Thesis:
A partial solution to the similarity extension problem

Noah Keuper 5863201
Supervised by: Stefano Marseglia
Second reader: Valentijn Karemaker

August 2, 2022

Utrecht University

Abstract

The Similarity Extension Theorem roughly states that two matrices are similar over every localisation of a specific ring if and only if there is a finite integral extension of that ring where they are similar. Since the Similarity Extension Theorem was proved a question that remained was finding this extension. The goal of this thesis is to dive into this problem and propose a method of solving it in a specific setting, with the hope that this can be extended to a broader setting in the future. This was done by going over the proof of the Similarity Extension Theorem and trying to adapt it by using a theorem from Watson such that it returns an explicit extension. We succeeded in finding a method that returns a solution for two 2×2 matrices with some additional conditions. However we suspect some of these conditions can be avoided or relaxed with some additional research. This method therefore could be a good addition to current methods whenever we are looking at 2×2 matrices. And can be a start for anyone trying to generalise this method to larger matrices.

Contents

1 Introduction

This thesis will focus on a theorem concerning the effect similarity of matrices over certain rings has on the similarity of those matrices over a different ring. So let us first define when two matrices are similar over a ring.

Definition 1. (R-Similar matrices) Let R be a commutative ring. Two $n \times n$ matrices A, B are called *R-similar* if there exists a matrix $P \in \mathrm{GL}_n(R)$ such that $PAP^{-1} = B$.

When the ring R is clear from the context we will omit it from the notation. And we will call two matrices locally D-similar for a prime $\mathfrak{p}$ whenever the matrices are similar over the localisation of D at the prime $\mathfrak{p}$ of D.
Note that similarity of matrices induces an equivalence relation where two matrices are equivalent if they are similar over a ring R. The equivalence classes of this relation are called similarity classes.
Similar matrices are matrices which can be viewed as descriptions of the same linear transformation in possibly different bases. This is also why the matrix P in the definition can be referred to as the change of basis matrix, from the basis where the linear transformation is described by A to the basis where it is described by B.
Answering the question whether two matrices are similar can help in understanding one matrix from the information already available from the other matrix. For example, as shown below, they will both have the same characteristic polynomial, trace, determinant, and eigenvalues.

Lemma 2. Similar matrices A, $B \in \mathbb{Z}^{2\times 2}$ have the same characteristic polynomial, trace, determinant, and eigenvalues.

Proof. Since A and B are similar we know that there exists a matrix C with $\det(C) \neq 0$ such that $CA = BC$. But then we find the following for the characteristic polynomial of A and B:

$$\begin{aligned}\chi_A &= \det(A - x\mathcal{I}_n)\\ &= \det(C)\det(A - x\mathcal{I}_n)\det(C^{-1})\\ &= \det(CAC^{-1} - Cx\mathcal{I}_nC^{-1})\\ &= \det(B - x\mathcal{I}_n)\\ &= \chi_B.\end{aligned}$$

Now since the eigenvalues of a matrix are exactly the roots of its characteristic polynomial these also have to be the same. And since the trace and determinant of a matrix appear as coefficients of specific terms in the characteristic polynomial, having the same characteristic polynomial implies these properties are also the same. □

In 1933 Claiborne Latimer and Cyrus MacDuffee proved that for matrices with a monic, irreducible characteristic polynomial $f \in \mathbb{Z}[x]$, the classes of $\mathbb{Z}$-similar matrices are in bijection with the fractional ideal classes of $\mathbb{Z}[\alpha]$, where α is a root of f. This theorem is also called the LM-correspondence, and drew the attention to algebraic approaches of determining similarity properties of matrices which led to the main theorem of interest for this thesis:

Theorem 3. (Similarity Extension Theorem) [Gur80, Theorem 7] Let D be the ring of algebraic integers in a finite extension of $\mathbb{Q}$. And let $A, B \in \mathbb{Z}^{n\times n}$ be matrices with a square-free characteristic polynomial $f \in \mathbb{Z}[X]$. Then A and B are locally D-similar for every prime if and only if there is a finite integral extension E of D such that A and B are similar over E.

We are mainly focused on the half of the theorem that states that the extension E exists as we want to find this extension. However there is no explicit way to find this extension yet, finding this extension is therefore called the Similarity Extension Problem. Our goal is to investigate this problem and give more insight into how we might be able to find this extension.

We will start by looking at the LM-correspondence and its proof as a generalisation of it is used in a partial solution to the Similarity Extension Problem proposed by Afandi [Afa21], which we will look at in chapter 4. Then we will, in chapter 3 look into the details of the Similarity Extension Theorem from Guralnick. At this point we will investigate the algorithm proposed by Afandi. Then, in chapter 5 we will show why the Similarity Extension Theorem is not explicit. In our last chapter, chapter 6, we will then introduce another approach to solve the conjugacy extension problem for 2×2 matrices, which is an adaptation of the proof of the Similarity Extension Theorem using a theorem by Watson instead of the theorem by Dade to make the proof explicit. In this chapter we will also demonstrate that we can solve a problem which could not be solved using Afandi's algorithm and talk about the limitations of our method compared to Afandi's algorithm.

2 Proof of the LM-correspondence

In this chapter we will give a proof of the LM-correspondence. But before we can do that we need some additional definitions. We will define fractional ideals and talk about the equivalence relation that splits all fractional ideals of a ring into fractional ideal classes. After this we will finish by presenting the proof of the LM-correspondence which will link the notions introduced in this and the previous chapter.

The LM-correspondence is only concerned with matrices that are $\mathbb{Z}$-similar, hence those will be the only ones we consider in this chapter. Later we will also be looking at matrices that are similar over several extensions of $\mathbb{Z}$.
Remember from the introduction that similar matrices have the same characteristic polynomial. The reverse however does not hold. Let us give an example of two matrices with the same characteristic polynomial that are not similar.

Example 4. Look at $A = \begin{pmatrix} 0 & 1 \\ -5 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix}$, then both have characteristic polynomial $f = x^2+5$. However we cannot find a matrix $P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $PA = BP$ such that $\det(P) = \pm 1$. Suppose we could then $PA = \begin{pmatrix} -5b & a \\ -5d & c \end{pmatrix}$ and $BP = \begin{pmatrix} -a+2c & -b+2d \\ -3a+c & -3b+d \end{pmatrix}$ hence $a = -b+2d$, and $c = -3b+d$. But then $\det(P) = ad - bc = 3b^2 - 2db + 2d^2 = \pm 1$. But when we then look at b as a constant we find using the abc-formula to calculate d that the discriminant is $4b^2 - 8(3b^2 \pm 1)$. And this discriminant is negative if $b \neq 0$, hence in those cases d will not be an integer, which is a contradiction. In case $b = 0$ we find that $\det(P) = 2d^2$ but this can never be ± 1 if d is an integer, hence this is also a contradiction.

Therefore in general the equivalence relation of being similar matrices is not trivial within the set of matrices with characteristic polynomial f. Equivalence classes under this equivalence relation are called similarity classes and for matrices with elements in $\mathbb{Z}$ and characteristic polynomial f this set of equivalence classes is denoted as $\mathcal{M}_f$.

Let us now shift our focus to fractional ideals. To be able to define what a fractional $\mathcal{O}$-ideal is we first need the notion of an order, $\mathcal{O}$.

Definition 5. An *order* $\mathcal{O}$ in a number field K is a subring of K which is finitely generated as a $\mathbb{Z}$-module and contains a $\mathbb{Q}$-basis of K.

Definition 6. Let $\mathcal{O}$ be an order in a number field K. Then a non-zero finitely generated $\mathcal{O}$-module in K is called a *fractional $\mathcal{O}$-ideal*.

Let us give a short example of an order and a fractional ideal in this order.

Example 7. Let α be an algebraic integer and let $K = \mathbb{Q}[\alpha]$ and $\mathcal{O} = \mathbb{Z}[\alpha]$. Then $\mathcal{O}$ is an order in K since $\mathbb{Z}[\alpha] \subset \mathbb{Q}[\alpha]$, it is generated by 1 and α over $\mathbb{Z}$, and 1 and α generate K over $\mathbb{Q}$. Now let $I = \frac{1}{2}\mathbb{Z}[\alpha] = \{\frac{o}{2} \mid o \in \mathcal{O}\}$. Then I is a fractional $\mathcal{O}$-ideal since it is non-zero, generated by the element $\frac{1}{2}$ in $\mathcal{O}$, and $\frac{1}{2}\mathbb{Z}[\alpha] \subset \mathbb{Q}[\alpha]$.

Let $\mathcal{O}$ be an order in a number field K. Then two fractional $\mathcal{O}$-ideals I and J are called equivalent if $I = xJ$ for some x which is a unit of K. The equivalence classes of this equivalence relation are called *fractional ideal classes*. The fractional ideal classes will form a monoid, under the multiplication operation given by $[I] \cdot [J] = [IJ]$, called the *ideal class monoid*. Here the notation for the ideal class monoid corresponding to an order $\mathcal{O}$ is $Cl(\mathcal{O})$.

We will now state the LM-corrspondence and give a proof based on the notes of Keith Conrad [K.] which are also used in other peer reviewed papers, for example the one by Stefano Marseglia [Mar20].

Theorem 8. (Latimer-MacDuffee) [LM33, Theorem 1] Let $f \in \mathbb{Z}[X]$ be a monic irreducible polynomial of degree n and let α be a root of $f(X)$. Then there is a bijection between $\mathcal{M}_f$ and $Cl(\mathbb{Z}[\alpha])$. Moreover this bijection can be explicitly constructed.

Proof. We define $\Psi : Cl(\mathbb{Z}[\alpha]) \to \mathcal{M}_f$ by sending $[I] \in Cl(\mathbb{Z}[\alpha])$ to $[[m_\alpha]_a]$ where $[m_\alpha]_a$ is the multiplication by α map on I viewed as a matrix in a basis a of I and the outer brackets indicate that we are looking at a class of matrices. Since we are looking at $Cl(\mathbb{Z}[\alpha])$ we will use $\mathcal{O}$ and $\mathbb{Z}[\alpha]$ interchangeably throughout this proof.
First note that we can always get this $[m_\alpha]_a$ since I is a finitely generated $\mathcal{O}$-module. Hence there is a finite $\mathcal{O}$-basis of I and since $\mathcal{O}$ is a finitely generated $\mathbb{Z}$-module we can thus choose a finite $\mathbb{Z}$-basis $a = (a_1, a_2, \ldots, a_r)$ for I. Since I is a module we know $1 \in I$ and hence $\mathcal{O} \subset I$. Therefore we know $r \geq n$. And since there exists an $s \in \mathbb{Z}[\alpha]$ such that $sI = \mathcal{O}$ we can choose a basis of $\mathcal{O}$ and multiply all elements with $\frac{1}{s}$. This will now be a basis of I hence $n \geq r$ we conclude that $r = n$

Now look at the multiplication by α map $m_\alpha : I \to I$ such that for $x \in I$ we have $m_\alpha(x) = \alpha x$. Which can be represented as a matrix with respect to the basis a by putting the (i, j)'th entry to be the a_{ij} for which $\alpha a_i = \sum_{j=1}^{n} a_{ij} a_j$. Then $[m_\alpha]_a$ is an $n \times n$ matrix with coefficients in $\mathbb{Z}$ as desired.
Let us now show the function Ψ is well defined by first showing it is independent of the choice of basis a of I and then showing it is independent of the choice of representative I of $[I]$.
To show Ψ is independent of the chosen basis a of I we now take an arbitrary basis a' of I. Then we denote the change of basis matrix from the basis a' to the basis a by $[1_a]_a^{a'}$. Hence $[1_a]_a^{a'}[m_\alpha]_{a'}^{a'}[1_a]_a^{a'-1} = [m_\alpha]_a$ Now since $[1_a]_a^{a'}$ has entries in $\mathbb{Z}$ we can conclude that $[m_\alpha]_{a'}^{a'}$ and $[m_\alpha]_a$ are similar. Hence they are part of the same similarity class and we can conclude that the mapping Ψ is independent of the choice of basis for I.
To show that Ψ is independent of the choice of representative of $[I]$ we choose an arbitrary representative I'. Then $I' = xI$ for some $x \in \mathbb{Q}[\alpha]^\times$. Now if $a = (a_1, \ldots, a_n)$ is a $\mathbb{Z}$-basis of I then $xa = (xa_1, \ldots, xa_n) = (b_1, \ldots, b_n)$ is a $\mathbb{Z}$-basis of I' since every element $k' \in I'$ can be written as $k' = xk$ for $k \in I$ and thus $k' = xk = x\sum_{i=1}^{n} a_{ij} a_j = \sum_{i=1}^{n} a_{ij} x a_j = \sum_{i=1}^{n} a_{ij} b_j$. They also have to be independent since I' has rank n and there are only n elements in the basis. Just as we saw when we multiplied k with x we note that multiplying a_i with x does not change the factors a_{ij} in the sum and hence $[m_\alpha]_a^a = [m_\alpha]_{xa}^{xa} = [m_\alpha]_b^b$. Hence Ψ is independent of the choice of representative of $[I]$ and we conclude that Ψ is well defined.
Now we will prove that Ψ is both injective and surjective to show it is a bijection.
We will start by proving Ψ is injective. To do this we start with $[I]$ and $[I']$ two classes of fractional ideals of $\mathbb{Z}[\alpha]$. Let $a = (a_1, \ldots, a_n)$, $a' = (a'_1, \ldots, a'_n)$ be the basis of I and I' respectively and suppose that $\Psi([I]) = \Psi([I'])$. Then by definition there is a matrix $U \in GL_n(\mathbb{Z})$ such that $U[m_\alpha]_a U^{-1} = [m_\alpha]_{a'}^{a'}$. Now let $[\cdot]_a : I \to \mathbb{Z}^n$ and $[\cdot]_{a'} : I' \to \mathbb{Z}^n$ be the column representation maps for I and I' respectively that is, the maps which send a_i to e_i where e_i is the i'th basis vector of the standard basis, e, in $\mathbb{Z}^n$. We now look at the map $[\cdot]_{a'}^{-1} U [\cdot]_a : I \to I'$. This map clearly has an inverse since all matrices in it are invertible. Moreover this map is a $\mathbb{Z}$-module homomorphism since it effectively linearly adds different rows of U. Hence it is a $\mathbb{Z}$-module isomorphism. Now note that it is also a $\mathbb{Z}[\alpha]$-module isomorphism since it commutes with the multiplication by α matrix m_α:

$$\begin{aligned}
[\cdot]_{a'}^{-1} U [\cdot]_a [m_\alpha]_e^e &= [\cdot]_{a'}^{-1} U [m_\alpha]_a [\cdot]_a \\
&= [\cdot]_{a'}^{-1} [m_\alpha]_{a'}^{a'} U [\cdot]_a \\
&= [m_\alpha]_e^e [\cdot]_{a'}^{-1} U [\cdot]_a.
\end{aligned}$$

$\mathbb{Z}[\alpha]$-module isomorphic fractional $\mathbb{Z}[\alpha]$-ideals are scalar multiples. Hence $I' = xI$ for some $x \in \mathbb{Q}[\alpha]^\times$. And hence $[I] = [I']$ and we conclude that Ψ is injective.
Now to prove surjectivity we take an arbitrary class of matrices $[A] \in \mathcal{M}_f$ represented by a matrix $A = (a_{ij})$ and we will show that there is a fractional $\mathbb{Z}[\alpha]$-ideal I with an ordered basis $a = (a_1, \ldots, a_n)$ such that $[m_\alpha]_a = A$. We start by equipping $\mathbb{Q}^n$ with a $\mathbb{Q}[\alpha]$-vector space structure by defining a multiplication. Let $x \in \mathbb{Q}[\alpha]$, $v \in \mathbb{Q}^n$ and choose $g(T) \in \mathbb{Q}[T]$ such that $g(\alpha) = x$. Then we define the multiplication as follows:

$$x \cdot v = g(A)v.$$

To check if this multiplication is well defined we have to check two things. First that we can always choose such a $g(T)$ and second that the multiplication is independent of our choice.
We can always choose such a $g(T)$ since x can be written as $x = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$ where n is the degree of f and $b_i \in \mathbb{Q}$ since every higher power of α can be written as a sum of lower powers in α using f. Now we can choose $g = b_0 + b_1 T + \ldots + b_{n-1} T^{n-1}$.

To see the multiplication does not depend on our choice for $g(T)$, suppose there is a second function $h(T)$ which also satisfies $h(\alpha) = x$. Then $(g-h)(\alpha) = 0$ and since f is monic and irreducible we know that f is also the minimal polynomial of α hence $f|(g-h)$. Therefore we see that:

$$\begin{aligned} g(A) &= (h + pf)(A) \quad \text{with } p \in \mathbb{Q}[T] \\ &= h(A) + pf(A) \\ &= h(A) \end{aligned}$$

Here we Made the last step since Cayley-Hamilton tells us that $f(A) = 0$ for f the characteristic polynomial of A. Thus we conclude the multiplication is well defined.
It is now straightforward to check that this induces a $\mathbb{Q}[\alpha]$-vector space structure on $\mathbb{Q}^n$. Now if we look at $\mathbb{Q}^n$ as both a $\mathbb{Q}$ and a $\mathbb{Q}[\alpha]$-vector space we can see that:

$$\begin{aligned} n &= \dim_{\mathbb{Q}}(\mathbb{Q}^n) \\ &= [\mathbb{Q}[\alpha] : \mathbb{Q}] \dim_{\mathbb{Q}[\alpha]}(\mathbb{Q}^n) \\ &= n \dim_{\mathbb{Q}[\alpha]}(\mathbb{Q}^n) \end{aligned}$$

Hence $\dim_{\mathbb{Q}[\alpha]}(\mathbb{Q}^n) = 1$. Therefore any $v_o \in \mathbb{Q}^n$ $\phi_{v_0} : \mathbb{Q}[\alpha] \to \mathbb{Q}^n$ with $\phi_{v_0}(x) = xv_0$ is an isomorphism of $\mathbb{Q}[\alpha]$-vector spaces. Let $e = (e_1, \ldots, e_n)$ be the standard $\mathbb{Q}$-basis of $\mathbb{Q}^n$, since ϕ_{v_0} is an isomorphism there is a unique $a_i \in \mathbb{Q}[\alpha]$ such that $\phi_{v_0}(a_i) = e_i$ for all e_i. Therefore $a = (a_1, \ldots, a_n)$ has to be a $\mathbb{Q}$-basis of $\mathbb{Q}[\alpha]$. Let $I = \bigoplus_{i=1}^n a_i\mathbb{Z}$ then to show that I is a fractional $\mathbb{Z}[\alpha]$ ideal we need to show that $\alpha a_i \in I$. Or equivalently that $\alpha a_i = \sum_{j=1}^n a'_{ij} a_j$ for some $a'_{ij} \in \mathbb{Z}$. Or equivalently since ϕ_{v_0} is an isomorphism that $\phi_{v_0}(\alpha a_i - \sum_{j=1}^n a'_{ij} a_j) = 0$. Now we look at the last equivalent statement where we choose $a'_{ij} = a_{ij}$:

$$\begin{aligned} \phi_{v_0}(\alpha a_i - \sum_{j=1}^n a'_{ij} a_j) &= \phi_{v_0}(\alpha a_i) - \phi_{v_0}(\sum_{j=1}^n a'_{ij} a_j) \\ &= \alpha e_i - \sum_{j=1}^n a'_{ij} \phi_{v_0}(a_j) \\ &= \alpha e_i - \sum_{j=1}^n a'_{ij} e_j \\ &= Ae_i - Ae_i = 0 \end{aligned}$$

Therefore we conclude that I is a fractional $\mathbb{Z}[\alpha]$ ideal with basis $a = (a_1, \ldots, a_n)$ such that $[m_\alpha]_a = A$. And hence Ψ is surjective completing the proof. □

3 Proof of the Similarity Extension Theorem

In this section we will discuss the Similarity Extension Theorem. We start by giving some motivation for the use of this theorem and then we will show the proof of the theorem, first given by Guralnick in [Gur80]. In this proof Guralnick uses the Theorem 2 from [Dad63], a paper by Dade, and the only theorem from [RZ61], by Reiner and Zassenhaus.
Let us first state the theorem again:
Theorem 3. (Similarity Extension Theorem) [Gur80, Theorem 7] Let D be the ring of algebraic integers in a finite extension of $\mathbb{Q}$ and let $A, B \in \mathbb{Z}^{n\times n}$ be matrices with characteristic polynomial f with $f \in \mathbb{Z}[X]$ square-free. Then, A and B are locally D-similar for every prime if and only if there is a finite integral extension E of D such that A and B are similar over E.

The theorem then gives us an interesting view on when matrices are similar as we know that if two matrices are similar in D they will be similar in every extension of D in particular all localisations. However the reverse does not hold which makes it fascinating that being similar in some extensions can still be used to determine similarity in another extension.

We will mainly focus on half of this theorem namely the half that says there is an extension of D where A and B are similar if they are similar locally for all primes of D. In the next chapters we will be looking at ways to explicitly find this extension.
So let us now take a look at the assumption that A and B are locally similar for every prime. An important question is if this assumption is difficult to check since if this is the case the theorem would become less useful. It turns out that it is manageable to check this assumption. As any two matrices $A, B \in \mathbb{Z}^{n\times n}$ will be locally similar for all but finitely many primes as a consequence of Theorem 11 from [AO83]. This is because all matrices that are similar over $\mathrm{SL}_n(\mathbb{Z})$ are similar over $\mathrm{GL}_n(\mathbb{Z})$. With the discriminant of a polynomial $f(x) = a_n x^n + \ldots + a_1 x + a_0$ with roots $\{\alpha_1, \ldots \alpha_n\}$ is defined as $\mathrm{Disc}(f) = a_n^{2n-2} \prod_{i<j}(\alpha_i - \alpha_j)^2$, the theorem from [AO83] then becomes:

Theorem 9. [AO83, Theorem 11] Let $A, B \in \mathbb{Z}^{n\times n}$ be matrices with characteristic polynomial $f \in \mathbb{Z}[X]$ square-free, and α a root of f. Then A and B are locally similar for any prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\alpha]$ over a prime p which does not divide the discriminant of f.

Of course it should still be checked that A and B are locally similar at the remaining primes. Checking this for specific primes can be done by finding the change of basis matrices from A to B by assuming there is such a matrix with unknown constants as inputs and then solving the resulting system of equations.

Let us proof the Similarity Extension Theorem:

Proof. We start by proving that if A and B are locally similar for every prime ideal $\mathfrak{p}$ of D, then there exists a finite integral extension E of D such that A and B are E-similar.
Let C_1' be the change of basis matrix for the matrices A and B in the localisation of some prime $\mathfrak{p}_1$. We can now choose $C_1 = aC_1'$ with $a \in D$ such that all entries of C_1 are in D by choosing a to be the least common multiple of all denominators of the entries of C_1'. Note that C_1 is still in $\mathrm{GL}_n(D_{\mathfrak{p}_1})$ since $\det(C_1) = a^n \det(C_1')$ and $a \in D\backslash\{\mathfrak{p}_1\}$ and hence $\frac{1}{a^n} \in D_{\mathfrak{p}_1}$. Now we look at the ideal $I_1 = (\det(C_1)) \subset D$. Note that $\det(C_1) \notin \mathfrak{p}_1$. Suppose the contrary then $\det(C_1) = a^n \det(C_1') \in \mathfrak{p}_1$ and $\det(C_1')$ is a unit in $D_{\mathfrak{p}_1}$ hence $\det(C_1') = \frac{r}{s}$ with $r, s \in D\backslash\mathfrak{p}_1$. Thus $a^n \frac{r}{s} \in \mathfrak{p}_1$ implies $a^n r \in s\mathfrak{p}_1 \subset \mathfrak{p}_1$ but then either $a \in \mathfrak{p}_1$ or $s \in \mathfrak{p}_1$ giving a contradiction.

Our goal is to make an ideal of the form $I_k = (\det(C_1), \ldots, \det(C_k)) = D$, where C_i are change of basis matrices form A to B just like C_1 from above is. If $I_1 = D$ we are done, so suppose $I_1 \neq D$ then, by Corollary 9.4 of [AM16], we have that $I_1 = \mathfrak{q}_1^{e_1} \ldots \mathfrak{q}_m^{e_m}$ for some prime ideals $\mathfrak{q}_i$ of D and integers e_i. Now choose $\mathfrak{p}_2$ to be $\mathfrak{q}_1$, note that $\mathfrak{p}_2 \neq \mathfrak{p}_1$ since $\det(C_1) \in \mathfrak{p}_2$ and $\det(C_1) \notin \mathfrak{p}_1$. By the same reasoning as before we can now construct C_2 from $\mathfrak{p}_2$. Then we know that $\det(C_2) \notin \mathfrak{p}_2 = \mathfrak{q}_1$ and hence it will not be in $\mathfrak{q}_1^{e_1} \ldots \mathfrak{q}_m^{e_m} = I_1$. Therefore I_1 is strictly contained in $I_2 = (\det(C_1), \det(C_2))$ and we know that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are not in the ideal factorisation of I_2.

We can repeat this process several times, and since I_1 has finite index in D we will get $I_k = D$ for some $k \leq m$. We will now show that the coefficients the polynomial $f(x_1, \ldots, x_k) := \det(x_1 C_1 + \ldots + x_k C_k)$ are relative prime.

Note that it is enough to show that some of the coefficients are relative prime since then the entire set of coefficients is. Since all C_i are $n \times n$ matrices we see that f will be a homogeneous polynomial of degree n. The determinant of f will consist of sums of products of its entries, and since the entries are sums of the variables $x_1, \ldots, x_k$ we see that the determinant of f consists of sums of products of sums of the variables $x_1, \ldots, x_k$. If we now look at the coefficients in front of the term x_i^n. We see that in the product of the entries the product has to take the term containing the x_i from every entry to end up in the coefficient of x_i^n. These terms are exactly the terms from C_i hence the coefficient in front of x_i^n will be $\det(C_i)$. We already know that $(\det(C_1), \ldots, \det(C_k)) = I_k = (1) = D$ hence the coefficients in front of the terms x_i^n for $i \in \{1, \ldots, k\}$ are relatively prime. And thus are all the coefficients of f together also relatively prime.
Therefore we can use Theorem 2 from Dade [Dad63]. This theorem tells us that for a polynomial of the same form as the one we are dealing with there exist $a_1, \ldots, a_k$ integral over D such that $f(a_1, \ldots, a_k) = e$ where e is a unit in $D[a_1, \ldots, a_k]$. This implies that $a_1C_1 + \ldots + a_kC_k \in \mathrm{GL}_n(D[a_1, \ldots, a_k])$. We also know that:

$$\begin{aligned}(\alpha_1C_1 + \ldots + \alpha_kC_k)A &= \alpha_1C_1A + \ldots + \alpha_kC_kA &(1)\\ &= \alpha_1BC_1 + \ldots + \alpha_kBC_k &(2)\\ &= B\alpha_1C_1 + \ldots + B\alpha_kC_k &(3)\\ &= B(\alpha_1C_1 + \ldots + \alpha_kC_k). &(4)\end{aligned}$$

Hence $D[a_1, \ldots, a_k]$ is a finite integral extension of D and A and B are similar over $D[a_1, \ldots, a_k]$. Thus we can choose $E = D[a_1, \ldots, a_k]$ and have proven our claim.

Now let us prove the reverse statement. Suppose A and B are similar over some finite integral extension E of D. Then A and B are similar over the localisation $E_{\mathfrak{q}}$ for every prime ideal $\mathfrak{q}$ of E. Now we can use the theorem from the paper by Reiner and Zassenhaus [RZ61]. Which says that A and B are similar over $D_{\mathfrak{p}}$ for every prime $\mathfrak{p}$ which can be written as $\mathfrak{p} = E \cap \mathfrak{q}$. Since every prime ideal in D can be written as $E \cap \mathfrak{q}$ for some prime $\mathfrak{q}$ of the extension E we have that A and B are locally similar over every prime of D. □

We see that the first direction of the implication in this proof is almost constructive, except for the theorem by Dade that is used in the end. We will refer to this theorem simply as Dade's theorem and it is the reason the Similarity Extension Theorem is not explicit and the Similarity Extension Problem exists.

4 Current research

In this chapter we will discuss some of the current research on the Similarity Extension Problem. In particular we will look at the paper [Afa21] by Afandi which inspired us to look at the problem in the first place. In this paper Afandi proposes a solution to the Similarity Extension Problem by giving an algorithm, which uses a generalisation of the LM-correspondence, that tries to find an algebraic extension of $\mathbb{Z}$ in which two matrices A and B are similar when A and B are locally similar for every prime p. Afandi however immediately gives an example in which the algorithm does not work. In this thesis we are trying to make an algorithm with the same goal which is why we will compare our findings to the algorithm proposed by Afandi at the end of the thesis.

Let us first discuss the general idea behind Afandi's proposed solution for the Similarity Extension Problem. Afandi started with generalising the LM-correspondence such that the characteristic polynomial f of the matrices can be chosen square-free with multiple irreducible components. This allowed for the adaptation of the algorithm from [Mar20] by Marseglia which gives the $\mathbb{Z}$ similarity classes of matrices whenever f is square-free. With this adaption the algorithm can now determine whether the matrices are R-similar for R an integral domain with $\mathbb{Z}$ as a subring. Afandi then obtained an algorithm that tests for R-similarity of integral matrices, where R is an integral domain with $\mathbb{Z}$ as a subring. The algorithm checks if two matrices A and B are similar by determining if a particular ideal is principal after the extension of scalars to R. Therefore Afandi decided to look at the ring of integers of Hilbert class field of R since in the ring of integers of the Hilbert class field every fractional ideal of $\mathcal{O}_K$, with K a number field, becomes principal. This however is not enough to solve the Similarity Extension Problem in full generality since it is possible that f has multiple irreducible factors in $R[x]$ which can cause the ideal not to be principal. It also has the downside that it is harder to check whether the ideal becomes principal.

Let us now discuss the generalisation Afandi made to the LM-correspondence. It was already known that the LM-correspondence can be generalised to the context of similarity over any integral domain and not just $\mathbb{Z}$ from [EG84]. Afandi works with a special case where the rings that are considered are integral domains with $\mathbb{Z}$ as a subring. Therefore Afandi is able to explicitly use the original LM-correspondence to define a bijection in the following way. Let R be an integral domain with $\mathbb{Z}$ as a subring and let the $\mathbb{Z}$-similarity class of a matrix A correspond to a fractional ideal I. Since a fractional ideal is a free $\mathbb{Z}$-module the tensor product $R \otimes_{\mathbb{Z}} I$ essentially only extends scalars. Hence Afandi argues that in the case the $\mathbb{Z}$-similarity class of a matrix A corresponds to the fractional ideal class I. Then we find that the R-similarity class of the same matrix A corresponds to the tensor product $R \otimes_{\mathbb{Z}} I$.
In this setting Afandi then notes that for a square-free polynomial f one can look at the different irreducible factors of the polynomial separately in a direct product. In this case a zero of f will also be interpreted component wise such that each individual component is in the situation as discussed before.

Now let us focus on the algorithms Afandi provides. Afandi uses three algorithms, one to determine if a pair of matrices is R-similar (Algorithm 3.2 in [Afa21]), and two to check if either a proper subfield of the Hilbert- or ray- class field is a solution to the Similarity Extension Problem (Test 3.6 and Test 3.9 in [Afa21]). Before I can explain the first algorithm I need one more definition:

Definition 10. Let I and J be ideals in a commutative ring R the colon ideal of I over J is the following:

$$(I : J) := \{x \in R : xJ \subset I\}.$$

The colon ideal of I with itself,

$$(I : I) := \{x \in R : xI \subset I\},$$

is also called the *multiplicator ring* of I.

The first algorithm, that determines whether two matrices are R-similar, has as an input two integral $n \times n$ matrices $A, B \in \mathcal{M}_f$ where $f \in \mathbb{Z}[X]$ square-free and an integral domain R containing $\mathbb{Z}$. It will then check whether A and B are R-similar. It does this by first computing the fractional ideals I, J corresponding to the pair of matrices A, B respectively using the generalised LM-correspondence. Then it checks whether the two ideals have the same multiplicator ring. If this is not the case the matrices are not similar. If the multiplicator rings are the same it sets $\mathcal{O}$ to be this multiplicator ring and goes to the next step. In the

next step it checks whether the colon ideal of $(I : J) \otimes_{\mathbb{Z}} \mathcal{O}$ is principal. If this is not the case the fractional ideals are not similar. Else the fractional ideals are similar and Afandi determines the change of basis matrix between A and B using the LM-correspondence.
The second algorithm checks whether a proper subfield of the Hilbert class field is a solution to the Similarity Extension Problem. So let us define the Hilbert class field.

Definition 11. The Hilbert class field of a number field K is the maximal abelian unramified extension of K. We will denote the Hilbert class field of K by K_1.

The Hilbert class field, as mentioned before, has a special property, namely every fractional $\mathcal{O}_K$-ideal is principal in $\mathcal{O}_{K_1}$.
Note that this statement does not hold for the "fractional ideals" in the broader sense Afandi defined using the direct product since these are not fractional ideals in the classical sense.
Also the algorithm is limited since if we choose f to not be irreducible it cannot determine if $R \otimes_{\mathbb{Z}} I$ is principal, hence the algorithm will require f to be irreducible in $\mathbb{Z}[x]$. The algorithm will now look for any proper subfield of $F \subset K_1$ and check the following two criteria. 1 f is irreducible in $\mathcal{O}_F[x]$. And 2 $\mathcal{O}_F \otimes_{\mathbb{Z}} (I : J) \otimes_{\mathbb{Z}} \mathcal{O}$ is principal. If F satisfies both criteria then $\mathcal{O}_F$ is a solution to the Similarity Extension Problem.

The last algorithm is similar to the previous algorithm but searches through the proper subfields of the ray class field, which is a generalisation of the Hilbert class field. That is, the ray class field of a number field K is similar to the Hilbert class field of K but contrary to Hilbert class fields they can be ramified at finitely many primes. Ray class fields have a similar property, that ideals become principal in the ring of integers if a ray class field, which allows Afandi to adapt her algorithm to subfields of the ray class field.

5 Why is Dade's theorem not explicit?

To develop our method we started by investigating Theorem 2 from Dade [Dad63] used in the Similarity Extension Theorem. This was the part of the proof for the Similarity Extension Theorem that was not explicit. We hoped we would be able to avoid the non explicit parts of the proof of Dade's theorem to make the Similarity Extension Theorem explicit. We explored Dade's theorem using an example which we will discuss more in the next chapter. We will now go over the proof and show at what point the theorem becomes an existence theorem.

Let us first state the theorem in question.

Theorem 12. (Dade's theorem) [Dad63, Theorem 2] Let K be the set of all algebraic elements of $\mathbb{C}$, let D be the integral closure of $\mathbb{Z}$ in K, and let $f(x_1, \ldots, x_n)$ be a polynomial with coefficients in D. If the coefficients of f are relative prime. Then there exist $y_1, \ldots, y_n \in D$ such that $f(y_1, \ldots, y_n) = u$ for u a unit of D.

To prove this theorem Dade shows that it is always possible to transform the function f in such a way that it satisfies the properties of the first theorem of the same paper. Let us state this theorem.

Theorem 13. [Dad63, Theorem 1] Let K and D be as in the above theorem, and let $f(x)$ be a polynomial with coefficients in D. If the coefficients of f are relative prime then there exist $y \in D$ such that $f(y) = u$ for a unit u of D.

Let us now show how the transformation from a function that can be used in Theorem 12 to a function that can be used in Theorem 13 is done.
First Dade writes

$$f(x_1, \ldots, x_n) = c_0 + c_1(x_1, \ldots, x_n) + \ldots + c_m(x_1, \ldots, x_n)$$

where c_0 is a constant and c_i is a homogeneous polynomial of degree i in $x_1, \ldots, x_n$ for $i \neq 0$. Dade then notes that we may assume $c_0 \neq 0$, since if it where 0 we could translate the function by changing all variables x_i to $x_i + 1$. Since f is not the zero polynomial we will then get a polynomial with $c_0 \neq 0$, we call this new polynomial f'. Our goal now is to find $u_1, \ldots, u_n \in D$ such that $c_0, c_i(u_1, \ldots, u_n)$ are relative prime in D for all i. Note that if we find those we have:

$$f'(u_1X, \ldots, u_nX) = c'_0 + c'_1(u_1, \ldots, u_n)X + \ldots + c'_m(u_1, \ldots, u_n)X^m.$$

And hence $f'(u_1X, \ldots, u_nX)$ satisfies the conditions we are looking for.
Dade then proceeds to prove this is always possible though we will only show it for the situation we were in when investigating this proof with our example, namely that all coefficients of f are in $\mathbb{Z}$.
Note that since all coefficients of f are relative prime integers so are those of f', since if f is of degree m all coefficients in front of terms of degree m are unchanged. The coefficients in front of terms of degree $m-1$ will have been changed by some sum of coefficients of degree m terms, hence we can recover the old terms by adding the appropriate amount of coefficients degree m terms to them. This process can then be repeated until we find that all original coefficients can be recovered as sums from the current coefficients. Hence since the original coefficients were relative prime so are the current coefficients.

Now since all coefficients of f' are relative prime integers we will show that the desired u_i exist. We will first prove this in the situation that c_0 is prime. In this case there is a coefficient that does not divide this prime. Suppose this coefficient is in front of the ith power of one variable then we can pick that variable to be 1 and the others to be 0 and see that that c_0 is relative prime to c_i. Suppose now that there is no coefficient in front of the ith power of one variable that is relative prime to c_0. Suppose the coefficient that is prime to c_0 is in front of the term, $x_i^{e_i}x_j^{e_j}$, that is a combination of two variables. Then we can take those two variables to be 1 and all others 0. And find that $c_{e_i+e_j} = a_{ii} + a_{ij} + a_{jj} \equiv a_{ij} \mod c_0$ is relative prime to c_0. We can repeat this argument for combinations of more different variables and conclude we can always find a solution when c_0 is prime. Suppose now that $c_0 = \Pi_i p_i$ where p_i are distinct primes. Then we can find the solution for all separate primes as discussed above, call these solutions y_i. Then $y = \sum_i \frac{c_0}{p_i} y_i$ is such that $c_0, c_1(y), \ldots, c_n(y)$ are relative prime. We thus found values for all u_i that solve the problem. And we know we can use Theorem 13. Theorem 13 then start with a lemma that it uses to rephrase the theorem in a new

setting. In this lemma Dade uses that a particular ideal which is constructed as generated by two elements has to be principal. This is however not done explicitly and we need the generator of this ideal for the next step. Since there is no algorithm that can always determine the generator of a principal ideal when we are dealing with such general rings the theorem stops being explicit.

6 Finding an extension explicitly

In this chapter we will show how we can use Theorems 1 or 2 from [Wat63] in the proof of the Similarity Extension Theorem instead of using Dade's theorem, discussed in the previous section. Using the theorems from Watson makes the process of finding an extension explicit, however it is only applicable in a more specific case. We will go over the proof of Watson's theorems. Then we will work out an example of our method to explicitly find an extension for a case where Afandi's algorithm was not able to find a one.

Let us start by giving a definition so we can state a combination of Watson's two theorems afterwards and explain how it fits into the proof of the Similarity Extension Theorem.

Definition 14. Let $f : V \to K$ be a homogeneous polynomial of degree 2, and let B be defined as:

$$B(v, w) = \frac{1}{2}(f(v + w) - f(v) - f(w)).$$

If then the set $\{v \in V \mid B(v, w) = 0 \quad \forall w \in V\}$ is equal to the set $\{0\}$, f is called *non-singular*.

Theorem 15. (Watson's theorem) [Wat63, Theorem 1 and Theorem 2] Let $f = (x_1, \ldots, x_n)$, $n \geq 3$, be a non-singular homogeneous polynomial of degree 2, which has coefficients in $\mathbb{Z}$ which are relatively prime. Then there exist $q, r \in \mathbb{Z}$ such that the equation

$$f(y_1 + z_1\sqrt{q} + w_1\sqrt{r}, \ldots, y_n + z_n\sqrt{q} + w_n\sqrt{r}) = 1$$

has a solution with $y_i, z_i, w_i \in \mathbb{Z}$.

We will refer to this theorem as Watson's theorem. The separate theorems in Watson's paper are even slightly more powerful than this theorem as it says that in case $n \geq 4$ we can choose all $w_i = 0$, so we do not need r.

If we now want to replace Dade's theorem in the proof of the Similarity Extension Theorem we still need to make sure that the function $f(x_1, \ldots, x_n) = \det(C_1x_1 + \ldots + C_nx_n)$ from the proof of the Similarity Extension Theorem is a non-singular homogeneous polynomial of degree 2 in at least 3 variables with coefficients in $\mathbb{Z}$.

To get a homogeneous polynomial of degree 2 we simply need that all C_i are 2×2 matrices. This is the case if and only if the matrices A and B, for which we are determining the extension where they are similar, are themselves 2×2 matrices. To ensure we get a polynomial in at least 3 variables we need there to be 3 or more matrices C_i. In itself this would not be a problem as we could take the same matrix several times to ensure we get a polynomial in at least 3 variables. But we will see that this causes f to become singular.

Proposition 16. Let $f(x_1, \ldots, x_n) = \det(C_1x_1 + \ldots + C_nx_n)$. Then $C_i = C_j$ for $i \neq j$ implies that $f(x_1, \ldots, x_n)$ is singular.

Proof. Let $C_i = C_j = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and for all other k we have $C_k = \begin{pmatrix} a_k & b_k \\ c_k & d_k \end{pmatrix}$. We find that

$$\begin{aligned} f(x_1, \ldots, x_n) = \det(C_1x_1 + \ldots + C_nx_n) &= \det \begin{pmatrix} a(x_i + x_j) + \sum_{k \neq i,j} a_k x_k & b(x_i + x_j) + \sum_{k \neq i,j} b_k x_k \\ c(x_i + x_j) + \sum_{k \neq i,j} c_k x_k & d(x_i + x_j) + \sum_{k \neq i,j} d_k x_k \end{pmatrix} \\ &= (a(x_i + x_j) + \sum_{k \neq i,j} a_k x_k)(d(x_i + x_j) + \sum_{k \neq i,j} d_k x_k) \\ &\quad - (b(x_i + x_j) + \sum_{k \neq i,j} b_k x_k)(c(x_i + x_j) + \sum_{k \neq i,j} c_k x_k). \end{aligned}$$

Since every time x_i or x_j arises in $f(x_1, \ldots, x_n)$ it is in the form $(x_i + x_j)$ we know every point that has $x_i = -x_j$ and $x_k = 0$ for all other k is in the kernel of the bilinear form associated with $f(x_1, \ldots, x_n)$. Therefore we conclude $f(x_1, \ldots, x_n)$ is singular.

□

Hence we need to pick at least three different matrices for C_i. We looked at a few examples of quadratic extensions of $\mathbb{Z}$ which we knew from [Afa21] satisfied the properties we needed as she used them as examples as well. In all examples we worked through it has not been a problem to pick at least three different matrices for C_i and therefore we suspect it might be possible to prove that it will always be possible to do this.
When this is done our method will be a good addition to Afandi's algorithm as both are able to solve the Similarity Extension Problem in situations the other is not.

6.1 Proof of Watson's theorem

We will now start working towards the proof of Watson's theorem. In this proof the function $f(x_1, \ldots, x_n)$ is first transformed to a simpler function $g(x_1, \ldots, x_n)$ using $\mathbb{Z}$-linear transformations. With these transformations we know that if we can find a solution to $g(y_1 + z_1\sqrt{q} + w_1\sqrt{r}, \ldots, x_n + z_n\sqrt{q} + w_n\sqrt{r}) = 1$ we are also able to find it for $f(x_1, \ldots, x_n)$.
We want to transform $f(x_1, \ldots, x_n)$ to a polynomial which only has factors x_i^2 in such a way that the coefficients in front of x_1 and x_2 are relatively prime. Before we start to prove this, let us give the definition of the coefficients matrix of a homogeneous polynomial of degree 2 and its discriminant.

Definition 17. Let $f(x_1, \ldots, x_n) = \sum_{(i,j)} b_{ij}x_ix_j$ be a homogeneous polynomial of degree 2. The coefficients matrix of f, $A(f)$, is defined as the $n \times n$ matrix with $A_{ij} = A_{ji} = a_{ij}$ for $i \neq j$ and $A_{ii} = 2a_{ii}$ otherwise.

Definition 18. Let $A(f)$ be the coefficients matrix of f then the discriminant of f, $d(f)$, is the following:

$$d(f) = \begin{cases} (-1)^{(1/2)n} \det(A(f)), & \text{for } n \text{ even} \\ \frac{1}{2}(-1)^{(1/2)(n-1)} \det(A(f)), & \text{for } n \text{ odd.} \end{cases}$$

Lemma 19. Based on Chapter 1.3 from [Wat60].
Let $f(x_1, \ldots, x_n)$ as in Theorem 15. Then there exists a transformation T with $\det(T) \neq 0$ from $f(x_1, \ldots, x_n)$ to $g(x_1, \ldots, x_n)$ such that $g(x_1, \ldots, x_n)$ has the following form:

$$g(x_1, \ldots, x_n) = a_{11}x_1^2 + \ldots + a_{nn}x_n^2.$$

With $\gcd(a_{11}, a_{22}) = 1$.

Proof. We start by transforming $f(x_1, \ldots, x_n) = \sum_{i,j} b_{ij}x_ix_j$ to a function were the coefficient in front of the x_1^2 term is relatively prime to $2\det(A(f))$ where $A(f)$ is the coefficients matrix of f. This will later ensure that we can pick g such that $\gcd(a_{11}, a_{22}) = 1$. To do this we note that we can change b_{11} term to any number, a, represented by $f(x_1, \ldots, x_n)$. By the following transformation: Let $f(y_1, \ldots, y_n) = a$, then we send x_1 to y_1x_1 and x_i to $y_ix_1 + x_i$ for $i \neq 1$. Note that this transformation will not have determinant 0 as long as $y_1 \neq 0$. We will now show that we can always find such $(y_1, \ldots, y_n)$.
First note that $f(x_1, \ldots, x_n)$ always represents b_{ii} and $b_{ii} + b_{ij} + b_{jj}$. So let us now prove that we can take b_{11} relatively prime to p for any fixed prime p. There has to be some b_{ij} relatively prime to it by assumption. If this is a coefficient in front of a square it is clearly represented. Else assume without loss of generality that there is no coefficient in front of a square that is relatively prime to p, and hence all $b_{ii} \equiv 0 \mod p$. We see that $b_{ii} + b_{ij} + b_{jj} \equiv b_{ij} \mod p$ hence $b_{ii} + b_{ij} + b_{jj}$ is relatively prime to p.

Now let $\Pi_i p_i$ be a product of distinct primes p_i dividing $2\det(A(f))$. Then for each of these primes we can find y_i such that $f(y_i)$ is relatively prime to p_i. Then $y = \sum_i \frac{2\det(A(f))}{p_i} y_i$ is relatively prime to $2\det(A(f))$ since for all i we see that $f(y) \equiv f(y_i) \mod p_i$. Now suppose that we end up with a transformation that would now send x_1 to 0, then we can send it to $2\det(A(f))x_1$ instead. The additional factors will then all fall away $\mod p_i$ for all primes in $2\det(A(f))$ hence it will still send b_{11} to a number which is relatively prime to $2\det(A(f))$.
We call the function we find after this transformation $f_1(x_1, \ldots, x_n)$. We will now transform $f_1(x_1, \ldots, x_n) = \sum_{i,j} c_{ij}x_ix_j$ to $f_2(x_1, \ldots, x_n)$ such that $f_2(x_1, \ldots, x_n)$ has the following form:

$$f_2(x_1, \ldots, x_n) = c_{11}x_1^2 + d_{12}x_1x_2 + h(x_2, \ldots, x_n)$$

for some $d_{12} \in \mathbb{Z}$ and polynomial, $h(x_2, \ldots, x_n)$, with integer coefficients . We do this using the following transformation matrix:

$$\begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & -c_{13} & -c_{14} & \ldots & -c_{1n} \\ 0 & 0 & c_{12} & 0 & \ldots & 0 \\ \vdots & 0 & 0 & \ddots & 0 & \vdots \\ 0 & 0 & 0 & 0 & c_{12} & 0 \\ 0 & 0 & 0 & \ldots & 0 & c_{12} \end{pmatrix}.$$

We will now transform $f_2(x_1, \ldots, x_n)$ to $f_3(x_1, \ldots, x_n)$ such that $f_3(x_1, \ldots, x_n)$ has the following form:

$$f_3(x_1, \ldots, x_n) = c_{11}x_1^2 + h(x_2, \ldots, x_n).$$

We do this using the following transformation matrix:

$$\begin{pmatrix} 1 & -d_{12} & 0 & \ldots & 0 & 0 \\ 0 & 2c_{11} & 0 & 0 & \ldots & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 \\ \vdots & 0 & 0 & \ddots & 0 & \vdots \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix}.$$

Note that since we transformed f such that the coefficient in front of the x_1^2 term is relatively prime to $2\det(A(f))$ we now have that $h(x_2, \ldots, x_n)$ represents an integer that is relatively prime to c_{11} according to the proof of Lemma 2 in [Wat63]. And hence we can now use a similar transformation as in Lemma 19 to transform f_3 into a function whose coefficient in front of the x_2^2 term is relatively prime to c_{11}.
Now we repeat the process of removing the cross terms until we are left with a function $g(x_1, \ldots, x_n) = a_{11}x_1^2 + \ldots + a_{nn}c_n^2$ with $\gcd(a_{11}, a_{22}) = 1$ as desired. □

If we now find a solution for the equation

$$g(x_1\sqrt{q}, x_2\sqrt{r} \ldots, x_n\sqrt{r}) = a_{11}qx_1^2 + a_{22}rx_2^2 + \ldots + a_{nn}rc_n^2 = 1,$$

then we have also found a solution for $f(x_1, \ldots, x_n)$ and have completed the proof. Let us now give another definition before we start the next lemma.

Definition 20. A homogeneous polynomial of degree 2 is called *indefinite* if it takes on both positive and negative values.

We will now show that we can choose q and r such that the above equation is soluble $\mod 8$ and $\mod p$ for any prime p, $g(x_1\sqrt{q}, x_2\sqrt{r} \ldots, x_n\sqrt{r})$ is indefinite and if $n = 3$ exactly one of the coefficients is positive. With these conditions we will then be able to prove that the equation above is soluble.

The proof of the following lemma is based on the proof of Theorem 2 from [Wat63]. Though at some points Watson claimed certain choices were possible and we explicitly showed they are.

Lemma 21. [Wat63, based on proof of Theorem 2] Let $g(x_1, \ldots, x_n)$ be as above. Then we can choose q and r such that the equation

$$g(x_1\sqrt{q}, x_2\sqrt{r} \ldots, x_n\sqrt{r}) = a_{11}qx_1^2 + a_{22}rx_2^2 + \ldots + a_{nn}rc_n^2 = 1,$$

is soluble $\mod 8$ and $\mod p$ for any prime p, that $g(x_1\sqrt{q}, x_2\sqrt{r} \ldots, x_n\sqrt{r})$ is indefinite and that, if $n = 3$, exactly one of the coefficients is positive.

Proof. Since we picked a_{11} to be relatively prime to 2 we know it is odd. Hence if we choose $q \equiv a_{11} \mod 8$ we find that $x_1 = 1$ and $x_i = 0$ for all other i is a solution to $g(x_1\sqrt{q}, x_2\sqrt{r}, \ldots, x_n\sqrt{r}) \equiv 1 \mod 8$.

Now we show $g(x_1\sqrt{q}, x_2\sqrt{r}, \ldots, x_n\sqrt{r}) \equiv 1 \mod p$ has a solution for all primes p. The statement is already true for $p = 2$ by the above argument so we will for now assume p is odd. Let us first look at all

$p \mid a_{11}$. Choose r such that $x_2 = 1$ and $x_i = 0$ for all other i is a solution to $g(x_1\sqrt{q}, x_2\sqrt{r}, \ldots, x_n\sqrt{r}) \equiv 1 \mod p$. This means we are looking for $ra_{22} \equiv 1 \mod p$ for all $p \mid a_{11}$. This is possible since $\gcd(a_{11}, a_{22}) = 1$ hence $a_{22} \not\equiv 0 \mod p$ for all $p \mid a_{11}$. Note that by this congruence we know that $r \nmid p$ for all these p and we can conclude $\gcd(r, a_{11}) = 1$.

Now let us look at all $p \mid a_{22}$ and $p \mid r$ then setting and $x_i = 0$ for $i \neq 1$ gives us the equation:

$$\begin{aligned} g(x_1\sqrt{q}, x_2\sqrt{r}, \ldots, x_n\sqrt{r}) &\equiv 1 \mod p \\ g(x_1\sqrt{q}, 0, \ldots, 0) &\equiv 1 \mod p \\ a_{11}^2 x_1^2 &\equiv 1 \mod p \\ (a_{11}x_1)^2 &\equiv 1 \mod p \\ &. \end{aligned}$$

To solve this we pick x_1 such that $a_{11}x_1 \equiv 1 \mod p$ which is possible since $\gcd(r, a_{11}) = 1$ and $\gcd(a_{22}, a_{11}) = 1$.

Now for all primes $p \nmid qa_{11}ra_{22}$ we know that it is soluble by Lemma 22 which we will prove below.

Without changing the proof we can choose the sign of r and we can then also pick $q = a_{11} - 8a_{22}rm$ for any integer m. Hence we are also able to ensure that $g(x_1\sqrt{q}, x_2\sqrt{r} \ldots, x_n\sqrt{r})$ is indefinite and that if $n = 3$ exactly one of the coefficients is positive. □

Now let us proof the missing lemma:

Lemma 22. Let $a, b, p \in \mathbb{Z}$ with p an odd prime. If $p \nmid a$ and $p \nmid b$ then the equation $ax_1^2 + bx_2^2 \equiv 1 \mod p$ has a solution with $x_1, x_2 \in \mathbb{Z}$.

Proof. This lemma is equivalent to saying there is a pair $(x_1, x_2) \in \{0, 1, 2, \ldots, \frac{1}{2}(p-1)\}^2$ such that $ax_1^2 \equiv 1 - bx_2^2 \mod p$, since every value of x_1 or x_2 would be equivalent up to sign to any of these values $\mod p$ and since x_1 and x_2 are both squared afterwards the signs of x_1 and x_2 do not change the result.
For now we will assume that ax_1^2 will take different values $\mod p$ for each $x_1 \in \{0, 1, 2, \ldots, \frac{1}{2}(p-1)\}$ and that the same holds for $1 - bx_2^2$, we will proof this later. With this assumption we see there are $\frac{1}{2}(p+1)$ possible different values $\mod p$ on both the left and right side of the equation $ax_1^2 \equiv 1 - bx_2^2 \mod p$. Hence in total there are $p + 1$ values $\mod p$. This implies two have to be the same $\mod p$. Since we assumed they are all distinct on each side of the equation there has to be a pair $(x_1, x_2) \in \{0, 1, 2, \ldots, \frac{1}{2}(p-1)\}^2$ such that $ax_1^2 \equiv 1 - bx_2^2 \mod p$.
We will now proof the assumption we made above. Note that it is enough to show that ax_1^2 will take different values $\mod p$ for each $x_1 \in \{0, 1, 2, \ldots, \frac{1}{2}(p-1)\}$. Then it immediately follows that the same holds for bx_2^2 and hence for $1 - bx_2^2$. Assume $ax_1^2 = ay_1^2 \mod p$ for $x_1, y_1 \in \{0, 1, 2, \ldots, \frac{1}{2}(p-1)\}$. Then we see the following:

$$\begin{aligned} ax_1^2 = np + k \qquad & ay_1^2 = mp + k, \quad \text{for some } n, m, k \in \mathbb{Z}. \\ ax_1^2 - ay_1^2 = a(x^2 - y^2) &= np - mp = (n - m)p. \\ \text{Since } p \nmid a \quad x_1^2 - y_1^2 &= lp, \quad \text{for some } l \in \mathbb{Z}. \\ (x_1 + y_1)(x_1 - y_1) &= lp \\ x_1 - y_1 = ip \quad \text{or} \quad & x_1 + y_1 = ip, \quad \text{for some } i \in \mathbb{Z}. \\ x_1 \equiv y_1 \mod p \quad \text{or} \quad & x_1 \equiv -y_1 \mod p \end{aligned}$$

If $x_1 \equiv y_1 \mod p$ we are done so suppose that $x_1 \equiv -y_1 \mod p$. We will now show that this is only possible if $x_1 \equiv y_1 \equiv 0 \mod p$. Suppose $y_1 \not\equiv 0 \mod p$ then we still have that $y_1 \in \{1, 2, \ldots, \frac{1}{2}(p-1)\}$. Hence we find that $x_1 = -y_1 \in \{\frac{1}{2}(p+1), \frac{1}{2}(p+1) + 1, \ldots, p-1\}$. But we know that $x_1 \in \{0, 1, 2, \ldots, \frac{1}{2}(p-1)\}$ thus giving a contradiction. Hence $x_1 \equiv y_1 \mod p$ completing the proof. □

Using the properties we just proved Watson used that $g(x_1\sqrt{q}, x_2\sqrt{r}, \ldots, x_n\sqrt{r}) = 1$ has a solution $\mod m$ for any integer m. We will now prove that this is true.

Lemma 23. Let $\phi(x_1, \ldots, x_n) = b_1x_1^2 + \ldots + b_nx_n^2$ with $b_i \in \mathbb{Z}$. Then if $\phi(x_1, \ldots, x_n) \equiv 1 \mod 8$ is soluble in integers x_i and $\phi(x_1, \ldots, x_n) \equiv 1 \mod p$ is soluble for every prime p in integers x_i the $\phi(x_1, \ldots, x_n) \equiv 1 \mod m$ is soluble for every $m \in \mathbb{Z}$ in integers x_i.

Proof. We start by proving that the statement holds for any prime power. We make a distinction between powers of 2 and other prime powers.
For powers of 2 we will show this using induction on the exponent. We already know there is a solution for $\phi(x_1, \ldots, x_n) \equiv 1 \mod 8$. Assume there is a solution for $\phi(x_1, \ldots, x_n) \equiv 1 \mod 2^l$ for $l \geq 3$. Let this solution be $x_i = a_i$ with $a_i \in \mathbb{Z}$ and $\phi(a_1, \ldots, a_n) = a \equiv 1 \mod 2^l$. Without loss of generality we may assume that $\gcd(b_1, 2) = 1$ and $\gcd(a_1, 2) = 1$. Since this has to be true for an i if $\phi(a_1, \ldots, a_n) \equiv 1 \mod 2$ and we can choose to let this $b_ix_i^2$ term be the first.

We know that $x_1 = a_1 + 2^{l-1}k$ with $k \in \mathbb{Z}$ and $x_i = a_i$ for $i \neq 1$ satisfies $\phi(a_1 + 2^{l-1}k, \ldots, a_n) = a + 2^lka_1b_1 + 2^{2l-2}k^2b_1$. Since $l \geq 3$ we know that $2l - 2 > l$ and since $\gcd(2, b_1) = 1$ and $\gcd(2, a_1) = 1$ we can choose k such that $a + 2^lka_1b_1 + 2^{2l-2}k^2b_1 \equiv a + 2^lka_1b_1 \equiv 1 \mod 2^{2l-2}$. Hence $\phi(x_1, \ldots, x_n) \equiv 1 \mod 2^{2l-2}$ is soluble but then it is also soluble for every power of two which is less than 2^{2l-2}. And since $2l - 2 \geq l$ we know $\phi(x_1, \ldots, x_n) \equiv 1 \mod 2^{l+1}$ is soluble. And therefore the induction implies the statement holds for all powers of 2.

In a similar way we will now prove the statement for powers of odd primes using induction. Let p be an odd prime. Since p is an odd prime we already know that there is a solution for the equivalence $\phi(x_1, \ldots, x_n) \equiv 1 \mod p$. Assume there is a solution for $\phi(x_1, \ldots, x_n) \equiv 1 \mod p^l$ for $l \geq 1$. Let this solution be $x_i = a_i$ with $a_i \in \mathbb{Z}$ and $\phi(a_1, \ldots, a_n) = a \equiv 1 \mod p^l$. We may without loss of generality assume that $\gcd(b_1, p) = 1$ and $\gcd(a_1, p) = 1$. Since this has to be true for an i and we can choose to let this $b_ix_i^2$ term be the first.

We then know that $x_1 = a_1 + p^lk$ with $k \in \mathbb{Z}$ and $x_i = a_i$ for $i \neq 1$ satisfies $\phi(a_1 + p^lk, \ldots, a_n) = a + 2p^lka_1b_1 + p^{2l}k^2b_1$. Since $l \geq 1$ we know that $2l > l$ and since $\gcd(p, b_1) = 1$, $\gcd(p, a_1) = 1$, and $\gcd(p, 2) = 1$ we can choose k such that $a + 2p^lka_1b_1 + p^{2l}k^2b_1 \equiv a + 2p^lka_1b_1 \equiv 1 \mod p^{2l}$. Hence $\phi(x_1, \ldots, x_n) \equiv 1 \mod p^{2l}$ is soluble but then it is also soluble for every power of p which is less than p^{2l}. And since $2l > l$ we know $\phi(x_1, \ldots, x_n) \equiv 1 \mod p^{l+1}$ is soluble. And therefore the induction implies the statement holds for all powers of p.

Now we will complete the proof by showing that as long as m_1 and m_2 are coprime and the statement holds for m_1 and for m_2 then it also does for m_1m_2.
Suppose that the solution for m_1 is $x_i = a_i$ with $a_i \in Z$ such that $\phi(a_1, \ldots, a_n) = a \equiv 1 \mod m_1$ and that the solution for m_2 is $x_i = c_i$ with $c_i \in Z$ such that $\phi(c_1, \ldots, c_n) = c \equiv 1 \mod m_2$. Then we look for integers k_i and r_i such that $a_i + k_im_1 = c_i + r_im_2 = d_i$, which always has a solution since m_1 and m_2 are coprime. And since $a_i + k_im_1 = a_i \mod m_1$ and $c_i + r_im_2 = c_i \mod m_2$ we know that $\phi(d_1, \ldots, d_n) = d \equiv 1 \mod m_1$ and $\phi(d_1, \ldots, d_n) = d \equiv 1 \mod m_2$. From this we conclude that since m_1 and m_2 are coprime $\phi(d_1, \ldots, d_n) = d \equiv 1 \mod m_1m_2$, which completes the proof. □

At this point Watson uses Theorem 53 from [Wat60] to find a solution. This proof takes an approach which is using a lot of computing power and is not useful in practice. However, since we know q and r we know that there will be an extension, E', of the form $E' = D[y_1 + z_1\sqrt{q} + w_1\sqrt{r}, \ldots, x_n + z_n\sqrt{q} + w_n\sqrt{r}]$ which solves the Similarity Extension Problem. This is not an explicit extension yet, since we do not know the values for y_i, z_i, and w_i, but since $E' \subset D[\sqrt{q}, \sqrt{r}] = E$ the extension E also solves the Similarity Extension Problem, and this extension is explicit. If we also want to find the change of basis matrix, P, such that $PA = BP$ in this extension then we can use algorithm 3.2 from [Afa21] by Afandi.

6.2 Finding the extension in an example

Here we will give an example of what happens when we try to find a solution of the Similarity Extension Problem by going through the proofs of Guralnick and Watson. We specifically take an example where Afandi's method does not find a solution to show the use of our method.

We know that Afandi's algorithm could not solve the case where $A = \begin{pmatrix} 0 & 1 \\ -5 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix}$ as she showed herself in example 3.5 of her paper [Afa21].

We will now see what extension we find using our method:
We start by looking at matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ that could be a change of basis matrix between A and B. We then find the following:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -5 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 2 \\ -3 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$
$$\begin{pmatrix} -5b & a \\ -5d & c \end{pmatrix} = \begin{pmatrix} 2c-a & 2d-b \\ c-3a & d-3b \end{pmatrix}$$

This simplifies to two restrictions on $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, namely $a = 2d - b$ and $c = d - 3b$. Hence every matrix we will be looking at will be of the form $\begin{pmatrix} 2d-b & b \\ d-3b & d \end{pmatrix}$.
We look at the prime $\mathfrak{p}_1 = (2, 1 + \sqrt{-5})$. We choose the matrix $C_1 = \begin{pmatrix} -1 & 1 \\ -3 & 0 \end{pmatrix}$ which fulfils the two above restrictions for a change of basis matrix. Furthermore we see it has inverse $C_1^{-1} = \begin{pmatrix} 0 & \frac{1}{3} \\ 1 & \frac{1}{3} \end{pmatrix}$. Since $3 \notin \mathfrak{p}_1$ we know that C_1 is a change of basis matrix from A to B in $\mathbb{Z}[\sqrt{-5}]_{\mathfrak{p}_1}$. We see that $\det(C_1) = 3$ hence $(\det(C_1)) \neq \mathbb{Z}[\sqrt{-5}]$.
We repeat the process for the prime $\mathfrak{p}_2 = (3, 1 + \sqrt{-5})$ and choose $C_2 = \begin{pmatrix} 3 & 1 \\ -1 & 2 \end{pmatrix}$ with inverse $C_2^{-1} = \begin{pmatrix} \frac{2}{7} & \frac{-1}{7} \\ \frac{1}{7} & \frac{3}{7} \end{pmatrix}$ which is in $\mathbb{Z}[\sqrt{-5}]_{\mathfrak{p}_2}$. Since $\det(C_2) = 7$ we have that $(\det(C_1), \det(C_2)) = (3, 7) = (1) = \mathbb{Z}[\sqrt{-5}]$.

This would be enough to use Dade's theorem, as it does restrict the number of variables in any way. But to use Watson's algorithm we need a polynomial in at least 3 variables, Hence we need to find another matrix $C_3 \in \mathbb{Z}^{2\times 2}$ such that $C_3 \neq C_1$ and $C_3 \neq C_2$ while still fulfilling the restrictions $a = 2d - b$ and $c = d - 3b$, having $\det(C_3) \neq 0$, and such that the corresponding function $f(x_1, x_2, x_3) = \det x_1C_1 + x_2C_2 + x_3C_3$ is non-singular. We will choose the matrix $C_3 = \begin{pmatrix} 1 & 1 \\ -2 & 1 \end{pmatrix}$. This would be enough using the theorem from Watson but if we find another matrix we will get a smaller extension as a final result. Therefore we will take another matrix $C_4 \neq C_3$ satisfying the same conditions as applied for C_3 above.
We will choose $C_4 = \begin{pmatrix} 2 & 0 \\ 1 & 1 \end{pmatrix}$ and find the following polynomial:

$$\begin{aligned} f(x_1, x_2, x_3, x_4) &= \det(x_1C_1 + x_2C_2 + x_3C_3 + x_4C_4) \\ &= \det\left(\begin{pmatrix} -x_1 & x_1 \\ -3x_1 & 0 \end{pmatrix} + \begin{pmatrix} 3x_2 & x_2 \\ -x_2 & 2x_2 \end{pmatrix} + \begin{pmatrix} x_3 & x_3 \\ -2x_3 & x_3 \end{pmatrix}\right) + \begin{pmatrix} 2x_4 & 0 \\ x_4 & x_4 \end{pmatrix} \\ &= (-x_1 + 3x_2 + x_3 + 2x_4)(2x_2 + x_3 + x_4) - (x_1 + x_2 + x_3)(-3x_1 - x_2 - 2x_3 + x_4) \\ &= 3x_1^2 + 2x_1x_2 + 4x_1x_3 - 2x_1x_4 + 7x_2^2 + 8x_2x_3 + 5x_2x_4 + 3x_3^2 + 3x_3x_4 + 2x_4^2. \end{aligned}$$

Note that $f(x_1, x_2, x_3, x_4)$ is indeed non-singular since the determinant of the matrix with as ij'th entry the coefficient in front of the x_ix_j term, M, is not zero:

$$\det(M) = \det\left(\begin{pmatrix} 3 & 2 & 4 & -2 \\ 2 & 7 & 8 & 5 \\ 4 & 8 & 3 & 3 \\ -2 & 5 & 3 & 2 \end{pmatrix}\right) \neq 0.$$

Hence our choices of C_3 and C_4 are good.
We are now going to transform f into a function of the form $g(x_1, x_2, x_3, x_4) = a_{11}x_1^2 + a_{22}x_2^2 + a_{33}x_3^2 + a_{44}x_4^2$ with $a_{11}, a_{22}, a_{33}, a_{44} \in \mathbb{Z}$ such that $\gcd(a_{11}, 2a_{22}) = 1$ and $\gcd(a_{11}, a_{33}) = 1$. First we need to make sure that the coefficient in front of x_1^2 is coprime to $2\det(A(f)) = -40 = 2^3 \cdot 5$ where $A(f)$ is the coefficients matrix of

f from definition 17. We see that this is already the case for this f. Now we are going to get rid of the x_1x_3, and x_1x_4 terms of this equation by multiplying with a transformation matrix as described earlier this chapter.

$$f_1(x_1,x_2,x_3,x_4) = f\left(\begin{pmatrix}1&0&0&0\\0&1&-2&2\\0&0&2&0\\0&0&0&2\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}\right) = 3x_1^2+2x_1x_2+7x_2^2-40x_2x_3+38x_2x_4+60x_3^2-112x_3x_4+56x_4^2.$$

Now let us remove the x_1x_2 term:

$$f_2(x_1,x_2,x_3,x_4) = f_1\left(\begin{pmatrix}1&-2&0&0\\0&6&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}\right) = 3x_1^2+30x_2^2-240x_2x_3+228x_2x_4+60x_3^2-112x_3x_4+56x_4^2.$$

Since we ensured that the the coefficient in front of x_1^2 is coprime with $2\det(A(f))$ we now know that it is coprime to the coefficient in front of the x_4^2 term, indeed $\gcd(3,56)=1$. Therefore we can now switch the names of x_2 and x_4 to make the coefficient in front of x_2^2 to be coprime to the coefficient in front of x_1^2. We then get:

$$f_3(x_1,x_2,x_3) = f_2(x_1,x_4,x_3,x_2) = 3x_1^2+56x_2^2-112x_2x_3+228x_2x_4+60x_3^2-240x_3x_4+30x_4^2.$$

We now remove the x_2x_4 term:

$$f_4(x_1,x_2,x_3,x_4) = f_3\left(\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&-228\\0&0&0&-112\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}\right) = 3x_1^2+56x_2^2-112x_2x_3+60x_3^2-480x_3x_4-2633280x_4^2.$$

Then we will remove the x_2x_3 term.

$$f_5(x_1,x_2,x_3,x_4) = f_4\left(\begin{pmatrix}1&0&0&0\\0&1&112&0\\0&0&112&0\\0&0&0&1\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}\right) = 3x_1^2+56x_2^2+50176x_3^2-480x_3x_4-2633280x_4^2.$$

Note that $\gcd(50176,3)=1$ as desired so we continue by removing the x_3x_4 term to find the desired g.

$$\begin{aligned} g(x_1,x_2,x_3,x_4) &= f_5\left(\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&480\\0&0&0&100352\end{pmatrix}\begin{pmatrix}x_1\\x_2\\x_3\\x_4\end{pmatrix}\right)\\ &= 3x_1^2+56x_2^2+50176x_3^2-26518520746475520x_4^2. \end{aligned}$$

Since we are working with a polynomial in 4 variables we can now show that $g(x_1\sqrt{q},x_2,x_3,x_4)=1$, as we do not need the additional parameter r for $n\geq 4$. We know that there is a solution for $f(x_1,x_2,x_3,x_4)=1$ where x_1, x_2, x_3 and x_4 are of the form $y_i+z_i\sqrt{q}$ with $y_i,z_i\in\mathbb{Z}$. To find this solution we will first determine q. As discussed in the proof of our method, we need that $q\equiv 3 \mod 8$, $q\equiv 3 \mod 56\cdot 50176$, and if all coefficients of g are of the same sign we need $q<0$ however this is not the case. A solution for q with these restrictions is $q=3$.
Hence we conclude that A and B are $\mathbb{Z}[\sqrt{-5},\sqrt{3}]$-similar.

Conclusion and open problems

In this thesis our goal was to find an extension that solves the Similarity Extension Theorem. To achieve this we investigated similar matrices and in particular the Similarity Extension Problem. We started by looking at the LM-correspondence as a background to current progress in solving the problem. We then looked at the proof of the Similarity Extension Theorem and using this we developed our own method of finding solutions to the Similarity Extension Problem. In this method we use a theorem which narrowed the input of our method down to 2×2 matrices, but we hope future research will be able to overcome this hurdle and generalise the method.

Therefore we partially succeeded in our goal of finding an extension that solves the Similarity Extension Problem. As we gave a method that can solve the problem in a specific situation. Since the problem is not solved yet we would like to point out some questions that arose during the process of writing this thesis. While we went over our method for solving the Similarity Extension Problem we already mentioned that there are several problems left which could extend the method or make it more reliable. We will list them here:

- Is it always possible to choose three different matrices C_1, C_2, C_3 as desired to use Watson's theorem?
- Does having three different matrices guarantee that f becomes non-singular?
- Why does setting the coefficient in front of the x_1^2 term of our function co-prime to $2\det(A(f))$ guarantee that the term in front of x_n^2 will be co-prime to it after the transformation?
- Can we generalise the method to more function with a bigger variety of matrices as inputs? For example 3×3 matrices.
- Is it possible to use the start of Dade's proof to find another method of solving the Similarity Extension Problem?

References

[Afa21] Rebecca Afandi. Conjugacy of Integral Matrices over Algebraic Extensions. *arXiv e-prints*, page arXiv:2109.02130, September 2021.

[AM16] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Series in Mathematics. Westview Press, Boulder, CO, economy edition, 2016. For the 1969 original see [MR0242802].

[AO83] H. Appelgate and H. Onishi. Similarity problem over SL(n, $\mathbf{Z}_p$). *Proc. Amer. Math. Soc.*, 87(2):233–238, 1983.

[Dad63] E. C. Dade. Algebraic integral representations by arbitrary forms. *Mathematika*, 10:96–100, 1963.

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

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

[K.] Conrad K. Ideal classes and matrix conjugation over z. note a link to the online notes.

[LM33] Claiborne G. Latimer and C. C. MacDuffee. A correspondence between classes of ideals and classes of matrices. *Ann. of Math. (2)*, 34(2):313–316, 1933.

[Mar20] Stefano Marseglia. Computing the ideal class monoid of an order. *J. Lond. Math. Soc. (2)*, 101(3):984–1007, 2020.

[RZ61] I. Reiner and H. Zassenhaus. Equivalence of representations under extensions of local ground rings. *Illinois J. Math.*, 5:409–411, 1961.

[Wat60] G. L. Watson. *Integral quadratic forms*. Cambridge Tracts in Mathematics and Mathematical Physics, No. 51. Cambridge University Press, New York, 1960.

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