DISSERTATION

THE CONJUGACY EXTENSION PROBLEM

Submitted by

Rebecca Afandi

Department of Mathematics

In partial fulfillment of the requirements

For the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Summer 2021

Doctoral Committee:

Advisor: Alexander Hulpke

Jeff Achter
Rachel Pries
Sanjay Rajopadhye

ABSTRACT

THE CONJUGACY EXTENSION PROBLEM

In this dissertation, we consider R-conjugacy of integral matrices for various commutative rings R. An existence theorem of Guralnick states that integral matrices which are $\mathbb{Z}_p$-conjugate for every prime p are conjugate over some algebraic extension of $\mathbb{Z}$. We refer to the problem of determining this algebraic extension as the *conjugacy extension problem.* We will describe our contributions to solving this problem.

We discuss how a correspondence between $\mathbb{Z}$-conjugacy classes of matrices and certain fractional ideal classes can be extended to the context of R-conjugacy for R an integral domain. In the case of integral matrices with a fixed irreducible characteristic polynomial, this theory allows us to implement an algorithm which tests for conjugacy of these matrices over the ring of integers of a specified number field. We also describe how class fields can be used to solve the conjugacy extension problem in some examples.

ACKNOWLEDGEMENTS

Alexander Hulpke, thank you for taking me on as your graduate student and for thoughtfully introducing me to a topic that merges my mathematical interests. You have been a great source of support and practical advice throughout the process of doing research and finding a future career path. Jeff Achter, thank you for your insightful suggestion to consider class fields for this project. Your suggestion propelled much of this work. Rachel Pries, thank you for taking time to advise me as a masters student even while you were on sabbatical and for your kindness in guiding me. Thank you to my community for being there to commiserate about the difficulties of graduate school and for giving me perspective by pointing me to what is important. Mom and Dad, thank you for providing stability and support over the years and for encouraging me to face challenges with confidence. Thank you for instilling in me a love of learning. Adam, thank you for reminding me of the beauty of mathematics and for your constancy in loving me throughout all of the chapters of this journey.

TABLE OF CONTENTS

Chapter 1

Conjugacy over a ring

The topic of matrix conjugacy, or similarity, is one of interest in many fields, as similar matrices may be interpreted as linear maps which are equivalent up to a change in basis. Matrix similarity is a powerful idea with several applications. For instance, diagonalization is a useful tool for solving systems of linear ODEs.

The theory of matrix conjugacy over a field is well-established and lies within the realm of linear algebra. A question of interest is whether this theory generalizes when we consider matrix conjugacy over a ring. We define precisely what we mean by this.

Definition 1.0.1. *For a ring R, we say that $A, B \in R^{n\times n}$ are R-**conjugate** or **conjugate over** R if there is a matrix $C \in \mathbf{GL}_n(R) = \{C \in R^{n\times n} : det(C) \in R^\times\}$ such that $C^{-1}AC = B$. Note that this condition on the determinant of C ensures that C^{-1} has coefficients in R. The R-**conjugacy class** of a matrix A is the equivalence class of A under R-conjugacy. We write $A \sim_R B$ to denote that A and B are R-conjugate.*

Much recent progress has been made in describing matrix conjugacy over the integers (see [24], [11], and [18]). For integral matrices A and B, we will also say that A and B are **integrally** conjugate to mean they are $\mathbb{Z}$-conjugate.

Before discussing what is known about integral conjugacy, we will summarize the more classical theory of conjugacy over a field. We will be especially interested in $\mathbb{Q}$-conjugacy, and we will say that A and B are **rationally conjugate** if they are $\mathbb{Q}$-conjugate.

For a field K, suppose we wish to describe the K-conjugacy class of a matrix $A \in K^{n\times n}$. One may do this by finding its rational canonical form, which depends to some extent on the minimal and characteristic polynomials of A. Considering K^n as a $K[x]$-module via the linear transformation A, we have that $K^n \cong K[x]/(f_1) \oplus K[x]/(f_2) \oplus ... \oplus K[x]/(f_m)$ as $K[x]$-modules since $K[x]$ is a principal ideal domain [10]. Here, the f_i are polynomials in $K[x]$ such that f_i divides f_{i+1}, the

minimal polynomial of the matrix A is f_m, and the product $\prod_{i=1}^{m} f_i$ is the characteristic polynomial of A [10].

Determining whether matrices are conjugate over a field is equivalent to computing a particular normal form called the **rational canonical form** [10]. Matrices are conjugate over a field if and only if they have the same rational canonical form [10]. The benefit of using the rational canonical form is that we do not require that our field be algebraically closed. In particular, one can find the rational canonical form of matrices defined over the field of rational numbers, hence its name.

For $f_i = x^d + c_{d-1}x^{d-1} + ... + c_1 x + c_0$, letting $\mathcal{C}_{f_i}$ denote the corresponding companion matrix of f_i, we have

$$\mathcal{C}_{f_i} = \begin{pmatrix} 0 & 0 & ... & 0 & -c_0 \\ 1 & 0 & ... & 0 & -c_1 \\ 0 & 1 & .... & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & .... & 1 & -c_{d-1} \end{pmatrix}.$$

Note that $\mathcal{C}_{f_i}$ has characteristic polynomial f_i.

For a matrix $A \in K^{n\times n}$, if $K^n \cong K[x]/(f_1) \oplus K[x]/(f_2) \oplus ... \oplus K[x]/(f_m)$ as $K[x]$-modules (where x acts via A), then the rational canonical form of A is the block-diagonal matrix with the $\mathcal{C}_{f_i}$ as blocks, conventionally ordered so that $f_i \mid f_{i+1}$ moving down the diagonal. A standard linear algebra result is that two matrices are conjugate over a field K if and only if they have the same rational canonical form [10]. Thus, determining whether two matrices are conjugate over a field only requires computation of the rational canonical form.

We will restrict ourselves to considering matrices which have square-free characteristic polynomial. In this case, the fact that the minimal polynomial and characteristic polynomial of a matrix share the same roots means that the square-free characteristic polynomial coincides with the minimal polynomial [10]. Thus, the only possible rational canonical form for such a matrix is the companion matrix of the characteristic polynomial, and so matrices with the same square-free characteristic polynomial are conjugate over a field.

Throughout this thesis, we will consider R-conjugacy of integral matrices for various rings R. The rings we are primarily interested in include $\mathbb{Z}$, the ring of p-adic integers (elements of this ring are infinite tuples $(z_1, z_2, .., z_i, ...)$ such that $z_i \in \mathbb{Z}/p^i\mathbb{Z}$ and $z_{i+1} \equiv z_i \pmod{p^i}$), which is denoted $\mathbb{Z}_p$, and algebraic extensions of $\mathbb{Z}$. We may consider R-conjugacy of integral matrices since there is an embedding of $\mathbb{Z}$ into each of the rings R we consider.

For any of the previously mentioned rings R, we will consider R-conjugacy of matrices which share a given square-free characteristic polynomial f. From here on, we let $\mathcal{M}_f$ denote the set defined by $\mathcal{M}_f = \{A \in \mathbb{Z}^{n\times n} : \det(xI - A) = f\}$ for a monic square-free integral polynomial f. If $K = \text{Frac}(R)$, the fraction field of R, then there is just a single K-conjugacy class within $\mathcal{M}_f$. However, it can happen that the set $\mathcal{M}_f$ consists of multiple R-conjugacy classes. Also, integral matrices cannot be R-conjugate if they are not first $\text{Frac}(R)$-conjugate, so it is enough to consider R-conjugacy among the matrices in $\mathcal{M}_f$.

1.1 The Latimer and MacDuffee correspondence for integral conjugacy

Let us now discuss what is known about conjugacy over the integers. Since we cannot make use of the standard results of linear algebra, the problem of integral conjugacy is much harder. We now illustrate the difficulty which arises when considering $\mathbb{Z}$-conjugacy. For the polynomial $f = (x^2 + 4x + 7)(x^3 - 9x^2 - 3x - 1)$, there are 852 $\text{GL}_5(\mathbb{Z})$-conjugacy classes which partition $\mathcal{M}_f$, while there is just a single $\text{GL}_5(\mathbb{Q})$-conjugacy class. We will later discuss this in more detail in Example 1.1.9. First, we must delve into the theory of integral conjugacy.

For a fixed square-free characteristic polynomial f of degree n and root α, Latimer and MacDuffee gave a theoretical correspondence between $\mathbb{Z}$-conjugacy classes within $\mathcal{M}_f$, and isomorphism classes of $\mathbb{Z}[\alpha]$-modules in $\mathbb{Q}(\alpha)$ which are also free $\mathbb{Z}$-modules of rank n [21].

One may consider $\mathbb{Z}^n$ to be a $\mathbb{Z}[\alpha]$-module where α acts as a matrix A with characteristic polynomial f. We may also consider $\mathbb{Z}^n$ as a $\mathbb{Z}[\alpha]$-module via another matrix B with characteristic polynomial f. The two resulting modules are isomorphic exactly when the matrices A and B are

$\mathrm{GL}_n(\mathbb{Z})$-conjugate [5]. Then it is not too surprising that $\mathrm{GL}_n(\mathbb{Z})$-conjugacy classes of matrices are related to $\mathbb{Z}[\alpha]$-isomorphism classes of the modules previously described.

In the case that f is irreducible, Taussky made the result more concrete by providing an explicit bijection [32]. Marseglia [24] and Husert [18] independently generalized Taussky's bijection to the square-free case. We will discuss the bijections in each case.

1.1.1 Irreducible characteristic polynomial

Before discussing Taussky's contributions to the Latimer and MacDuffee correspondence in the irreducible case, we must define a few terms. The following definitions are standard and can be found in [26].

Definition 1.1.1. *Let R be an integral domain with field of fractions K. Then a **fractional R-ideal** of K is a non-zero finitely generated R-submodule of K.*

While any ideal of R is a fractional R-ideal, a fractional ideal is more general than an ideal since its elements need not be in R, but may be in its field of fractions. The ring R is itself a fractional R-ideal, called the **trivial ideal**.

Beginning with an irreducible polynomial f, we let $K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$. For the purposes of Taussky's bijection, we are concerned with $\mathbb{Z}[\alpha]$-fractional ideals of the field K. It is easy to see that $\mathbb{Z}[\alpha]$ is a free $\mathbb{Z}$-module of rank $n = [K : Q]$ since it has $\mathbb{Z}$-basis $\{1, \alpha, ..., \alpha^{n-1}\}$. Considering any fractional $\mathbb{Z}[\alpha]$-ideal I as a $\mathbb{Z}$-module, it follows that I is also free of rank n.

Definition 1.1.2. *We say fractional R-ideals I and J are **equivalent** if there exists an element $k \in K = Frac(R)$ such that $kI = J$. The **ideal class** of a fractional ideal I is the equivalence class of I under the equivalence of fractional ideals.*

This notion of ideal class equivalence is the same as R-module isomorphism [5]. For each fractional ideal class, one can clear denominators of a basis of a given representative to find a representative which is an R-ideal.

Under the operation induced by ideal multiplication of the representatives, the set of fractional ideal classes form a monoid with the trivial ideal R as identity. We now discuss those ideal classes which are invertible.

Theorem 1.1.3. *For a ring R, the invertible fractional ideal classes form a group called the **Picard group of** R and denoted by Pic(R). This group is finite. Of particular importance is Pic$(\mathcal{O}_K)$, where $\mathcal{O}_K$ is the ring of integers of a field K. In this case, Pic$(\mathcal{O}_K)$ is called the **ideal class group of** K, and its order is called the **class number of** K.*

Since we will be concerned with fractional $\mathbb{Z}[\alpha]$-ideals, we must take care when $\mathbb{Z}[\alpha]$ is a proper subring of $\mathcal{O}_K$. Since $\mathcal{O}_K$ is also a $\mathbb{Z}[\alpha]$-ideal, the set of all $\mathbb{Z}[\alpha]$-ideals will contain at least the elements of Pic$(\mathbb{Z}[\alpha])$ and Pic$(\mathcal{O}_K)$ when $\mathbb{Z}[\alpha] \subsetneq \mathcal{O}_K$. We will return to a discussion of this subtlety when we discuss the more general case of square-free characteristic polynomial. For now, let us denote the set of fractional $\mathbb{Z}[\alpha]$-ideals in $\mathbb{Q}(\alpha)$ by $\mathcal{I}(\alpha)$.

We now describe Taussky's bijection, which provides more detail to Latimer and MacDuffee's correspondence.

Let $\varphi : \mathcal{I}(\alpha)/_{\cong \mathbb{Z}[\alpha]} \to \mathcal{M}_f/_{\sim \mathbb{Z}}$ be defined in the following way. For a fractional $\mathbb{Z}[\alpha]$-ideal class, pick a representative I and a $\mathbb{Z}$-basis $\{w_1, .., w_n\}$ of I. Define $\varphi([I]) = [A]$ where A is the multiplication-by-α matrix with respect to this $\mathbb{Z}$-basis. One may show that φ does not depend on the choice of representative or $\mathbb{Z}$-basis.

Theorem 1.1.4. ***(Latimer and MacDuffee, Taussky)** [21], [32]*
Let $f \in \mathbb{Z}[x]$ be an irreducible monic polynomial of degree n and root α. Then there is a one-to-one correspondence between the $\mathbb{Z}$-conjugacy classes of matrices within $\mathcal{M}_f$ and classes of fractional ideals in $\mathcal{I}(\alpha)$. Furthermore, the map φ defined above gives this bijection.

Taussky showed that φ is an injective map and that for $A = (a_{ij}) \in \mathcal{M}_f$, the inverse image of $[A]$ can be found as follows. Let $\mathbf{w} = (w_1, ..., w_n)^t$ be an eigenvector of A with eigenvalue α and let $I = w_1\mathbb{Z} \oplus ... \oplus w_n\mathbb{Z}$. Since $\alpha\mathbf{w} = A\mathbf{w}$, we have that $\alpha w_i = \sum_{j=1}^{n} a_{i,j} w_j \in I$, and so I is a fractional $\mathbb{Z}[\alpha]$-ideal.

We now illustrate in an example how to use Taussky's bijection to obtain information about $\mathrm{GL}_n(\mathbb{Z})$-conjugacy. Using Magma, we may obtain $\mathbb{Z}$-bases for representatives of the $\mathbb{Z}[\alpha]$-ideal classes. From there, it is straightforward to compute the matrix which represents multiplication-by-α with respect to this $\mathbb{Z}$-basis and list the representatives of the $\mathrm{GL}_n(\mathbb{Z})$-conjugacy classes.

Example 1.1.5. *Let $f = x^2 - 10$. The number field $K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$ has class number 2. In this case, $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and $\mathcal{I}(\alpha) = Pic(\mathcal{O}_K)$, the ideal class group. In Magma, we find that $\mathbb{Z}[\alpha] = 1\mathbb{Z} \oplus \alpha\mathbb{Z}$ and the non-principal fractional ideal $2\mathbb{Z} \oplus \alpha\mathbb{Z}$ are representatives for the elements in $Pic(\mathcal{O}_K)$.*

We obtain representatives for the $GL_2(\mathbb{Q})$-conjugacy classes by computing the multiplication-by-α matrices. We have

$$\begin{aligned} \alpha \cdot 1 &= 0 \cdot 1 + 1 \cdot \alpha \\ \alpha^2 &= 10 \cdot 1 + 0 \cdot \alpha \end{aligned}$$

and

$$\begin{aligned} \alpha \cdot 2 &= 0 \cdot 2 + 2 \cdot \alpha \\ \alpha^2 &= 5 \cdot 2 + 0 \cdot \alpha. \end{aligned}$$

Thus, the $GL_2(\mathbb{Z})$-conjugacy classes of matrices within $\mathcal{M}_f$ for $f = x^2 - 10$ are given by the set of representatives

$$\left\{ \begin{pmatrix} 0 & 1 \\ 10 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 5 & 0 \end{pmatrix} \right\}.$$

In the previous example, one of the matrix representatives is the transpose of the companion matrix of $f = x^2 + 10$. It is easy to check that under Taussky's bijection, $\mathbb{Z}[\alpha]$ always corresponds to $\mathcal{C}_f^t$. This is because $(1, \alpha, ..., \alpha^{n-1})^t$ is an eigenvector of $\mathcal{C}_f^t$ with eigenvalue α.

1.1.2 A generalization to square-free characteristic polynomial

We now discuss Marseglia's generalization of the previous correspondence to matrices with square-free characteristic polynomial [24]. In order to state the generalized correspondence, we introduce some preliminary definitions, following Marseglia's notational conventions.

We will now consider $\mathbb{Z}$-conjugacy of matrices with characteristic polynomial $f = \prod_{i=1}^{m} f_i$. For the remainder of the chapter, we will let K denote the corresponding finite-dimensional $\mathbb{Q}$-algebra $K = \prod_{i=1}^{m} K_i$ where $K_i = \mathbb{Q}[x]/(f_i)$. If α_i denotes a root of f_i, then each K_i is isomorphic to the number field $\mathbb{Q}(\alpha_i)$. Operations in this $\mathbb{Q}$-algebra include componentwise addition and multiplication, and $\mathbb{Q}$ acts on an element of K by scalar multiplication.

Definition 1.1.6. *[24]*

*Let K be a $\mathbb{Q}$-algebra. An **order in** K, or a K-**order** is a commutative subring of K with unity which has no non-zero nilpotent elements, and which is a finitely generated $\mathbb{Z}$-module.*

We will describe some K-orders of interest. First, recall that an element is called an **algebraic integer** if it is a root of a monic polynomial with coefficients in $\mathbb{Z}$. An algebraic integer in $K = \prod_{i=1}^{m} \mathbb{Q}(\alpha_i)$ is an element of the form $(r_1, .., r_m)$ such that $(p(r_1), .., p(r_m)) = (0, ..., 0)$ for some polynomial $p(x) \in \mathbb{Z}[x]$.

Let $\mathcal{O}_K$ denote the ring of algebraic integers of K. This is the maximal order in K with respect to inclusion. In the case that $K = \prod K_i$, we have that $\mathcal{O}_K = \prod \mathcal{O}_{K_i}$ where $\mathcal{O}_{K_i}$ is the ring of integers of K_i [24].

We denote another important K-order by $\mathbb{Z}[\alpha]$ where $\alpha = (\alpha_1, ...\alpha_m)$. We define $\mathbb{Z}[\alpha]$ by

$$\mathbb{Z}[\alpha] = \{(z_1 + z_2\alpha_1 + ... + z_n\alpha_1^{1-n}, ..., z_1 + z_2\alpha_m + ... + z_n\alpha_m^{1-n}) : z_i \in \mathbb{Z}\}.$$

Identifying an element $z \in \mathbb{Z}$ with the constant tuple $(z, ..., z)$ in K, we see that the above coincides with the usual definition of $\mathbb{Z}[\alpha]$.

It is clear that $\mathbb{Z}[\alpha] \subseteq \mathcal{O}_K$ since α and all integral polynomials in α are algebraic integers. A non-maximal order cannot always be written as a product of orders in each of the fields K_i. Husert [18] provides the following example of a K-order that is not a product of K_i-orders.

Example 1.1.7. *Consider $f(x) = (x+1)(x^2+1)$, which is associated to the $\mathbb{Q}$-algebra $K = \mathbb{Q} \times \mathbb{Q}(i)$. Then $\alpha = (-1, i)$ and $\mathbb{Z}[\alpha] = \{(x-y, x+iy) : x, y \in \mathbb{Z}\}$. This order is not equal to $\mathbb{Z} \times \mathbb{Z}[i]$, nor is it a product of K_i-orders. To see this, note that $(0,1) \notin \mathbb{Z}[\alpha]$ since $(0,1)$ cannot be expressed as $(x-y, x+iy)$ for integers x and y. Since every K_i-order contains unity, $\mathbb{Z}[\alpha]$ cannot be a product of K_i-orders.*

The ring of integers of K is the product $\mathbb{Z} \times \mathbb{Z}[i]$. In this case, we have $\mathbb{Z}[(1,i)] \subsetneq \mathbb{Z} \times \mathbb{Z}[i]$.

This observation hints at the fact that when $\mathbb{Z}[\alpha]$ is a proper subring of $\mathcal{O}_K$, the generalized correspondence is not as straightforward as building up from the irreducible case.

In general, there can be other intermediate rings between $\mathbb{Z}[\alpha]$ and $\mathcal{O}_K$. Any ring R satisfying $\mathbb{Z}[\alpha] \subseteq R \subseteq \mathcal{O}_K$ is called an **over-order** of $\mathbb{Z}[\alpha]$.

For any over-order R of $\mathbb{Z}[\alpha]$, a **fractional R-ideal** is an R-module which is a free $\mathbb{Z}$-module of rank n. Writing an R-ideal I with respect to a $\mathbb{Z}$-basis $\{v_i\}$, we have $I = \bigoplus_{i=1}^{n} v_i\mathbb{Z}$. Here, the v_i are m-tuples since I is an object within the algebra $\prod_{i=1}^{m} K_i$. As before, fractional R-ideals I and J are in the same equivalence classes if they are isomorphic as R-modules.

In the irreducible case, we noted that fractional ideals are equivalent if one fractional ideal is a scalar multiple of the other. When K is a product of number fields, the only difference is that we must avoid zero-divisors. In other words, we say I and J are equivalent if $I = kJ$ for a non-zero-divisor $k \in K$. Again, let us denote the set of all fractional $\mathbb{Z}[\alpha]$-ideals by $\mathcal{I}(\alpha)$. This set is finite, and we denote its order by $\#\mathcal{I}(\alpha)$.

In the case that $R = \mathcal{O}_K$, the maximal order in K with respect to inclusion, all of the R-ideals are invertible and so the set of R-ideal classes forms a group, which we also denote by $\mathrm{Pic}(\mathcal{O}_K)$ [24]. It is known that for $K = \prod K_i$, we have $\mathrm{Pic}(\mathcal{O}_K) = \prod \mathrm{Pic}(\mathcal{O}_{K_i})$ [29].

For any over-order R of $\mathbb{Z}[\alpha]$, the set of invertible R-ideal classes forms a finite group with identity R, which we denote by $\text{Pic}(R)$. The class number of K divides the order $\text{Pic}(R)$ because the map

$$\text{Pic}(R) \to \text{Pic}(\mathcal{O}_K)$$
$$I \mapsto I\mathcal{O}_K$$

is surjective (see Corollary 2.1.11. of [9]).

Lemma 3.6 of [24] asserts that $\mathcal{I}(\alpha) \supseteq \bigsqcup \text{Pic}(R)$ where R ranges over the over-orders of $\mathbb{Z}[\alpha]$. According to Proposition 3.7 of [24], if $\mathcal{O}_K/\mathbb{Z}[\alpha]$ is cyclic, meaning that $\mathcal{O}_K = \mathbb{Z}[\alpha] + x\mathbb{Z}[\alpha]$ for some $x \in \mathcal{O}_K$, then $\mathcal{I}(\alpha) = \bigsqcup \text{Pic}(R)$. For instance $\mathcal{O}_K/\mathbb{Z}$ is cyclic whenever f is quadratic, and so in this case, each $\mathbb{Z}[\alpha]$-ideal lies in $\text{Pic}(R)$ for some over-order R.

In general, $\mathcal{I}(\alpha)$ need not only consist of invertible fractional ideals. Marseglia provided an algorithm for computing $\mathcal{I}(\alpha)$, which he refers to as the ideal class monoid and denotes by ICM(R) [24]. This is a new contribution because previously it was only known how to compute the invertible fractional ideals [24].

We may now discuss Marseglia's bijection, which generalizes Taussky's bijection and which makes the Latimer and MacDuffee correspondence more concrete.

For f square-free, we define the map $\varphi : \mathcal{I}(\alpha)/_{\sim_{\mathbb{Z}[\alpha]}} \to \mathcal{M}_f/_{\sim_{\mathbb{Z}}}$ in the same way as in Taussky's bijection. In other words, $\varphi([I]) = [A]$ where A is the multiplication-by-α matrix with respect to some $\mathbb{Z}$-basis for I.

Theorem 1.1.8. *(Latimer and MacDuffee, Marseglia) [21], [24]*
Let $f(x) = \prod_{i=1}^{m} f_i \in \mathbb{Z}[x]$ *be a square-free polynomial. Let* $\alpha = (\alpha_1, ..., \alpha_m)$ *denote the tuple of roots of the irreducible factors. Then there is a one-to-one correspondence between the integer similarity classes of matrices in* $\mathcal{M}_f$ *and elements in* $\mathcal{I}(\alpha)$*. Furthermore, the map* φ *defined above gives this bijection.*

There are some subtleties in the proof that arise from the fact that elements in $\mathcal{I}(\alpha)$ are m-tuples. For instance, finding $\varphi^{-1}([A])$ for $A \in \mathcal{M}_f$ is a little more involved than in Taussky's bijection. We must find eigenvectors v_i corresponding to α_i for $i = 1, ..., m$. If $v_i = (v_{1i}, v_{2i}, ..., v_{ni})^t$, then the inverse image of $[A]$ is $\varphi^{-1}([A]) = (v_{11}, ..., v_{1m})\mathbb{Z} \oplus ... \oplus (v_{n1}, ..., v_{nm})\mathbb{Z}$ [24].

Together with Marseglia's algorithms for computing $\mathcal{I}(\alpha)$, Theorem 1.1.8 provides a way of obtaining the conjugacy classes for matrices in the square-free case. Marseglia implemented an algorithm in Magma [2] which uses this correspondence to compute $\mathrm{GL}_n(\mathbb{Z})$-conjugacy classes for matrices in $\mathcal{M}_f$ for f square-free [24].

As mentioned before, when the order $\mathbb{Z}[\alpha]$ is not maximal, then not all elements in $\mathcal{I}(\alpha)$ can be expressed as a product of elements in $\mathcal{I}(\alpha_i)$. We illustrate how this is related to block-diagonalization of matrices in the next example.

Example 1.1.9. *Consider matrices with square-free characteristic polynomial $f = f_1 f_2$ where $f_1 = x^2 + 4x + 7$ and $f_2 = x^3 - 9x^2 - 3x - 1$. Let α_i denote the root of f_i, $R = \mathbb{Z}[(\alpha_1, \alpha_2)]$, and $R_i = \mathbb{Z}[\alpha_i]$. The orders R_i are not maximal in K_i. We have that $R \subset R_1 \times R_2 \subsetneq \mathcal{O}_{K_1} \times \mathcal{O}_{K_2} = \mathcal{O}_K$. Since $R = \mathbb{Z}[(\alpha_1, \alpha_2)]$ is not maximal, R is not necessarily a product of orders in the K_i.*

One can compute that $\#\mathcal{I}(\alpha_1) = 2$ and $\#\mathcal{I}(\alpha_2) = 6$. If R could be written as a product of orders, then there would be 12 R-ideal classes. In this situation, we could write the representatives of the $GL_5(\mathbb{Z})$-conjugacy classes as block-diagonal matrices with blocks in $\mathcal{M}_{f_i}$. However, we will see that not every matrix is $\mathbb{Z}$-conjugate to such a block-diagonal matrix.

Consider $A = \begin{pmatrix} -1 & 2 & 3 & 2 & 4 \\ -2 & -3 & 0 & 0 & -4 \\ 0 & 0 & 0 & -1 & -4 \\ 0 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 2 & 9 \end{pmatrix}$, *which has characteristic polynomial f.*

To attempt to block-diagonalize A, we compute the A-invariant $\mathbb{Z}$-modules $N_i :=$ Null$(f_i(A))$. If the union of the N_i span $\mathbb{Z}^5$, then the basis elements of the N_i may be used to create a change of basis matrix which block-diagonalizes A.

We find that $N_1 = Null(f_1(A))$ *has* $\mathbb{Z}$*-basis* $\{(1,0,0,0,0)^t, (0,-1,0,0,0)^t\}$ *and* N_2 *has* $\mathbb{Z}$*-basis* $\{(6,-1,-10,0,8)^t, (1,0,1,1-2)^t, (-1,0,-2,0,2)^t\}$.

The matrix with these basis elements as columns has determinant -4*. Thus,* A *is not* $\mathbb{Z}$*-conjugate to a block-diagonal matrix. Then there are more than the 12* R*-ideal classes which we can build up from the irreducible case, meaning that* R *is not a product of orders in* K_i*.*

Marseglia computed that there are 852 R*-ideal classes and, thus, 852* $GL_5(\mathbb{Z})$*-conjugacy classes within* $\mathcal{M}_f$*.*

Note that Eick, Hofmann, and O'Brien [11] also developed an algorithm for computing the $\mathrm{GL}_n(\mathbb{Z})$-conjugacy classes of integral matrices. Their algorithm is based on ideas suggested by Grunewald in [16]. Instead of using the Latimer and MacDuffee correspondence, the algorithm given in [11] relies on isomorphism-testing of certain submodules.

These algorithms can be used to efficiently compute conjugacy classes in many but not all cases. It seems that the complexity of these algorithms is exponential (for more discussion on this, see section 5.1.2). One potential difficulty is computing the ideal class group in a number field, for instance when the discriminant of the minimal polynomial is very large [11]. Another obstacle arises if the number of submodules which may need to be constructed is very large [11]. The algorithm in [11] is more general than in [24] since it applies to matrices with non-square-free characteristic polynomial, but the algorithm in [24] had a shorter running time in the square-free case in several examples (see Table 3 of [24]).

1.2 Connections to local conjugacy

While the previous results answer the integer conjugacy problem to a large extent, computations can still be unwieldy. We will therefore discuss conjugacy over various local rings and how this is connected to integer conjugacy. For instance, one may reduce a matrix modulo a prime p and work with conjugacy over $\mathbb{F}_p$, the finite field of order p. If there is a matrix $C \in \mathrm{GL}_n(\mathbb{Z})$ which conjugates A to B, then this means that $AC = CB$ with $\det(C) = \pm 1$. Then if A and B are integrally similar, their reductions modulo any prime p are similar over $\mathbb{F}_p$.

A quick way to see that matrices are *not* integrally conjugate is to show that they have different rational canonical forms over $\mathbb{F}_p$ for some prime p. If we have fixed a prime p, we will write $\overline{A}$ to indicate the reduction of the integral matrix A modulo p.

Example 1.2.1. *Consider* $A = \begin{pmatrix} -1 & 3 \\ 3 & -10 \end{pmatrix}$ *and* $B = \begin{pmatrix} 0 & -1 \\ 1 & -11 \end{pmatrix}$, *which have irreducible characteristic polynomial* $x^2 + 11x + 1$. *Since* A *and* B *share the same irreducible characteristic polynomial, they are rationally conjugate. In fact,* $C = \begin{pmatrix} 0 & 3 \\ 1 & -10 \end{pmatrix} \in GL_2(\mathbb{Q})$ *conjugates* A *to* B. *Note that* B *is the rational canonical form of* A.

Since $3 \mid det(C)$, *reducing* C *modulo any prime* p *besides 3 yields a conjugating matrix in* $\mathbb{F}_p$. *We must still consider* $p = 3$. *Reducing modulo 3, we get* $\overline{A} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ *and* $\overline{B} = \begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix}$. *Since* $\overline{A}$ *is a scalar matrix, it is not conjugate to* $\overline{B}$ *over* $\mathbb{F}_3$. *Thus,* A *and* B *are not integrally conjugate.*

Since the characteristic polynomial factors as $(x + 1)^2$ *over* $\mathbb{F}_3$, *we no longer have just one possible rational canonical form. Actually,* $\overline{A}$ *and* $\overline{B}$ *give the two distinct rational canonical forms of matrices with characteristic polynomial* f *over* $\mathbb{F}_3$. *This tells us that are at least two different* $GL_2(\mathbb{Z})$*-conjugacy classes.*

While integral conjugacy implies $\mathbb{F}_p$-conjugacy for all primes p, the converse does not hold, as we see in the following example from [25].

Example 1.2.2. *The following is an example of matrices which are* $\mathbb{F}_p$*-conjugate for every prime* p *but are not* $\mathbb{Z}$*-conjugate.*

Consider the matrices $A = \begin{pmatrix} 0 & -6 \\ 1 & 0 \end{pmatrix}$ *and* $B = \begin{pmatrix} 0 & 2 \\ -3 & 0 \end{pmatrix}$, *which have characteristic polynomial* $x^2 + 6$.

The matrix $C_1 = \begin{pmatrix} -3 & 0 \\ 0 & 1 \end{pmatrix}$ *conjugates* A *to* B *and satisfies det*$(C_1) \notin (2)$. *Then* C_1 *conjugates* $\overline{A}$ *to* $\overline{B}$ *over* $\mathbb{F}_p$ *for all primes* $p \neq 2$.

On the other hand, the matrix $C_2 = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$ *conjugates* A *to* B *and has det*$(C_2) \notin (3)$. *Then* $A \sim B$ *over* $\mathbb{F}_p$ *for all primes* p.

However, if there were a conjugating matrix $C = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *in* $GL_2(\mathbb{Z})$, *it would have to satisfy the system*

$$a = -3d$$

$$b = 2c$$

$$ad - bc = \pm 1,$$

which is equivalent to satisfying $2c^2 + 3d^2 = 1$. *Clearly, this equation has no integer solution. Thus,* A *and* B *are not* $GL_2(\mathbb{Z})$*-conjugate.*

Perhaps the previous example is not very surprising, for if there is a matrix C satisfying $AC = CB$ and $\det(C) = \pm 1$, then these equations hold modulo any *power* of p. Then a natural question to ask is whether $\mathbb{Z}_p$-conjugacy for every prime p implies integral conjugacy. We explore $\mathbb{Z}_p$-conjugacy and consider this question more in the next chapter.

In Chapter 2, we discuss a theorem of Guralnick, which tells us that if A and B are conjugate over $\mathbb{Z}_p$ for every prime p, then they are conjugate over some integral extension of $\mathbb{Z}$ [17]. This result is an existence theorem, as it is based on a non-constructive method by Dade outlined in [7]. We will refer to the question of determining this extension as the **conjugacy extension problem**. The focus of the remainder of the thesis is to make contributions to solving this problem.

In Chapter 3, we disucss Dade's method for how one might obtain the extension as in Guralnick's theorem. As we will see, the method can result in an extension of larger degree than we

would like. We also discuss quadratic forms as a way to approach the conjugacy extension problem for two-by-two matrices.

We generalize the Latimer and MacDuffee correspondence to apply to conjugacy over integral domains in Chapter 4. This is helpful in solving the conjugacy extension problem since it allows us to translate the question of conjugacy over an algebra extension to a question about an extension of ideals.

In Chapter 5, we outline how the generalized correspondence can be used to give an algorithm for testing whether matrices are conjugate over a given extension. We were able to implement an algorithm for matrices in $\mathcal{M}_f$ for f irreducible, but some obstacles arise in the square-free case when considering conjugacy over an extension. We also provide a method which makes use of class fields in searching for extensions over which matrices are conjugate.

We summarize our results in Chapter 6 and provide some examples in which the method with class fields worked. We show that the Hilbert class field does not necessarily answer the conjugacy extension problem, so we also list some open problems.

Chapter 2

Local conjugacy

The Hasse principle, or the local-global principle, is a philosophy in mathematics which says that global information can be obtained from local information at every prime (see Chapter VI of [26]). In other words, the idea of the Hasse principle is that if a property holds modulo all powers of p for every prime p, then the property should hold in characteristic 0. It is desirable, but not guaranteed, that the local-global principle holds, since it is typically easier to work locally and since usually only finitely many primes need to be considered.

In this chapter, we will consider conjugacy over the ring $\mathbb{Z}/p^a\mathbb{Z}$ for a natural number a. For a fixed prime p, one may consider conjugacy for all such rings as a ranges over $\mathbb{N}$ by studying conjugacy over $\mathbb{Z}_p$, the ring of p-adic integers. We will see that $\mathbb{Z}_p$-conjugacy is equivalent to $\mathbb{Z}_{(p)}$-conjugacy, where $\mathbb{Z}_{(p)}$ denotes the localization of $\mathbb{Z}$ at (p). We will refer to conjugacy over $\mathbb{Z}_p$ or $\mathbb{Z}_{(p)}$ as **local conjugacy**. In this section, we explore the relationship between local conjugacy and conjugacy over $\mathbb{Z}$.

Fix a prime p and let R be one of aforementioned rings. For $A, B \in \mathbb{Z}^{n\times n}$, we are concerned with solutions $V \in R^{n\times n}$ to

$$AV = VB \text{ with } \det(V) \notin (p). \tag{2.1}$$

Here, we identify A and B as having entries in the appropriate ring through embedding or by reducing modulo p^a. We will say that (2.1) has a solution over R if there is a $V \in R^{n\times n}$ satisfying (2.1). Note that having a solution to (2.1) when $R = \mathbb{Z}$ does *not* imply that $V \in \mathrm{GL}_n(\mathbb{Z})$ since we only require $\det(V) \notin (p)$ and so V^{-1} is not necessarily integral. We have rewritten $V^{-1}AV = B$ as $AV = VB$ to make more clear that when V is a solution over $\mathbb{Z}$ to (2.1), it not necessarily an element of $\mathrm{GL}_n(\mathbb{Z})$ which conjugates A to B. However, having a solution V to (2.1) over the other rings implies that $V \in \mathrm{GL}_n(R)$.

We wish to explore the ways in which the existence of solutions to over these different rings are related. For instance, it is easy to see that there is a solution over $\mathbb{Z}_{(p)}$ iff there exists a solution over $\mathbb{Z}$. You can clear denominators of the solution over the localization, and you will still have a determinant not in (p). Of course, the converse holds as a solution over $\mathbb{Z}$ yields a solution over $\mathbb{Z}_{(p)}$, since $\mathbb{Z}$ naturally embeds in the localization.

We may also consider solutions over $\mathbb{Z}_p$ in relation to solutions over $\mathbb{Z}/p^a\mathbb{Z}$. One could either think of a matrix in $\mathbb{Z}_p^{n\times n}$ as having entries which are infinite tuples or by considering an infinite sequence of matrices defined over the rings $\mathbb{Z}/p^a\mathbb{Z}$ as a ranges through $\mathbb{N}$. Since the components of an element in $\mathbb{Z}_p$ must satisfy some compatibility requirements, the sequence of matrices must do so also.

Definition 2.0.1. *We define a **sequence of lifts for (2.1)** to be a sequence $\{C_1, C_2, ..., C_a, ...\}$ such that C_a is a solution to (2.1) for $R = \mathbb{Z}/p^a\mathbb{Z}$ and C_{a+1} (mod p^a) $\equiv C_a$. We say that C_{a+1} is a **lift** of C_a.*

Definition 2.0.2. *We say that A and B are p**-adically conjugate** if there is a matrix in $\mathbb{Z}_p^{n\times n}$ which conjugates A to B. This is equivalent to there being a sequence of lifts for (2.1).*

Before discussing the relationships among conjugacy over these various rings, we describe a method for lifting solutions.

2.1 Lifting conjugating matrices

Suppose $C_{p^a} \in \mathbb{Z}^{n\times n}$ is a solution to $AC \equiv CB \pmod{p^a}$ with $\det(C_{p^a}) \notin (p)$. Then C_{p^a} conjugates A to B over $\mathbb{Z}/p^a\mathbb{Z}^\times$. Note that this means that $AC_{p^a} - C_{p^a}B = p^aD$ for some $D \in \mathbb{Z}^{n\times n}$.

We wish to lift, if possible, C_{p^a} to a matrix, call it $C_{p^{a+1}}$, which conjugates A to B over $\mathbb{Z}/p^{a+1}\mathbb{Z}$. Such a lift must satisfy $C_{p^{a+1}} \equiv C_{p^a} \pmod{p^a}$, so we know that $C_{p^{a+1}}$ is of the form $C_{p^a} + p^aX$ for some $X \in \mathbb{Z}^{n\times n}$.

If such a lift $C_{p^{a+1}}$ were to exist, we would have that $AC_{p^{a+1}} - C_{p^{a+1}}B = p^{a+1}Y$ for some $Y \in \mathbb{Z}^{n\times n}$, so that

$$\begin{aligned} p^{a+1}Y &= AC_{p^{a+1}} - C_{p^{a+1}}B \\ &= A(C_{p^a} + p^aX) - (C_{p^a} + p^aX)B \\ &= AC_{p^a} - C_{p^a}B + p^a(AX - XB) \\ &= p^aD + p^a(AX - XB), \end{aligned}$$

from which we obtain

$$pY = D + (AX - XB).$$

In order to find a lift, we must find an $X \in \mathbb{Z}^{n\times n}$ with $AX - XB \equiv -D \pmod p$. Since we are assuming that $\det(C_{p^a}) \notin (p)$, we will still have that $\det(C_{p^{a+1}}) \notin (p)$. Thus, obtaining a lift comes down to solving a linear system over $\mathbb{F}_p$. We implemented this lifting algorithm in GAP [15].

Lifts do not necessarily exist, even for matrices which are integrally conjugate, as seen in the next example.

Example 2.1.1. *Let* $A = \begin{pmatrix} -1 & 3 \\ 3 & -10 \end{pmatrix}$ *and* $B = \begin{pmatrix} 11 & 3 \\ -81 & -22 \end{pmatrix}$.

These matrices have irreducible characteristic polynomial $x^2 + 11x + 1$. *Since* $A \equiv B$ *modulo 3, we have that* $C_3 = I$ *conjugates* A *to* B *over* $\mathbb{F}_3$.

If we wish to find C_9, *a lift of* C_3 *to* $\mathbb{Z}/9\mathbb{Z}$, *we must solve the equation*

$$AX - XB \equiv -D \text{ (mod } 3)$$

where

$$D = \frac{1}{3}(AC_3 - C_3B) = \begin{pmatrix} -4 & 0 \\ 28 & 4 \end{pmatrix}.$$

We may describe the linear transformation $X \mapsto AX - XB$ by the four-by-four matrix

$$T = \begin{pmatrix} -12 & 81 & 3 & 0 \\ -3 & 21 & 0 & 3 \\ 3 & 0 & -21 & 81 \\ 0 & 3 & -3 & 12 \end{pmatrix}.$$

Then solving Equation 2.2 is equivalent to solving $T\boldsymbol{x} = (4, 0, -28, -4)^t \equiv (1, 0, 2, 2)^t$ (modulo 3). There is no solution since T is equivalent to the zero matrix modulo 3, so the identity matrix has no lift in $\mathbb{Z}/9\mathbb{Z}$.

This does not mean that A and B are not conjugate modulo 9. The matrices A and B are actually $GL_2(\mathbb{Z})$-conjugate with conjugating matrix $C = \begin{pmatrix} -7 & -1 \\ -1 & 0 \end{pmatrix}$. Reducing C modulo 3^a yields a chain of lifts.

We now discuss how conjugacy over the localization, $\mathbb{Z}_{(p)}$, and the p-adic integers, $\mathbb{Z}_p$, are related.

Lemma 2.1.2. *If V is a solution over the localization $\mathbb{Z}_{(p)}$, then defining $C_a := V$ (mod p^a) yields a chain of lifts $\{C_1, .., C_a, ...\}$. Thus a solution over $\mathbb{Z}_{(p)}$ implies a solution over $\mathbb{Z}_p$.*

Remark: A straightforward way to justify the lemma is to note that $\mathbb{Z}_p$ is the completion of $\mathbb{Z}_{(p)}$ with respect to the p-adic norm. In the next proof, we take a different perspective and more concretely show that an element in the localization corresponds to a sequence of lifts in the rings $\mathbb{Z}/p^a\mathbb{Z}$.

Proof:

Let $\frac{a}{b}$ be an entry in lowest terms of a solution V to (2.1) over $\mathbb{Z}_{(p)}$. We discuss how to lift this entry, since the matrix can be lifted componentwise. We have that $\frac{a}{b} \notin \mathbb{Z}_{(p)}$ so that $p \nmid b$. Then $(b, p^i) = 1$ for any $i \in \mathbb{N}$, implying that $b \in \mathbb{Z}/p^i\mathbb{Z}^\times$. Then there is a unique solution x_i to $bx_i = a$ in $\mathbb{Z}/p^i\mathbb{Z}^\times$. The corresponding entry to $\frac{a}{b}$ in C_i is x_i.

We now show $x_{i+1} (\text{mod } p^i) \equiv x_i$ to prove that we get a chain of lifts. We have $bx_{i+1} - a = p^{(i+1)}k$. Let $x_{i+1} (\text{mod } p^i) = r$ where $x_{i+1} = p^i q + r$. To show $r = x_i$, we have

$$\begin{aligned} bx_{i+1} - a &= p^{(i+1)}k \\ b(p^i q + r) - a &= p^{(i+1)}k \\ br - a &= p^{(i+1)}k - bp^i q \\ br - a &= p^i(pk - bq) \end{aligned}$$

Then $br \equiv a \ (\text{mod } p^i)$, but we said that x_i is the unique solution, so $x_{i+1} \ (\text{mod } p^i) = r = x_i$.

□

One may ask whether the converse of Lemma 2.1.2 holds. In other words, is it true that having a solution over over $\mathbb{Z}_p$ will imply a solution over $\mathbb{Z}_{(p)}$? The converse follows from a result of Guralnick [17]. We first need a lemma.

Lemma 2.1.3. *(See Lemma 3 in [17].)*
Let $T : \mathbb{Z}^n \to \mathbb{Z}^n$ a linear map with rank r, and denote the image of T by Im(T). Fix a prime p. Pick $a \in \mathbb{N}$ such that there exists an $r \times r$ minor of T with determinant not in (p^a). Then the chosen a satisfies $p^a\mathbb{Z}^n \cap$ Im$(T) \subseteq p$Im(T).

The proof follows from the Artin-Rees lemma (see page 255 of [35]). In the proof of Proposition 2.2.4, we will show the details for proving this inclusion when $a = 1$ for a particular linear map and for certain primes.

The next theorem is stated more generally as Theorem 4 in [17]. We may restate the theorem and apply it to our situation since $\mathbb{Z}_{(p)}$ is a principal ideal domain.

Theorem 2.1.4. *[17] There exists an $a \in \mathbb{N}$ such that (2.1) has a solution over $\mathbb{Z}/p^a\mathbb{Z}$ if and only if (2.1) has a solution over $\mathbb{Z}$.*

Proof:

A solution over $\mathbb{Z}$ may be reduced modulo p^a to get a solution over $\mathbb{Z}/p^a\mathbb{Z}$.

For the other direction, identify A and B as vectors of length n^2 and consider the linear map $T(X) = AX - XB$ as an $n^2 \times n^2$ matrix C with rank r. Taking an $r \times r$ minor of C with non-zero determinant d, you can pick a such that $d \notin p^a$. Then a will satisfy $p^a\mathbb{Z}^{n^2} \cap \text{Im}(T) \subseteq p\text{Im}(T)$ by the previous lemma.

If there is a solution modulo p^a, then $T(X) \in p^a\mathbb{Z}^{n^2}$ and by the previous inclusion, we have $T(X) \in p\text{Im}(T)$. Then $T(X) = T(pY)$ for some $Y \in \mathbb{Z}^{n^2}$. From this, we obtain $T(X - pY) = T(X) - T(pY) = 0$ and $\det(X - pY) \equiv \det X$, which is non-zero modulo p. Thus, $X - pY$ is the solution over $\mathbb{Z}$.

□

As a consequence of this theorem, a solution over $\mathbb{Z}_p$ implies a solution over $\mathbb{Z}$, which then implies a solution over $\mathbb{Z}_{(p)}$. Then, for the most part, solutions over the various rings we considered are equivalent. The exception is that if a' does not satisfy the inclusion in Lemma 2.1.3, then a solution over $\mathbb{Z}/p^{a'}\mathbb{Z}$ need not imply a solution over $\mathbb{Z}$. Remember that a solution V over $\mathbb{Z}$ only required $\det(V) \notin (p)$, and does not mean that V belongs to $\text{GL}_n(\mathbb{Z})$.

2.2 Primes not dividing the discriminant

We will soon discuss to what extent local conjugacy will inform us about conjugacy over $\mathbb{Z}$. First, we provide a result which tells us that we only need to concern ourselves with finitely many primes when considering local conjugacy. Let $A, B \in \mathbb{Z}^{n\times n}$ with square-free characteristic polynomial f. Let p be prime which does not divide the discriminant, $\text{disc}(f)$, i.e., f is square-free modulo p. We will show that for such a p, Equation (2.1) (rewritten below)

$$AV = VB \text{ with } \det(V) \notin (p)$$

has a solution for $R = \mathbb{Z}_p$. This is equivalent to there being a solution over $\mathbb{Z}$ (but not necessarily a solution in $\mathrm{GL}_n(\mathbb{Z})$). Then, when considering local conjugacy for matrices with square-free characteristic polynomial, we only need concern ourselves with the finitely many primes dividing the discriminant.

The proof requires a standard result from linear algebra concerning the rank of the centralizer of a matrix over a field. We will denote the centralizer of A in a field F by $\mathrm{Cent}_F(A)$ and define it by $\mathrm{Cent}_F(A) = \{C \in F^{n\times n} : AC = CA\}$. While this result is well-known, (see for instance page 100 of [30]) we provide the proof for clarity.

Lemma 2.2.1. *Let F be a field and $A \in F^{n\times n}$ with square-free characteristic polynomial over F. Then dim($\mathrm{Cent}_F(A)$) $= n$.*

Proof: Let f denote the characteristic polynomial of A. Assume without loss of generality that A is in its rational canonical form. Since f is square-free, the rational canonical form is the companion matrix of f. Let $\{\mathbf{e}_i\}_{i=1}^n$ denote the standard basis of F^n. Then $A^0\mathbf{e}_1 = \mathbf{e}_1$ and $A^i\mathbf{e}_1 = \mathbf{e}_{1+i}$ for $1 \le i \le n-1$. Then $\{A^i\mathbf{e}_1 : 0 \le i \le n-1\}$ is a basis for F^n.

Now let $B \in \mathrm{Cent}_F(A)$. As $\{A^i\mathbf{e}_1 : 0 \le i \le n-1\}$ is a basis, there exist $\alpha_i \in F$ such that $B\mathbf{e}_1 = \sum_{i=0}^{n-1} \alpha_i A^i\mathbf{e}_1$. Then $B\mathbf{e}_1 = f(A)\mathbf{e}_1$ for $f(x) = \sum \alpha_i x^i$. Since B commutes with A, it also commutes with powers of A. So

$$B(A^i\mathbf{e}_1) = A^iB\mathbf{e}_1 = A^if(A)\mathbf{e}_1 = f(A)(A^i\mathbf{e}_1)$$

for $1 \le i \le n$. Since B and $f(A)$ agree on a basis of F, we have that $B = f(A)$. Thus, $\mathrm{Cent}_F(A) = \{g(A) : g(x) \in F[x]\}$. Finally, this space has dimension n since the minimal polynomial of A has degree n.

□

For a prime p, let A_p denote the image of A modulo p.

Corollary 2.2.2. *Suppose $A \in \mathcal{M}_f$ with f square-free. Let $C_A : \mathbb{Z}^{n^2} \to \mathbb{Z}^{n^2}$ be the linear map given by $C_A(X) = XA - AX$. For a prime p, let $C_{A_p} : (\mathbb{Z}/p\mathbb{Z})^{n^2} \to (\mathbb{Z}/p\mathbb{Z})^{n^2}$ be defined as $C_{A_p}(X) = XA_p - A_pX$. For any prime $p \nmid \mathrm{disc}(f)$, these maps have rank $n^2 - n$.*

Proof:

Pick a prime p with $p \nmid \text{disc}(f)$. Then f is square-free over $\mathbb{F}_p$. In the previous lemma it was shown that $\dim(\text{Cent}_{\mathbb{F}_p}(A)) = n$.

The rank of C_A is at most $n^2 - n$ since $I, A, A^2, ..., A^{n-1}$ are linearly independent elements in the null space of C_A. (If they were linearly dependent, this would contradict that the minimal polynomial has degree n.)

Since C_{A_p} is obtained from C_A by reducing A modulo p, the rank of C_A is at least the rank of C_{A_p}. Thus, C_A and C_{A_p} both have rank $n^2 - n$.

□

Note 2.2.3. *Let $C_{A,B}(X) = XA - BX$. Since A and B have the same characteristic polynomial, they are $GL_n(\mathbb{Q})$-conjugate, so $A = D^{-1}BD$ for some $D \in GL_n(\mathbb{Q})$. Then*

$$\begin{aligned} C_{A,B}(X) &= XA - BX \\ &= (DD^{-1})XA - (DAD^{-1})X \\ &= D((D^{-1}X)A - A(D^{-1}X)) \\ &= DC_A(D^{-1}(X)). \end{aligned}$$

Thus, $C_{A,B} = DC_AD^{-1}$ are similar $\mathbb{Q}$-linear transformations. Then both maps have the same $\mathbb{Q}$-rank (and $\mathbb{Z}$-rank), $n^2 - n$.

One may consider $C_{A,B}$ as an $n^2 \times n^2$ matrix $\mathcal{C}$. Let $\mathcal{P}, \mathcal{Q} \in \text{GL}_{n^2}(\mathbb{Z})$ such that $\mathcal{PCQ} = \mathcal{S}$, the Smith normal form of $\mathcal{C}$. Then $\mathcal{S}_p$ is the Smith normal form of the $n^2 \times n^2$ matrix associated to C_{A_p,B_p}. The Smith normal forms, $\mathcal{S}$ and $\mathcal{S}_p$, also have rank $n^2 - n$ for $p \nmid \text{disc}(f)$.

Proposition 2.2.4. *Let A and B be integral matrices with square-free characteristic polynomial f. For any prime $p \nmid \text{disc}(f)$, A and B are $\mathbb{Z}_p$-conjugate.*

Proof:

Let p be a prime with $p \nmid \text{disc}(f)$. Recall that a p-adic conjugating matrix is equivalent to a sequence of lifts $\{X_1, X_2, ..., X_a, ...\}$ such that X_a is a conjugating matrix over $\mathbb{Z}/p^a\mathbb{Z}$. We may conjugate A_p and B_p over $\text{GL}_n(\mathbb{F}_p)$ to their rational canonical forms. Since f is square-free modulo p, the only possible rational canonical form is the companion matrix of f. Thus, there is one conjugacy class over $\mathbb{F}_p$, meaning there exists a conjugating matrix X_1 over $R = \mathbb{Z}/p\mathbb{Z}$.

Keeping the same notation as before, we have $C_{A,B}(X) = XA - BX$. Since X_1 is a solution to (2.1), we have $C_{A_p,B_p}(X_1) \equiv 0 \pmod{p}$.

We wish to show that $C_{A,B}$ satisfies the inclusion

$$p\mathbb{Z}^{n^2} \cap \text{Im}(C_{A,B}) \subseteq p\text{Im}(C_{A,B}) \tag{2.2}$$

As (2.2) is a statement about submodules of $\mathbb{Z}^{n^2}$, it does not depend on the basis for $\text{Im}(C_{A,B})$.

As before, let $\mathcal{C} \in \mathbb{Z}^{n^2 \times n^2}$ be the matrix associated to $C_{A,B}$ and suppose that $\mathcal{PCQ} = \mathcal{S}$ is the Smith normal form of $\mathcal{C}$. We will define a linear map T which acts as $C_{A,B}$ but with the image written with respect to the $\mathbb{Z}$-basis $\{\mathcal{P}\mathbf{e}_i\}$ of $\mathbb{Z}^{n^2}$. We define $T : \mathbb{Z}^{n^2} \to \mathbb{Z}^{n^2}$ by $T(\mathbf{x}) = \mathcal{P}^{-1}\mathcal{C}\mathbf{x}$ so that $\text{Im}(T) = \text{Span}_{\mathbb{Z}}(T(\mathbf{e}_i)) = \text{Span}_{\mathbb{Z}}(\mathcal{P}^{-1}\mathcal{C}\mathbf{e}_i)$ Then $C_{A,B}$ satisfies (2.2) iff T does.

Now let $S : \mathbb{Z}^{n^2} \to \mathbb{Z}^{n^2}$ be given by $S(\mathbf{x}) := \mathcal{S}\mathbf{x}$. Then $\text{Im}(S) = \text{Span}_{\mathbb{Z}}(\mathcal{S}\mathbf{e}_i) = \text{Span}_{\mathbb{Z}}(\mathcal{P}^{-1}\mathcal{C}\mathcal{Q}^{-1}\mathbf{e}_i)$. Since $\{\mathcal{Q}^{-1}\mathbf{e}_i\}$ is a $\mathbb{Z}$-basis for $\mathbb{Z}^{n^2}$, we have that $\text{Im}(T) = \text{Im}(S)$. Thus, we may simply consider (2.2) for S rather than for $C_{A,B}$.

Say $\mathcal{S} = \text{diag}(s_i)$. Both $\mathcal{S}$ and $\mathcal{S}_p$ have rank $r = n^2 - n$, meaning $p \nmid s_i$ for $1 \leq i \leq r$. Then

$$\begin{aligned} p\mathbb{Z}^{n^2} \cap \text{Im}(S) &= (p\mathbb{Z} \times ... \times p\mathbb{Z}) \cap (s_1\mathbb{Z} \times ... \times s_r\mathbb{Z}) \\ &= \text{LCM}(p, s_1)\mathbb{Z} \times ... \times \text{LCM}(p, s_r)\mathbb{Z} \\ &= ps_1\mathbb{Z} \times ... \times ps_r\mathbb{Z} \qquad (\text{as } p \nmid s_i) \\ &= p\text{Im}(S). \end{aligned}$$

We have shown the inclusion from Lemma 2.1.3 holds for $a = 1$. We now follow Lemma 2.1.4 to lift X_1 to a matrix $X \in \mathbb{Z}^{n\times n}$ satisfying $XA - XB = 0$ with $\det(X) \notin (p)$.

One may reduce X modulo powers of p to obtain a chain of lifts, which may be identified with a conjugating matrix in $\mathbb{Z}_p$.

□

2.3 Failure of the local to global principle

For the rest of the dissertation, we say integral matrices A and B are **locally conjugate** if they are $\mathbb{Z}_p$-conjugate for every prime p. We wish to determine whether locally conjugate matrices are necessarily $\mathbb{Z}$-conjugate.

By the previous result in Proposition 2.2.4, we know that any two matrices sharing the same square-free characteristic polynomial f are $\mathbb{Z}_p$-conjugate for $p \nmid \operatorname{disc}(f)$. Then to determine whether matrices are locally conjugate, we must only check for $\mathbb{Z}_p$-conjugacy for the finitely many primes dividing the discriminant.

In the next example, we return to the matrices from example 1.2.2. We will now not only consider $\mathbb{F}_p$-conjugacy but $\mathbb{Z}_p$-conjugacy for every prime p. We previously saw that the matrices A and B are not $\mathbb{Z}$-conjugate. In this example, we show that they are conjugate over an algebraic extension of $\mathbb{Z}$.

Example 2.3.1. *The matrices* $A = \begin{pmatrix} 0 & -6 \\ 1 & 0 \end{pmatrix}$ *and* $B = \begin{pmatrix} 0 & 2 \\ -3 & 0 \end{pmatrix}$ *with characteristic polynomial* $f = x^2 + 6$ *are not* $\mathbb{Z}$*-conjugate, but are* $\mathbb{F}_p$*-conjugate for every prime* p*.*

Since $\operatorname{disc}(f) = -2^3 \cdot 3$*, Proposition 2.2.4 says that* A *and* B *are* $\mathbb{Z}_p$*-conjugate for* $p \neq 2, 3$*.*

According to Note 2.2.5, because B *is* $\mathbb{F}_p$*-conjugate to the rational canonical form* A *for* $p = 2$ *and* $p = 3$*, we obtain a chain of lifts for every prime. More concretely, we saw that* $C_2 = \begin{pmatrix} -3 & 0 \\ 0 & 1 \end{pmatrix}$ *with* $\det(C_2) \notin (2)$ *and* $C_3 = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$ *with* $\det(C_3) \notin (3)$

are matrices which conjugate A to B. Reducing C_p modulo powers of p yields a sequence of lifts, where each matrix conjugates A to B. Then A and B are locally conjugate matrices.

Recall that in Example 1.2.2, we observed before that a conjugating matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *with determinant* ± 1 *must satisfy*

$$a = -3d \text{ and } b = 2c$$

which means we need

$$-3d^2 - 2c^2 = \pm 1.$$

While this equation has no integer solution, it is easy to notice that taking $c = 1$ *and* $d = i$*, one finds that* $\begin{pmatrix} -3i & 2 \\ 1 & i \end{pmatrix}$ *conjugates A to B and has determinant one.*

This example shows that locally conjugate matrices need not be $\mathbb{Z}$-conjugate. It is no coincidence that we were able to find an algebraic extension of $\mathbb{Z}$ over which A and B in the last example were conjugate. A theorem of Guralnick (see Theorem 7 in [17]) asserts what can be said regarding conjugacy over an algebraic extension of locally conjugate matrices. Rather than stating Guralnick's theorem in full generality, we list a more specific version in Theorem 2.3.3 that is enough for our purposes.

We must first state Theorem 3 of [7], as Theorem 2.3.3 hinges on it.

Theorem 2.3.2. *(Dade) [7]*

Let $f(x_1, ..., x_m)$ be a homogeneous polynomial with relatively prime integral coefficients. Then $f(\alpha_1, .., \alpha_m) = 1$ for suitable algebraic integers $\alpha_1, ...\alpha_m$.

We may now state Guralnick's theorem. We also include the proof found in [17] for completeness.

Theorem 2.3.3. *(Guralnick) [17]*

Let $A, B \in \mathbb{Z}^{n\times n}$. If $A \sim B$ over $\mathbb{Z}_p$ for every prime p, then $A \sim B$ over some finite integral extension E of $\mathbb{Z}$.

Proof: Fix a prime p_0. If one has a solution over $\mathbb{Z}_{p_0}$, one can can obtain a solution $C_0 \in \mathbb{Z}^{n\times n}$ to $AV = VB$ with $\det(V) \notin (p_0)$ by Theorem 2.1.4.

While $\det(V) \notin (p_0)$, the determinant is contained in finitely many prime ideals $(p_1), ..., (p_k)$ of $\mathbb{Z}$. By our assumption, we have that $A \sim B$ over $\mathbb{Z}_{(p_i)}$ for (p_i) with $i \in \{1, ..., k\}$. In other words, we may pick the remaining C_i so that $AC_i = C_iB$ and $\det(C_i) \notin (p_i)$. Then $\{\det(C_i)\}_{i=0,...,k}$ is a set of relatively prime numbers, i.e., there is no prime ideal containing all of these determinants. However, $\langle \det(C_i)\rangle_{i=0,...,k}$ is an ideal in $\mathbb{Z}$. Every proper ideal is contained in a maximal ideal. Since $\langle \det(C_i)\rangle_{i=0,...,k}$ is not contained in any prime ideal, it generates all of $\mathbb{Z}$.

Let $\overline{\mathbb{Z}}$ denote the algebraic closure of $\mathbb{Z}$. Consider the degree n form $f : \overline{\mathbb{Z}}^{k+1} \to \overline{\mathbb{Z}}$ defined by $f(x_0, .., x_k) = \det(x_0C_1 + ... + x_kC_k)$.

In the case that $k = 1$, this is a binary form, and we have by the definition of determinant that $\det(A + B) = \sum_{r=0}^{n} \sum_{\alpha,\beta} (-1)^{s(\alpha)+s(\beta)} \det(A[\alpha \mid \beta]) \det(B(\alpha \mid \beta))$ [23].

Here, α and β are strictly increasing sequences of of length r chosen from $\{1, ..., n\}$, $s(\alpha)$ is the sum of the integer sequence, $A[\alpha \mid \beta]$ denotes the $r \times r$ minor of A comprised of the rows listed in the sequence α and columns listed in the sequence β, and $B(\alpha \mid \beta)$ denotes the $(n-r)\times(n-r)$ minor of B comprised of the rows omitted from the sequence α and the columns omitted from the sequence β [23].

The sum corresponding to $r = 0$ is $\det(B)$ and the sum corresponding to $r = n$ is $\det(A)$ [23]. Then we have

$$\begin{aligned}\det(xA + yB) &= \det(xA) + \det(yB) + \sum_{r=1}^{n-1} \sum_{\alpha,\beta} (-1)^{s(\alpha)+s(\beta)} \det(xA[\alpha \mid \beta]) \det(yB(\alpha \mid \beta)) \\ &= x^n \det A + y^n \det(B) + \text{“mixed terms”}.\end{aligned}$$

For $k > 1$, the situation is similar. We have

$\det(x_1C_1 + ... + x_kC_k) = x_1^n\det(C_1) + ... + x_k^n\det(C_k) +$ "mixed terms".

Since $\{\det(C_i)\}$ is a set of relatively prime numbers, the coefficients of the form

$f(x_1, .., x_k) = \det(x_1C_1 + ... + x_kC_k) = x_1^n\det(C_1) + ... + x_k^n\det(C_k) +$ "other terms"

are also relatively prime.

Then by Theorem 2.3.2, there are algebraic integers α_i such that $f(\alpha_1, .., \alpha_k)$ is a unit. This means there are algebraic elements α_i such that $M = \alpha_1C_1 + ... + \alpha_kC_k$ has unit determinant. We also have $AM = A(\alpha_1C_1 + ... + \alpha_kC_k) = \alpha_1AC_1 + ... + \alpha_kAC_k = \alpha_1C_1B + ... + \alpha_kC_kB = MB$. Thus, over the extension $E = \mathbb{Z}[\alpha_1, ..., \alpha_k]$, the matrix M conjugates A to B and has determinant a unit in E.

□

Neither Theorem 2.3.2 nor (by extension) Theorem 2.3.3 is constructive, but is only an existence theorem. While we are able to easily see that the locally conjugate matrices A and B in example 2.3.1 are conjugate over $\mathbb{Z}[i]$, there is currently no algorithmic way of determining such an extension.

We will refer to the problem of computing the extension over which locally conjugate matrices are conjugate as the *conjugacy extension problem*. The rest of the dissertation is devoted to addressing this problem.

In the next chapter, we consider a method which Dade outlined in his proof of Theorem 2.3.2 for determining algebraic integers for which a primitive form realizes 1. We will also consider whether we can simplify this problem for two-by-two matrices by making use of the theory of quadratic forms.

Chapter 3

Conjugacy extension problem

3.1 A theorem of Dade

As we saw in the previous chapter, Theorem 2.3.3 ensures that locally conjugate matrices A and B (matrices which are $\mathbb{Z}_p$-conjugate for every prime p) are conjugate over an algebraic extension of $\mathbb{Z}$. Recall that we refer to the problem of determining this extension as the *conjugacy extension problem*. In this chapter, we discuss how the conjugacy extension problem may be approached by considering whether certain homogeneous forms realize a unit.

If $\{C_1, .., C_s\}$ is a set of matrices which conjugate A to B over $\mathbb{Q}$, we can attempt to find an algebraic extension E over which A and B are $\mathrm{GL}_n(E)$-conjugate by finding algebraic integers x_i so that the homogeneous form $\det(\sum x_i C_i)$ realizes a unit. A solution gives a conjugating matrix $\sum x_i C_i$ in $\mathrm{GL}_n(E)$ where $E = \mathbb{Z}[x_1, .., x_s]$. According to a theorem by Dade (see Theorem 2.3.2), there is an algebraic integral solution such that a homogeneous form with relatively prime coefficients realizes a unit [7]. In the case that A and B are locally conjugate, the C_i may be chosen so that $\{\det(C_i)\}$ is a relatively prime set, and we may apply Dade's theorem.

While Dade's theorem is not constructive, he does outline some steps one could take to find the desired algebraic solution [7]. We will discuss Dade's method next. As we will see in an example, the method can result in an algebraic extension of very large degree. Later, we will see if we can simplify things by restricting ourselves to quadratic forms, which would arise when considering the conjugacy extension problem for two-by-two matrices.

Below, we outline the steps in Dade's method for finding an algebraic extension over which the form f realizes a unit [7]. The following steps may be applied to a homogeneous form of any degree with relatively prime coefficients. In a later example, we will illustrate how the method can be applied to the specific case of a quadratic form in two variables. For this reason, we only discuss

the details of each step of Dade's method in the case of a form $ax^2 + bxy + cy^2$ where $a, b, c \in \mathbb{Z}$. To see how these steps can be applied to more general forms, see [7].

Step 1: Obtain a univariate polynomial with relatively prime coefficients from f.

Dade's theorem on homogeneous forms is a corollary of Theorem 1 in [7] which says that a univariate polynomial with relatively prime coefficients realizes a unit over an extension. To do this, we first translate one of the variables to obtain $\tilde{f}$, an inhomogeneous form with a non-zero constant term. For instance, if $f = ax^2 + bxy + cy^2$, one could substitute $x - 1$ for x to get $\tilde{f}(x, y) = f(x, y) - 2ax + by + a$. Let c_i denote the degree i homogeneous component of $\tilde{f}$.

Next we must find integers u_i such that $\tilde{f}(u_1 x, u_2 x)$ is a univariate polynomial with relatively prime coefficients. We want u_i such that the $c_i(u_1, u_2)$ are relatively prime. Since we ensured that c_0 was non-zero, we reduce the other homogeneous component modulo p for primes p which divide the constant term. We know that $c_2 = f(x, y)$ cannot be zero modulo p since f has relatively prime coefficients. If c is non-zero modulo p, then one can pick $(u_1, u_2) = (0, 1)$. Otherwise, b must be non-zero modulo p, and one can pick $(u_1, u_2) = (1, 1)$. If there are multiple primes dividing c_0, one may find an integral tuple (u_1, u_2) which satisfy all of the congruence conditions for each prime by the Chinese remainder theorem.

Note that for forms of higher degree, obtaining the u_i may be more subtle (see [7]).

Step 2: Find a unit.

Let $g = \tilde{f}(u_1 x, u_2 x)$ be the polynomial with relatively prime coefficients obtained from the previous step. Let $\frac{a_i}{b_i}$ denote the roots of g where a_i and b_i are relatively prime algebraic integers. Then

$$g(x) = \frac{c}{b_1 b_2}(b_1 x - a_1)(b_2 x - a_2)$$

where c denotes the leading term of g. We know that $\frac{c}{b_1 b_2}$ is a unit because it divides each of the relatively prime coefficients of g. In order for g to realize a unit, we need an algebraic integer α such that $b_i \alpha - a_i$ are units for each i.

We wish to determine a positive integer t and algebraic integers z_i so that the polynomial $h(x) = x^t + z_1 x^{t-1} + ... + z_t$ has a root α such that $b_i \alpha - a_i$ are units. If α is a root of h,

then $b_i\alpha - a_i$ is a root of the polynomial $b_i^t h(\frac{x+a_i}{b_i})$. The constant term of $b_i^t h(\frac{x+a_i}{b_i})$ is given by $b_i^t h(\frac{a_i}{b_i}) = a_i^t + z_1 a_i^{t-1} b_i + z_2 a_i^{t-2} b_i^2 + ... + z_t$. If there are algebraic integers z_j so that $b_i^t h(\frac{a_i}{b_i}) = 1$, then $b_i\alpha - a_i$ is a unit since it divides the constant term. We want $b_i\alpha - a_i$ to be a unit for each i.

Finding a polynomial h which satisfies all of these properties amounts to finding a natural number t so that the system $a_i^t + z_1 a_i^{(t-1)} b_i + z_2 a_i^{(t-2)} b_i^2 + ... + z_t = 1, i = 1, 2$ has an algebraic integral solution $\mathbf{z} = (z_1, .., z_t)$. In other words, we want t so that $M(t)\mathbf{z} = \mathbf{v}(t)$ has an algebraic integral solution where $M(t) = [a_i^{t-j} b^j]$ for $1 \leq i \leq 2$, and $1 \leq j \leq t$ and $\mathbf{v}(t) = (1 - a_i^t)$.

Letting $\delta(M)$ denote the ideal in $\mathbb{Z}[a_i, b_i]$ generated by the two-by-two minors of a matrix M, a theorem of Steinitz [28] tells us that the aforementioned system will have an algebraic integral solution iff $\delta(M(t)|\mathbf{v}(t)) = \delta(M(t))$ (this also applies for forms of degree n). Dade lists some specific conditions on t for this equality to hold (see [7] and [8]). There will be a natural number t which satisfies all these conditions, and the smallest such natural number will be strictly greater than the degree of the form. Therefore, we know that an algebraic integral solution $\mathbf{z}$ to $M(t)\mathbf{z} = \mathbf{v}(t)$ exists.

While a solution exists in theory, there is no bound on the degree of the algebraic extension from which the z_i come. Therefore, this is a method and not an algorithm.

Assume that $\mathbf{z} = (z_1, ...z_t)$ is a solution. Let α denote the root of $h(x) = x^t + a_1 x^{t-1} + ... + z_t$. Then by the previous discussion, $g(\alpha)$ is a unit. Tracking the transformations needed to get from the homogeneous form f to the polynomial g, we can apply the inverse transformations to obtain a solution (x_0, y_0) over $\mathbb{Z}[\alpha]$ such that $f(x_0, y_0) = g(\alpha)$. Then $\det(x_0 C_1 + y_0 C_2) = g(\alpha)$ is a unit, and $x_0 C_1 + y_0 C_2$ conjugates A to B.

(Optional) Step 3: Find a conjugating matrix with determinant one.

We may actually find an algebraic extension E so that A and B are $\mathrm{SL}_2(E)$-conjugate. Let $u = g(\alpha)$, the unit that f realizes over the extension $\mathbb{Z}[\alpha]$. So far, we have found a conjugating matrix with determinant u. We may find a new extension E in which u is a square so that we may divide our current solution (x_0, y_0) by the square-root of u. Then $f(\frac{x_0}{\sqrt{u}}, \frac{y_0}{\sqrt{u}}) = \frac{1}{u} f(x_0, y_0) = 1$.

More generally, one would have to find an extension in which there is an n-th root of u if f is an n-form.

We now wish to illustrate Dade's method in an example. We return once more to example 2.3.1, in which we showed that $A = \begin{pmatrix} 0 & -6 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 2 \\ -3 & 0 \end{pmatrix}$ are conjugate over $\mathbb{Z}_p$ for every prime p, but are not integrally conjugate. We previously found in Example 2.3.1 that $\begin{pmatrix} -3i & 2 \\ 1 & i \end{pmatrix}$ conjugates A to B and has determinant one. We now follow Dade to find another algebraic extension E of $\mathbb{Z}$ besides $\mathbb{Z}[i]$ over which A and B are $\mathrm{SL}_2(E)$-conjugate.

Example 3.1.1. *Consider* $A = \begin{pmatrix} 0 & -6 \\ 1 & 0 \end{pmatrix}$ *and* $B = \begin{pmatrix} 0 & 2 \\ -3 & 0 \end{pmatrix}$, *which have characteristic polynomial* $x^2 + 6$.

Recall that $C_1 = \begin{pmatrix} -3 & 0 \\ 0 & 1 \end{pmatrix}$ *and* $C_2 = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$ *conjugate* A *to* B.

Following Dade's method, we wish to find an algebraic integral solution (x_0, y_0) *which is a solution to* $det(xC_1 + yC_2) = 1$. *Then if* $E = \mathbb{Z}[x_0, y_0]$, *we have* $x_0C_1 + y_2C_2 \in SL_n(E)$. *While it is easy to observe that* $(i, 1)$ *is one such solution, we will go through each of the steps in Dade's method.*

In our example, we wish to determine the extension over which the quadratic form $f(x, y) = det(xC_1 + yC_2) = -3x^2 - 2y^2$ *realizes 1.*

Substituting $y - 1$ *for* y, *we get* $\tilde{f}(x, y) = f(x, y - 1) = -2 + 4y - 3x^2 - 2y^2$. *Let* $c_i(x, y)$ *denote the degree* i *homogeneous component of* $\tilde{f}$.

In our case, since 2 *is the only prime dividing* c_0, *we want to find values* u_1, u_2 *so that not all of the* $c_i(u_1, u_2)$ *are divisible by 2. We have* $-3x^2 - 2y^2 \equiv x^2 \pmod 2$ *which is non-zero if evaluating at* $(u_1, u_2) = (1, 0)$.

We define $g(x) = \tilde{f}(u_1x, u_2x) = \tilde{f}(x, 0) = -2 - 3x^2$. *The roots of* $g(x)$ *are* $\pm\sqrt{\frac{2}{3}}i$. *Following Dade's notation, we write these roots as the quotient of algebraic integers* $\frac{a_i}{b_i}$. *Then* $a_1 = \sqrt{2}i, a_2 = -\sqrt{2}i$, *and* $b_i = \sqrt{3}$ *for* $i = 1, 2$.

The smallest value of t for which $M(t)\boldsymbol{z} = \boldsymbol{v}(t)$ has a solution is $t = 4$. The following is a table of the powers of the algebraic integers of concern.

t	a_1^t	a_2^t	b_i^t
1	$\sqrt{2}i$	$-\sqrt{2}i$	$\sqrt{3}$
2	-2	-2	3
3	$-2\sqrt{2}i$	$2\sqrt{2}i$	$3\sqrt{3}$
4	4	4	9

We have

$$\begin{pmatrix} -2\sqrt{6}i & -6 & 3\sqrt{6}i & 9 \\ 2\sqrt{6}i & -6 & -3\sqrt{6}i & 9 \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix} = \begin{pmatrix} -3 \\ -3 \end{pmatrix}.$$

Assuming that there is an integral solution, this yields the system

$$-2\sqrt{6}iz_1 + 3\sqrt{6}iz_3 = 0 \implies -2z_1 + 3z_3 = 0$$

$$-6z_2 + 9z_4 = -3$$

which has solution $\boldsymbol{z} = (3, -1, 2, -1)$. Then $h(x) = x^4 + 3x^3 - x^2 + 2x - 1$ has root α so that $g(\alpha)$ is a unit. An element is an algebraic integral unit iff its minimal polynomial is monic with a unit for its constant term. Thus, one can verify in GAP that $g(\alpha)$ is a unit by computing its minimal polynomial, $x^4 - 41x^3 + 105x^2 - 14x + 1$.

Let u denote the unit $g(\alpha)$ in the extension $\mathbb{Z}[\alpha]$ where α is a root of h. We see that $u = g(\alpha) = \tilde{f}(\alpha, 0) = f(\alpha, -1)$. So $\alpha C_1 - C_2 = \begin{pmatrix} -3\alpha & -1 \\ -1 & \alpha \end{pmatrix}$ conjugates A to B and has determinant u.

If we want to find a conjugating matrix with determinant 1, we must work within an extension in which we can divide by $\sqrt{u}$. Since u is not a square in the current extension, we will find a new extension in which it is. Letting $m(x)$ denote the minimal polynomial of u, we will define a new

extension E by the polynomial $m(x^2) = x^8 - 41x^6 + 105x^4 - 14x^2 + 1$. The primitive element in this extension is $\sqrt{u}$. Then in this new degree 8 extension, we have $f(\frac{\alpha}{\sqrt{u}}, \frac{-1}{\sqrt{u}}) = 1$.

Thus, $\frac{\alpha}{\sqrt{u}}C_1 - \frac{1}{\sqrt{u}}C_2 \in SL_2(E)$, and this matrix conjugates A to B.

We have seen that the matrices from the previous example are $\mathrm{SL}_2(E)$-conjugate over different extensions E. We first saw that A and B are conjugate over the degree 2 extension $\mathbb{Z}[i]$, while following Dade's method gave a different degree 8 extension. Then following Dade's process may not yield an extension of minimal degree. In fact, it is not possible to obtain a degree 2 extension by Dade's method since the degree of the polynomial h must be strictly larger than 2.

It is important to note that this example was very simple since we were able to find integers z_i that satisfied the system. Generally, the z_i are algebraic integers, and it can be much more difficult to find a solution. We now demonstrate a more complicated example of Dade's method.

Example 3.1.2. *Consider matrices with characteristic polynomial $f = x^2 - x - 117$. The matrix $A = \begin{pmatrix} -2 & 37 \\ 3 & 3 \end{pmatrix}$ is not $\mathbb{Z}$-conjugate to the companion matrix $C_f = \begin{pmatrix} 0 & 117 \\ 1 & 1 \end{pmatrix}$, but these matrices are locally conjugate.*

Let $C_1 = \begin{pmatrix} 3 & -6 \\ 0 & 9 \end{pmatrix}$ and $C_2 = \begin{pmatrix} -10 & -538 \\ 14 & 12 \end{pmatrix}$ be two matrices which conjugate A to C_f with relatively prime determinants.

We define the quadratic form $f(x, y) = det(xC_1 + yC_2) = 27x^2 + 30xy - 7652y^2$. We transform this into the univariate polynomial $g(x) = f(x, 1) = 27x^2 + 30x - 7652$.

We express the roots of g as $\frac{a_i}{b_i}$ where a_i and b_i are relatively prime algebraic integers. We then try to find a natural number t so that the system $M(t)\mathbf{z} = \mathbf{v}(t)$ has a solution. (Recall that $M(t) = \left(a_i^{t-j} b_i^j\right)$ and $\mathbf{v}(t) = (1 - a_i^t)$ for $1 \leq j \leq t, 1 \leq i \leq 2$.)

Using the criterion that this will have a solution iff $\delta(M(t)) = \delta(M(t)|\mathbf{v}(t))$, we find that $t = 462$ is the smallest natural number which yields a solution. Even if there is an integral solution to the system, the size of the system makes the computation difficult.

We will not actually attempt to solve the system, but the solution yields a degree 462 *polynomial* $h(x)$ *with algebraic integers as coefficients. If* α *is the root of* $h(x)$*, then* $g(\alpha) = f(\alpha, 1)$ *is a unit. Then the matrix* $\alpha C_1 + C2$ *has unit determinant in the extension* $\mathbb{Z}[\alpha]$ *and conjugates* A *to* B*.*

It is desirable to find a more constructive means of addressing the conjugacy extension problem. We will restrict ourselves to two-by-two matrices and see what can be said in this context. The hope is that the theory of quadratic forms will allow us to more easily determine an extension over which a form realizes a unit.

3.2 Quadratic forms

We now focus on the conjugacy extension problem for two-by-two matrices, so that we are restricting our attention to quadratic forms. We will use ideas from Watson in [34], in which he provides a more constructive approach to finding an extension over which quadratic forms realize a unit. At first glance, it may seem that Watson's theorem answers the extension problem for two-by-two matrices. However, Watson imposes restrictions on the quadratic forms which renders his theorem inapplicable to our context.

In this section, we will discuss why Watson's result is not exactly relevant for our purposes. We will also discuss some general theory of quadratic forms and attempt to modify Watson's result to the desired context. First, we need some definitions.

3.2.1 Note on singularity

We say that a form f is **non-singular** iff its coefficient matrix $Mf := (\partial^2 f/\partial x_i \partial x_j)_{i,j}$ has non-zero determinant. Otherwise, we say that the form is **singular** [33].

Watson provides the following result on non-singular quadratic forms in at least three variables [34].

Theorem 3.2.1. *Suppose that* f *is a non-singular* n*-ary quadratic form with relatively prime coefficients.*

1. *If $n \geq 4$, then there is an integer q and $\alpha_i \in \mathbb{Z}[\sqrt{q}]$ such that $f(\alpha_1, ..., \alpha_n) = 1$.*

2. *If $n = 3$, then there are integers q and r and $\alpha_i \in \mathbb{Z}[\sqrt{q}, \sqrt{r}]$ such that $f(\alpha_1, ..., \alpha_n) = 1$.*

We discuss why this theorem does not help us answer the conjugacy extension problem for two-by-two integral matrices. Suppose that C_i are integral matrices with non-zero determinant which conjugate A to B. Then considering the conjugacy extension problem is equivalent to asking whether the quadratic form $\det(\sum_i x_i C_i)$ realizes a unit over some extension. It is not difficult to ensure that we are working with a form with relatively prime coefficients. As mentioned in the proof of Theorem 2.3.3, one may choose conjugating matrices with relatively prime determinants since we assume that A and B are locally conjugate for every prime. The obstruction to using Watson's result comes from the condition that the form must be non-singular in at least three variables.

The following result will be useful for considering the singularity of a form $\det(\sum x_i C_i)$.

Proposition 3.2.2. *Let $f = det(\sum_{i=1}^{n-1} x_i C_i)$. If $g = det(\sum_{i=1}^{n} x_i C_i)$, then*

1. *The coefficient matrix Mg has the coefficient matrix Mf as its upper left $(n-1) \times (n-1)$ corner.*

2. *If $C_n = \sum_{i=1}^{n-1} a_i C_i$ for some $a_i \in \mathbb{Q}$, and if $\boldsymbol{v}_i$ denotes the i-th column vector of the coefficient matrix Mg, then $\boldsymbol{v}_n = \sum_{i=1}^{n-1} a_i \boldsymbol{v}_i$. In particular, g is a singular form.*

Proof:

1. To obtain the upper left $(n-1)\times(n-1)$ corner of Mg, we just disregard the terms $\partial^2 g/\partial x_i x_n$. When considering $\partial^2 g/\partial x_i x_j$ for $j \neq n$, we may ignore x_n completely. Then $\partial^2 g/\partial x_i x_j = \partial^2 g(x_1, ..., x_{n-1}, 0)/\partial x_i x_j = \partial^2 f/\partial x_i x_j$. This proves 1.

2. Now suppose $g = \det(\sum_{i=1}^{n-1} x_i C_i + x_n(\sum_{i=1}^{n-1} a_i C_i))$. Clearly, $g = f(x_1 + a_1 x_n, ...x_{n-1} + a_{n-1} x_n)$. Suppose that $f = \sum_{1 \leq i \leq n-1, i \leq j} c_{i,j} x_i x_j$.

By part 1, $Mg = \begin{pmatrix} 2c_{1,1} & c_{1,2} & \dots & c_{1,n-1} & \partial^2 g/\partial x_n \partial x_1 \\ c_{1,2} & \ddots & & c_{2,n-1} & \partial^2 g/\partial x_n \partial x_2 \\ \vdots & & \ddots & & \vdots \\ c_{1,n-1} & c_{2,n-1} & \dots & 2c_{n-1,n-1} & \partial^2 g/\partial x_n \partial x_{n-1} \\ \partial^2 g/\partial x_n \partial x_1 & \partial^2 g/\partial x_n \partial x_2 & \dots & \dots & \partial^2 g/\partial x_n^2 \end{pmatrix}$.

We now work out a relation among the n-th column of Mg with the previous columns.

For any $i \leq n-1$, we have

$$\begin{aligned} \partial^2 g/\partial x_n \partial x_i &= \partial^2 f(x_1 + a_1 x_1, ..., x_{n-1} + a_{n-1} x_n)/\partial x_n \partial x_i \\ &= \partial/\partial x_n [\partial f(x_1 + a_1 x_1, ..., x_{n-1} + a_{n-1} x_n)/\partial x_i] \\ &= \partial f/\partial x_i \mid_{(a_1,..,a_n)} . \end{aligned}$$

The last equality holds because $\partial f(x_1 + a_1 x_n, .., x_{n-1} + a_{n-1} x_n)/\partial x_i$ is a degree one form, so taking the derivative with respect to x_n yields the coefficient of x_n in $\partial f(x_1 + a_1 x_n, .., x_{n-1} + a_{n-1} x_n)/\partial x_i$.

Thus, the second order partial derivative is equal to setting $x_n = 1$ and $x_i = 0$ for $i \neq n$ in $\partial f(x_1 + a_1 x_n, .., x_{n-1} + a_{n-1} x_n)/\partial x_i$.

By a similar argument, we get that $\partial^2 f/\partial x_j \partial x_i = \partial/\partial x_j [\partial f/\partial x_i] = \partial f/\partial x_i \mid_{\mathbf{e}_j}$.

So far we have the equations

$$\partial^2 g/\partial x_n \partial x_i = \partial f/\partial x_i \mid_{(a_1,..,a_n)} \text{ for } 1 \leq i \leq n-1 \tag{3.1}$$

and

$$\partial^2 f/\partial x_j \partial x_i = \partial f/\partial x_i \mid_{\mathbf{e}_j} \text{ for } 1 \leq i, j \leq n-1. \tag{3.2}$$

Fix row i of Mg with $1 \leq i \leq n-1$. Then

$$\begin{aligned}
\sum_{j=1}^{n-1} a_j \partial^2 f/\partial x_j \partial x_i &= \sum_{j=1}^{n-1} a_j \partial f/\partial x_i \mid_{\mathbf{e}_j} \quad \text{(by equation (3.2))} \\
&= \sum_{j=1}^{n-1} \partial f(a_j x_1, ..., a_j x_{n_1})/\partial x_i \mid_{\mathbf{e}_j} \quad (f_{x_i} \text{ is a form of degree one}) \\
&= \sum_{j=1}^{n} \partial f/\partial x_i \mid_{a_j \mathbf{e}_j} \\
&= \partial f/\partial x_i \mid_{(a_1,...,a_n)} \quad (f_{x_i} \text{ has no mixed terms}) \\
&= \partial^2 g/\partial x_n \partial x_i \quad \text{(by equation (3.1))}.
\end{aligned}$$

Now we must show a similar result for the last row of Mg in order to prove the result. The x_n^2 coefficient of g is $g(\mathbf{e}_n) = f(a_1, ..., a_n)$, so we know that Mg has $2f(a_1, .., a_n)$ as its lower right entry.

Above, we showed that

$$\begin{aligned}
\partial^2 g/\partial x_n \partial x_i &= \sum_{j=1}^{n-1} a_j \partial^2 f/\partial x_j \partial x_i, \text{ which implies} \\
\sum_{i=1}^{n-1} a_i \partial^2 g/\partial x_n \partial x_i &= \sum_{i=1}^{n-1} a_i \sum_{j=1}^{n-1} a_j \partial^2 f/\partial x_j x_i.
\end{aligned}$$

Each of the $\partial f^2/x_i^2$ terms shows up exactly once in the sum and $\partial^2 f/\partial x_i^2$ is twice the coefficient of x_i^2, or $2c_{i,i}$. The mixed partial derivatives show up twice in the sum and $\partial^2 f/\partial x_j x_i = c_{i,j}$. If we restrict $i \leq j$ in the sum, we will only count the mixed partial derivatives once. So instead we write

$$\begin{aligned}
\sum_{i=1}^{n-1} a_i \partial^2 g/\partial x_n \partial x_i &= 2 \sum_{1 \leq i \leq n-1, i \leq j} c_{i,j} a_i a_j \\
&= 2f(a_1, ..., a_n).
\end{aligned}$$

We have shown that $\mathbf{v}_n = \sum_{i=1}^{n-1} a_i \mathbf{v}_i$, meaning that the columns of Mg are not linearly independent. Thus, g is a singular form.

□

The following example shows how one might use the previous result to see that Watson's theorem does not apply.

Example 3.2.3. *Watson's theorem does not apply to the extension problem for* $A = \begin{pmatrix} 0 & -6 \\ 1 & 0 \end{pmatrix}$ *and* $B = \begin{pmatrix} 0 & 2 \\ -3 & 0 \end{pmatrix}$. *We have previously seen that these matrices are* p*-adicallly conjugate for every prime* p. *We also know that* $C_1 = \begin{pmatrix} -3 & 0 \\ 0 & 1 \end{pmatrix}$ *and* $C_2 = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$ *conjugate* A *to* B *over* $\mathbb{Q}$. *From these matrices, we may obtain the non-singular binary form* $f = det(xC_1 + yC_2) = -3x^2 - 2y^2$. *However, one cannot obtain a non-singular form in more than two variables, as we show now.*

Let $C_3 \in \mathbb{Z}^{2\times 2}$ *be any other conjugating matrix with non-zero determinant. Then* $C_3 = p(A)C_1$ *where* $p(x) = ax + b$ *is a linear polynomial in* $\mathbb{Q}[x]$. *This follows from the fact that* A *has square-free characteristic polynomial so that centralizing elements are polynomials in* A *and that the minimal polynomial is of degree two.*

For the same reason, $C_2 = q(A)C_1$ *for another rational polynomial* $q(a)$. *In fact, one can check that* $C_2 = -\frac{1}{3}AC_1$ *or* $AC_1 = -3C_2$.

Then we may see that

$$\begin{aligned} C_3 &= p(A)C_1 \\ &= (aA + b)C_1 \\ &= aAC_1 + bC_1 \\ &= a(-3C_2) + bC_1. \end{aligned}$$

This shows that any other conjugating matrix is a linear combination of C_1 and C_2. By Proposition 3.2.2, the ternary form det$(xC_1 + yC_2 + zC_3)$ is singular. Therefore, we cannot apply Watson's constructive method to obtain an extension.

The previous example is illustrative of what happens more generally. The following is a consequence of Proposition 3.2.2.

Corollary 3.2.4. *Let f be a square-free quadratic monic polynomial and $A, B \in \mathcal{M}_f$ which are locally conjugate matrices. Let $\{C_1, ..C_s\}$ be a set of matrices with relatively prime determinants such that $C_i^{-1}AC_i = B$. Then if $s > 2$, the form det$(\sum_{i=1}^{s} x_iC_i)$ is singular.*

Proof: Note that all the matrices C_i are of the form $p(A)C_1$ for a linear polynomial $p(x) \in \mathbb{Q}[x]$. Suppose $C_2 = (aA + b)C_1$. If $s > 2$, there is a third matrix C_3 which we express as $C_3 = (cA + d)C_1$. Now if $a \neq 0$ then

$$\begin{aligned} C_3 &= c(A + d)C_1 \\ &= \frac{1}{a}(C_2 - bC_1) + dC_1 \\ &= \frac{1}{a}C_2 + \left(\frac{-b + da}{a}\right) C_1. \end{aligned}$$

Since C_3 is a linear combination of C_1 and C_2, the form det$(\sum_{i=1}^{s} x_iC_i)$ is singular.

On the other hand, if $a = 0$, then $C_2 = bC_1$. In this case, the form det$(x_1C_1 + x_2C_2)$ is singular.

□

3.2.2 Transforming quadratic forms

Even though Watson's result is not relevant, his paper outlines some classic techniques for manipulating quadratic forms which do not require non-singularity [34].

Definition 3.2.5. *[33] We say that a form f **represents** another form g if there is an integral matrix H with non-zero determinant such that $g(\boldsymbol{x}) = f(H\boldsymbol{x})$. If det$(H) = 1$, we say that H gives a **unimodular transformation** of f.*

If f represents g, then f realizes 1 if g realizes 1. We will therefore find a simpler form g which is represented by f. If Mf is the coefficient matrix of f, then the coefficient matrix of $f(H\mathbf{x})$ is $H^t(Mf)H$.

Diagonalization of forms

We now discuss how to diagonalize f. By this, we mean we can find a form $g = \sum a_i x_i^2$ which is represented by f. We list the steps for diagonalizing a form f. These steps are standard, and can be found in [33], for example.

Step 1: Clear mixed terms x_1x_j for $j > 2$.

If one starts with a form that is not already diagonal, there is a non-zero mixed term. One can assume without loss of generality (by interchanging variables) that the x_1x_2 term is non-zero. From there, one can clear out the terms x_1x_j for $j > 2$ via a unimodular transformation by making use of the Euclidean algorithm. Suppose that the term x_1x_j is non-zero. Then we have $f = a_1x_1^2 + ax_1x_2 + bx_1x_j +$ " other terms " with a, b non-zero integers. We may interchange variables so that $a \geq b$.

Suppose $a = bq + r$. Then the substitution $x_j \mapsto x_j - qx_1$ (and all other variables are fixed) is represented by a unimodular matrix U. Here, U differs from the identity matrix only by $-q$ in row j, column i.

Then $g = f(U\mathbf{x}) = a_1x_1^2 + rx_1x_2 + bx_1x_j +$ " other terms ". By applying the Euclidean algorithm several times, one eventually gets $g = a_1x_1^2 + dx_1x_2 + bx_1x_j +$ " other terms " where $d = gcd(a, b)$. So $b = dk$ for some $k \in \mathbb{N}$.

Suppose the substitution $x_2 \mapsto x_2 - kx_j$ (and all other variables fixed) is given by the unimodular matrix V. Then

$$\begin{aligned} g(V\mathbf{x}) &= a_1x_1^2 + dx_1(x_2 - kx_j) + bx_1x_j + \text{" other terms "} \\ &a_1x_1^2 + dx_1x_2 + (-dk + b)x_1x_j + \text{" other terms "} \\ &= a_1x_1^2 + dx_1x_2 + 0x_1x_j + \text{" other terms "}. \end{aligned}$$

This procedure may be repeated until all the quadratic form's mixed terms x_1x_j for $j > 2$ are cleared.

Step 2: Clear x_1x_2 term.

After applying the first step, we obtain the form $\tilde{f} = a_1x_1^2 + cx_1x_2 + f(0, x_2, .., x_n)$. The term cx_1x_2 can also be cleared out by using something like completing the square.

Let $d = \gcd(c, 2a_1)$. One can cancel the term cx_1x_2 by the substitution $x_1 \mapsto x_1 - \frac{c}{d}x_2$, $x_2 \mapsto \frac{2a_1}{d}x_2$. If H is the matrix representing this transformation, then it has determinant $\frac{2a_1}{d}$.

Then $\tilde{f}(H\mathbf{x}) = a_1x_1^2 + F(x_2, ..., x_n)$ with $F = (\frac{4a_2a_1^2 - a_1c^2}{d^2})x_2^2 +$ " other terms ".

Step 3: Repeat.

One may now repeat steps 1 and 2 for F, relabeling the variables x_i as x_{i-1}. Eventually one will obtain a diagonal form which is represented by f.

Changing the leading coefficient of a form

We also discuss a classic result for quadratic forms regarding altering the leading coefficient of the form. We say that a is an integer which is **properly represented** by f if there is a primitive tuple $(t_1, ..., t_n)$ such that $f(t_1, .., t_n) = a$ [33]. The next theorem and its proof can be found in [33].

Theorem 3.2.6. *If a is an integer which is properly represented by f, then f represents a form $\tilde{f}$ with a as its leading coefficient. More specifically, the matrix U with $\tilde{f}(\boldsymbol{x}) = f(U\boldsymbol{x})$ has the tuple (t_i) as its first column and is unimodular.*

Proof: This result is easy for binary forms. If $f(t_1, t_2) = a$ for a primitive tuple (t_1, t_2), then there are integers z_1 and z_2 such that $t_1z_2 - t_2z_1 = 1$ so that the substitution $x \mapsto t_1x + z_1y$, $y \mapsto t_2x + z_2y$ given by $\begin{pmatrix} t_1 & z_1 \\ t_2 & z_2 \end{pmatrix}$ is unimodular. The leading term of $f(t_1x + z_1y, t_2x + z_2y)$, which can be found by setting $x = 1, y = 0$, is $f(t_1, t_2) = a$.

Say the result holds for $(n-1)$-ary forms. Let f be an n-ary form with $f(t_1, ..., t_n) = a$ and (t_i) a primitive tuple. Let h be the largest number which divides t_i for $i \geq 2$. One can write

$\mathbf{t} = (t_1, hz_1, hz_2, ..., hz_{n-1})$. Here, we have that h is relatively prime to t_1 and the z_i are relatively prime.

Let T be the $(n-1) \times (n-1)$ unimodular matrix with the tuple (z_i) in the first column. Since $(t, h) = 1$, there are integers a and b with $t_1 a - hb = 1$. Now,

$$U = \begin{pmatrix} 1 & \\ & T \end{pmatrix} \begin{pmatrix} t_1 & b & \\ h & a & \\ & & I_{n-2} \end{pmatrix} = \begin{pmatrix} t_1 & b & & & \\ hz_1 & * & * & * & * \\ \vdots & * & * & * & * \\ hz_n & * & * & * & * \end{pmatrix}$$

is an $n \times n$ unimodular matrix with t_i in the first column.

Again, the leading coefficient of $\tilde{f}(\mathbf{x}) = f(U\mathbf{x})$ is found by setting $x_1 = 1$ and all other variables equal to 0. So the leading coefficient is $\tilde{f}(1, 0, .., 0) = f(t_1, t_1, .., t_n) = a$.

□

To summarize, we can consider a diagonal form g in place of our original form f. If we can also alter the leading coefficient of g in a particular way, this will provide us with a method for solving the conjugacy extension problem in some cases.

3.2.3 Limited method for conjugacy extension problem

We now discuss a class of quadratic forms for which there is a nice answer to the conjugacy extension problem. What we discuss next is still only a method since this approach only works for a quadratic form if it realizes a number satisfying several conditions. It is not easy in general to determine whether a quadratic form realizes such a number.

We will now consider a situation in which finding the extension over which a form realizes 1 is easy. Say $f = \det(\sum x_i C_i)$ is a quadratic form which represents a diagonal form $g = \sum a_i x_i^2$. Also suppose there are two coefficients, call them a_i and a_j, of this diagonal form which are relatively prime. Then there are integers q and r such that $a_i q + a_j r = 1$. Letting $x_i = \sqrt{q}, x_j = \sqrt{r}$ and $x_k = 0$ for all other variables yields a solution to $g = 1$. Then A and B are conjugate over the extension $\mathbb{Z}[\sqrt{q}, \sqrt{r}]$.

While diagonalizing a form is straightforward, one cannot guarantee that there will be two relatively prime coefficients. Applying the previous theorem to change the leading coefficient before diagonalizing may be necessary.

Let us now restrict our focus to binary quadratic forms. Suppose that $f = ax^2 + bxy + cy^2$. If $f(t_1, t_2) = \tilde{a}$ with $(t_1, t_2) = 1$, then there are integers s and r with $t_1 r - t_2 s = 1$, and the matrix $\begin{pmatrix} t_1 & s \\ t_2 & r \end{pmatrix}$ represents a transformation which changes f to $\tilde{f} = \tilde{a}x^2 + \tilde{b}xy + \frac{\tilde{b}^2 - d}{4\tilde{a}}y^2$ (see [33]). Here, $\tilde{b} = 2(at_1 s + ct_2 r + bt_2 s) + b$ (notice that $\tilde{b}$ and b have the same parity) and $d = -4ac + b^2$, the discriminant of f.

After diagonalizing $\tilde{f}$, one obtains $g = \tilde{a}x^2 + \frac{-d\tilde{a}}{\gcd(2\tilde{a}, \tilde{b})^2}y^2$. In order for these coefficients to be relatively prime, it is necessary that $\tilde{a}$ divides $\tilde{b}$ so that $g = \tilde{a}x^2 + \frac{-d}{\tilde{a}}y^2$ if $\tilde{b}$ is odd and $g = \tilde{a}x^2 + \frac{-d}{4\tilde{a}}y^2$ if $\tilde{b}$ is even. If $\tilde{b}$ is even, so is b, and the discriminant is divisible by four. The coefficients of g must be integers, so if $\tilde{a}$ divides $\tilde{b}$, then it must also divide the discriminant. Even with these conditions on $\tilde{a}$, it is still possible that $\tilde{a}$ and $\frac{d}{\tilde{a}}$ (or $\frac{d}{4\tilde{a}}$) are not relatively prime. This can happen if and only if $\text{ord}_p(\tilde{a}) < \text{ord}_p(d)$ (or $\text{ord}_p(\tilde{a}) < \text{ord}_p(d/4)$). Also note that we cannot have $\text{ord}_p(\tilde{a}) > \text{ord}_p(d)$ since $\frac{d}{\tilde{a}}$ is an integer. Thus, we have the following.

Proposition 3.2.7. *A quadratic form $f = ax^2 + bxy + cy^2$ may be diagonalized with relatively prime coefficients iff it properly realizes an integer $\tilde{a}$ (so $f(t_1, t_2) = \tilde{a}$ and there are integers s and r with $t_1 r - t_2 s = 1$) satisfying the following conditions:*

1. $\tilde{a} \mid \tilde{b} = 2(at_1 s + ct_2 r + bt_2 s) + b$
2. *If $\tilde{b}$ is odd, then $ord_p(\tilde{a}) = ord_p(d)$ for every prime p dividing $\tilde{a}$.*
3. *If $\tilde{b}$ is even, then condition 3 must hold for every odd prime dividing $\tilde{a}$ and we must have $ord_2(\tilde{a}) = ord_2(d) - 2$.*

There are several conditions on the number which the given binary quadratic form must satisfy in order to use this method. We will now give an example in which we were able to diagonalize our form with relatively prime coefficients.

Example 3.2.8. *The matrices* $A = \begin{pmatrix} -1 & 3 \\ 3 & -10 \end{pmatrix}$ *and* $B = \begin{pmatrix} -22 & 3 \\ -81 & 11 \end{pmatrix}$ *are conjugate over* $GL_2(\mathbb{Z})$ *and have characteristic polynomial with discriminant* $3^2 \cdot 13$*. We have that*

$C_1 = \begin{pmatrix} -27 & 7 \\ 0 & 1 \end{pmatrix}$ *and* $C_2 = \begin{pmatrix} -47 & 12 \\ 5 & 1 \end{pmatrix}$ *are matrices in* $GL_n(\mathbb{Q})$ *which conjugate* A *to* B *and which have relatively prime determinants.*

We consider the quadratic form $f = det(xC_1 + yC_2) = -27x^2 - 109xy - 107y^2$*. Due to the fact that* $a = -27 \nmid d = 3^2 \cdot 13$*, we wish to see whether* f *properly realizes an integer which satisfies the conditions of the previous proposition.*

We find that $f(5, -2) = -13$ *divides* $d = 3^2 \cdot 13$*. We let* $\tilde{a} = -13$ *and check that it satisfies the necessary conditions. Notice also that* $ord_{13}(13) = ord_{13}(d) = 1$*. Transforming by the matrix* $U_1 = \begin{pmatrix} 5 & -2 \\ -2 & 1 \end{pmatrix}$*, we obtain* $\tilde{f} = -13x^2 - 13xy + 3y^2$*. We also have that* $\tilde{b} = -13$*, so that* $\tilde{a} \mid \tilde{b}$*. All of the conditions on* $\tilde{a}$ *are satisfied, so we may diagonalize* $\tilde{f}$ *via the matrix* $U_2 = \begin{pmatrix} 1 & 1 \\ 0 & -2 \end{pmatrix}$ *to obtain* $g = -13x^2 + 25y^2$*, which has relatively prime coefficients.*

Since $-13(-2) + 25(-1) = 1$*, we see that* $g(\sqrt{2}i, i) = 1$*. Keeping track of the transformation that were applied to* f*, we see that*

$$\begin{aligned} 1 &= g(\sqrt{2}i, i) \\ &= \tilde{f}(\sqrt{2}i + i, -2i) \\ &= f(5(\sqrt{2}i + i) + -2(-2i), -2(\sqrt{2}i + i) - 2i) \\ &= f((5\sqrt{2} + 9)i, (-2\sqrt{2} - 4)i). \end{aligned}$$

Then $(5\sqrt{2}+9)iC_1 + (-2\sqrt{2}-4)iC_2$ *is an element of* $SL_2(\mathbb{Z}[\sqrt{2}i, i])$ *which conjugates* A *to* B.

In this chapter we considered the conjugacy extension problem by asking whether certain homogeneous forms realize a unit over an extension. We discussed a method by Dade, which is not constructive. The algebraic extension we are after is defined by a polynomial $h \in E[x]$ where E is some ring of algebraic integers. While such an h exists, the difficulty is that there is no bound on the degree of E. As we saw in Example 3.1.2, the degree of h may also be very large, making it even more difficult to determine h.

We also considered a more constructive result by Watson which applies to particular quadratic forms [34]. However, this result requires non-singular quadratic forms in at least three variables. In Proposition 3.2.4, we saw that no such quadratic form can arise from the determinant of a linear combination of conjugating matrices.

Finally, we considered more standard transformations that can be applied to quadratic forms. If we can diagonalize a quadratic form so that it has relatively prime coefficients, one can easily obtain the desired extension from the Euclidean algorithm. The limitation of this method is determining whether a quadratic form properly represents a number $\tilde{a}$ satisfying all of the conditions of Proposition 3.2.7. This approach does not help to build an extension constructively because even if we know that a given form should theoretically realize a particular integer, it is not clear how to select the corresponding primitive tuple (t_1, t_2).

We will now move away from homogeneous forms and approach the conjugacy extension problem from a different perspective. In the next chapter, we will show that the Latimer and MacDuffee correspondence for $\mathrm{GL}_n(\mathbb{Z})$-conjugacy which we discussed in Chapter 1 can be generalized to describe $\mathrm{GL}_n(R)$-conjugacy for any integral domain R. This will allow us to translate the conjugacy extension problem to a question about analogues of fractional $\mathbb{Z}[\alpha]$-ideals.

Chapter 4

The Latimer and MacDuffee correspondence for arbitrary integral domains

Throughout this chapter, let f be a square-free monic polynomial of degree n in $\mathbb{Z}[x]$. In [21], Latimer and MacDuffee give a correspondence between $\mathrm{GL}_n(\mathbb{Z})$-conjugacy classes of $\mathcal{C}_f$ and certain fractional ideal classes associated to f. We will discuss how the Latimer and MacDuffee (LM) correspondence can be generalized by replacing the ring of integers with any integral domain. Let us briefly review the details of this correspondence in its original context.

4.1 LM correspondence over $\mathbb{Z}$

The LM correspondence gives a theoretical description of $\mathrm{GL}_n(\mathbb{Z})$-conjugacy for integral matrices in $\mathcal{M}_f$, the set of matrices with characteristic polynomial f.

In order to describe the correspondence more concretely, we discuss a bijection given by Taussky [32] in the case that f is irreducible and a generalization of this bijection due to Marseglia [24] in the case that f has multiple irreducible factors.

Case 1: f is irreducible

In the case that f is irreducible with root α, Taussky provides a bijection φ from the fractional $\mathbb{Z}[\alpha]$-ideal classes to the $\mathrm{GL}_n(\mathbb{Z})$-classes of $\mathcal{C}_f$ by

$$\varphi : \mathcal{I}(\alpha)/_{\cong_{\mathbb{Z}[\alpha]}} \to \mathcal{M}_f/_{\sim_{\mathbb{Z}}}$$
$$[I] \mapsto [A]$$

where A is the multiplication-by-α matrix with respect to a $\mathbb{Z}$-basis $\{v_1, .., v_n\}$ of I. In other words, if $\mathbf{v} = (v_1, .., v_n)^t$, then $A\mathbf{v} = \alpha\mathbf{v}$.

The following example illustrates how we may use this bijection to obtain representatives of the $\mathrm{GL}_2(\mathbb{Z})$-conjugacy classes within $\mathcal{M}_f$ for $f = x^2 + 11x + 1$.

Example 4.1.1. *Let α denote the root of $f = x^2 + 11x + 1$. Letting $K = \mathbb{Q}[x]/(f)$, we see that $h_K = |Pic(\mathcal{O}_K)| = 1$. However, this does not mean that there is only one $GL_2(\mathbb{Z})$-conjugacy class of $\mathcal{C}_f$. Extra care must be taken because $\mathcal{O}_K = 1\mathbb{Z} \oplus (\frac{\alpha+7}{3})\mathbb{Z} \neq \mathbb{Z}[\alpha]$. Actually, the set $\{\mathbb{Z}[\alpha], \mathcal{O}_K\}$ is a full set of representatives for the $\mathbb{Z}[\alpha]$-ideal classes in $\mathcal{I}(\alpha)$, and so there are two $GL_2(\mathbb{Z})$-conjugacy classes.*

To find the representatives of the conjugacy classes, we compute the multiplication-by-α matrix with respect to a $\mathbb{Z}$-basis of each of these fractional ideals. For $\mathcal{O}_K$, we have that

$$\alpha \cdot 1 = -7 \cdot 1 + 3 \cdot \left(\frac{\alpha + 7}{3}\right)$$

and

$$\begin{aligned} \alpha \cdot \left(\frac{\alpha + 7}{3}\right) &= \frac{\alpha^2 + 7\alpha}{3} \\ &= \frac{-1 - 4\alpha}{3} \\ &= 9 \cdot 1 - 4\left(\frac{\alpha + 7}{3}\right). \end{aligned}$$

Thus, $\begin{pmatrix} -7 & 3 \\ 9 & -4 \end{pmatrix}$ is a representative of the conjugacy class corresponding to the ideal class of $\mathcal{O}_K$.

Corresponding to the class of $\mathbb{Z}[\alpha]$ is the conjugacy class of $\mathcal{C}_f^t$. Thus, the $GL_2(\mathbb{Z})$-conjugacy classes in $\mathcal{M}_f$ are given by the set of representatives

$$\left\{ \begin{pmatrix} -7 & 3 \\ 9 & -4 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & -11 \end{pmatrix} \right\}.$$

Next we review Marseglia's bijection for the more general case of matrices with square-free characteristic polynomial.

Case 2: f has distinct irreducible factors

In the case that f has m distinct irreducible factors over $\mathbb{Z}[x]$, we will describe a bijection due to Marseglia [24]. The following definitions are found in [24] and in Chapter 1 of this dissertation.

Recall that in this case, we let $\alpha = (\alpha_1, .., \alpha_m)$, where α_i is a root of the i-th irreducible factor. Here, $\mathbb{Z}[\alpha]$ denotes the ring of tuples of the form $(p(\alpha_1), .., p(\alpha_m))$ where $p(x) \in \mathbb{Z}[x]$, and there is a natural inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}[\alpha]$ by identifying an integer z with a constant tuple. In this context, the set $\mathcal{I}(\alpha)$ denotes all the fractional $\mathbb{Z}[\alpha]$-ideals ($\mathbb{Z}[\alpha]$-submodules in $K = \prod_{i=1}^{m} \mathbb{Q}(\alpha_i)$ which are also free $\mathbb{Z}$-modules of rank n).

We say that I and J are **equivalent** if they are isomorphic as $\mathbb{Z}[\alpha]$-modules, or equivalently, if there is a non-zero divisor $x \in \prod \mathbb{Q}(\alpha_i)$ such that $I = xJ$.

As in the irreducible case, there is a bijection

$$\varphi : \mathcal{I}(\alpha)/_{\cong_{\mathbb{Z}[\alpha]}} \to \mathcal{M}_f/_{\sim\mathbb{Z}}$$
$$[I] \mapsto [A]$$

where A is the multiplication-by-$(\alpha_1, .., \alpha_m)$ matrix with respect to a $\mathbb{Z}$-basis for I. Note that multiplication here is component-wise.

4.2 LM correspondence over an integral domain R

We will give two separate proofs that the LM correspondence still holds if we replace $\mathbb{Z}$ by any integral domain. The first proof is more theoretical in nature and is based on results in [12] by Estes and Guralnick. The second proof aligns very closely to a proof in [24] due to Marseglia except that some objects are replaced, but we include it since it illustrates the bijection more concretely.

In order to emphasize to which version of the LM correspondence we are referring, let us introduce the following notation. We will write LM-R to indicate the LM correspondence for describing $\mathrm{GL}_n(R)$-conjugacy for any integral domain R. We will use LM-$\mathbb{Z}$ to refer to the original LM correspondence.

4.2.1 A theoretical proof

Estes and Guralnick actually proved that LM-R holds for any integral domain R in the case that f is irreducible [12]. We will now introduce some notation and results of Estes and Guralnick before showing that LM-R holds for f square-free in $R[x]$.

Estes and Guralnick set the following notational conventions, assuming that R is an integral domain:

1. $S := \text{Frac}(R)$ is the fraction field of R.

2. $\mathcal{A} := R[\alpha]$ is a rank n projective R-module. Just as in the case over $\mathbb{Z}$ when f has m distinct irreducible factors, we let α denote an m-tuple.

3. $\mathcal{M}_{\mathcal{A}} := \{M : M \text{ is a faithful left } \mathcal{A}\text{-module and a projective } R\text{-module of rank } n\}$. If one considers the $\mathcal{A}$-module isomorphism classes of $\mathcal{M}_{\mathcal{A}}$, this corresponds to $\text{GL}_n(R)$-conjugacy classes of $\mathcal{C}_f$. This is because we may consider modules in $\mathcal{M}_{\mathcal{A}}$ to be of the form $R^n(T)$ where T is a matrix with characteristic polynomial f.

4. $\mathcal{M}_{\mathcal{A}}(S) := \{M \in \mathcal{M}_{\mathcal{A}} : S \otimes_R M \cong S \otimes_R \mathcal{A}\}$. Here, we mean isomorphism as $S \otimes_R \mathcal{A}$-modules.

5. $\mathcal{I}_{\mathcal{A}}(S) := \{I : I \text{ is a left } \mathcal{A}\text{-module in } S \otimes_R \mathcal{A} \text{ and a projective } R\text{-module of rank } n \text{ with } (S \otimes_R \mathcal{A})I = S \otimes_R \mathcal{A}\}$. Objects in $\mathcal{I}_{\mathcal{A}}(S)$ are the analogues of fractional $\mathbb{Z}[\alpha]$-ideals in our new context.

6. For the sets defined in 3-5, we may apply Cls() to take the $\mathcal{A}$-module isomorphism classes of any of those sets. Note that we obtain LM-R when the isomorphism classes in $\mathcal{M}_{\mathcal{A}}$ correspond to those in $\mathcal{I}_{\mathcal{A}}(S)$; we express this by saying $\text{Cls}(\mathcal{M}_{\mathcal{A}}) = \text{Cls}(\mathcal{I}_{\mathcal{A}}(S))$.

Keeping with the previously defined notation, we list the following theorem due to Estes and Guralnick [12].

Theorem 4.2.1. *([12])*

1. *Cls*$(\mathcal{M}_{\mathcal{A}}(S)) =$ *Cls*$(\mathcal{I}_{\mathcal{A}}(S))$.

2. *If* S *is the fraction field of an integral domain* R*, then* $\mathcal{M}_{\mathcal{A}} = \mathcal{M}_{\mathcal{A}}(S)$ *if and only if* *Hom*$_R(\mathcal{A}, R) \in \mathcal{M}_{\mathcal{A}}(S)$.

3. *If* *Hom*$_R(\mathcal{A}, R) \in \mathcal{M}_{\mathcal{A}}(S)$*, then LM-*$R$ *holds.*

The theorem in [12] is actually stated more generally, but the version given above is enough for our purposes. For the proof of part 1, see Theorem 1 of [12] and Theorem 2 of [12] for the proof of part 2. Since we will use the third part of this theorem, we show how that follows from the other two parts in the proof below.

Proof: For LM-R to hold means that $\text{Cls}(\mathcal{I}_{\mathcal{A}}(S)) = \text{Cls}(\mathcal{M}_{\mathcal{A}})$.

$$\begin{aligned} \text{Hom}_R(\mathcal{A}, R) \in \mathcal{M}_{\mathcal{A}}(S) &\implies \mathcal{M}_{\mathcal{A}}(S) = \mathcal{M}_{\mathcal{A}} \ \text{(Item 2.)} \\ &\implies \text{Cls}(\mathcal{M}_{\mathcal{A}}(S)) = \text{Cls}(\mathcal{M}_{\mathcal{A}}) \\ &\implies \text{Cls}(\mathcal{I}_{\mathcal{A}}(S)) = \text{Cls}(\mathcal{M}_{\mathcal{A}}) \ \text{(Item 1.)} \end{aligned}$$

□

Theorem 4.2.1 says that in order to prove the LM-R correspondence, it is enough to show that $\text{Hom}_R(\mathcal{A}, R) \in \mathcal{M}_{\mathcal{A}}(S)$. Estes and Guralnick prove that LM-R holds in the case that f is irreducible (see Corollary 2 of [12]). The proof is quite succinct, so we provide it next.

Proposition 4.2.2. *(Estes and Guralnick)*
Let R *be an integral domain and let* f *be an irreducible monic polynomial in* $R[x]$*. The* $GL_n(R)$*-conjugacy classes of* $\mathcal{C}_f$ *are in correspondence with the* $R[\alpha]$*-isomorphism classes of* $\mathcal{I}_{R[\alpha]}(S)$.

Proof: We have

$$\begin{aligned}\mathrm{Hom}_R(\mathcal{A}, R) &\cong_{\mathcal{A}} R^n(\mathcal{C}_f^t) \\ &\cong_{\mathcal{A}} R^n(\mathcal{C}_f) \text{ (because the companion matrix is conjugate to its transpose)} \\ &\cong_{\mathcal{A}} \mathcal{A}\end{aligned}$$

so $\mathrm{Hom}_R(\mathcal{A}, R) \in \mathcal{M}_{\mathcal{A}}(S)$, implying that LM-$R$ holds.

□

Before proving LM-R for multiple distinct irreducible factors, we must discuss the trace-dual of an object in $\mathcal{I}_{\mathcal{A}}(S)$ and state a few lemmas.

Since f has no repeated roots over $R[x]$ (nor over $S[x]$), f is separable over $S[x]$. Let F be the splitting field of f over S. Given $I \in \mathcal{I}_{\mathcal{A}}(S)$, we have $I = \oplus v_i R$ for some $v_i \in S(\alpha)$. The **trace-dual** of I is denoted I^t and is given by $I^t = \oplus v_i^* R$ where $\{v_i^*\}$ is a dual-basis with respect to the R-module homomorphism $\mathrm{Tr}_{F/S} : I \to R$ which assigns to an input x the trace of the multiplication-by-x matrix with respect to $\{v_i\}$.

This means that $\mathrm{Tr}(v_i v_j^*) = \delta_i(j)$, the Kronecker delta function. If f has m irreducible factors, note that $\delta_i(j) = \begin{cases} \overline{1} & i = j \\ \overline{0} & i \neq j \end{cases}$, where $\overline{r}$ denotes the constant m-tuple for any $r \in R$.

Lemma 4.2.3. *Define $\phi : I^t \to Hom_R(I, R)$ by $\phi(x) = \varphi_x$ where $\varphi_x(y) = Tr(xy)$. Then ϕ is an R-module isomorphism.*

The proof of this result is standard, so we give it in the appendix.

While we usually write α to denote the m-tuple of the roots of the f_i, we alternate between working with tuples and components of the tuples in the following proof. For clarity, we will write $\overline{\alpha}$ to denote the m-tuple of roots.

Lemma 4.2.4. *Let $f = \prod_{i=1}^{m} f_i \in R[x]$ be a degree n monic, square-free polynomial and let α_i denote a root of f_i. Letting $\overline{\alpha} = (\alpha_1, .., \alpha_m)$, an R-basis for $R[\overline{\alpha}]^t$ is $\{\frac{1}{f'(\overline{\alpha})}, \frac{\overline{\alpha}}{f'(\overline{\alpha})}, ..., \frac{\overline{\alpha}^{n-1}}{f'(\overline{\alpha})}\}$. Therefore, $R[\overline{\alpha}]^t = \frac{1}{f'(\overline{\alpha})} R[\overline{\alpha}]$ and $R[\overline{\alpha}]^t \cong_{R[\overline{\alpha}]} R[\overline{\alpha}]$.*

In Theorem 3.7 of [6], Conrad shows that $\mathbb{Z}[\alpha]^t = \frac{1}{f'(\alpha)}\mathbb{Z}[\alpha]$ where $f \in \mathbb{Z}[x]$ is the square-free minimal polynomial of α. The following proof only differs from Conrad's proof in a few places. First, we consider f with coefficients in a general integral domain R rather than just over $\mathbb{Z}$, so we consider f' as the formal derivative. We are only ever working with polynomials throughout the proof, so the argument carries through. Second, we show that the result holds for m-tuples in $R[\overline{\alpha}]$ by using Galois conjugates. Although this proof is very similar to Conrad's proof, we provide all of the details for completeness.

Proof:

Let $S = \text{Frac}(R)$. Since f is separable over S, we will work over the splitting field of f over S. Let $F = S(\alpha_1, ..., \alpha_n)$ be this splitting field, labeling the roots so that we still have $f_i(\alpha_i) = 0$ for $i = 1, ..., m$.

In $S[x]$, we may write $f = (x - \alpha_1)(c_0(\alpha_1) + ... + c_{n-1}(\alpha_1)x^{n-1})$ where $c_i(\alpha_1)$ is a polynomial in α_1 with coefficients in R. To se this, note that if $f = \sum_{j=1}^{n} r_j x^j$, then we have

$$\begin{aligned}
\frac{f(x)}{(x-\alpha)} &= \frac{f(x) - f(\alpha)}{x - \alpha} \\
&= \frac{1}{x-\alpha} \sum r_i (x^i - \alpha^i) \\
&= \sum r_i \frac{x^i - \alpha^i}{x - \alpha} \\
&= \sum_{i=1}^{n} r_i \sum_{j=0}^{i-1} \alpha^{i-1-j} x^j \\
&= \sum_{j=0}^{n-1} (\sum_{i=j+1}^{n} r_i \alpha^{i-1-j}) x^j
\end{aligned}$$

Thus, we have that $c_j(\alpha) = \sum_{i=j+1}^{n} r_i \alpha^{i-1-j}$. Next, we justify two claims which will give us a particular R-basis for $R[\overline{\alpha}]^t$.

Claim 1: An R-basis for $R[\overline{\alpha}]^t$ is $\{\frac{c_i(\overline{\alpha})}{f'(\overline{\alpha})}\}$.

First, we prove the identity $\sum_{i=1}^{n} \frac{1}{f'(\alpha_i)} \frac{f(x)}{(x-\alpha_i)} = 1$ over R. Note that the polynomial on the left-hand side has degree less than n, so it is enough to show that the equality holds after evaluating at α_j for $j = 1, .., n$.

Because $f = \prod_{i=1}^{n}(x - \alpha_i)$ in $F(x)$, we have

$$\sum_{i=1}^{n} \frac{1}{f'(\alpha_i)} \frac{f(x)}{(x-\alpha_i)} = \sum_{i=1}^{n} \frac{\prod_{k\neq i}(x-\alpha_k)}{f'(\alpha_i)}, \text{ and so}$$

$$\begin{aligned} \sum_{i=1}^{n} \frac{1}{f'(\alpha_i)} \frac{f(\alpha_j)}{(\alpha_j-\alpha_i)} &= \sum_{i=1}^{n} \frac{\prod_{k\neq i}(\alpha_j-\alpha_k)}{f'(\alpha_i)} \\ &= \frac{\prod_{k\neq j}(\alpha_j-\alpha_k)}{f'(\alpha_j)}. \end{aligned}$$

Applying the product rule, we obtain

$f' = \frac{d}{dx}\prod(x-\alpha_i) = \prod_{k\neq j}(x-\alpha_k) + (x-\alpha_j)\frac{d}{dx}\prod_{k\neq j}(x-\alpha_k)$, and so $f'(\alpha_j) = \prod_{k\neq j}(\alpha_j-\alpha_k)$.

Therefore, $\sum_{i=1}^{n} \frac{1}{f'(\alpha_i)} \frac{f(\alpha_j)}{(\alpha_j-\alpha_i)} = \frac{\prod_{k\neq j}(\alpha_j-\alpha_k)}{f'(\alpha_j)} = \frac{\prod_{k\neq j}(\alpha_j-\alpha_k)}{\prod_{k\neq j}(\alpha_j-\alpha_k)} = 1$ for $j = 1, ..., n$.

We have verified that $\sum_{i=1}^{n} \frac{1}{f'(\alpha_i)} \frac{f(x)}{(x-\alpha_i)} = 1$.

Now for $k < n$, we may again evaluate $\sum_{i=1}^{n} \frac{\alpha_i^k}{f'(\alpha_i)} \frac{f(x)}{(x-\alpha_i)}$ at each of the α_j to obtain

$$\sum_{i=1}^{n} \frac{\alpha_i^k}{f'(\alpha_i)} \frac{f(x)}{(x-\alpha_i)} = x^k. \tag{4.1}$$

Using the factorization from the beginning of the proof, we also have that

$$\sum_{i=1}^{n} \frac{\alpha_i^k}{f'(\alpha_i)} \frac{f(x)}{(x-\alpha_i)} = \sum_{i=1}^{n} \frac{\alpha_i^k}{f'(\alpha_i)} (c_0(\alpha_i) + ... + c_{n-1}(\alpha_i)^{n-1} x^{n-1}).$$

Equating the coefficient in front of x^j on both sides of equation (1.1), we have

$$\sum_{i=1}^{n} \frac{\alpha_i^k}{f'(\alpha_i)} c_j(\alpha_i) = 0 \text{ if } j \neq k \text{ and}$$
$$\sum_{i=1}^{n} \frac{\alpha_i^k}{f'(\alpha_i)} c_j(\alpha_i) = 1 \text{ if } j = k, \text{meaning that}$$
$$\text{Tr}_{F/S} \left(\frac{\alpha_1^k c_j(\alpha_1)}{f'(\alpha_1)} \right) = \sum_{i=1}^{n} \frac{\alpha_i^k c_j(\alpha_i)}{f'(\alpha_i)} = \delta_j(k).$$

We may also consider $\text{Tr}_{F/S}(\frac{\alpha_1^k c_j}{f'(\alpha_1)}) = tr(M_{jk})$ where M_{jk} denotes the multiplication-by-$\frac{\alpha_1^k c_j}{f'(\alpha_1)}$ matrix on $R[\alpha_1]$. If $M_{jk} = (m_{li}) \in R^{n \times n}$, then we have that $\frac{\alpha_1^k c_j}{f'(\alpha_1)} \cdot \alpha_1^l = \sum_{i=1}^{n} m_{li} \alpha_1^i$. Using the previous argument, we have that $tr(M) = \begin{cases} 1 & j = k \\ 0 & j \neq k \end{cases}$.

Let us now extend this result to the tuple $\overline{\alpha}$. Since $\alpha_1, .., \alpha_m$ are Galois conjugates, there are elements $\sigma_i \in \text{Gal}(F/S)$ with $\alpha_i = \sigma_i(\alpha_1)$. Recalling that the c_i are polynomials with coefficients in R, we see that $\sigma_i(\frac{\alpha_1^k c_j(\alpha_1)}{f'(\alpha_1)} \cdot \alpha_1^l) = \sigma_i(\sum_{i=1}^{n} m_{li} \alpha_1^i) \implies \frac{\alpha_i^k c_j(\alpha_i)}{f'(\alpha_i)} \cdot \alpha_i^l = \sum_{j=1}^{n} m_{lj} \alpha_i^j$ so that the multipication-by-$\frac{\alpha_i^k c_j(\alpha_i)}{f'(\alpha_i)}$ matrix is the same as the multiplication-by-$\frac{\alpha_1^k c_j(\alpha_1)}{f'(\alpha_1)}$ matrix. Then $\text{Tr}_{F/S} \left(\frac{\alpha_i^k c_j(\alpha_i)}{f'(\alpha_i)} \right) = \delta_j(k)$ for $i = 1, ..., m$.

Thus, $\frac{\overline{\alpha}^k c_j(\overline{\alpha})}{f'(\overline{\alpha})} \cdot \overline{\alpha}^l = \sum_{j=1}^{n} \overline{m_{lj}}\overline{\alpha}^j$ and $tr((\overline{m_{lj}})) = \begin{cases} \overline{1} & j = k \\ \overline{0} & j \neq k \end{cases}$, so $\{\frac{c_i(\overline{\alpha})}{f'(\overline{\alpha})}\}$ is an R-basis for $R[\overline{\alpha}]^t$.

Claim 2: $R[\overline{\alpha}] = \oplus c_0(\overline{\alpha})R \oplus ... \oplus c_{n-1}(\overline{\alpha})R$.

Recall that if $f = \sum_{i=1} r_i x^i$, then

$$c_i(\alpha_1) = \sum_{j=i+1}^{n} r_j \alpha_1^{j-1-i}. \tag{4.2}$$

The transition matrix which has the coefficients of c_{n-j} with respect to the basis $\{\alpha_1^k\}$ in the j-th column is upper triangular with determinant r_n^{n-1}. Since f is monic, $r_n = 1$ and so the transition matrix is an element of $\mathrm{GL}_n(R)$.

Applying σ_l to equation 1.2, we have that $c_j(\alpha_l) = \sum_{j=i+1}^{n} r_j \alpha_l^{j-1-i}$. Then $c_j(\overline{\alpha}) = \sum_{j=i+1}^{n} \overline{r_j}\overline{\alpha}^{j-1-i}$ and so the transition matrix has determinant $\overline{r_n}^{n-1} = \overline{1}$.

Thus, $R[\overline{\alpha}] = \bigoplus_{i=1}^{n} \overline{\alpha}^i R = \bigoplus_{i=1}^{n} c_{i-1}(\overline{\alpha})R$.

Combining claims 1 and 2, we have $R[\overline{\alpha}]^t = \bigoplus_{i=1}^{n} \frac{c_{i-1}(\overline{\alpha})}{f'(\overline{\alpha})} R = \frac{1}{f'(\overline{\alpha})} \bigoplus_{i=1}^{n} c_{i-1}(\overline{\alpha})R = \frac{1}{f'(\overline{\alpha})} R[\overline{\alpha}]$.

Note that $f'(\overline{\alpha})$ is not a zero divisor in $R[\overline{\alpha}]$. Supposing it is, we would have $f'(\alpha_i) = 0$ for some $i \in [1, ..., m]$ and $(x - \alpha_i) \mid \gcd(f, f')$. This contradicts that f is square-free. Then $R[\overline{\alpha}]^t = \frac{1}{f'(\overline{\alpha})} R[\overline{\alpha}]$ implies that $R[\overline{\alpha}]^t \cong R[\overline{\alpha}]$ as $R[\overline{\alpha}]$-modules.

□

We will return to denoting an m-tuple of roots by α rather than $\overline{\alpha}$.

Theorem 4.2.5. *Let R be an integral domain and let f be a polynomial which is square-free over $R[x]$. The $GL_n(R)$-conjugacy classes of $\mathcal{C}_f$ are in correspondence with the $R[\alpha]$-isomorphism classes of $\mathcal{I}_{R[\alpha]}(S)$.*

Referring back to Theorem 4.2.1, it is enough to show that $\text{Hom}_R(R[\alpha], R) \in \mathcal{M}_{R[\alpha]}(S)$.

Proof:

In Lemma 4.2.3, we listed the standard R-module isomorphism $\phi : I^t \to \text{Hom}_R(I, R)$ defined by $\phi(x) = \varphi_x$ where $\varphi_x(y) = \text{Tr}(xy)$. In the case that $I = R[\alpha]$, we may show that ϕ is also an $R[\alpha]$-module homomorphism.

In order to do this, we first define an $R[\alpha]$-module action on $\text{Hom}_R(R[\alpha], R)$ by $x \cdot \varphi_t := \varphi_{xt}$. This is an action because Tr is R-linear.

For any $y \in R[\alpha]$, $\phi(yx) = \varphi_{yx} = y \cdot \varphi_x = y \cdot \phi(x)$, so ϕ is an $R[\alpha]$-module isomorphism. Thus $R[\alpha]^t \cong \text{Hom}_R(R[\alpha], R)$ as $R[\alpha]$-modules via ϕ.

From Lemma 4.2.4, we have that $R[\alpha]^t = \frac{1}{f'(\alpha)} R[\alpha]$ and so $R[\alpha]^t \cong_{R[\alpha]} R[\alpha]$.

We have $\text{Hom}_R(R[\alpha], R) \cong_{R[\alpha]} R[\alpha]^t \cong_{R[\alpha]} R[\alpha]$, so $\text{Hom}_R(R[\alpha], R)$ is a faithful left $R[\alpha]$-module. Since ϕ is an R-module isomorphism, $\text{Hom}_R(R[\alpha], R)$ is a projective R-module of rank n. We also have that $S \otimes_R \text{Hom}_R(R[\alpha], R) \cong_{S \otimes_R R[\alpha]} S \otimes_R R[\alpha]$. Thus, $\text{Hom}_R(R[\alpha], R) \in \mathcal{M}_{R[\alpha]}(S)$. □

4.2.2 The LM-R bijection

We will give an alternate proof that LM-R holds by giving a slight modification of Marseglia's proof of Theorem 8.1 in [24]. Changes include replacing $\mathbb{Z}$ by R and making analogous substitutions. This proof is helpful because it demonstrates the bijection more concretely than the previous proof.

First let us define objects analogous to those in [24].

We define a **fractional $R[\alpha]$-ideal** to be an $R[\alpha]$-submodule of $S(\alpha)$ which is a free R-module of rank n. Just as before, if $f = \prod_{i=1}^{m} f_i$ over $R[x]$ and $f_i(\alpha_i) = 0$, we consider $R[\alpha]$ to consist of polynomials in $\alpha = (\alpha_1, .., \alpha_m)$. We will reuse Estes and Guralnick's notation from the last section

and let $\mathcal{I}_{\mathcal{A}}(S)$ denote the set of fractional $R[\alpha]$-ideals. This is compatible with the definition of $\mathcal{I}_{\mathcal{A}}(S)$ in the previous section because a fractional $R[\alpha]$-ideal is a sub-$R[\alpha]$-module of $S(\alpha)$ and since $S(\alpha) \cong_{R[\alpha]} S \otimes_R R[\alpha]$. We also have that $(S \otimes_R \mathcal{A})I = S \otimes_R \mathcal{A}$ since $S(\alpha)I = S(\alpha)$.

We may partition $\mathcal{I}_{\mathcal{A}}(S)$ into $R[\alpha]$-module isomorphism classes. We say that I and J are equivalent in $\mathcal{I}_{\mathcal{A}}(S)$ if and only if they are isomorphic as $R[\alpha]$-modules. This is equivalent to there being a non-zero divisor $x \in S(\alpha) = \prod_{i=1}^{m} S(\alpha_i)$ such that $I = xJ$. We will maintain Estes and Guralnick's notation and let $\mathrm{Cl}(\mathcal{I}_{\mathcal{A}}(S))$ denote the set of fractional ideal classes.

If $I \in \mathcal{I}_{\mathcal{A}}(S)$, then we may write $I = \oplus v_i R$ where $\{v_i\}$ is an R-basis for I. Then we define

$$\phi : \mathcal{I}_{\mathcal{A}}(S) \to \mathcal{C}_f^{\mathrm{GL}_n(S)}/_{\sim R}$$
$$I \mapsto [T]$$

where T is the multiplication-by-α matrix with respect to an R-basis $\{v_i\}$ of I. With this definition, ϕ is a function independent of the choice of basis for I. This is because if we take another basis given by the vector v', we have $v' = Uv$ for $U \in \mathrm{GL}_n(R)$, and then $\phi(I) = [UTU^{-1}]$ since

$$(UTU^{-1})Uv = UTv = U\alpha v = \alpha Uv.$$

This map is defined analogously to the map in [24], which Marseglia denotes by ϕ. From now on, we will write it as $\phi_{\mathbb{Z}}$ to distinguish the map

$$\phi_{\mathbb{Z}} : \mathcal{I}(\alpha) \to \mathcal{M}_f/_{\sim \mathbb{Z}}$$
$$I \mapsto [T]$$

(here T is the multiplication-by-α matrix with respect to a $\mathbb{Z}$-basis of I) from its generalization, the map ϕ defined previously.

Theorem 4.2.6. *The map ϕ defined before induces a bijection $\widetilde{\phi} : Cl(\mathcal{I}_{\mathcal{A}}(S)) \to \mathcal{C}_f^{GL_n(S)}/_{\sim R}$.*

For completeness, we give the full proof of Theorem 4.2.6 even though it agrees with Marseglia's proof of Theorem 8.1 in [24], apart from the replacement of some objects and with more details provided in some places.

Proof:

$\widetilde{\phi}$ is a function:

Suppose we have $I, J \in \mathcal{I}_{\mathcal{A}}(S)$ and $I \cong J$ as $\mathcal{A}$-modules. Then there is an $\mathcal{A}$-module isomorphism $\varphi : I \to J$. Still suppose that $\{v_i\}_{i=1}^n$ is an R-basis for I and that $\phi(I) = [T]$. Letting $\varphi(v_i)$ be the basis for J, we have that

$$\begin{aligned} T\varphi(v) &= \varphi(Tv) \qquad (\varphi \text{ is } R\text{-linear}) \\ &= \varphi(\alpha v) \\ &= \alpha\varphi(v). \end{aligned}$$

From this we conclude that $\widetilde{\phi}(I) = \widetilde{\phi}(J)$, showing that $\widetilde{\phi}$ is well-defined.

$\widetilde{\phi}$ is injective:

Suppose that there are $I, J \in \mathcal{I}_{\mathcal{A}}(S)$ so that $\widetilde{\phi}(I) = [A], \widetilde{\phi}(J) = [B]$ and $U^{-1}AU = B$. Suppose $\{w_i\}_{i=1}^n$ is an R-basis for J and $w = (w_1, .., w_n)^t$ so that $Bw = \alpha w$. Let $w' = Uw$ give a new R-basis for J. We have

$$\begin{aligned} Aw' &= AUw \\ &= UBU^{-1}Uw \\ &= UBw \\ &= U\alpha w \\ &= \alpha Uw \\ &= \alpha w' \end{aligned}$$

so that I and J correspond to the same matrix with respect to these bases. Now let $\varphi : I \to J$ be the R-module isomorphism defined by $\varphi(v_i) = w_i'$. Then

$$\begin{aligned}
\varphi(\alpha v) &= \varphi(Av) \\
&= A\varphi(v) \quad (\varphi \text{ is } R\text{-linear}) \\
&= Aw' \\
&= \alpha w' \\
&= \alpha\varphi(v)
\end{aligned}$$

so that φ is an $R[\alpha]$-module isomorphism. Then $I \cong J$ via φ.

$\widetilde{\phi}$ is surjective:

We do this by defining a map $\psi : \mathcal{C}_f^{\mathrm{GL}_n(S)} \to \mathrm{Cl}(\mathcal{I}_{\mathcal{A}}(S))$ which induces an injective map $\widetilde{\psi}$ on the conjugacy classes which is the inverse to $\widetilde{\phi}$.

For $A \in \mathcal{C}_f^{\mathrm{GL}_n(S)}$, define $\psi(A)$ as follows. Let $\alpha = (\alpha_1, .., \alpha_m)$. For each α_i find an eigenvector $\overline{v}_i$ with $A\overline{v}_i = \alpha_i\overline{v}_i$. Putting the eigenvectors in as rows in a $m \times n$ matrix, let w_j denote the column vectors of this matrix, so $w_j \in \prod \mathbb{Q}(\alpha_i)$. Let $\psi(A) = [I]$ where $I = \oplus w_i R$.

ψ is well-defined:

The definition of ψ depends on the choice of eigenvectors. A different choice is just given by scaling each eigenvector by a non-zero element $\lambda_i \in S(\alpha_i)$. Let $\overline{\lambda}$ denote the tuple of these scalars. Since

$$\begin{gathered}
S(\alpha) \to S(\alpha) \\
s = (p(\alpha_1), ...p(\alpha_m)) \mapsto \overline{\lambda}s = (\lambda_1 p(\alpha_1), ...\lambda_r p(\alpha_m))
\end{gathered}$$

is an automorphism, we have that $I \cong \overline{\lambda}I$ as $R[\alpha]$-modules. From the map ψ, we get an induced map on conjugacy classes $\widetilde{\psi} : \mathcal{C}_f^{\mathrm{GL}_n(S)}/_{\sim R} \to \mathrm{Cl}(\mathcal{I}_{\mathcal{A}}(S))$.

$\widetilde{\phi}$ is well-defined:

Suppose $B = U^{-1}AU$ for $U \in \mathrm{GL}_n(R)$. Then in defining $\psi(B)$, one may take $U^{-1}\overline{v}_i$ to be the eigenvectors of B. This replaces the w_j by $U^{-1}w_j$, and $\oplus U^{-1}w_j R = \oplus w_j R$ since $U^{-1} \in \mathrm{GL}_n(R)$.

$[I]$ is in the codomain of $\widetilde{\psi}$:

Note that $\alpha w_j = \sum a_{j,h} w_h \in I$. This shows that I is an $R[\alpha]$-module and that $\alpha w = Aw$ so that $\varphi(\psi(A)) = [A]$.

Next is the argument that $S \otimes_R I = S(\alpha)$ so that $I \in \mathcal{I}_{\mathcal{A}}(S)$. Now, $S \otimes_R I$ is an S-vector space, and it can be made into a $S(\alpha)$-vector space via the matrix A. Since f is square-free over $S[x]$, the matrix A is semi-simple and so there is a decomposition $S \otimes_R I = \bigoplus_{i=1}^{k} V_i$ where the V_i are S-vector spaces which are stable under the action of A.

Suppose that the minimal polynomial of $A_{|V_i}$ is g_i. Since V_i is irreducible, we have that g_i is irreducible over $S[x]$ of degree $\dim(V_i)$. Then we have $\prod_{i=1}^{k} g_i(A)(v) = 0$ for all $v \in S \otimes_R I$, meaning that $f \mid \prod_{i=1}^{k} g_i$ since f is the minimal polynomial of A. If $f = \prod_{i=1}^{r} f_i$ where the f_i are irreducible factors, then we must have that $f_i = g_i$ (possibly after relabeling) and $m = k$. So we may assume that $A_{|V_i}$ has minimal polynomial f_i and $\dim(V_i) = \deg(f_i)$.

If $\min(A_{|V_i}) = f_i$ and $f_i(\alpha_i) = 0$, then A acts as α_i on V_i, so that V_i is an $S(\alpha_i)$-vector space. We have an eigenvector v of A corresponding to α_i, so $\mathrm{Span}_{S(\alpha_i)}(v) \subseteq V_i$ and so $\dim_{S(\alpha_i)}(V_i) \geq 1$. Then $\dim_S(V_i) = [S(\alpha_i) : S]\dim_{S(\alpha_i)}(V_i) \geq n_i$ where $n_i = \deg(f_i)$ (because f_i is irreducible over S). Thus, $\dim(S \otimes_R I) = \sum \dim(V_i) \geq \sum n_i = n$ and so $S \otimes_R I = S(\alpha)$.

Since $\widetilde{\psi}$ is the inverse map to $\widetilde{\phi}$, the map $\widetilde{\phi}$ is a bijection.

□

This result has implications for the conjugacy extension problem. First, note that the function ψ in Theorem 4.2.6 is defined analogously to the corresponding map in Theorem 8.1 of [24] (let us denote the latter map by $\psi_{\mathbb{Z}}$ to distinguish it from ψ). In either context, the basis of the corresponding ideal depends only on eigenvectors of the integral matrix in question.

Let us make this more precise. Suppose we consider conjugacy of an integral matrix A with characteristic polynomial f. Say that $\psi_{\mathbb{Z}}(A) = [I]$ and $I = \oplus v_i\mathbb{Z}$. After clearing denominators each v_i can be expressed as a polynomial in α, say $v_i = p_i(\alpha)$ for $p_i \in \mathbb{Z}[x]$. Recall that α denotes a m-tuple of roots where m is the number of irreducible factors of f in $\mathbb{Z}[x]$.

Now consider conjugacy over an integral domain R containing $\mathbb{Z}$. Since f may factor further in $R[x]$, let $\tilde{\alpha}$ denote the tuple of roots of irreducible factors of f over $R[x]$. Since a square-free polynomial in $\mathbb{Z}[x]$ is square-free in $R[x]$ as long as $\mathbb{Z} \subseteq R$, LM-R holds. (To see this, note that if f is square-free in $\mathbb{Z}[x]$, then it is square-free in $\mathbb{Q}[x]$. Then there are polynomials $a, b \in \mathbb{Q}[x]$ with $af + bf' = 1$. If $S = \text{Frac}(R)$ and $\mathbb{Z} \subseteq R$, then $\mathbb{Q} \subset S$. So $af + bf' = 1$ over S, meaning that f is square-free over $S[x]$ and thus over $R[x]$.)

Then we have that $\psi(A) = [\tilde{I}]$ where $\tilde{I} := \oplus \tilde{v_i}R$ and $\tilde{v_i} := p_i(\tilde{\alpha})$. We know that $\{\tilde{v_i}\}$ is an R-basis for $\tilde{I}$ because in the proof of Theorem 4.2.6, it was shown that $\psi(A)$ has full rank.

In the following example, we see how $\psi_{\mathbb{Z}}(A)$ and $\psi(A)$ are related in the case that we begin with an irreducible polynomial f which factors further over R.

Example 4.2.7. *Consider $f = x^4 - 2$ and let $R = \mathbb{Z}[\sqrt[4]{2}]$. Over $R[x]$, we have that f factors as $f = (x^2 + \sqrt{2})(x - \sqrt[4]{2})(x + \sqrt[4]{2})$. Letting α_1 denote a root of $x^2 + \sqrt{2}$, we denote the tuple of roots by $\tilde{\alpha} = (\alpha_1, \sqrt[4]{2}, -\sqrt[4]{2})$.*

The $GL_4(\mathbb{Z})$-conjugacy class of $\mathcal{C}_f^t$ corresponds to $\mathbb{Z}[\alpha]$. We have $\psi_{\mathbb{Z}}(\mathcal{C}_f^t) = [\mathbb{Z}[\alpha]]$. We may express $\mathbb{Z}[\alpha]$ as a free $\mathbb{Z}$-module by writing $\mathbb{Z}[\alpha] = \bigoplus_{i=1}^{4} \alpha^{i-1}\mathbb{Z}$.

The $GL_4(R)$-conjugacy class of the companion matrix corresponds to the ideal class of $\psi(A) = [\widetilde{\mathbb{Z}[\alpha]}]$ where $\widetilde{\mathbb{Z}[\alpha]} = R[\tilde{\alpha}] = \bigoplus_{i=1}^{4}(\alpha_1^{i-1}, \sqrt[4]{2}^{i-1}, (-\sqrt[4]{2})^{i-1})R$. In general, elements in $R[\tilde{\alpha}]$ are of the form $(p(\alpha_1), p(\sqrt[4]{2}), p(-\sqrt[4]{2}))$ where $p \in R[x]$.

Instead of always writing $R[\tilde{\alpha}]$, we will just write $R[\alpha]$ from now on, since what we mean by α is clear from the factorization of f over $R[x]$.

The following proposition tells us that we can describe the relationship between I and $\tilde{I}$ via the tensor product.

Proposition 4.2.8. *Suppose that $I = \oplus v_i\mathbb{Z}$. Then $\varphi_I : R \otimes_{\mathbb{Z}} I \to \oplus \tilde{v}_i R$, defined on simple tensors by $\varphi(r \otimes (v_1 z_1, .., v_n z_n)) = r(v_1 z_1, .., v_n z_n)$, and then extended in the natural way, is an $R[\alpha]$-module isomorphism which is independent of the choice of basis v_i. Furthermore, if $J = \oplus w_i\mathbb{Z}$, then $R \otimes I \cong R \otimes J$ as $R \otimes \mathbb{Z}[\alpha]$-modules if and only if $\oplus \tilde{v}_i R \cong \oplus \tilde{w}_i R$ as $R[\alpha]$-modules.*

See the appendix for the proof.

The previous proposition allows us to denote the extension of a $\mathbb{Z}[\alpha]$-ideal $I = \oplus v_i\mathbb{Z}$ to a ring R (which has $\mathbb{Z}$ as a subring) by $R \otimes_{\mathbb{Z}} I$. So we write $R \otimes I$ to denote the $R[\alpha]$-ideal $\oplus \tilde{v}_i R$.

To summarize, if the $\mathrm{GL}_n(\mathbb{Z})$-conjugacy class of a matrix A corresponds to the $\mathbb{Z}[\alpha]$-class of $I = \oplus v_i\mathbb{Z}$, then the $\mathrm{GL}_n(R)$-conjugacy class of A corresponds to the $R[\alpha]$-class of $R \otimes I$.

According to theorem 4.2.6, there is a bijection $\widetilde{\psi} : \mathcal{C}_f^{\mathrm{GL}_n(S)}/_{\sim R} \to \mathrm{Cl}(\mathcal{I}_{\mathcal{A}}(S))$. For the purposes of the conjugacy extension problem, we wish to restrict our attention to the $\mathrm{GL}_n(R)$-conjugacy classes of $\mathcal{C}_f^{\mathrm{GL}_n(\mathbb{Q})}$ and we have the restricted bijection

$$\begin{aligned} \mathcal{C}_f^{\mathrm{GL}_n(\mathbb{Q})}/_{\sim R} &\to R \otimes_{\mathbb{Z}} \mathcal{I}_{\mathbb{Z}[\alpha]} \\ [A] &\mapsto [R \otimes \psi_{\mathbb{Z}}([A])] \end{aligned}$$

Extending scalars of $\mathbb{Z}[\alpha]$-ideals from $\mathbb{Z}$ to R is compatible with many ideal operations, as we see next. Recall that $(I : J) := \{x \in K : xJ \subseteq I\}$.

Proposition 4.2.9. *If I and J are fractional $\mathbb{Z}[\alpha]$-ideals, and R is a ring containing $\mathbb{Z}$, then $(R \otimes I : R \otimes J) = R \otimes (I : J)$.*

Proof: Suppose $I = \oplus v_i\mathbb{Z}$, $J = \oplus w_i\mathbb{Z}$, and $(I : J) = \oplus x_i\mathbb{Z}$. Then $x_i w_j \in \oplus v_i\mathbb{Z}$ for any $i, j \in [1...n]$ by definition. Since also $x_i w_j \in \oplus v_i R$, we have that

$$R \otimes (I : J) = \oplus x_i R \subseteq (R \otimes I : R \otimes J).$$

The x_i are R-linearly independent and $(R \otimes I : R \otimes J)$ is of rank n, so $(R \otimes I : R \otimes J) = R \otimes (I : J)$.

□

In the next chapter, we will discuss how the results of this section can be used to implement an algorithm which tests for $\mathrm{GL}_n(R)$-conjugacy. First, we must introduce some terminology due to Marseglia [24] which addresses the subtlety that arises when $\mathbb{Z}[\alpha]$ is not equal to $\mathcal{O}_K = \prod \mathcal{O}_{\mathbb{Q}(\alpha_i)}$, the ring of integers in $K = \prod \mathbb{Q}(\alpha_i)$.

In Example 4.1.1, we saw that because $\mathbb{Z}[\alpha]$ is not the ring of integers $K = \mathbb{Q}[x]/(f)$, the set of fractional $\mathbb{Z}[\alpha]$-ideal classes is more than just the Picard group of $\mathcal{O}_K$. To handle this issue, we must consider all of the $\mathbb{Z}[\alpha]$ ideals which contain 1 (and so contain $\mathbb{Z}[\alpha]$). Recall that we say that a $\mathbb{Z}[\alpha]$-ideal which is also a ring with identity is an **over-order** of $\mathbb{Z}[\alpha]$. In Lemma 2.2 of [24], Marseglia shows that the set of over-orders of $\mathbb{Z}[\alpha]$ is the set $\{\mathcal{O} \in \mathcal{I}_{\mathbb{Z}[\alpha]} : \mathcal{O}\mathcal{O} = \mathcal{O}\}$, and he later notes that there are finitely many over-orders.

The $\mathbb{Z}[\alpha]$-ideal classes may be partitioned according to these over-orders. The **multiplicator ring** of a fractional I, denoted by $(I : I)$, is defined to be the largest over-order $\mathcal{O}$ of $\mathbb{Z}[\alpha]$ such that I is an $\mathcal{O}$-module.

It is not too difficult to see that equivalent fractional ideals must have the same multiplicator ring, for if $I = xJ$, then $(I : I) = (xJ : xJ) = x\frac{1}{x}(J : J) = (J : J)$. Also note that $(\mathcal{O} : \mathcal{O}) = \mathcal{O}$ since $\mathcal{O}^2 = \mathcal{O}$, and so distinct over-orders are not equivalent to each other. So we may partition $\mathcal{I}(\alpha)$ into sets of ideals which share the same multiplicator ring and then test for equivalence among ideals in each partition.

We may maintain the same notions of multiplicator ring and over-order for $R[\alpha]$-ideals. As a consequence of Proposition 4.2.9, we have that $(R \otimes I : R \otimes I) = R \otimes (I : I)$, and so these notions are compatible.

Next, we discuss how the result of this section allow us to relate local conjugacy of integral matrices to weak equivalence of ideals.

4.3 Weak equivalence

Via the LM correspondence, we have translated the problem of determining whether matrices are $\mathrm{GL}_n(R)$-conjugate to determining whether certain fractional ideals are equivalent, or isomor-

phic as $R[\alpha]$-modules. There is a notion of local equivalence called **weak equivalence** [24]. We will discuss weak equivalence and its connection to local conjugacy of matrices.

For a fractional $\mathbb{Z}[\alpha]$-ideal I, let $I_{(p)} := \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} I$. We say that $I_{(p)}$ is equivalent to $J_{(p)}$ if they are isomorphic as $\mathbb{Z}[\alpha]_{(p)}$-modules. For $I = \oplus v_i\mathbb{Z}$, Proposition 4.2.8 tells us that $I_{(p)} \cong \oplus \tilde{v_i}\mathbb{Z}_{(p)}$ as $\mathbb{Z}[\alpha]_{(p)}$-modules. Proposition 4.2.9 tells us that $(I_{(p)} : J_{(p)}) = (I : J)_{(p)}$.

We will now prove a slightly altered version of Proposition 4.1 of [24], which is used to define weak equivalence. The next proposition replaces

Statement (a) of Proposition 4.1 in [24]: $I_{\mathfrak{p}}$ and $J_{\mathfrak{p}}$ are isomorphic for every prime $\mathfrak{p}$ of $\mathbb{Z}[\alpha]$ with

Statement 1. of Proposition 4.3.2: $I_{(p)} \cong J_{(p)}$ as $\mathbb{Z}[\alpha]_{(p)}$-modules for all rational primes p.

In Remark 4.3 of [24], Marseglia notes that the replacement can be easily made. Fractional ideals I and J are said to be in the same **genus** if and only if $I_{(p)}$ and $J_{(p)}$ are isomorphic as $\mathbb{Z}[\alpha]_{(p)}$-modules. Therefore, making this replacement shows that weak equivalence coincides with the classical notion of genus (for more on the genus of an ideal see, for example, the last section in Chapter 6 of [27]).

Before the stating the next proposition, we need a lemma by Gilmer from [14].

Lemma 4.3.1. *(Gilmer)*
Let T be a ring with finitely many maximal ideals and let I be a T-ideal. Then I is invertible in T iff I is principal and generated by a non-zero-divisor.

For any ring R, since ideals in $R[\alpha]$ correspond to ideals in $R[x]$ containing (f), we have finitely many maximal ideals, one for each irreducible factor f_i of f. So we may reference this lemma with $T = R[\alpha]$ in the proof of the next proposition.

Proposition 4.3.2. *The following are equivalent. Fractional $\mathbb{Z}[\alpha]$-ideals I and J which satisfy any of the following statements are called **weakly equivalent**.*

1. *$I_{(p)} \cong J_{(p)}$ as $\mathbb{Z}[\alpha]_{(p)}$-modules for all rational primes p.*
2. *$1 \in (I : J)(J : I)$*

3. *I and J have the same multiplicator ring. Let $\mathcal{O} = (I : I) = (J : J)$. Also, $I = (I : J)J$ and $(I : J)$ is an invertible $\mathcal{O}$-ideal.*

Proof:

1. implies 2.

For an arbitrary prime p, suppose $I_{(p)} \cong J_{(p)}$ as $\mathbb{Z}[\alpha]_{(p)}$-modules. Then there is an non-zero divisor x in the total quotient ring of $\mathbb{Z}[\alpha]_{(p)}$ such that $xI_{(p)} = J_{(p)}$. So

$$\begin{aligned}(I : J)(J : I)_{(p)} &= (I : J)_{(p)}(J : I)_{(p)} \\ &= (I_{(p)} : J_{(p)})(J_{(p)} : I_{(p)}) \\ &= (I_{(p)} : xI_{(p)})(xI_{(p)} : I_{(p)}) \\ &= \frac{1}{x}(I_{(p)} : I_{(p)})x(I_{(p)} : I_{(p)}) \\ &= (I_{(p)} : I_{(p)}).\end{aligned}$$

If $a \in (I : J)$ so that $aJ \subseteq I$ and $b \in (J : I)$ so that $bI \subseteq J$, then $ab \in (I : I)$. We have an inclusion $(I : J)(J : I) \hookrightarrow (I : I)$. We wish to show that this map is surjective.

Let $z \in (I : I) \subset (I : I)_{(p)}$. Since $(I_{(p)} : J_{(p)}) = (I : J)_{(p)}(J : I)_{(p)}$, we know that $z = x_p y_p$ for $x_p \in (I : J)_{(p)}$ and $y_p \in (J : I)_{(p)}$. Letting $\{v_i\}$ and $\{w_i\}$ be $\mathbb{Z}_{(p)}$-bases for $(I : J)_{(p)}$ and $(J : I)_{(p)}$, respectively, we may write $x_p = \sum \frac{x_{1i}}{x_{2i}} v_i$ and $y_p = \sum \frac{y_{1i}}{y_{2i}} w_i$ where $x_{ji}, y_{ji} \in \mathbb{Z}$ and $x_{2i}, y_{2i} \notin (p)$.

Clearing denominators, we obtain $mz = \sum x_{1i} v_i \sum y_{1i} w_i$ for some integer m with $m \notin (p)$. Set $x = \sum x_{1i} v_i$ and $y = \sum y_{1i} w_i$. Note that $x \in (I : J)$ and $y \in (J : I)$.

Now fix a prime p_1. By the previous argument, there is $m_1 \notin (p_1)$ and x_1, y_1 in $(I : J)$ and $(J : I)$, respectively, with $m_1 z = x_1 y_1$. For each p_i dividing m_1, we also obtain m_i and x_i, y_i with $m_i z = x_i y_i$ and $m_i \notin (p_i)$. The set $\{m_1, m_2, .., m_k\}$ is relatively prime, so there are integers c_i with $1 = \sum c_i m_i$. From the equation $1 = \sum c_i \frac{x_i y_i}{z}$, we obtain $z = \sum c_i x_i y_i \in (I : J)(J : I)$. Thus, $(I : J)(J : I) = (I : I)$ and $1 \in (I : I)$.

We do not provide the proof of *2. implies 3.*; see the corresponding part of the proof of Proposition 4.1 in [24].

3. implies 1.

This proof is identical to the proof in proposition 4.1 in [24], the only difference being that we consider the ring $\mathbb{Z}[\alpha]_{(p)}$ for a rational prime p rather than $\mathbb{Z}[\alpha]_{\mathfrak{p}}$ for a prime $\mathfrak{p}$ in $\mathbb{Z}[\alpha]$. Since we may still apply Lemma 4.3.1, the only difference is notational.

□

With this notion of weak equivalence, we may now prove a corollary of LM-R.

Corollary 4.3.3. *Let $A, B \in \mathbb{Z}^{n\times n}$ with irreducible characteristic polynomial f and denote a root of f by α. Let I and J be the fractional $\mathbb{Z}[\alpha]$-ideals which correspond to A and B, respectively, via LM-$\mathbb{Z}$. Then A and B are locally conjugate if and only if I and J are weakly equivalent.*

Proof: Suppose that $I = \oplus v_i\mathbb{Z}$ and $J = \oplus w_i\mathbb{Z}$ are the fractional $\mathbb{Z}[\alpha]$-ideals corresponding to A and B, respectively. In the following proof, we will let $\tilde{I}_p$ denote $\oplus\tilde{v_i}\mathbb{Z}_{(p)}$. Also recall that $I_{(p)} = \mathbb{Z}_{(p)} \otimes I$. Then we have

$$
\begin{aligned}
A \text{ and } B \text{ are locally conjugate} &\iff A \sim_{\mathbb{Z}_{(p)}} B \text{ for all primes } p \\
&\iff \tilde{I}_p \text{ is equivalent to } \tilde{J}_p \text{ as } \mathbb{Z}_{(p)}[\alpha]\text{-ideals } \forall\, p \quad (\text{by LM-}\mathbb{Z}_{(p)}) \\
&\iff I_{(p)} \cong J_{(p)} \text{ as } \mathbb{Z}_{(p)} \otimes \mathbb{Z}[\alpha]\text{-modules} \quad (\text{by Proposition } 4.2.8) \\
&\iff I \text{ is weakly equivalent to } J.
\end{aligned}
$$

□

This result has implications for adapting Marseglia's algorithm to test for conjugacy over an extension. For our purposes, we always start with matrices which are locally conjugate so by the previous result, their corresponding fractional ideals are weakly equivalent. Proposition 4.3.2 shows that weakly equivalent fractional ideals have the multiplicator ring.

For R an algebraic extension of $\mathbb{Z}$, we have $(R \otimes I : R \otimes I) = R \otimes (I : I)$ according to Proposition 4.2.9. So we see that $R \otimes I$ and $R \otimes J$ also have the same multiplicator ring. In our extended algorithm, we do not need to check whether fractional ideals have the same multiplicator ring; this is immediate given our assumption of local conjugacy.

Chapter 5

Investigating conjugacy over extensions

5.1 Algorithms

Throughout this section, we preserve the notation used in previous sections. For an integral domain R, we denote its field of fractions by S.

Marseglia gives an algorithm in [24] for determining whether integral matrices with square-free characteristic polynomial are $\mathrm{GL}_n(\mathbb{Z})$-conjugate. This algorithm makes use of the bijection $\psi_{\mathbb{Z}} : \mathcal{C}_f^{\mathrm{GL}_n(\mathbb{Z})} \to \mathrm{Cl}(\mathcal{I}_{\mathbb{Z}[\alpha]}(\mathbb{Q}))$ discussed in the previous section. Since we may obtain a generalized bijection, $\psi : \mathcal{C}_f^{\mathrm{GL}_n(S)} \to \mathrm{Cl}(\mathcal{I}_{R[\alpha]}(S))$, over an integral domain R, we may also adapt Marseglia's algorithm to test for $\mathrm{GL}_n(R)$-conjugacy.

We now give a broad discussion of the steps in an adaptation of Marseglia's algorithm for determining whether integral matrices A and B are $\mathrm{GL}_n(R)$-conjugate for an integral domain R which has $\mathbb{Z}$ as a subring. From now on, we refer to this algorithm as the **$\mathbf{GL}_n(R)$-conjugacy algorithm**. As we will note, the algorithm is valid for matrices in $\mathcal{M}_f$ for square-free f, but it is only possible to implement this adapted algorithm in Magma in the case that f is irreducible in $R[x]$.

5.1.1 The $\mathbf{GL}_n(R)$-conjugacy algorithm

The following are the steps of the $\mathrm{GL}_n(R)$-conjugacy algorithm.

1. Compute the fractional ideal classes $\psi(A)$ and $\psi(B)$.

   If we begin with integral matrices, we may use the restricted bijection

$$\begin{aligned} \mathcal{C}_f^{\mathrm{GL}_n(\mathbb{Q})}/_{\sim R} &\to R \otimes_{\mathbb{Z}} \mathcal{I}_{\mathbb{Z}[\alpha]} \\ [A] &\mapsto [R \otimes \psi_{\mathbb{Z}}([A])]. \end{aligned}$$

If $\psi_{\mathbb{Z}}(A) = I$ where $I = \oplus v_i\mathbb{Z}$, then the $\mathrm{GL}_n(R)$-conjugacy class of A corresponds to the $R[\alpha]$-class of $R \otimes I$. In order for A and B to be $\mathrm{GL}_n(R)$-conjugate, $R \otimes I$ and $R \otimes J$ must be in the same fractional $R[\alpha]$-ideal class.

2. We now consider the multiplicator rings of $R \otimes I$ and $R \otimes J$. If $R \otimes I$ and $R \otimes J$ have different multiplicator rings, then $R \otimes I$ and $R \otimes J$ are not equivalent and A and B are not $\mathrm{GL}_n(R)$-conjugate.

   Since $(R \otimes I : R \otimes I) = R \otimes (I : I)$ (see Proposition 4.2.9), we have that

$$\begin{aligned}(R \otimes I : R \otimes I) = (R \otimes J : R \otimes J) &\iff (I : I) = (J : J) \\ &\iff A \text{ and } B \text{ are locally conjugate.}\end{aligned}$$

   So for the purposes of the conjugacy extension problem, we automatically get that $(R \otimes I : R \otimes I) = (R \otimes J : R \otimes J)$. If $\mathcal{O} = (I : I) = (J : J)$, then $R \otimes \mathcal{O}$ is the shared multiplicator ring of $R \otimes I$ and $R \otimes J$.

Before discussing the final step of the algorithm, we discuss the subtlety of defining the fractional ideals within the proper ring. Since $R \otimes \mathcal{O}$ is the largest over-order of $R[\alpha]$ such that $R \otimes I$ and $R \otimes J$ are $R \otimes \mathcal{O}$-modules, we have that $R \otimes I \sim R \otimes J$ iff $R \otimes I\mathcal{O} = x(R \otimes J\mathcal{O})$ for some $x \in R[\alpha]$.

We also know that in $R \otimes \mathcal{O}$, we have $R \otimes I = R \otimes (I : J)J$ since $I = (I : J)J$ as $\mathcal{O}$-ideals according to Proposition 4.3.2. Then $R \otimes I = x(R \otimes J)$ in $R \otimes \mathcal{O}$ iff $(R \otimes I : R \otimes J) = x(R \otimes \mathcal{O})$. It is important that we define the ideals within $R \otimes \mathcal{O}$ rather than just $R[\alpha]$ because it is possible that $(R \otimes I : R \otimes J) \neq xR[\alpha]$ but $(R \otimes I : R \otimes J) = x(R \otimes \mathcal{O})$ as we see in the next example over $R = \mathbb{Z}$.

Example 5.1.1. *Consider $f = x^2 - 65$ and let $K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$. In this case, we have two over-orders, $\mathbb{Z}[\alpha]$ and $\mathcal{O}_K = 1\mathbb{Z} \oplus \left(\frac{1+\alpha}{2}\right)\mathbb{Z}$. The matrix corresponding to the class*

of $\mathcal{O}_K$ *is* $\begin{pmatrix} -1 & 2 \\ 32 & 1 \end{pmatrix}$. *Taking* $U = \begin{pmatrix} 0 & -1 \\ -1 & 11 \end{pmatrix} \in$ *GL*$_2(\mathbb{Z})$, *we obtain a conjugate matrix,* $B := U^{-1}AU = \begin{pmatrix} -1 & 32 \\ 2 & 1 \end{pmatrix}$.

Now, $\psi_{\mathbb{Z}}(B) = [I]$ *where* $I = 1\mathbb{Z} \oplus \left(\frac{1+\alpha}{32}\right)\mathbb{Z}$. *Since* A *and* B *are* *GL*$_2(\mathbb{Z})$*-conjugate, we know that* J *is in the same ideal class as* $\mathcal{O}_K$. *Let us still go through the process of verifying this to demonstrate why we should work over the correct over-order of* $\mathbb{Z}[\alpha]$.

One may compute that $(I : I) = \mathcal{O}_K$. *So over* $\mathcal{O}_K$, *we have that* $I = (I : \mathcal{O}_K)\mathcal{O}_K$ *and* $(I : \mathcal{O}_K) = I$. *So we must test whether* I *is principal. The following Magma transcript shows the importance of defining* I *over* $\mathcal{O}_K$ *before testing this.*

```
> _<x>:=PolynomialRing(Integers());
> f:=x^2-65;
> K<a>:=NumberField(f);
> OK:=RingOfIntegers(K);
>Za:=sub<OK|a>
```

Za is the sub $\mathbb{Z}$*-module of* $\mathcal{O}_K$ *generated by* α, *so Za=*$\mathbb{Z}[\alpha]$.

```
>I:=ideal<Za|1,(1+a)/32>;
> IsPrincipal(I);
false
> I:=ideal<OK|1,(1+a)/32>;
> IsPrincipal(I);
true
```

This demonstrates that I *is not principal in* $\mathbb{Z}[\alpha]$ *(nor should it be because then we would have that* $B \sim_{\mathbb{Z}} \mathcal{C}_f$, *which is not true), but it is principal in* $\mathcal{O}_K$.

Thus, the final step of the algorithm is to test whether the colon ideal defined over $R \otimes \mathcal{O}$ is principal.

3. If $(R \otimes I\mathcal{O} : R \otimes J\mathcal{O}) = x(R \otimes \mathcal{O})$, then $R \otimes I = x(R \otimes J)$ as $R \otimes \mathcal{O}$-modules and A and B are $\mathrm{GL}_n(R)$-conjugate. If $R \otimes I = \oplus \tilde{v}_i R$ and $R \otimes J = \oplus \tilde{w}_i R$, the conjugating matrix is the change of basis between $\{\tilde{v}_i\}$ and $\{x\tilde{w}_i\}$.

   If $(R \otimes I\mathcal{O} : R \otimes J\mathcal{O})$ is not principal, then $R \otimes I$ and $R \otimes J$ are not equivalent, meaning that A and B are not $\mathrm{GL}_n(R)$-conjugate.

This algorithm is valid for matrices with square-free characteristic polynomial, but it is only in the irreducible case that we can easily implement this generalized algorithm in Magma. If f is irreducible in $R[x]$, then Step 3 may be carried out using the subroutine IsPrincipal. In the case that the characteristic polynomial has multiple irreducible factors in $R[x]$, then the fractional ideals are defined within an algebra of the form $\prod_i S(\alpha_i)$, where $S = \mathrm{Frac}(R)$. In Magma, the IsPrincipal function may not be applied to such fractional ideals since they do not live in an étale algebra defined over $\mathbb{Q}$. Therefore, it is not obvious how one might implement this algorithm in Magma in the non-irreducible case.

Next, we illustrate how the generalized algorithm may be used in an example.

Example 5.1.2. *The matrix* $A = \begin{pmatrix} -2 & 3 \\ 26 & 2 \end{pmatrix}$ *has irreducible characteristic polynomial* $f = x^2 - 82$. *Let* α *denote a root of* f.

We will show that A *is not* $\mathrm{GL}_2(\mathbb{Z})$*-conjugate to* $\mathcal{C}_f$*, but that it is* $\mathrm{GL}_2(R)$*-conjugate to* $\mathcal{C}_f$ *for* R *the ring of integers of the number field* $L = \mathbb{Q}(\beta) \cong \mathbb{Q}[x]/(x^4 - 28x^2 + 32)$. *Note that* f *remains irreducible in* $R[x]$. *(We will later discuss how we chose this ring* R*.)*

Let us first make use of LM-$\mathbb{Z}$ *to consider* $\mathrm{GL}_2(\mathbb{Z})$*-conjugacy of these matrices. We compute* $\psi_{\mathbb{Z}}(A)$ *by finding that* $(3, \alpha + 2)^t$ *is an eigenvector of* A *with eigenvalue* α. *Then* $\psi_{\mathbb{Z}}(A) = [I]$ *where* $I = 3\mathbb{Z} \oplus (\alpha + 2)\mathbb{Z}$. *Similarly,* $\psi_{\mathbb{Z}}(\mathcal{C}_f) = [1\mathbb{Z} \oplus \alpha\mathbb{Z}]$.

In this situation, $\mathbb{Z}[\alpha]$ is the ring of integers of $K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$. Since $\mathbb{Z}[\alpha]$ is the only over-order, we know that I and $\mathbb{Z}[\alpha]$ both have multiplicator ring $\mathbb{Z}[\alpha]$. The fact that I and $\mathbb{Z}[\alpha]$ are weakly equivalent corresponds to the fact that A and $\mathcal{C}_f$ are locally conjugate.

Next, we find that $(I : \mathbb{Z}[\alpha]) = I$ is not principal as a $\mathbb{Z}[\alpha]$-ideal, and so we conclude that A is not $GL_2(\mathbb{Z})$-conjugate to $\mathcal{C}_f$.

Now let us apply the generalized algorithm to consider conjugacy over $R = \mathcal{O}_L$. Since f remains irreducible over R, we simply have that $\psi(A) = [R \otimes I]$ where $R \otimes I = 3R \oplus (\alpha + 2)R$ and $\psi(\mathcal{C}_f) = [1R \oplus \alpha R]$.

Since $(R \otimes I : R \otimes I) = R \otimes (I : I) = R \otimes \mathbb{Z}[\alpha] = R[\alpha]$, we see that $R \otimes I$ and $R[\alpha]$ share the same multiplicator ring.

Next, we find that $(R \otimes I : R[\alpha]) = R \otimes I$ is principal as an $R[\alpha]$-ideal. Letting x denote the generator so that $R \otimes I = xR[\alpha]$, we compute the change of basis between the R-bases $\{x, x \cdot \alpha\}$ and $\{3, \alpha + 2\}$ of $R \otimes I$.

Letting (v_1, v_2, v_3, v_4) denote the coordinates of an element in R with respect to the $\mathbb{Z}$-basis $\{1, \frac{1}{2}\beta, \frac{1}{4}\beta^2, \frac{1}{16}(\beta^3 - 2\beta^2)\}$, we find that the transition matrix C is

$$\begin{pmatrix} (1816703, -701754, -3735950, 4702848) & (16450528, -6354814, -33828528, 42587180) \\ (772459, -298397, -1588478, 1999726) & (6995027, -2702056, -14384806, 18107996) \end{pmatrix}.$$

Furthermore, we can check that determinant of C is a unit in R, and $C^{-1}AC = \mathcal{C}_f$.

5.1.2 Complexity

We now briefly discuss the complexity of the $\mathrm{GL}_n(R)$-conjugacy algorithm in the case that $R = \mathbb{Z}$. Keeping with the notation used thus far, we assume that the input matrices, denoted A and B, have characteristic polynomial f of degree n and root α. We consider the run time of the algorithm in terms of n and d_K, the discriminant of $K = \mathbb{Q}[x]/(f)$.

Some steps of the algorithm will run in polynomial time. For instance, the first step of the algorithm entails finding the corresponding ideal class representatives associated to the given matrices.

This amounts to computing eigenvectors of the matrix, which takes polynomial time in n (see for instance, [13]).

However, the third step entails testing whether a particular fractional $\mathbb{Z}[\alpha]$-ideal is principal. For a number field K, the problem of testing for principality of fractional $\mathcal{O}_K$-ideals is considered to be no simpler than the problem of computing the class group and unit group of $\mathcal{O}_K$ [19]. The most efficient known algorithm for solving the latter problem is Buchmann's algorithm [3], which has run time $d_K^{1/2}(\log(d_K))^{O(n)}$ [22]. Thus, it appears that the $\mathrm{GL}_n(R)$-conjugacy algorithm has run time which is exponential in n.

In the next section, we compute examples of solving the conjugacy extension problem in Magma. Due to the limitations of IsPrincipal discussed previously, we primarily consider integral matrices in $\mathcal{M}_f$ where f is irreducible in $R[x]$.

5.2 Subfields of the Hilbert class field

We will now discuss how class field theory can be used to generate candidates for solutions to the conjugacy extension problem. Suppose we are working with locally conjugate integral matrices in $\mathcal{M}_f$ with f irreducible, and let α denote a root of f. If the matrices are not $\mathrm{GL}_n(\mathbb{Z})$-conjugate, then the ideals, I and J, corresponding to those matrices, are not equivalent.

However, we know that I and J are weakly equivalent and so they share the same multiplicator ring, call it $\mathcal{O}$. We know that $(I : J)$ is invertible in $\mathcal{O}$ by Proposition 4.3.2. Lemma 2.5 of [24] tells us that if I is an invertible $\mathcal{O}$-ideal, then $(I : I) = \mathcal{O}$, so $(I : J)$ has multiplicator ring $\mathcal{O}$.

Since I and J are not equivalent as $\mathcal{O}$-ideals, that means that $(I : J)$ is not principal in $\mathcal{O}$. We will now give the definition of the Hilbert class field and discuss how it provides an extension in which $(I : J)$ is principal.

Definition 5.2.1. *(see Chapter 6, Section 4 of [4])*
For a number field K, the Hilbert class field of K is the maximal unramified abelian extension of K. Denoting the Hilbert class field by L, we have that Gal(L/K) is isomorphic to the ideal class group so that $[L : K] = h_K$.

We may now state the following useful theorem from class field theory, known as the Principal Ideal Theorem.

Theorem 5.2.2. *(See Theorem 4.2 of [4]).*
Let $K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$ and let L be the Hilbert class field of K. In the ring of integers $\mathcal{O}_L$, every fractional $\mathcal{O}_K$-ideal becomes principal.

For any over-order $\mathcal{O}$ of $\mathbb{Z}[\alpha]$, we have that $\mathcal{O} \subseteq \mathcal{O}_K$ and so we have the following composition of maps:

$$\text{Pic}(\mathcal{O}) \to \text{Pic}(\mathcal{O}_K) \to \text{Pic}(\mathcal{O}_L)$$
$$I \mapsto I\mathcal{O}_K \mapsto I\mathcal{O}_L$$

By the Principal Ideal Theorem, for any $I \in \text{Pic}(\mathcal{O})$, we know that $I\mathcal{O}_K$ becomes principal in $\mathcal{O}_L$. In other words, $I\mathcal{O}_L$ is principal for any invertible fractional $\mathcal{O}$-ideal I, including $(I : J)$.

At first glance, $\mathcal{O}_L$ seems to solve the conjugacy extension problem. However, some difficulties arise since $\alpha \in \mathcal{O}_L$, meaning f no longer remains irreducible in $\mathcal{O}_L[x]$. Suppose that $f = \prod_{i=1}^{m} f_i$ over $\mathcal{O}_L$. Determining whether matrices are $\mathcal{O}_L$-conjugate amounts to determining whether a fractional $\mathcal{O}_L[\alpha]$-ideal in L^m is principal. This does not immediately follow from the fact that the ideals formed by isolating each component become principal.

Let us illustrate what we have discussed so far in an example.

Example 5.2.3. *Let $f = x^2 + 5$ and $K = \mathbb{Q}[x]/(f)$. The fractional ideal $I = 2\mathbb{Z} \oplus (\alpha + 1)\mathbb{Z}$ is not principal and corresponds to $A = \begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix}$ via the LM-$\mathbb{Z}$ correspondence. Since $\mathbb{Z}[\alpha]$ is the ring of integers of K, the only over-order is $\mathbb{Z}[\alpha]$, meaning I is weakly equivalent to $\mathbb{Z}[\alpha]$ and A is locally conjugate to $\mathcal{C}_f$.*

Let L denote the Hilbert class field of K. Due to the fact that $h_K = 2$ in this example, we have that $[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] = h_K \cdot 2 = 4$.

More specifically, $L = \mathbb{Q}(\beta) \cong \mathbb{Q}[x]/(x^4 + 12x^2 + 16)$. *Let us also discuss the LM*$-R$ *correspondence for* $R = \mathcal{O}_L$. *Since* $\alpha \in \mathcal{O}_L$, *we have that* $f = (x - \alpha)(x + \alpha)$ *in* $R[x]$. *Then* $R[\alpha] = R[(\alpha, -\alpha)]$ *and we have the embedding* $R \hookrightarrow R[(\alpha, -\alpha)]$ *by considering elements in* R *as constant tuples.*

The $GL_2(R)$*-conjugacy class of* A *corresponds to the fractional* $R[(\alpha, -\alpha)]$*-ideal class of* $R \otimes I = (2, 2)R \oplus (\alpha + 1, -\alpha + 1)R$. *Considering each component, we know that* $2R \oplus (\alpha + 1)R$ *and* $2R \oplus (-\alpha + 1)R$ *are each principal. However, this does not imply that* $R \otimes I$ *is principal as an* $R[(\alpha, -\alpha)]$*-ideal. We will determine whether* $R \otimes I$ *is principal by considering solutions to an* R*-linear system. We will do this by making use of the* $\mathbb{Z}$*-basis* $\mathcal{B} = \{1, \frac{1}{2}\beta, \frac{1}{4}\beta^2, \frac{1}{8}\beta^3\}$ *for* R. *We will denote the* i*-th basis element of* $\mathcal{B}$ *by* $\mathcal{B}_i$.

In order for $R \otimes I$ *to be principal, there must be a generator* $(\gamma_1, \gamma_2) \in L(\alpha) \times L(-\alpha) = L \times L$ *and there must exist* $(r_i, r_i) \in R$ *with*

$$(2, 2)(r_1, r_1) + (\alpha + 1, -\alpha + 1)(r_2, r_2) = (\gamma_1, \gamma_2)$$
$$(2, 2)(r_3, r_3) + (\alpha + 1, -\alpha + 1)(r_4, r_4) = (\gamma_1\alpha, -\gamma_2\alpha).$$

We also require that the determinant of this change of basis is a unit in R. *However, we will be able to show that the system does not have a solution even before considering determinants.*

As mentioned previously, we cannot easily test whether $R \otimes I$ *is principal using the IsPrincipal function since* $R \otimes I$ *is defined within* $L \times L$, *an algebra which is not an étale* $\mathbb{Q}$*-algebra.*

Considering each component separately, we see that both $2R \oplus (\alpha + 1)R$ *and* $2R \oplus (-\alpha + 1)R$ *become principal in* R. *In fact,* $2R \oplus (\alpha + 1)R = 2R \oplus (-\alpha + 1)R = (g)$ *where* $g = \mathcal{B}_1 - 2\mathcal{B}_1 - \mathcal{B}_4$.

If $(2, 2)R \oplus (\alpha + 1, -\alpha + 1)R = (\gamma_1, \gamma_2)R \oplus (\gamma_1\alpha, -\gamma_2\alpha)R$, *then*

$$2R \oplus (\alpha + 1)R = (\gamma_1)$$

and

$$2R \oplus (-\alpha + 1)R = (\gamma_2).$$

So we must have $\gamma_1 = gu_1$ and $\gamma_2 = gu_2$ for some units u_1 and u_2 in R. Scaling the equations by u_1^{-1}, we may assume that $\gamma_1 = g$ and $\gamma_2 = gu$ for some $u \in R^\times$.

If $R \otimes I$ is principal, there must be a solution (r_1, r_2, r_3, r_4) over R satisfying the equations

$$2r_1 + (\alpha+1)r_2 = g \qquad 2r_3 + (\alpha+1)r_4 = g\alpha$$
$$2r_1 + (-\alpha+1)r_2 = gu \qquad 2r_3 + (-\alpha+1)r_4 = -gu\alpha.$$

Working with respect to the basis $\mathcal{B}$, we will translate this to solving a linear system over the integers. Throughout this example, let M_x denote the multiplication-by-x matrix on R with respect to the basis $\mathcal{B}$. Let $r_1 = \sum_{i=1}^{4} x_i\mathcal{B}_i$ and $r_2 = \sum_{i=1}^{4} y_i\mathcal{B}_i$, $T_1 = [2I_4 \mid M_{\alpha+1}]$ and $T_2 = [2I_4 \mid M_{-\alpha+1}]$. For an element $x \in \mathcal{O}_L$, we will denote the coefficient vector of x with respect to $\mathcal{B}$ by $[x]_\mathcal{B}$. We will also let $\begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix}$ denote the vector $(x_1, .., x_4, y_1, ..y_4)$.

Then solving

$$2r_1 + (\alpha+1)r_2 = g$$
$$2r_1 + (-\alpha+1)r_2 = gu$$

over R is equivalent to solving

$$T_1 \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} = M_g[1]_\mathcal{B} \text{ and } T_2 \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} = M_g[u]_\mathcal{B} \text{ over } \mathbb{Z}.$$

A solution to the above system must satisfy the equation

$$(T_1 - T_2) \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} = M_g([1-u]_\mathcal{B}). \tag{5.1}$$

Thus, we will consider integral solutions to Equation 5.1. Note that here, the matrix $T_1 - T_2 = [0_{4\times4} \mid M_{2\alpha}]$.

For a given unit u, we can attempt to solve equation (5.1) using the Smith normal form. There are matrices $P \in GL_4(\mathbb{Z})$ and $Q \in GL_8(\mathbb{Z})$ with $P(T_1 - T_2)Q = S$ where

$$S = \left(\begin{array}{cccc|c} 2 & & & & \\ & 2 & & & \\ & & 10 & & \mathbf{0}_{4\times 4} \\ & & & 10 & \end{array}\right).$$

We know Equation 5.1 has an integral solution $\begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} = Q \begin{pmatrix} \boldsymbol{v}_{4\times 1} \\ \hline \boldsymbol{z}_{4\times 1} \end{pmatrix}$ *exactly if the vector* $\boldsymbol{v} = \left(\frac{PM_g[1-u]_{\mathcal{B}}}{(2,2,10,10)^t}\right)$ *has integral components (this division is component-wise). Note that* $\boldsymbol{z}$ *denotes any vector in* $\mathbb{Z}^4$ *. The null space of* $T_1 - T_2$ *is Span*$_{\mathbb{Z}}(\mathbf{e_1}, \mathbf{e_2}, \mathbf{e_3}, \mathbf{e_4}) \subseteq \mathbb{Z}^{\mathbf{8}}$*, meaning that given a solution* $(r_1, r_2) \in R^2$*, the set of all solutions is* $\{(r, r_2) : r \in R\}$*.*

We now ask whether $(2, 2, 10, 10)^t$ *is in the column space of* PM_g*. We find that the solution space of* $PM_g\overline{x} = (2, 2, 10, 10)^t$ *is given by Span*$_{\mathbb{Z}}((-1, -1, 1, -4)^t)$*. In order for Equation 5.1 to have a solution, we must have that* $[1 - u]_{\mathcal{B}}$ *is some integral multiple of* $(-1, -1, 1, -4)^t$*.*

We will consider whether it is possible for there to be a unit $u \in R$ *such that*

$$1 - u = k(-\mathcal{B}_1 - \mathcal{B}_2 + \mathcal{B}_3 - 4\mathcal{B}_4), \text{ or}$$
$$u = 1 + k(\mathcal{B}_1 + \mathcal{B}_2 - \mathcal{B}_3 + 4\mathcal{B}_4) \text{ for } k \in \mathbb{Z}.$$

Note that if $u = 1$*, this corresponds to* $k = 0$*. In this situation, the solution set to Equation 5.1 is* $\overline{0}$ + *Span*$_{\mathbb{Z}}(\mathbf{e_1}, \mathbf{e_2}, \mathbf{e_3}, \mathbf{e_4})$*. Written as a tuple in* R^2*, solutions are given by* $\{(r_1, r_2) = (r, 0) : r \in R\}$*.*

Thus, any solution to

$$2r_1 + (\alpha + 1)r_2 = g$$
$$2r_1 + (-\alpha + 1)r_2 = g$$

must satisfy $r_2 = 0$. *From the previous constraint, we see that there is a unique solution, the tuple* $(\frac{g}{2}, 0)$.

We repeat the same argument for the system

$$2r_3 + (\alpha + 1)r_4 = g\alpha$$
$$2r_3 + (-\alpha + 1)r_4 = -g\alpha.$$

A solution to the previous system must satisfy $(T_1 - T_2)\begin{pmatrix} \mathbf{x} \\ \\ \mathbf{y} \end{pmatrix} = M_g([2\alpha]_{\mathcal{B}})$.

Using the Smith normal form, we find that $PM_g([2\alpha]_{\mathcal{B}}) = (-4, -10, -14, -10)$ *is not divisible by* $(2, 2, 10, 10)$*, meaning there is no solution to the second system when* $u = 1$. *This work shows that as* $R[(\alpha, -\alpha)]$*-ideals,* $(2, 2)R \oplus (\alpha + 1, -\alpha + 1) \neq (\gamma, \gamma)R$ *for any* $\gamma \in L$.

We now consider whether there are other units which could lead to a solution to equation (5.1) by making a norm argument. If

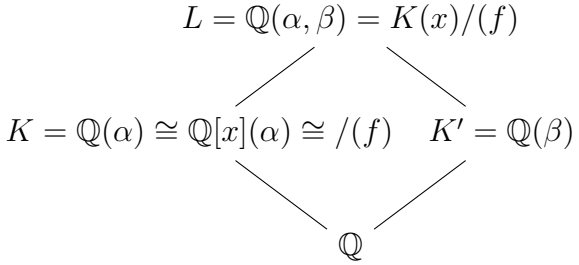
$$u = 1 + k(\mathcal{B}_1 + \mathcal{B}_2 - \mathcal{B}_3 + 4\mathcal{B}_4) \text{ for some } k \in \mathbb{Z}, \text{ then}$$
$$\pm 1 = N_{L/\mathbb{Q}}(u) = \prod_{\sigma \in Gal(L/\mathbb{Q})} 1 + k\sigma(\mathcal{B}_1 + \mathcal{B}_2 - \mathcal{B}_3 + 4\mathcal{B}_4)$$
$$= 500k^4 + 700k^3 + 270k^2 + 10k + 1$$

One may check that $500k^4 + 700k^3 + 270k^2 + 10k + 1 = -1$ *has no integer root and that the only integer root of* $500k^4 + 700k^3 + 270k^2 + 10k + 1 = 1$ *is* $k = 0$*, but we already addressed that case. This shows that for any* $u \in R^\times \setminus \{1\}$, $PM_g[1 - u]_{\mathcal{B}}$ *is not a multiple of* $(2, 2, 10, 10)^t$*, and so there is no integral solution to equation (5.1).*

We have shown that $(2, 2)R \oplus (\alpha + 1, -\alpha + 1)R \neq (g, ug)R[\alpha]$ *for any* $u \in R^\times$. *Thus,* $R \otimes I$ *is not a principal* $R[(\alpha, -\alpha)]$*-ideal. We conclude that* A *is not conjugate to* $\mathcal{C}_f$ *over the ring of integers of the Hilbert class field of* K.

This example shows that if L denotes the Hilbert class field of $\mathbb{Q}[x]/(f)$, then $\mathcal{O}_L$ does not necessarily provide an algebraic extension over which locally conjugate matrices in $\mathcal{M}_f$ are conjugate. Although fractional $\mathbb{Z}[\alpha]$-ideals become principal in $\mathcal{O}_L$, the fact that f factors further over $\mathcal{O}_L$ means that $\mathcal{O}_L$-conjugacy classes correspond to objects within a product of number fields. Computing whether such objects are principal is non-trivial and does not immediately follow from the fact that each component becomes principal.

To avoid the computational difficulties that arise in the non-irreducible case, we may attempt to find a subfield K' of L which has the property that $\alpha \notin K'$ so that f remains irreducible in K' and we get the following extension of fields:



We also want a subfield K' of L such that $(I : J)$ is principal in $O_{K'} \otimes_{\mathbb{Z}} \mathcal{O}$, where $\mathcal{O}$ is the over-order of $(I : J)$. If we can find such a subfield, then A and B are $\mathcal{O}_{K'}$-conjugate. We cannot guarantee that such a subfield exists, but this line of thinking provides a helpful method for searching for solutions to the conjugacy extension problem.

The following is an example in which the method of searching through subfields of the Hilbert class field was successful.

Example 5.2.4. *Let $f = x^2 - 15$ and $K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$, which has class number 2. We have that $\mathbb{Z}[\alpha]$ is the maximal order and $(2, \alpha + 1)$ is a non-principal ideal corresponding to $A = \begin{pmatrix} -1 & 7 \\ 2 & 1 \end{pmatrix}$. Since there is only one over-order, all fractional $\mathbb{Z}[\alpha]$-ideals are weakly equivalent and so A is locally conjugate to $\mathcal{C}_f$.*

Let L denote the Hilbert class field of K. Since $h_K = 2$, we have $[L : \mathbb{Q}] = 2[K : \mathbb{Q}] = 4$. In Magma we find that there are three degree 2 subfields of L. One of these subfields can be defined by $g = x^2 + 2x - 11$. Letting $K' = \mathbb{Q}[x]/(g)$, we find that f remains irreducible over K'.

We will work over the sub-ring $\mathcal{O}_{K'}[\alpha]$ of $\mathcal{O}_L$. Letting y denote the primitive element of L, we have that $\mathcal{B} = \{1, y, \frac{1}{4}(y^2 + 2y + 10), \frac{1}{12}(y^3 + 6y + 4)\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_{K'}[\alpha]$. Denote the i-th basis element by $\mathcal{B}_i$.

We find that I is principal as an $\mathcal{O}_{K'}[\alpha]$-ideal, with generator $\gamma = -170 - 89\mathcal{B}_2 + 20\mathcal{B}_3 + 17\mathcal{B}_4$. Then $\{2, \alpha + 1\}$ and $\{\gamma, \gamma\alpha\}$ are both $\mathcal{O}_{K'}$-bases for I. Letting β denote a root of g, we find that

$$\gamma = 2(-\beta - 8) + (\alpha + 1)(\beta + 2)$$

and

$$\gamma \cdot \alpha = 2(8\beta + 22) + (\alpha + 1)(-\beta - 14).$$

Thus, the transition matrix $\begin{pmatrix} -\beta - 8 & 8\beta + 22 \\ \beta + 2 & -\beta - 14 \end{pmatrix}$ *conjugates A to $\mathcal{C}_f$. The determinant of this conjugating matrix is a unit in $\mathcal{O}_{K'}$.*

Example 5.2.5. *This method was the means by which we obtained R in example 5.1.2. For $f = x^2 - 82$ and $K = \mathbb{Q}[x]/(f)$, we found that $K' = \mathbb{Q}[x]/(x^4 - 28x^2 + 32)$ is a subfield of the Hilbert class field of K with the desired properties. For one, f remains irreducible over $\mathcal{O}_{K'}[x]$. We also find that the non-principal ideal $I = 3\mathbb{Z} \oplus (\alpha + 2)\mathbb{Z}$ with multiplicator ring $\mathcal{O}_K$ (in this case, $\mathbb{Z}[\alpha] = \mathcal{O}_K$ so there is only one over-order) is principal as an $\mathcal{O}_{K'}[\alpha]$-ideal. This is how we found that the matrix A in example 5.1.2 is $GL_2(\mathcal{O}_{K'})$-conjugate to $\mathcal{C}_f$.*

While we have seen some examples in which we were able to solve the conjugacy extension problem with the ring of integers of a certain subfield of the Hilbert class field, we cannot always find a subfield that satisfies the necessary criteria. Let us go back to the number field from Example 5.2.3.

Example 5.2.6. *Let $f = x^2 + 5$. Recall that $A = \begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix}$ corresponds to the non-principal $\mathbb{Z}[\alpha]$-ideal $I = 2\mathbb{Z} \oplus (\alpha + 1)\mathbb{Z}$. Since the only over-order of $\mathbb{Z}[\alpha]$ is itself, A is locally conjugate to $\mathcal{C}_f$.*

The Hilbert class field of K is $L = \mathbb{Q}[x]/(x^4 + 12x^2 + 16)$. There are three proper subfields of L. In two of these subfields, call them F_1 and F_2, f is irreducible. However, $\mathcal{O}_{F_i} \otimes_{\mathbb{Z}} I$ is not principal as an $\mathcal{O}_{F_i}[\alpha]$-ideal for $i = 1, 2$.

This agrees with our findings from Example 5.2.3. We previously showed that A is not conjugate to $\mathcal{C}_f$ over $\mathcal{O}_L$, so they cannot be conjugate over the ring of integers of any proper subfield of L.

If L denotes the Hilbert class field of $\mathbb{Q}[x]/(f)$, it is of course possible that matrices in $\mathcal{M}_f$ could be conjugate over $\mathcal{O}_L$, but not over $\mathcal{O}_F$ for any proper subfield F of L. However, since f factors further over $\mathcal{O}_L$, determining whether an ideal is principal becomes quite difficult as we saw in Example 5.2.3. While the Hilbert class field does not necessarily solve the conjugacy extension problem, we have had some success in finding proper subfields F of L in which f remains irreducible and ideals are principal after extending to $\mathcal{O}_F$.

In this section, we saw that the Hilbert class field of K is the maximal unramified abelian extension of K. We may have more success in solving the conjugacy extension problem if we search through subfields of a larger extension of K, so we will now discuss the notion of a ray class field, which generalizes the Hilbert class field by allowing for ramification at finitely many primes.

5.2.1 Subfields of the ray class field

In the previous section, we gave a method for searching through subfields of the Hilbert class field of $\mathbb{Q}[x]/(f)$ in an attempt to solve the conjugacy extension problem for matrices in $\mathcal{M}_f$. We will now discuss how we can transfer this method to a slightly different context. We may do this because there is analogue of the Principal Ideal Theorem for ray class fields. First we need some definitions.

Definition 5.2.7. *(See Chapter 2, Section 1 of [4].)*
*A **modulus** $\mathfrak{m}$ of K is a formal product of infinite primes, which are real embeddings of K into $\mathbb{C}$, and primes of K. We can write a modulus $\mathfrak{m}$ as $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ where $\mathfrak{m}_0$ is a finite product of*

the primes of K (and so it is an ideal of $\mathcal{O}_K$) and $\mathfrak{m}_\infty$ is a formal product of a subset of the real embeddings of K (embeddings of K into $\mathbb{C}$ with real image).

For a modulus $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ we say that

$$x \equiv 1 \bmod \mathfrak{m} \iff \begin{cases} \text{ord}_\mathfrak{p}(x-1) \geq \text{ord}_\mathfrak{p}(\mathfrak{m}_0) & \text{for all } \mathfrak{p} \mid \mathfrak{m}_0 \\ \sigma(x) > 0 & \text{for all } \sigma \mid \mathfrak{m}_\infty \end{cases}$$

(see Section 2.3 of [1]). Note that in the above, $\text{ord}_\mathfrak{p}(x)$ denotes the power of $\mathfrak{p}$ in the factorization of x.

We may now define the ray class group of K with modulus $\mathfrak{m}$.

Definition 5.2.8. *[1]*

Let $I_\mathfrak{m}$ denote the set of ideals of $\mathcal{O}_K$ which are relatively prime to $\mathfrak{m}_0$.
*Let $K_\mathfrak{m} = \{x \in K : x \equiv 1 \text{ mod } \mathfrak{m}\}$ and $P_\mathfrak{m} = \{I \in I_\mathfrak{m} : I = (x) \text{ for some } x \in K_\mathfrak{m}\}$. Then the **ray class group with modulus** $\mathfrak{m}$ is defined to be the quotient $Cl_\mathfrak{m} = I_\mathfrak{m}/P_\mathfrak{m}$.*

The ray class group is a generalization of the usual ideal class group. As with the ideal class group, it is known that the ray class group is a finite abelian group [1]. We wish to discuss the conductor of a ray class group, as it is important to the description of ray class fields.

Definition 5.2.9. *[1] For two moduli $\mathfrak{n}$ and $\mathfrak{m}$, we say that $\mathfrak{n} \mid \mathfrak{m}$ if $\mathfrak{n}_0 \mid \mathfrak{m}_0$ and $\mathfrak{n}_\infty \subseteq \mathfrak{m}_\infty$. If $\mathfrak{n} \mid \mathfrak{m}$, then there is a surjection*

$$\varphi : Cl_\mathfrak{m} \to Cl_\mathfrak{n}$$
$$\mathfrak{a}P_\mathfrak{m} \mapsto \mathfrak{a}P_\mathfrak{n}.$$

*We say that $\mathfrak{n}$ is **admissible** if φ is injective. The **conductor** of $Cl_\mathfrak{m}$ is the smallest admissible modulus, and we denote it by $\mathfrak{f}$.*

Corresponding to ray class groups, there are objects called ray class fields. The conductor gives the primes that ramify in the ray class field. We say that an infinite prime ramifies in $K_{\mathfrak{m}}$ if it extends to an embedding of $\mathbb{C}$ which is not real [4].

Theorem 5.2.10. *[1]*

*For a number field K, the **ray class field** with modulus $\mathfrak{m}$, denoted by $K_{\mathfrak{m}}$, is the maximal abelian extension of K which is ramified exactly at the primes dividing the conductor $\mathfrak{f}$ of $Cl_{\mathfrak{m}}$. This ray class field has the property that $Gal(K_{\mathfrak{m}}/K) \cong Cl_{\mathfrak{m}}$.*

Note that when $\mathfrak{m} = \mathcal{O}_K$, the ray class field, $K_{\mathfrak{m}}$, is the Hilbert class field. For this reason, we can denote the Hilbert class field by $K_{(1)}$.

We now state a result for ray class fields which is analogous to the Principal Ideal Theorem for Hilbert class fields.

Theorem 5.2.11. *(See Theorem 2 in [31].)*

Let $K_{\mathfrak{f}}$ be the ray class field with conductor $\mathfrak{f} = \mathfrak{f}_0\mathfrak{f}_\infty$ of K. Then every ideal I in $I_{\mathfrak{f}}$ has the property that $I\mathcal{O}_{K_{\mathfrak{f}}}$ is principal.

Suppose $K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f)$. For $\mathbb{Z}[\alpha]$-ideals I and J, the previous theorem tells us that the ideal $(I : J)\mathcal{O}_{K_{\mathfrak{f}}}$ is principal as long as $\mathfrak{f}_0$ is chosen to be relatively prime to $(I : J)$. As before, such a ray class field does not automatically solve the conjugacy extension problem since f factors further over $K_{\mathfrak{f}}[x]$. However, we can extend our previous method involving the Hilbert class field to ray class fields by once again searching for a subfield F of $K_{\mathfrak{f}}$ with the properties:

1. f remains irreducible in $F[x]$
2. $(I : J)\mathcal{O}_F$ is a principal ideal.

Once again, there is no obvious reason why such a proper subfield of a given ray class field should be guaranteed to exist. There are many different choices of modulus that one can make, so even if a subfield with the desired properties cannot be found in one ray class field, perhaps such a subfield can be found in another.

Since ray fields have larger degree over K than the Hilbert class field, we will generally have more subfields to consider. However, this presents some computational difficulties since it can be expensive to work with fields of high degree. We only tried this method in a small number of examples because of these challenges.

We return now to the matrices which we observed were not conjugate over the ring of integers of the Hilbert class field in Example 5.2.3 .

Example 5.2.12. *Let $f = x^2 + 5$ and $K = \mathbb{Q}[x]/(f)$. The $GL_2(\mathbb{Z})$-conjugacy classes of matrices within $\mathcal{M}_f$ are given by representatives*

$$\mathcal{C}_f = \begin{pmatrix} 0 & 1 \\ -5 & 0 \end{pmatrix} \text{ and } A = \begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix}.$$

The fractional ideal corresponding to A is $I = 2\mathbb{Z} \oplus (\alpha+1)\mathbb{Z}$. In order to find a ring R over which A and B are conjugate, we search for a ring so that $2R \oplus (\alpha+1)R$ is principal.

We will consider subfields of a particular ray class field to find such an R. Note that because f defines an imaginary quadratic field, there are no real embeddings to consider, and so we only need to work with a K-modulus of the form $\mathfrak{m}_0$. Computing the norm, we find that $\mathcal{N}(I) = 2$, and so we may pick any modulus relatively prime to 2.

In Magma, we compute the ray class field $K_\mathfrak{m}$ with modulus $\mathfrak{m} = 3\mathcal{O}_K$. We check that this ray class field has conductor $3\mathcal{O}_K$, and we find that it is defined by $x^8 + 12x^6 + 158x^4 - 228x^2 + 3721$. We obtain a proper subfield F of $K_\mathfrak{m}$ with the desired properties.

We have $F = \mathbb{Q}(\beta) \cong \mathbb{Q}[x]/(x^4 - 12x^3 + 158x^2 + 228x + 3721)$. A $\mathbb{Z}$-basis for $\mathcal{O}_F$ is given by $\mathcal{B} = \{1, \frac{1}{8}(\beta-1), \frac{1}{64}(\beta^2 - 2\beta + 1), \frac{1}{1024}(\beta^3 - 3\beta^2 + 3\beta - 513)\}$. Letting $\mathcal{B}_i$ denote the i-th basis element, we obtain that

$$C = \begin{pmatrix} -\mathcal{B}_2 & -1 - \mathcal{B}_4 \\ 3 + \mathcal{B}_2 + 3\mathcal{B}_4 & -1 - 2\mathcal{B} - 2 - \mathcal{B}_4 \end{pmatrix}$$

is a matrix in $GL_2(\mathcal{O}_F)$ which conjugates C_f to A.

This example shows that while we may not be able to find a suitable subfield of the Hilbert class field which solves the conjugacy extension problem, ray class fields may provide an answer. This method using the ray class field was successful in a few more examples. Due to the computational difficulties of working in a large field extension, we did not attempt this method in many cases.

In the final chapter, we summarize our results and include the data of additional examples in which we applied the methods discussed in this chapter.

Chapter 6

Summary

We now summarize the progress we made in addressing the conjugacy extension problem. In [12], Estes and Guralnick prove that the Latimer and MacDuffee correspondence holds over any integral domain R (we call this LM-R for short) if one considers $\mathrm{GL}_n(R)$-conjugacy for matrices in $\mathcal{M}_f$ with f irreducible in $R[x]$. Theorem 4.2.1 extends this result by showing that LM-R holds for matrices with square-free characteristic polynomial.

Say A and B are locally conjugate with corresponding fractional ideals I and J, respectively. As a corollary of LM-R for $R = \mathbb{Z}_{(p)}$, we obtain that I and J are weakly equivalent. Then I and J have the same multiplicator ring; let $\mathcal{O} = (I : I) = (J : J)$. We showed in Proposition 4.2.9 that for a ring R with subring $\mathbb{Z}$, we have that $R \otimes \mathcal{O}$ is the multiplicator ring of $R \otimes I$ and $R \otimes J$. Considering $R \otimes I$ and $R \otimes J$ as fractional $R \otimes \mathcal{O}$-ideals, the matrices A and B are R-conjugate iff $R \otimes (I : J)$ is principal.

We used this theory to adapt Marseglia's algorithm in [24] to the context of $\mathrm{GL}_n(R)$-conjugacy for R an integral domain. We implemented the $\mathrm{GL}_n(R)$-conjugacy algorithm in Magma in the case that R is the ring of integers of a number field and the matrices in question have characteristic polynomial f which is irreducible in $R[x]$. While the algorithm can theoretically be adapted for f square-free, there is an obstacle to implementing an algorithm when f is not irreducible. Suppose we consider matrices with square-free characteristic polynomial $f = \prod_{i=1}^{k} f_i$ where each f_i is irreducible with root α_i. If we wish to consider $\mathcal{O}_K$-conjugacy for a number field K then by LM-$\mathcal{O}_K$, we must work with fractional ideals within the K-algebra $\prod K(\alpha_i)$. The IsPrincipal function can only be applied to ideals defined within such an algebra if $K = \mathbb{Q}$. Since determining whether a certain ideal is principal is crucial to testing for $\mathcal{O}_K$-conjugacy of matrices, we could only implement an algorithm in Magma in the case of irreducible characteristic polynomial.

Next we considered whether the Hilbert class field of $K = \mathbb{Q}[x]/(f)$ could provide a means for solving the conjugacy extension problem for matrices in $\mathcal{M}_f$. This is natural to consider

since every fractional $\mathcal{O}_K$-ideal becomes principal in the ring of integers of the Hilbert class field. From now on, let $K_{(1)}$ denote the Hilbert class field of K. Since f factors further in $\mathcal{O}_{K_{(1)}}[x]$, testing whether a fractional ideal is principal is difficult, as we noted in the previous discussion. In Example 5.2.3, we provided an example of a fractional ideal in a product of number fields which is not principal although it is principal in each component. The matrices considered in this example are not conjugate over $\mathcal{O}_{K_{(1)}}$. Thus, the ring of integers of the Hilbert class field does not necessarily solve the conjugacy extension problem.

To avoid the subtlety that arises when f factors further, we searched through proper subfields of the Hilbert class field in which f remains irreducible. In some cases, we were able to find a subfield of $K_{(1)}$ such that the fractional ideal in question is principal in its ring of integers. Such a subfield of the Hilbert class field need not exist, but we were able to use this method to answer the conjugacy extension problem in several examples.

In a few examples in which the method with the Hilbert class field failed, we found subfields of certain ray class fields which provided an answer to the conjugacy extension problem. We did not consider the method with ray class fields in all examples because the degree of a ray class field can be large enough to make computations with its subfields very expensive.

6.1 Data

We now provide some data which demonstrates the frequency with which the Hilbert class field method works in a collection of examples. We consider various irreducible polynomials f with the property that $K = \mathbb{Q}[x]/(f)$ has class number greater than one. We obtained number fields K of a specified degree, range of discriminants, and range of class numbers from the LMFDB [20].

We summarize our results in some tables. In the first column, we list the irreducible characteristic polynomial f. The third column gives the class number of K. The fourth column lists a matrix A which is not $\mathbb{Z}$-conjugate to the companion matrix of f. This last column records whether A is conjugate to $\mathcal{C}_f$ over a proper subfield of $K_{(1)}$, the Hilbert class field of K. If so, the polynomial defining the subfield is given in most cases. If the polynomial takes too much space to display, we

just write "Yes" to indicate that the method we outlined was successful. A "No" in the last column indicates that there is no *proper* subfield F of the Hilbert class field such that f is irreducible over $F[x]$ and A is $\mathcal{O}_F$-conjugate to $\mathcal{C}_f$. We did not actually attempt to determine in every example whether the matrices were conjugate over a subfield F of $K_{(1)}$ if f factors further in $F[x]$. This is because we cannot easily determine whether the ideal of interest is principal in that case.

The following table lists some examples when f defines a real quadratic field. 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 $h_K = 4$.

Table 6.1: Hilbert class field method for $\mathcal{M}_f$ with f real quadratic.

f	disc(f)	h_K	A	Conjugate over subfield of $K_{(1)}$?
$x^2 - 10$	$2^3 \cdot 5$	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

Note that for all the polynomials f given in the table, the field $K = \mathbb{Q}[x]/(f)$ has $\mathbb{Z}[\alpha]$ as its ring of integers. Then every fractional $\mathbb{Z}[\alpha]$-ideal has over-order $\mathbb{Z}[\alpha]$, meaning that all matrices in $\mathcal{M}_f$ are locally conjugate.

Note that for all polynomials f listed in the table, the class group of $K = \mathbb{Q}[x]/(f)$ is cyclic. Thus, for each example in which the method did work, letting F be the number field given by the polynomial in the last column, there is a single $\mathrm{GL}_2(\mathcal{O}_F)$-conjugacy class within $\mathcal{M}_f$.

For the sample of polynomials f given in the table, searching through the subfields of the Hilbert class field worked in all cases except when $f = x^2 - x - 117$. Corresponding to the matrix $\begin{pmatrix} -2 & 3 \\ 37 & 3 \end{pmatrix}$ is the non-principal $\mathbb{Z}[\alpha]$-ideal $I = 3\mathbb{Z} \oplus (\alpha + 2)\mathbb{Z}$. This means that for the Hilbert class field $K_{(1)}$ of $\mathbb{Q}[x]/(x^2 - x - 117)$, there was no proper subfield F of $K_{(1)}$ in which f remains irreducible and the ideal $\mathcal{O}_F \otimes I$ is principal. However, the ray class field method was successful in this example. We provide the details next.

Example 6.1.1. *Consider $f = x^2 - x - 117$, which has discriminant $disc(f) = 7 \cdot 67$. There are three $\mathbb{Z}$-conjugacy classes but the class group is cyclic, so we just need to find extension over which $A = \begin{pmatrix} -2 & 3 \\ 37 & 3 \end{pmatrix}$ is conjugate to $\mathcal{C}_f$*

We will discuss how to obtain a ring R such that there is one $GL_2(R)$-conjugacy class within $\mathcal{M}_f$ by considering subfields of a particular ray class field of $K = \mathbb{Q}[x]/(f)$.

The norm of $I = 3\mathbb{Z} \oplus (\alpha + 2)\mathbb{Z}$ is 3, so we may consider a ray class field with modulus relatively prime to 3. In this example, we choose to work with the modulus $\mathfrak{p} = 7\mathbb{Z} \oplus (3 + \alpha)\mathbb{Z}$. This is a prime ideal of $\mathcal{O}_K$ with $\mathfrak{p}^2 = 7\mathcal{O}_K$. (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 in this example divides the discriminant of f).

Letting $\mathfrak{m} = \mathfrak{p}$, we find that the ray class field $K_\mathfrak{m}$ has degree 18 over $\mathbb{Q}$. The conductor of $K_\mathfrak{m}$ equals the modulus $\mathfrak{p}$. Searching through the proper subfields of $K_\mathfrak{m}$, we find that the subfield F defined by the cubic polynomial

$x^3+c_2x^2x + c_1x + c_0$ *where*

$c_2 = 22427531465691$

$c_1 = 870192055039415679429350 16$ *and*

$c_0 = -16986335647621370099918963484532 3984727$

has the property that there is a single $GL_2(\mathcal{O}_F)$*-conjugacy class within* $\mathcal{M}_f$*.*

We write an element in $\mathcal{O}_F$ *as* (c_1, c_2, c_3, c_4) *where* c_i *denotes the coefficient with respect to the* i*-th element of a particular* $\mathbb{Z}$*-basis for* $\mathcal{O}_F$*. For*

$$a = (-125710942708475, 750246916436719, -1153803406920806),$$

$$b = (28731787124879, -171472222144795, 263706827403713),$$

$$c = (11235025718269, -67050991899409, 103117601946829), \text{ and}$$

$$d = (-2486645014964, 14840376776716, -22822989218387),$$

the matrix $C = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *has unit determinant and conjugates the companion matrix to* A*.*

Next we try the method with the Hilbert class field for some imaginary quadratic fields defined by the polynomials f in the following table. The table lists number fields K with discriminant ranging from -100 to -1 and class number ranging from 2 to 4.

One will notice that in this sample of number fields defined by f, there are several examples in which the method of Hilbert class field subfields did not work. In some of these cases, we found that ray class field method works. Since there are no real embeddings of these fields into $\mathbb{C}$, there are no infinite primes to consider.

Table 6.2: Hilbert class field method for $\mathcal{M}_f$ with f imaginary quadratic.

f	disc(f)	h_K	A	Conjugate over subfield of $K_{(1)}$?
$x^2 - x + 4$	$-3 \cdot 5$	2	$\begin{pmatrix} -1 & 2 \\ -3 & 2 \end{pmatrix}$	$x^2 + 2x + 4$
$x^2 + 5$	$-2^2 \cdot 5$	2	$\begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix}$	No
$x^2 + 6$	$-2^3 \cdot 3$	2	$\begin{pmatrix} 0 & 2 \\ -3 & 0 \end{pmatrix}$	$x^2 - 8x + 64$
$x^2 - x + 9$	$-5 \cdot 7$	2	$\begin{pmatrix} -2 & 3 \\ -5 & 3 \end{pmatrix}$	$x^2 + 7$
$x^2 + 10$	$-2^3 \cdot 5$	2	$\begin{pmatrix} 0 & 2 \\ -5 & 0 \end{pmatrix}$	$x^2 + 2$
$x^2 - x + 13$	$-3 \cdot 17$	2	$\begin{pmatrix} -1 & 3 \\ -5 & 2 \end{pmatrix}$	$x^2 + 8x + 19$
$x^2 + 13$	$-2^2 \cdot 13$	2	$\begin{pmatrix} -1 & 2 \\ -7 & 1 \end{pmatrix}$	No
$x^2 + 22$	$-2^3 \cdot 11$	2	$\begin{pmatrix} 0 & 2 \\ -11 & 0 \end{pmatrix}$	$x^2 - 40x + 576$
$x^2 - x + 23$	$-7 \cdot 13$	2	$\begin{pmatrix} -3 & 5 \\ -7 & 4 \end{pmatrix}$	$x^2 + 7$
$x^2 - x + 6$	-23	3	$\begin{pmatrix} 0 & 2 \\ -3 & 1 \end{pmatrix}$	$x^3 + 6x^2 + 9x - 23$
$x^2 - x + 8$	-31	3	$\begin{pmatrix} -1 & 2 \\ -5 & 2 \end{pmatrix}$	No
$x^2 - x + 15$	-59	3	$\begin{pmatrix} -2 & 3 \\ -7 & 3 \end{pmatrix}$	$x^3 - 3x^2 - 124844$
$x^2 - x + 21$	-83	3	$\begin{pmatrix} -2 & 3 \\ -9 & 3 \end{pmatrix}$	$x^3 - 3x^2 - 17107628$
$x^2 - x + 14$	$-5 \cdot 11$	4	$\begin{pmatrix} 0 & 2 \\ -7 & 1 \end{pmatrix}$	No
$x^2 + 14$	$-2^3 \cdot 7$	4	$\begin{pmatrix} -2 & 3 \\ -6 & 2 \end{pmatrix}$	No
$x^2 + 17$	$-2^2 \cdot 17$	4	$\begin{pmatrix} -2 & 3 \\ -7 & 2 \end{pmatrix}$	No
$x^2 + 21$	$-2^2 \cdot 3 \cdot 7$	4	$\begin{pmatrix} -2 & 5 \\ -5 & 2 \end{pmatrix}$	Yes (see below)

For f in the table besides $f = x^2 + 21$, the fields $K = \mathbb{Q}[x]/(f)$ have cyclic class group. One may also check that $\mathbb{Z}[\alpha]$ is the ring of integers of K for each of these fields. So if a polynomial

is given in the last column, then it defines a number field F such that which there is just one $\mathrm{GL}_2(\mathcal{O}_F)$-conjugacy class within $\mathcal{M}_f$.

In the next example, we discuss the case of the last polynomial f with non-cyclic class group in more detail.

Example 6.1.2. *If $f = x^2 + 21$, then we find that the Hilbert class field $K_{(1)}$ of $\mathbb{Q}[x]/(f)$ has defining polynomial $x^8+84x^6+3038x^4-12348x^2+405769$. The matrix $\begin{pmatrix} -2 & 5 \\ -5 & 2 \end{pmatrix}$ corresponds to the non-principal fractional ideal $I = 5\mathbb{Z} \oplus (\alpha + 2)\mathbb{Z}$. There are two subfields F of $K_{(1)}$ in which I is principal and f is irreducible.*

For the subfield F_1 given by $x^2 + 1078x + 405769$ we can check that $\mathcal{O}_{F_1} \otimes I$ is principal. Since the class group of $\mathbb{Q}(\sqrt{-21})$ is not cyclic, there is another generator of class group, $J = -7\mathbb{Z} \oplus \alpha\mathbb{Z}$. The matrix corresponding to J is $\begin{pmatrix} 0 & -7 \\ 3 & 0 \end{pmatrix}$. The fractional ideal $\mathcal{O}_{F_1} \otimes J$ is not principal, so there are two $GL_2(\mathcal{O}_{F_1})$-conjugacy classes within $\mathcal{M}_f$, given by representatives $\begin{pmatrix} 0 & 1 \\ -21 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & -7 \\ 3 & 0 \end{pmatrix}$.

For the subfield F_2 defined by $x^4-32x^3+1616x^2-21760x+396544$, we find that both $\mathcal{O}_{F_2} \otimes I$ and $\mathcal{O}_{F_2} \otimes J$ are principal. Then $\mathcal{M}_f$ consists of a single $GL_2(\mathcal{O}_{F_2})$-conjugacy class.

The following table summarizes what we found when we applied the ray class field method for some of the examples which were not solved by the Hilbert class field method. In column 3 of the following table, we list $\mathcal{N}(I)$, the norm of a non-principal fractional $\mathbb{Z}[\alpha]$-ideal I. The fourth column gives a conductor $\mathfrak{f}$ of $K = \mathbb{Q}[x]/(f)$ which is relatively prime to $\mathcal{N}(I)$. The last column gives a polynomial which defines a proper subfield of the ray class field with conductor $\mathfrak{f}$. In the ring of integers R of this subfield, there is a single $\mathrm{GL}_2(R)$-conjugacy class within $\mathcal{M}_f$.

Note that the conductor in the last row is a prime ideal in $\mathbb{Z}[\alpha]$ which has the property that $(2\mathbb{Z} \oplus \alpha\mathbb{Z})^2 = (2)$.

Table 6.3: Ray class field method for $\mathcal{M}_f$ with f imaginary quadratic.

f	$\mathcal{N}(I)$	$\mathfrak{f}$	Conjugate over subfield of $K_{\mathfrak{f}}$?
x^2+5	2	$3\mathbb{Z}[\alpha]$	$x^2-74x+3721$
x^2+13	2	$3\mathbb{Z}[\alpha]$	$x^4-1548x^3-3055050x^2-2822525676x+3324557815569$
x^2+14	3	$2\mathbb{Z}\oplus\alpha\mathbb{Z}$	$x^2-232x+29584$

Next, we consider the Hilbert class field method for some examples of number fields which are defined by cubic polynomials f. If we consider the six non-isomoprhic cubic fields with class number 2 and discriminant ranging from -1000 to 1000, the method fails, so we do not list these fields in the next table.

The following table includes cubic fields K with discriminant ranging from -1000 to 1000 for class number 3. Of course, all class groups of K are cyclic. We will no longer list a matrix which is not $\mathbb{Z}$-conjugate to $\mathcal{C}_f$. Instead, we will list the number of over-orders of $\mathbb{Z}[\alpha]$. If the last column lists a polynomial, then it defines a number field F such that the number of $\mathrm{GL}_3(\mathcal{O}_F)$-conjugacy class of matrices in $\mathcal{M}_f$ coincides with the number of over-orders of $\mathbb{Z}[\alpha]$. Otherwise, no proper subfield of the Hilbert class field has ring of integers over which the matrices in $\mathcal{M}_f$ are all conjugate.

Table 6.4: Hilbert class field method for $\mathcal{M}_f$ with f cubic.

f	disc(f)	h_K	#Over-orders	Conjugate over subfield of $K_{(1)}$?
x^3-x^2+5x+1	$-2^2\cdot 3\cdot 7^2$	3	1	$x^3-3x^2-60x+251$
$x^3-3x-10$	$-2^3\cdot 3^4$	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	$3^4\cdot 11$	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	$x^3+3x^2-60x+127$

There are seven non-isomorphic cubic fields with discriminant ranging from -2000 to 2000 with class number 4 or 5. For all of these fields, the method failed.

In the next table, we will list quartic polynomials f for which the method worked. Instead of listing all those fields for which the method failed, we will just mention that we checked the seven

non-isomorphic 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.

Table 6.5: Hilbert class field method for $\mathcal{M}_f$ with f quartic.

f	disc(f)	h_K	#Over-orders	Conjugate over subfield of $K_{(1)}$?
x^4+4x^2+1	$2^8 \cdot 3^2$	2	1	$x^2-10x+73$
x^4+9	$2^8 \cdot 3^2$	2	3	$x^2-10x+73$
$x^4-x^3+4x^2+x+1$	$2^3 \cdot 23^2$	3	1	$x^3+30x^2-45x-12501$
$x^4-2x^3+4x^2+2x+1$	$2^6 \cdot 5^3$	4	1	$x^4+6x^3+111x^2+526x+761$
$x^4-x^3+x^2-6x+6$	$2^3 \cdot 3^2 \cdot 5^3$	4	1	$x^4+32x^2+544x^2+4608x+15616$
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 class groups are all cyclic. Then the last column gives a polynomial which defines a number field F so that the number of $\mathrm{GL}_4(\mathcal{O}_F)$-conjugacy classes within $\mathcal{M}_f$ is given by the number of over-orders of $\mathbb{Z}[\alpha]$.

6.2 Open problems

There is still much progress to be made in solving the conjugacy extension problem. For an integral domain R, we focused our attention on $\mathrm{GL}_n(R)$-conjugacy of matrices with irreducible characteristic polynomial because otherwise, we must consider $R[\alpha]$-modules where α denotes a tuple of roots. We have noted that testing for $\mathrm{GL}_n(R)$-conjugacy amounts to determining whether a fractional $R[\alpha]$-ideal is principal, which is much more challenging in the non-irreducible case. When working with ideals within an algebra $\mathcal{A}$ which is a product of number fields, the IsPrincipal function in Magma is only valid if $\mathcal{A}$ is a $\mathbb{Q}$-algebra. For this reason, we were only able to implement an algorithm which tests for $\mathrm{GL}_n(R)$-conjugacy in the irreducible case. An open problem is to develop an algorithm which tests whether an ideal is principal and produces its generator in the case that $\mathcal{A}$ is an R-algebra. Once that is accomplished, one could implement an algorithm for $\mathrm{GL}_n(R)$-conjugacy in the square-free case.

In considering matrix conjugacy for matrices in $\mathcal{M}_f$ with irreducible f, we have offered a method of searching through subfields of the Hilbert class field of $\mathbb{Q}[x]/(f)$ to find a field F over which f remains irreducible and a particular fractional ideal is principal in $\mathcal{O}_F$. In the previous subsection, we gave several examples in which the method worked as well as several in which the method failed. An open problem is to try to find a nice classification for the the type of fields for which this method is successful.

We also gave a similar method which searches through subfields of the ray class field of $\mathbb{Q}[x]/(f)$. While this method provides more options than the Hilbert class field method, computational difficulties arise when the degree of ray class field is very large. A natural question to ask is whether there are certain ray class fields we should consider, and whether the primes dividing the discriminant of f are related in any way to the conductors of these ray class fields. An open problem is to determine how often this method will successfully answer the conjugacy extension problem.

Making use of the generalized Latimer and MacDuffee correspondence allowed us to see that the conjugacy extension problem is equivalent to the problem of finding a field extension in which an ideal becomes principal. This is easy to test as long as the characteristic polynomial f is irreducible and does not factor further in that extension. While our approach did not always succeed, it seems to be more tractable than Dade's non-constructive method for determining the extension over which a homogeneous form realizes a unit. For instance, in Example 3.1.2, we tried to use Dade's method to solve the conjugacy extension problem for matrices with characteristic polynomial $f = x^2 - x - 117$. This method would result in a number field of at least degree 462. In Example 6.1.1, we searched through subfields of a particular ray class field and found a field F of degree 3 such that the matrices in $\mathcal{M}_f$ are $\mathrm{GL}_2(\mathcal{O}_F)$-conjugate. It remains to be determined whether ray class fields provide an answer to the conjugacy extension problem in general.

Bibliography

[1] Wieb Bosma and John Cannon. *Discovering mathematics with Magma*. Springer, 2006.

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

[3] 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.

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

[5] Keith Conrad. Some basic module-theoretic notions and examples.

[6] Keith Conrad. The different ideal. *Expository papers/Lecture notes. Available at: http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/different.pdf*, 2009.

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

[8] Everett Clarence Dade. A correction. *Mathematika*, 1964.

[9] Everett Clarence Dade, Olga Taussky, and Hans Zassenhaus. On the theory of orders, in particular on the semigroup of ideal classes and genera of an order in an algebraic number field. *Mathematische Annalen*, 148(1):31–64, 1962.

[10] David Steven Dummit and Richard M Foote. *Abstract algebra*. Wiley Hoboken, 2004.

[11] 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.

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

[13] John GF Francis. The QR transformation—part 2. *The Computer Journal*, 4(4):332–345, 1962.

[14] Robert Gilmer. Multiplicative ideal theory. *Queen's Papers in Pure and Applied Mathematics*, 90, 1992.

[15] The GAP group. Gap- groups, algorithms, and programming. http://www.sagemath.org, 2019.

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

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

[18] David Husert. *Similarity of Integer Matrices*. PhD thesis, Universität Paderborn, Fakultät für Elektrotechnik, Informatik und Mathematik, 2017.

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

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

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

[22] Hendrik W Lenstra. Algorithms in algebraic number theory. *Bulletin of the American Mathematical Society*, 26(2):211–244, 1992.

[23] Marvin Marcus. Determinants of sums. *The College Mathematics Journal*, 21(2):130–135, 1990.

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

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

[26] Jürgen Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013.

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

[28] Ernstteinitz Steinitz. Vorlesungen über die theorie der algebraischen dahlen. *Leipzig*, page 121, 1923.

[29] Peter Stevenhagen. The arithmetic of number rings. *Algorithmic number theory: lattices, number fields, curves and cryptography*, 44:209–266, 2008.

[30] Robert R Stoll. *Linear algebra and matrix theory*. Courier Corporation, 2013.

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

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

[33] GL Watson. *Quadratic forms*, volume 1. Cambridge England University Press, 1960.

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

[35] Oscar Zariski and Pierre Samuel. *Commutative algebra: Volume II*. Van Nostrand, 1960.

Appendix A

Proofs

Lemma 4.2.3

Define $\phi : I^t \to Hom_R(I, R)$ by $\phi(x) = \varphi(x)$ where $\varphi_x(y) = Tr(xy)$. Then ϕ is an R-module isomorphism.

Proof:

Note that ϕ is R-linear because Tr is R-linear.

If $I^t = \oplus v_i^* R$ then ϕ is determined by $\phi(v_i^*) = \varphi_{v_i^*}$. Suppose that $\phi(\sum a_i v_i^*) = \phi(\sum b_i v_i^*)$ so that $\varphi_{\sum a_i v_i^*} = \varphi_{\sum b_i v_i^*}$. This means that for all v_j, $j = 1, .., n$ we have

$$\varphi_{\sum a_i v_i^*}(v_j) = \varphi_{\sum b_i v_i^*}(v_j)$$
$$\text{Tr}(\sum a_i v_i^* v_j) = \text{Tr}(\sum b_i v_i^* v_j)$$
$$\sum a_i \text{Tr}(v_i^* v_j) \sum b_i \text{Tr}(v_i^* v_j)$$
$$a_j = b_j$$

for $j = 1, .., n$ so that $\sum a_i v_i^* = \sum b_i v_i^*$ and ϕ is injective.

Let $\varphi \in \text{Hom}(I, R)$ and say $\varphi(v_i) = r_i$. We also have $\sum r_j \varphi_{v_j^*}(v_i) = r_i$ for $j = 1, ..., n$ so that $\varphi = \sum r_j \varphi_{v_j^*}$.

Now, $\sum r_j \varphi_{v_j^*}(x) = \sum r_j \text{Tr}(v_j^* x) = \text{Tr}(\sum r_j v_j^* x) = \sum \varphi_{\sum r_j v_j^*}(x)$. Thus, $\phi(\sum r_j v_j^*) = \varphi_{\sum r_j v_j^*} = \sum r_j \varphi_{v_j^*} = \varphi$ and ϕ is surjective.

□

Proposition 4.2.8 *Suppose that $I = \oplus v_i\mathbb{Z}$ and $\tilde{I} = \tilde{v}_i R$. Then*

$$\varphi_I : R \otimes_{\mathbb{Z}} I \to \tilde{I}$$

defined on simple tensors by

$$r \otimes (v_1 z_1, .., v_n z_n) \mapsto r(v_1 z_1, .., v_n z_n)$$

and then extended in the natural way, is an $R[\alpha]$-module isomorphism which is independent of the choice of basis v_i. Furthermore, if $J = \oplus w_i\mathbb{Z}$, then $R \otimes I \cong R \otimes J$ as $R \otimes \mathbb{Z}[\alpha]$-modules if and only if $\oplus \tilde{v}_i R \cong \oplus \tilde{w}_i R$ as $R[\alpha]$-modules.

We prove this proposition by proving several lemmas.

Lemma 1. *Suppose that $I = \oplus v_i\mathbb{Z}$. Then $\varphi_I : R \otimes I \to \tilde{I}$, defined on simple tensors by $\varphi(\zeta \otimes (v_1 z_1, .., v_n z_n)) = \zeta(v_1 z_1, .., v_n z_n)$ and then extended in the natural way, is a R-module isomorphism which is independent of the choice of basis v_i.*

Proof: Let us denote φ_I by φ. The map

$$\varphi : R \otimes_{\mathbb{Z}} \oplus v_i\mathbb{Z} \to \oplus v_i R$$

$$\zeta \otimes (v_1 z_1, .., v_n z_n) \mapsto \zeta(v_1 z_1, .., v_n z_n)$$

is known to be a $\mathbb{Z}$-module isomorphism with inverse
$\varphi^{-1}((v_1\zeta_1, ..., v_n\zeta_n)) = \zeta_1 \otimes v_1\mathbf{e}_1 + ... + \zeta_n \otimes v_n\mathbf{e}_n$.

The map φ is independent of the choice of basis of I. If we replace v_i with v_i', there is a matrix $U \in \mathrm{GL}_n(\mathbb{Z})$ with $v' = Uv$. Clearly, $\oplus v_i R = \oplus v_i' R$.

For $\gamma \in R$, we have

$$\begin{aligned}\gamma\varphi(\zeta \otimes (v_1 z_1, .., v_n z_n)) &= \gamma\zeta(v_1 z_1, .., v_n z_n) \\ &= \varphi(\gamma\zeta \otimes (v_1 z_1, .., v_n z_n)\end{aligned}$$

and

$$\begin{aligned}\gamma\varphi^{-1}((v_1\zeta_1,...,v_n\zeta_n) &= \gamma(\zeta_1 \otimes v_1\mathbf{e}_1 + ... + \zeta_n \otimes v_n\mathbf{e}_n) \\ &= \gamma\zeta_1 \otimes v_1\mathbf{e}_1 + ... + \gamma\zeta_n \otimes v_n\mathbf{e}_n \\ &= \varphi^{-1}(\gamma(v_1\zeta_1,...,v_n\zeta_n)).\end{aligned}$$

Thus, φ and φ^{-1} are R-modules.

□

Lemma 2. *The R-module isomorphism $\varphi_{\mathbb{Z}[\alpha]} : R \otimes \mathbb{Z}[\alpha] \to R[\alpha]$ is a ring isomorphism. An isomorphism of $R \otimes \mathbb{Z}[\alpha]$-modules is just multiplication by element in fraction field of $R \otimes \mathbb{Z}[\alpha]$.*

Proof:

Denote $\varphi_{\mathbb{Z}[\alpha]}$ by φ_0. We can define multiplication on $R \otimes \mathbb{Z}[\alpha]$ by $t_1t_2 = \varphi_0^{-1}(\varphi_0(t_1)\varphi_0(t_2))$. Then $\varphi_0(t_1t_2) = \varphi_0(\varphi_0^{-1}(\varphi_0(t_1)\varphi_0(t_2)) = \varphi_0(t_1)\varphi_0(t_2)$ so that φ_0 is a ring isomorphism.

On simple tensors, this multiplication is given by $\zeta_1 \otimes p_1(\alpha) \cdot \zeta_2 \otimes p_2(\alpha) = \zeta_1\zeta_2 \otimes p_1(\alpha)p_2(\alpha)$.

Since $R \otimes \mathbb{Z}[\alpha]$ is ring isomorphic to $R[\alpha]$, it is an integral domain. Then we have that any $R \otimes \mathbb{Z}[\alpha]$-module isomorphism is multiplication by element in Frac$(R \otimes \mathbb{Z}[\alpha])$.

□

We may define a $R \otimes \mathbb{Z}[\alpha]$-module action on $R \otimes_{\mathbb{Z}} I$. Assume that $I = \oplus v_i\mathbb{Z}$. We define the action by $\gamma \otimes \alpha^k \cdot (\zeta \otimes (z_1v_1, .., z_nv_n) := \gamma\zeta \otimes (c_1v_1, .., c_nv_n)$ where $\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = A^k \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}$. The full action by $R \otimes \mathbb{Z}[\alpha]$ is defined by extending linearly.

Similarly, $R[\alpha]$ acts on $\tilde{I}$ by $\gamma\alpha^k \cdot (\zeta_1 v_1, .., \zeta_n v_n) := \gamma(c_1 v_1, .., c_n v_n)$ where $\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = A^k \begin{pmatrix} \zeta_1 \\ \vdots \\ \zeta_n \end{pmatrix}$ and by extending linearly.

We check that this is an action. This action is well-defined because two elements in $R[\alpha]$ are equal if they differ by a multiple of the minimal polynomial of α, call it f. (In the irreducible case, α has the same minimal polynomial over R as over $\mathbb{Z}$). Note that $f(\alpha) \cdot (\zeta_1 v_1, .., \zeta_n v_n) = (c_1 v_1, .., c_n v_n)$ where $\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = f(A) \begin{pmatrix} \zeta_1 \\ \vdots \\ \zeta_n \end{pmatrix}$. Now, $f(A) = 0$ because $0 = f(\alpha)\overline{v} = f(A)\overline{v}$ and one can say the same for the n Galois-conjugates of $\overline{v}$

We now show this is an action. We let $*$ denote component-wise multiplication.

$$\begin{aligned} p(\alpha) \cdot ((v_i y_i) + (v_i z_i)) &= p(\alpha) \cdot ((y_i + z_i)v)i) \\ &= p(A)(y_i + z_i) * (v_i) \\ &= p(A)(y_i) * (v_i) + p(A)(z_i) * v_i \\ &= p(\alpha) \cdot (v_i y_i) + p(\alpha) \cdot (v_i z_i) \end{aligned}$$

$$\begin{aligned} (p_1(\alpha) + p_2(\alpha)) \cdot (v_i z_i) &= (p_1(A) + p_2(A))(z_i) * (v_i) \\ &= p_1(A)(z_i) * (v_i) + p_2(A)(z_i) * (v_i) \\ &= p_1(\alpha)(v_i z_i) + p_2(\alpha)(v_i z_i) \end{aligned}$$

$$\begin{aligned}(p_1(\alpha)(p_2(\alpha)) \cdot (v_i z_i) &= p_1(A)p_2(A)(z_i) * (v_i)) \\ &= p_1(A)(p_2(A)(z_i) * (v_i)) \\ &= p_1(A)\overline{c} * v_i \text{ where } \overline{c} = p_2(A)\overline{z} \\ &= p_1(\alpha) \cdot (c_1 v_1, .., c_n v_n) \\ &= p_1(\alpha) \cdot p_2(\alpha) \cdot (z_i v_i)\end{aligned}$$

We may define a $R \otimes \mathbb{Z}[\alpha]$ action on $R \otimes \oplus v_i\mathbb{Z}$ by $\gamma \otimes \alpha^k \cdot (\zeta \otimes (z_1 v_1, .., z_n v_n)) := \gamma\zeta \otimes (c_1 v_1, .., c_n v_n)$ where $\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = A^k \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}$ and extending linearly. This is equivalent to defining the action using the previous action: For $t \in R \otimes \mathbb{Z}[\alpha]$ and $s \in \mathbb{Z} \otimes I$, let $\varphi = \varphi_I$ and $\varphi_0 = \varphi_{\mathbb{Z}[\alpha]}$ and define $t \cdot s = \varphi^{-1}(\varphi_0(t) \cdot \varphi(s))$.

This well-defined since φ_0 and φ^{-1} are functions. The fact that this is an action follows from the additive properties of φ_0, φ, the fact that φ_0 is a ring isomorphism, and since it is defined in terms of another action. For instance,

$$\begin{aligned}(t_1 + t_2) \cdot s &= \varphi^{-1}(\varphi_0(t_1 + t_2) \cdot \varphi(s)) \\ &= \varphi^{-1}((\varphi_0(t_1) + \varphi_0(t_2)) \cdot \varphi(s)) \\ &= \varphi^{-1}(\varphi_0(t_1) \cdot \varphi(s) + \varphi_0(t_2) \cdot \varphi(s)) \qquad \text{(other action property)} \\ &= \varphi^{-1}(\varphi_0(t_1) \cdot \varphi(s)) + \varphi^{-1}(\varphi_0(t_2) \cdot \varphi(s)) \\ &= t_1 \cdot s + t_2 \cdot s\end{aligned}$$

and

$$\begin{aligned} t_1 \cdot (t_2 \cdot s) &= t_1 \cdot \varphi^{-1}(\varphi_0(t_2) \cdot \varphi(s)) \\ &= \varphi^{-1}(\varphi_0(t_1) \cdot \varphi(\varphi^{-1}(\varphi_0(t_2) \cdot \varphi(s)) \\ &= \varphi^{-1}(\varphi_0(t_1) \cdot (\varphi_0(t_2) \cdot \varphi(s)) \\ &= \varphi^{-1}((\varphi_0(t_1)\varphi_0(t_2)) \cdot \varphi(s)) \qquad \text{(other action property)} \\ &= \varphi^{-1}(\varphi_0(t_1 t_2) \cdot \varphi(s)) \\ &= t_1 t_2 \cdot s \end{aligned}$$

Lemma 3. *Let $I \in \mathcal{I}_{\mathbb{Z}[\alpha]}$. For ease of notation, let $\varphi = \varphi_I$ and let $\varphi_0 = \varphi_{\mathbb{Z}[\alpha]}$.*

1. *For $x \in R[\alpha]$ and $y \in R \otimes I$ we have $x \cdot \varphi(y) = \varphi(\varphi_0^{-1}(x) \cdot y)$.*

2. *For $x \in R[\alpha]$ and $y \in \tilde{I}$, we have $\varphi^{-1}(x \cdot y) = \varphi_0^{-1}(x) \cdot \varphi^{-1}(y)$.*

Proof:

Note that because the actions and maps are R-linear, it is enough to show the results for α^k. Suppose that $A^k = (a_{ij})$.

Proof of statement 1:

$$\begin{aligned} \zeta_k \alpha^k \cdot \varphi(y) &= \zeta_k \alpha^k \cdot \gamma(z_1 v_1, ..., z_n v_n) \\ &= \zeta_k \gamma((z_1 a_{11} + ... + z_n a_{1n}) v_1, .., (z_1 a_{n1} + ... + z_n a_{nn}) v_n) \end{aligned}$$

and

$$\begin{aligned} \varphi(\varphi_0^{-1}(x) \cdot y) &= \varphi(\zeta_k \otimes \alpha^k \cdot \gamma \otimes (z_1 v_1, ... z_n v_n)) \\ &= \varphi(\zeta_k \gamma \otimes ((z_1 a_{11} + ... + z_n a_{1n}) v_1, .., (z_1 a_{n1} + ... + z_n a_{nn}) v_n)) \\ &= \zeta^k \gamma((z_1 a_{11} + ... + z_n a_{1n}) v_1, .., (z_1 a_{n1} + ... + z_n a_{nn}) v_n). \end{aligned}$$

Proof of statement 2:

$$\begin{aligned}\varphi^{-1}(\zeta_k\alpha^k \cdot y) &= \varphi^{-1}(\zeta_k((\gamma_1 a_{11} + ... + \gamma_n a_{1n})v_1, ..., (\gamma_1 a_{n1} + ... + \gamma_n a_{nn})v_n) \\ &= \sum_{j=1}^{n} \zeta_k(\gamma_1 a_{j1} + ... + \gamma_{jn} a_{jn}) \otimes v_j \mathbf{e}_j\end{aligned}$$

On the other hand,

$$\begin{aligned}\varphi_0^{-1}(\zeta_k\alpha^k) \cdot \varphi^{-1}(y) &= (\zeta_k \otimes \alpha^k) \cdot (\gamma_1 \otimes v_1\mathbf{e}_1 + ... + \gamma_n \otimes v_n\mathbf{e}_n) \\ &= \zeta_k\gamma_1 \otimes (a_{11}v_1 + ... + a_{n1}v_n) + ... + \zeta_k\gamma_n \otimes (a_{1n}v_1 + ... + a_{nn}v_n) \\ &= \sum_{j=1}^{n} \zeta_k(\gamma_1\alpha_{j1} + ... + \gamma_n\alpha_{jn}) \otimes v_j\mathbf{e}_j\end{aligned}$$

The last equality holds because if we isolate the summand with v_j we have

$$\begin{aligned}\zeta_k(\gamma_1 \otimes a_{j1}v_j\mathbf{e}_j + ... + \gamma_n \otimes a_{jn}v_j\mathbf{e}_j) &= \zeta_k(\gamma_1 a_{j1} \otimes v_j\mathbf{e}_j + ... + \gamma_n a_{jn}v_j\mathbf{e}_j) \\ &= \zeta_k(\gamma_1\alpha_{j1} + ... + \gamma_n\alpha_{jn}) \otimes v_j\mathbf{e}_j\end{aligned}$$

because $a_{ij} \in \mathbb{Z}$.

□

Lemma 4. *Define* $\tilde{\varphi} : R \otimes \mathcal{I}_{\mathbb{Z}[\alpha]}/_\sim \to \mathcal{I}_{R[\alpha]}/_\sim$ *by* $\tilde{\varphi}(R \otimes I) = \varphi_I(R \otimes I) = \tilde{I}$. *Then* $\tilde{\varphi}$ *is an injective map.*

Proof: We show that $\tilde{\varphi}$ is well-defined.

Suppose that $R \otimes I$ and $R \otimes J$ are isomorphic as $R \otimes \mathbb{Z}[\alpha]$-modules. Then there are elements $r, s \in R \otimes \mathbb{Z}[\alpha]$ such that $r(R \otimes I) = s(R \otimes J)$. Since $s(R \otimes J)$ is isomorphic to $R \otimes J$, we can assume that $r(R \otimes I) = R \otimes J$ for some $r \in R \otimes \mathbb{Z}[\alpha]$.

Note that the actions are the same as the ring multiplication definitions. We have

$$\begin{aligned}
\tilde{\varphi}(r(R \otimes I)) &= \tilde{\varphi}(\{r \cdot t : t \in R \otimes I\}) \\
&= \{\varphi_I(r \cdot t) : t \in R \otimes I\} \\
&= \{\varphi_I(\varphi^{-1}_{\mathbb{Z}[\alpha]}(\tilde{r}) \cdot t) : t \in R \otimes I\} \quad \text{for } \tilde{r} \in R[\alpha] \text{ (because } \varphi_{\mathbb{Z}[\alpha]} \text{ is an isomorphism)} \\
&= \{\tilde{r} \cdot \varphi_I(t) : t \in R \otimes I\} \quad \text{(by Lemma 3)} \\
&= \tilde{r} \cdot \tilde{\varphi}(R \otimes I) \\
&= \tilde{r}\tilde{I}
\end{aligned}$$

and $\tilde{r}\tilde{I}$ is in the same class as $\tilde{I}$.

We show that $\tilde{\varphi}$ is injective. We will do this by defining $\tilde{\varphi}'(\tilde{I}) := \varphi_I^{-1}(\tilde{I}) = R \otimes I$. It is easy to see that as long as $\tilde{\varphi}'$ is a function, it is the inverse to $\tilde{\varphi}$.

Suppose that $\tilde{\varphi}(R \otimes I) \sim \tilde{\varphi}(R \otimes J)$, so $r\tilde{I} = \tilde{J}$ for some $r \in R[\alpha]$ (you can make the same argument as above). Then

$$\begin{aligned}
\tilde{\varphi}'(r\tilde{I}) &= \tilde{\varphi}^{-1}(\{r \cdot t : t \in \tilde{I}\}) \\
&= \{\varphi_I^{-1}(r \cdot t) : t \in \tilde{I}\} \\
&= \{\varphi^{-1}_{\mathbb{Z}[\alpha]}(r) \cdot \varphi_I^{-1}(t) : t \in \tilde{I}\} \quad \text{(by Lemma 3)} \\
&= \{\tilde{r} \cdot \varphi_I^{-1}(t) : t \in \tilde{I}\} \quad \text{where } \tilde{r} \in R \otimes \mathbb{Z}[\alpha] \\
&= \tilde{r}\tilde{\varphi}'(\tilde{I}) \\
&= \tilde{r}(R \otimes I)
\end{aligned}$$

and $\tilde{r}(R \otimes I)$ is in the same class as $\mathbb{Z} \otimes I$. Therefore, $\tilde{\varphi}' = \tilde{\varphi}^{-1}$ and $\tilde{\varphi}$ is injective.

□

Now that we have given the proofs of all the necessary lemmas, we may prove the main proposition.

Proposition 4.2.8 *Suppose that $I = \oplus v_i\mathbb{Z}$. Then $\varphi_I : R \otimes_{\mathbb{Z}} I \to \oplus \tilde{v}_i R$, defined on simple tensors by $\varphi(r \otimes (v_1 z_1, .., v_n z_n)) = r(v_1 z_1, .., v_n z_n)$, and then extended in the natural way, is an $R[\alpha]$-module isomorphism which is independent of the choice of basis v_i. Furthermore, if $J = \oplus w_i\mathbb{Z}$, then $R \otimes I \cong R \otimes J$ as $R \otimes \mathbb{Z}[\alpha]$-modules if and only if $\oplus \tilde{v}_i R \cong \oplus \tilde{w}_i R$ as $R[\alpha]$-modules.*

Proof: Lemmas 1-3 show that φ_I is an $R[\alpha]$-module isomorphism. While the map

$$\tilde{\varphi} : R \otimes \mathcal{I}_{\mathbb{Z}[\alpha]}/_{\sim} \to \mathcal{I}_{R[\alpha]}/_{\sim}$$
$$R \otimes I \mapsto \tilde{I}$$

from Lemma 4 is not surjective, the image is $\text{Im}(\tilde{\varphi}) = \{\tilde{I} : I \in \mathcal{I}_{\mathbb{Z}[\alpha]}\}$. Since $\tilde{\varphi}$ is an injective map, it follows that $R \otimes I \cong R \otimes J$ as $R \otimes \mathbb{Z}[\alpha]$-modules if and only if $\tilde{I} \cong \tilde{J}$ as $R[\alpha]$-modules. $\square$