pmatrix} -1 & 2 \\ 31 & 2 \end{pmatrix}$ | $x^3 + 270x^2 - 1498824$ |
| $x^2 - 79$   | $2^2 \cdot 79$ | 3     | $\begin{pmatrix} -2 & 3 \\ 25 & 2 \end{pmatrix}$ | $x^3 - 66x^2 + 1089x - 1058$ |
| $x^2 - x - 80$ | 3 \cdot 107 | 3     | $\begin{pmatrix} -1 & 2 \\ 39 & 2 \end{pmatrix}$ | $x^3 - 33x + 9$ |
| $x^2 - x - 117$ | 7 \cdot 67 | 3     | $\begin{pmatrix} -2 & 3 \\ 37 & 3 \end{pmatrix}$ | No |
| $x^2 - x - 118$ | 11 \cdot 43 | 3     | $\begin{pmatrix} 0 & 2 \\ 59 & 1 \end{pmatrix}$ | $x^3 + 90x^2 - 102168$ |
| $x^2 - x - 36$ | 5 \cdot 29 | 4     | $\begin{pmatrix} -1 & 2 \\ 17 & 2 \end{pmatrix}$ | $x^4 - 44x^2 + 464$ |
| $x^2 - 82$   | $2^3 \cdot 41$ | 4     | $\begin{pmatrix} -2 & 3 \\ 26 & 2 \end{pmatrix}$ | $x^4 - 28x^2 + 32$ |
| $x^2 - x - 111$ | 5 \cdot 89 | 4     | $\begin{pmatrix} -2 & 3 \\ 35 & 3 \end{pmatrix}$ | Yes |

Because the ideal class groups were cyclic for this sample of number fields, and since $A$ corresponds to the class group generator, the polynomial in the last column defines a number field with ring of integers $E$ satisfying that all matrices in $M_f$ are $E$-conjugate.

Notice that Test 3.6 did not work for the given example of matrices with characteristic polynomial $f = x^2 - x - 117$. We will find an extension over which matrices in $M_f$ are conjugate in Example 3.11.

We also give a table recording how often Test 3.6 worked for a sample of imaginary quadratic fields defined by the polynomials $f$ in the following table. This sample was again pulled from the LMFDB [LID].

For each number field $K$ defined by $f$ in Table 2, the ring of integers of $K$ is $\mathbb{Z}[\alpha]$. Once again, all matrices in $M_f$ are locally conjugate. Other than the number field defined by $f = x^2 + 21$, the number fields represented in the table have cyclic ideal class group, and $A$ corresponds to a generator of the group.
Table 2: We use Test 3.6 for $M_f$ with $f$ defining an imaginary quadratic field $K$. The table lists number fields $K$ with discriminant ranging from $-100$ to $-1$ and class number ranging from 2 to 4.

| $f$           | $\text{disc}(f)$ | $h_K$ | $A$                      | Test 3.6 successful? |
|---------------|------------------|-------|--------------------------|-----------------------|
| $x^2 - x + 4$ | $-3 \cdot 5$    | 2     | $\left(\begin{array}{rr}
-1 & 2 \\
-3 & 2 \\
\end{array}\right)$ | $x^2 + 2x + 4$        |
| $x^2 + 5$     | $-2^2 \cdot 5$  | 2     | $\left(\begin{array}{rr}
-1 & 2 \\
-3 & 1 \\
\end{array}\right)$ | No                    |
| $x^2 + 6$     | $-2^3 \cdot 3$  | 2     | $\left(\begin{array}{rr}
0 & 2 \\
-3 & 0 \\
\end{array}\right)$ | $x^2 - 8x + 64$       |
| $x^2 - x + 9$ | $-5 \cdot 7$    | 2     | $\left(\begin{array}{rr}
-2 & 3 \\
-5 & 3 \\
\end{array}\right)$ | $x^2 + 7$             |
| $x^2 + 10$    | $-2^3 \cdot 5$  | 2     | $\left(\begin{array}{rr}
0 & 2 \\
-5 & 0 \\
\end{array}\right)$ | $x^2 + 2$             |
| $x^2 - x + 13$| $-3 \cdot 17$   | 2     | $\left(\begin{array}{rr}
-1 & 3 \\
-5 & 2 \\
\end{array}\right)$ | $x^2 + 8x + 19$       |
| $x^2 + 13$    | $-2^2 \cdot 13$ | 2     | $\left(\begin{array}{rr}
-1 & 2 \\
-7 & 1 \\
\end{array}\right)$ | No                    |
| $x^2 + 22$    | $-2^3 \cdot 11$ | 2     | $\left(\begin{array}{rr}
0 & 2 \\
-11 & 0 \\
\end{array}\right)$ | $x^2 - 40x + 576$    |
| $x^2 - x + 23$| $-7 \cdot 13$   | 2     | $\left(\begin{array}{rr}
-3 & 5 \\
-7 & 4 \\
\end{array}\right)$ | $x^2 + 7$             |
| $x^2 - x + 6$ | $-23$            | 3     | $\left(\begin{array}{rr}
0 & 2 \\
-3 & 1 \\
\end{array}\right)$ | $x^3 + 6x^2 + 9x - 23$|
| $x^2 - x + 8$ | $-31$            | 3     | $\left(\begin{array}{rr}
-1 & 2 \\
-5 & 2 \\
\end{array}\right)$ | No                    |
| $x^2 - x + 15$| $-59$            | 3     | $\left(\begin{array}{rr}
-2 & 3 \\
-7 & 3 \\
\end{array}\right)$ | $x^3 - 3x^2 - 124844$|
| $x^2 - x + 21$| $-83$            | 3     | $\left(\begin{array}{rr}
-2 & 3 \\
-9 & 3 \\
\end{array}\right)$ | $x^3 - 3x^2 - 17107628$|
| $x^2 - x + 14$| $-5 \cdot 11$   | 4     | $\left(\begin{array}{rr}
0 & 2 \\
-7 & 1 \\
\end{array}\right)$ | No                    |
| $x^2 + 14$    | $-2^3 \cdot 7$  | 4     | $\left(\begin{array}{rr}
-2 & 3 \\
-6 & 2 \\
\end{array}\right)$ | No                    |
| $x^2 + 17$    | $-2^2 \cdot 17$ | 4     | $\left(\begin{array}{rr}
-2 & 3 \\
-7 & 2 \\
\end{array}\right)$ | No                    |
| $x^2 + 21$    | $-2^2 \cdot 3 \cdot 7$ | 4 | $\left(\begin{array}{rr}
-2 & 5 \\
-5 & 2 \\
\end{array}\right)$ | Yes                   |

The following example gives more details regarding the example from the table with non-cyclic class group.

**Example 3.7.** For $f = x^2 + 21$ and $K$ defined by $f$, the Hilbert class field $K_1$ has defining polynomial $x^8 + 84x^6 + 3038x^4 - 12348x^2 + 405769$. The matrix $A = \left(\begin{array}{rr}
-2 & 5 \\
-5 & 2 \\
\end{array}\right)$ corresponds to the non-principal fractional ideal $I := 5\mathbb{Z} \oplus (\alpha + 2)\mathbb{Z}$.

The ideal class group of $K$ is not cyclic, so we must also consider another non-principal $\mathbb{Z}[\alpha]$-ideal $J := -7\mathbb{Z} \oplus \alpha\mathbb{Z}$. The matrix corresponding to $J$ is $B = \left(\begin{array}{rr}
0 & -7 \\
3 & 0 \\
\end{array}\right)$.

Let $F$ denote the subfield of $K_1$ defined by $x^4 - 32x^3 + 1616x^2 - 21760x + 396544$ and let $E = \mathcal{O}_F$. We have that $f$ remains irreducible in $E[x]$ and both $E \otimes I$ and $E \otimes J$ are principal. Then $C_f \sim_E A \sim_E B$. 

13
When Test 3.6 was successful for the sample of polynomials $f$ in Table 2, the resulting extension $E$ is such that there is a single $E$-conjugacy class within $\mathcal{M}_f$.

Note that for $f = x^2 + 5$, we already showed in Example 3.5 that $A$ and $C_f$ are not conjugate over the Hilbert class field, so they cannot be conjugate over any proper subfield of $K_1$ either. There are several other instances in which this method did not work. This is not surprising since there is no obvious reason for why there must be a subfield of the Hilbert class field satisfying the criteria of Test 3.6. However, Hilbert class fields provide a natural place to look for candidates for a solution to Problem 1.1.

We list some more data for non-quadratic fields in the appendix.

### 3.3 Ray class fields

We will extend the work of the previous section to ray class fields. Ray class fields are generalizations of the Hilbert class field, differing only in that ray class fields can be ramified at a finite number of primes. Since the condition on ray class fields is not as stringent as requiring all primes to be unramified, ray class fields can be large in degree and have many subfields in comparison to Hilbert class fields. Ray class fields also have a principal ideal property. This allows us to adapt Test 3.6 to ray class fields, which provides more potential solutions to Problem 1.1.

We will define ray class fields and list their principal ideal property. More details for the description below can be found in [Chi08] and [Mil97].

For a number field $K$, a $K$-modulus, denoted by $m$, is the formal product $m = m_0m_\infty$ where $m_0$ is an ideal of $\mathcal{O}_K$ and $m_\infty$ is a formal product of infinite primes, or real embeddings of $K$.

For a given modulus $m$, there exists an associated field satisfying certain properties called the ray class field of $K$ with modulus $m$, conventionally denoted $K_m$. The modulus is said to be admissible for $K_m$. There exists a least admissible modulus of a class field $K_m$ is called the conductor $f$ of $K_m$.

Given a number field $K$, we may describe the ray class field, $K_m$, as the maximal, abelian extension of $K$ which is ramified exactly at the primes which divide the conductor $f$ of $K_m$.

Note that when $m = 1$, the ray class field must be unramified at all primes, and so we obtain that $K_1$ is the Hilbert class field of $K$.

In the context of ray class fields, we have the following principal ideal property.

**Property 3.8.** [Tan58] Let $K$ be a number field and $m$ a $K$-modulus. Suppose the ray class field $K_m$ has conductor $f = f_0f_\infty$. Then every fractional $\mathcal{O}_K$-ideal relatively prime to $f_0$ is principal in $\mathcal{O}_{K_m}$.

Due to the previous property, it is natural to extend our work from Section 3.2.2 to ray class fields.

#### 3.3.1 Subfields of the ray class field

Despite Property 3.8, the fact that $f$ will factor further in $K_m$ means that $\mathcal{O}_{K_m}$ does not necessarily solve Problem 1.1. However, we can adapt Test 3.6 to ray class fields and again search for a suitable subfield.

**Test 3.9.** **Subfields of $K_m$**

The setup is identical to that in Test 3.6.
Pick a $K$-modulus $m$ which is relatively prime to $(I : J)O$. Let $K_m$ denote the ray class field of $K$ with modulus $m$.

We search through subfields of $K_m$ and search for a subfield $F$ satisfying the same criteria as in Test 3.6. If $F$ satisfies the above criteria, then $O_F$ is a solution to Problem 1.1 for $A$ and $B$.

Note that we obtain Test 3.6 from Test 3.9 by setting $m = 1$.

Referring to Example 3.9 we showed that locally conjugate matrices $A$ and $B$ in $M_f$ need not be $O_{K_1} -$conjugate for $K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$. We show that a subfield of a particular ray class field solves Problem 1.1 for the matrices from this example.

**Example 3.10.** The matrices $A = \begin{pmatrix} 0 & 1 \\ 15 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix}$ are representatives of the two $\mathbb{Z}$-conjugacy classes within $M_f$ for $f = x^2 + 5$. Let $K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$.

Corresponding to these matrices are the fractional $\mathbb{Z}[\alpha]$-ideals $\mathbb{Z}[\alpha] = 1\mathbb{Z} \oplus \alpha\mathbb{Z}$ and $I = 2\mathbb{Z} \oplus (1 + \alpha)\mathbb{Z}$. As previously noted, both of these fractional ideals have multiplicator ring $\mathbb{Z}([\alpha])$.

We wish to find an algebraic extension $R$ of $\mathbb{Z}$ in which $R \otimes (I : \mathbb{Z}[\alpha]) = R \otimes I$ is principal. We compute that $N_{K/\mathbb{Q}}(I) = 2$, meaning that we must select a modulus relatively prime to $2\mathbb{O}_K$. Letting $m = 3\mathbb{O}_K$, we find that $K_m$ is the number field defined by $x^5 + 12x^3 + 158x^3 - 228x^2 + 3721$ and has conductor $m$.

Applying Test 3.6, we find a subfield $F$ of $K_m$ given by

$$F = \mathbb{Q}(\beta) \cong \mathbb{Q}[x]/(x^4 - 12x^3 + 158x^2 + 228x + 3721)$$

satisfying the method’s criteria. Thus, $A$ and $B$ are $R$-conjugate for $R = \mathbb{O}_F$.

We computed the conjugating matrix in this example. Working with respect to the $\mathbb{Z}$-basis

$$B = \left\{ 1, \frac{1}{8}(\beta - 1), \frac{1}{64}(\beta^2 - 2\beta + 1), \frac{1}{1024}(\beta^3 - 3\beta^2 + 3\beta - 513) \right\}$$

of $R$, and letting $B_i$ denote the $i$-th basis element, we find that

$$C = \begin{pmatrix} -B_2 & -1 - B_4 \\ 3 + B_2 + 3B_4 & -1 - 2B - 2 - B_4 \end{pmatrix}$$

is an element in $GL_2(R)$ which conjugates $A$ to $B$.

Based on the data that we collected, Test 3.6 seems to typically result in extensions of smaller degree than Dade’s method from [Dad63]. In particular, Dade’s method always yields an extension of degree strictly greater than $n$, while we found extensions of degree $n$ in several instances, e.g., see Tables 1 and 2 (in these tables, the degree of extensions actually coincides with the class number of $K$). In the following example, we found a noteworthy difference in the degree of the extension resulting from each method.

**Example 3.11.** The matrices $A = \begin{pmatrix} -2 & 37 \\ 3 & 3 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 117 \\ 1 & 1 \end{pmatrix}$ are locally conjugate matrices which are not $\mathbb{Z}$-conjugate. These matrices have characteristic polynomial $f = x^2 - x - 117$, and $\text{disc}(f) = 7 \cdot 67$.

The rational matrices $C_1 = \begin{pmatrix} 3 & -6 \\ 0 & 9 \end{pmatrix}$ and $C_2 = \begin{pmatrix} -10 & -538 \\ 14 & 12 \end{pmatrix}$ conjugate $A$ to $B$ and have relatively prime determinants.
Following Dade’s method, we find that the quadratic form \( f(x,y) = \det(xC_1 + yC_2) \) realizes a unit over an algebraic extension of degree larger than 462. We did not explicitly work out the polynomial defining the extension, nor did we solve for \( x \) and \( y \), since this degree is so large.

On the other hand, Test 3.9 requires that we find an algebraic extension \( R \) so that \( R \otimes I \) is principal for \( I = 3\mathbb{Z} \oplus (2 + \alpha)\mathbb{Z} \). Letting \( K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f) \), we pick the modulus to be the \( O_K \)-ideal \( p = 7\mathbb{Z} \oplus (3 + \alpha)\mathbb{Z} \). This is a prime ideal of \( O_K \) with \( p^2 = (7) \). (We do not have results which narrow down which moduli relatively prime to the norm of the ideal should be considered, but it is interesting to note that the modulus is a prime dividing 7, which divides the discriminant of \( f \)).

Letting \( m = p \), we find that the ray class field \( K_m \) has degree 18 over \( \mathbb{Q} \) and has conductor \( p \). Searching through the proper subfields of \( K_m \), we find that the subfield \( F \) defined by the cubic polynomial

\[
x^3 + c_2 x^2 + c_1 x + c_0 \quad \text{with}
\]

\[
c_2 = 22427531465691
\]

\[
c_1 = 87019205503941567942935016 \quad \text{and}
\]

\[
c_0 = -169863356476213700099189634845323984727
\]

satisfies the criteria of Test 3.9. Therefore, the matrices \( A \) and \( B \) are \( GL_2(O_F) \)-conjugate, and \( O_F \) is an algebraic extension of degree 3 over \( \mathbb{Z} \).

In looking for a solution to Problem 1.1, this method opens up for consideration subfields of the ray class field of any modulus that is relatively prime to \( (I : J)O \). However, the degree and quantity of subfields of ray class fields can be very large. This presents computational difficulties, as testing whether an ideal is principal in a number field of large degree is costly.

Due to the expense of these computations, we only used Test 3.9 with \( m \neq 1 \) for solving Problem 1.1 in a limited number of examples in which the degree of the ray class field was not too large. These examples are listed in the appendix.

4 Conclusion and Open Problems

We have seen that Hilbert class fields do not always provide a solution to Problem 1.1. While we offered Test 3.9 which incorporates ray class fields, we could only carry out this method in a few cases due to computational difficulties. Thus, several open problems remain in this area of research, including the following.

1. Is there always a modulus \( m \) for which there is a subfield meeting the criteria of Test 3.9? Is there a way to characterize those moduli for which this holds? This would be a helpful contribution since as of now we only require that the modulus be relatively prime to a particular fractional ideal. In Example 3.7, our choice of modulus, which was related to the discriminant of the characteristic polynomial, proved successful. Should this hold in general?

2. Can one make the \( R \)-conjugacy algorithm more efficient? The algorithm which tests for principality of ideals seems to take exponential time in \( n \), and it is not clear whether this can be improved.

3. Can one write an algorithm which tests whether a fractional ideal defined in an \( R \)-algebra of the form \( \prod_{i=1}^r \text{Frac}(R)(\alpha_i), k > 1 \) is principal? This would allow us to extend the \( R \)-conjugacy algorithm to matrices which have square-free characteristic polynomial with multiple irreducible factors.
5 Appendix

Throughout the appendix, we obtained all number fields of consideration from the LMFDB [LfD].

5.1 Test 3.6 for cubic and quartic number fields

For the six cubic fields with class number 2 and discriminant ranging from -1,000 to 1,000 from the LMFDB, Test 3.6 does not yield a solution to Problem 1.1. We do not list these fields in a table.

The next table lists cubic polynomials \( f \) which give number fields \( K \) with discriminant ranging from -1,000 to 1,000 and class number 3.

In the examples for which Method 3.6 was successful, a polynomial is listed in the last column which defines a number field \( F \) such that the number of \( \text{GL}_3(\mathcal{O}_F) \)-conjugacy class of matrices in \( \mathcal{M}_f \) coincides with the number of local conjugacy classes. We also recorded when Test 3.6 failed.

| \( f \)         | \( \text{disc}(f) \) | \( h_K \) | \#Local conjugacy classes | Test 3.6 successful? |
|----------------|----------------------|----------|---------------------------|---------------------|
| \( x^3 - x^2 + 5x + 1 \) | \(-2^2 \cdot 3 \cdot 7^2\) | 3        | 1                         | \( x^3 - 3x^2 - 60x + 251 \) |
| \( x^3 - 3x - 10 \)      | \(-2^3 \cdot 3^3\)   | 3        | 2                         | No                  |
| \( x^3 - x^2 - 4x + 12 \) | \(-2^2 \cdot 13^2\)  | 3        | 2                         | \( x^3 - 3x^2 - 114x + 467 \) |
| \( x^3 + 6x - 1 \)       | \(3^3 \cdot 11\)     | 3        | 1                         | No                  |
| \( x^3 - x^2 + 5x - 6 \)  | \(-7^2 \cdot 19\)    | 3        | 1                         | \( x^3 + 3x^2 - 8376x - 303407 \) |
| \( x^3 - x^2 + 5x - 13 \)| \(-2^2 \cdot 5 \cdot 7^2\) | 3        | 2                         | \( x^3 + 3x^2 - 60x + 127 \) |

Test 3.6 failed for the seven cubic fields with discriminant ranging from -2,000 to 2,000 and class number 4 or 5 listed in the LMFDB.

We checked the seven quartic fields with class number 2 and discriminants ranging from -2,500 to 2,500, the four fields with class number 3 and discriminants in -5,000 to 5,000, and the four fields with class number 4 and discriminants from -10,000 to 10,000 from the LMFDB. Of these, only the quartic polynomials \( f \) for which Test 3.6 was successful are given in the next table.

The last column gives a polynomial which defines a number field \( F \) so that the number of \( \text{GL}_4(\mathcal{O}_F) \)-conjugacy classes within \( \mathcal{M}_f \) is given by the number of local conjugacy classes.

| \( f \)         | \( \text{disc}(f) \) | \( h_K \) | \#Local conjugacy classes | Test 3.6 successful? |
|----------------|----------------------|----------|---------------------------|---------------------|
| \( x^4 + 4x^2 + 1 \) | \(2^6 \cdot 3^2\)   | 2        | 1                         | \( x^2 - 10x + 73 \) |
| \( x^4 + 9 \)       | \(2^6 \cdot 3^2\)   | 2        | 3                         | \( x^2 - 10x + 73 \) |
| \( x^4 - x^2 + 8x^2 + x + 1 \) | \(2^2 \cdot 23^2\)  | 3        | 1                         | \( x^3 + 30x^2 - 45x - 12501 \) |
| \( x^4 - 2x^3 + 4x^2 + 2x + 1 \) | \(2^2 \cdot 5^3\)  | 4        | 1                         | \( x^4 + 6x^3 + 111x^2 + 526x + 761 \) |
| \( x^4 - x^3 + 3x^2 - 6x + 6 \)  | \(2^3 \cdot 3^2 \cdot 5^3\) | 4        | 1                         | \( x^4 + 32x^3 + 544x^2 + 4608x + 15616 \) |
| \( x^4 + 5x^2 + 10 \)    | \(2^3 \cdot 3^2 \cdot 5^3\) | 4        | 2                         | \( x^4 + 32x^3 + 384x^2 - 512x + 4096 \) |

In the previous table, the number fields defined by \( f \) in the first and second row have the same Hilbert class field, and the same subfield satisfies the criteria of Test 3.6 in each case.
5.2 Additional examples applying Test 3.9

Just as we used Test 3.9 to solve Problem 3.1 in Examples 3.10 and 3.11, we apply Test 3.9 to the following examples. These are examples in which Test 3.6 failed, as noted in Table 2.

Example 5.1. Let \( K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f) \) for \( f = x^2 + 13 \). The fractional ideal \( I = 2\mathbb{Z} \oplus (1 + \alpha)\mathbb{Z} \) is non-principal with \( N_{K/\mathbb{Q}}(I) = 4 \). We choose modulus \( m = 3\mathbb{Z}[\alpha] \) which is relatively prime to \( I \). The ray class field of \( K \) with modulus (and conductor) \( m \) is the number field defined by

\[
\begin{align*}
    x^{16} - 32x^{14} + 5676x^{12} - 316256x^{10} + 16999606x^8 - 689734368x^6 + \\
    19963313676x^4 - 378823819680x^2 + 3324557815569
\end{align*}
\]

over \( \mathbb{Q} \).

The subfield \( F \) of \( K_m \) defined by \( x^2 - 74x + 3721 \) satisfies the criteria of Test 3.9. Therefore, there is a single \( E \)-conjugacy class within \( M_f \) for \( E = \mathcal{O}_F \).

Example 5.2. Let \( f = x^2 + 14 \), and \( K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f) \). We consider the non-principal ideal \( I = 3\mathbb{Z} \oplus (-1 + \alpha)\mathbb{Z} \). Since \( N_{K/\mathbb{Q}}(I) = 9 \), we pick \( m = 2\mathbb{Z} \oplus \alpha\mathbb{Z} \), a prime ideal dividing \( (2) \).

The ray class field \( K_m \) is defined by

\[
\begin{align*}
    x^{16} - 32x^{14} + 5676x^{12} - 316256x^{10} + 16999606x^8 - 689734368x^6 + \\
    19963313676x^4 - 378823819680x^2 + 3324557815569
\end{align*}
\]

and has conductor \( m \). Using the criteria of Test 3.9, we find the subfield \( F \) of \( K_m \) defined by

\[
x^4 - 1548x^3 - 3055050x^2 - 2822525676x + 3324557815569.
\]

Then for \( E = \mathcal{O}_F \), all matrices in \( M_f \) are \( E \)-conjugate.
References

[Afa21] Rebecca Afandi. *The Conjugacy Extension Problem*. PhD thesis, Colorado State University, 2021.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.

[Buc88] Johannes Buchmann. A subexponential algorithm for the determination of class groups and regulators of algebraic number fields. *Séminaire de théorie des nombres, Paris*, 1989(1990):27–41, 1988.

[Chi08] Nancy Childress. *Class Field Theory*. Springer Science & Business Media, 2008.

[Coh13] Henri Cohen. *A course in computational algebraic number theory*, volume 138. Springer Science & Business Media, 2013.

[Dad63] Everett Clarence Dade. Algebraic integral representations by arbitrary forms. *Mathematika*, 10(2):96–100, 1963.

[EG84] Dennis R Estes and Robert M Guralnick. Representations under ring extensions: Latimer-MacDuffee and Taussky correspondences. *Advances in Mathematics*, 54(3):302–313, 1984.

[EHO19] Bettina Eick, Tommy Hofmann, and Eamonn A O’Brien. The conjugacy problem in gl(n,z). *Journal of the London Mathematical Society*, 100(3):731–756, 2019.

[Gru80] Fritz J Grunewald. Solution of the conjugacy problem in certain arithmetic groups. *Studies in Logic and the Foundations of Mathematics*, 95:101–139, 1980.

[Gur80] Robert M Guralnick. A note on the local-global principle for similarity of matrices. *Linear Algebra and its Applications*, 30:241–245, 1980.

[KP05] Jürgen Klüners and Sebastian Pauli. Computing residue class rings and picard groups of orders. *Journal of Algebra*, 292(1):47–64, 2005.

[KV10] Markus Kirschmer and John Voight. Algorithmic enumeration of ideal classes for quaternion orders. *SIAM Journal on Computing*, 39(5):1714–1747, 2010.

[LiD] The L-functions and Modular Forms Database. The LMFDB Collaboration.

[LM33] Claiborne G Latimer and CC MacDuffee. A correspondence between classes of ideals and classes of matrices. *Annals of Mathematics*, pages 313–316, 1933.

[Mar20] Stefano Marseglia. Computing the ideal class monoid of an order. *Journal of the London Mathematical Society*, 101(3):984–1007, 2020.

[Mil97] James S Milne. Class field theory, 1997.

[Neb19] Gabriele Nebe. On conjugacy of diagonalizable integral matrices. *arXiv preprint arXiv:1910.05974*, 2019.

[Rei75] Irving Reiner. Maximal orders. *New York-London*, 1975.

[Tan58] Tadao Tannaka. A generalized principal ideal theorem and a proof of a conjecture of Deuring. *Annals of Mathematics*, pages 574–58, 1958.

[Tau49] Olga Taussky. On a theorem of Latimer and MacDuffee. *Canadian Journal of Mathematics*, 1(3):300–302, 1949.

[Wat63] GL Watson. A problem of dade on quadratic forms. *Mathematika*, 10(2):101–106, 1963.