Master's thesis

NTNU
Norwegian University of Science and Technology

Therese Strand

Representativity Results in Motivic Degree Theory

Master's thesis in MSMNFMA
Supervisor: Gereon Quick and Glen Matthew Wilson
June 2020

NTNU
Kunnskap for en bedre verden

Therese Strand

Representativity Results in Motivic Degree Theory

Master's thesis in MSMNFMA
Supervisor: Gereon Quick and Glen Matthew Wilson
June 2020

Norwegian University of Science and Technology

NTNU
Norwegian University of
Science and Technology

Abstract

This thesis studies a method described by Kass and Wickelgren [4] that takes a polynomial with an isolated zero at the origin and produces an element of the Grothendieck-Witt ring. We first study some theory about bilinear forms and polynomial rings that will be necessary to be able to use the method. We then prove various results about the method, such as the fact that all bilinear forms of dimension ≥ 2 that are produced by the method always has a hyperbolic plane $\mathbb{H}$ as an orthogonal summand. We finish by proving which elements in $\mathrm{GW}(k)$ we can realise with the method when k is a finite field.

Sammendrag

Denne masteroppgaven studerer en metode beskrevet av Kass og Wickelgren [4] som tar et polynom med et isolert nullpunkt i origo og produserer et element i Grothendieck-Witt-ringen. Vi studerer først litt teori om bilineære former og polynomringer som vil bli nødvendig for å kunne bruke metoden. Vi beviser så diverse resultater om metoden, som at alle bilineære former av dimensjon ≥ 2 som produseres av metoden alltid har et hyperbolsk plan $\mathbb{H}$ som en ortogonal summand. Vi avslutter med å bevise hvilke elementer i $\mathrm{GW}(k)$ vi kan oppnå med metoden når k er en endelig kropp.

Acknowledgements

First and foremost, I would like to thank my supervisors, Professor Gereon Quick and Doctor Glen Wilson, for their guidance and support throughout the writing of this thesis. In particular, thanks to Glen Wilson for suggesting the topic of this thesis, for many useful discussions, and for providing detailed feedback on my writing.

I wish to thank Eiolf Kaspersen for proofreading this thesis. I also want to thank my fellow students at Linjeforeningen Delta for providing me with a social and academic community during my time as a student. Finally, I want to thank my family for the support.

Table of Contents

Chapter 1

Introduction

In [4], Jesse Leo Kass and Kristen Wickelgren describe various results in $\mathbb{A}^1$-homotopy theory. In particular, they consider the degree map

$$\deg^{\mathbb{A}^1} : [\mathbb{P}^n_k/\mathbb{P}^{n-1}_k, \mathbb{P}^n_k/\mathbb{P}^{n-1}_k] \to \mathrm{GW}(k)$$

and their main result is that when $f\colon \mathbb{A}^n_k \to \mathbb{A}^n_k$ has an isolated zero at the origin, then $\deg^{\mathbb{A}^1}_0(f)$ is the stable isomorphism class of a non-degenerate, symmetric bilinear form denoted by $w_0(f)$, and they provide a method for computing $w_0(f)$. The paper is primarily concerned with proving this main result and other related results. As a result Kass and Wickelgren end up computing only a few examples using the algorithm they described.

In this thesis we are interested in studying the algorithm itself and to explore some of its properties. Looking at the computations that Kass and Wickelgren did, it is notable that the hyperbolic plane $\mathbb{H}$ shows up in all the examples there. So one question to explore is whether this is a general phenomenon and that the method will always produce a hyperbolic plane, provided dimension is at least 2. Another thing that motivates our investigations is the question of which bilinear forms it is even possible to have as output of the algorithm and if there are some that can not be realised.

Before getting to any of these questions, though, there is quite a bit of theory we need to establish first. In order to use the algorithm, we need to be familiar with computations with bilinear spaces and computations with polynomial rings. So we will begin by exploring those topics.

In Chapter 2, we examine the theory of bilinear forms. One aim of this chapter is to develop the techniques to do computations with bilinear forms and spaces, in particular we will make heavy use of this theory's close relationship with matrices. Another goal is to construct the Grothendieck-Witt ring $\mathrm{GW}(k)$, which is where the elements that the algorithm produces are contained and so

it is essential to develop an understanding of this ring.

In Chapter 3, we study the polynomial ring $k[x_1, \ldots, x_n]$, and particularly the quotient ring $k[x_1, \ldots, x_n]/I$ where I is an ideal of $k[x_1, \ldots, x_n]$. A big goal in this chapter is to familiarise ourselves with computations that use Gröbner bases of ideals in $k[x_1, \ldots, x_n]$, and this involves us examining a few algorithms. Once that is in order we also look at how to find k-bases of the quotient ring and how to compute localisations.

And finally, in Chapter 4 we state the method and explore various properties of it. We name a few cases where the form at the end of the method can be more or less deduced just from the polynomials with which we start. We explore the question of which forms are realisable, and in that process we prove that any form over an algebraically closed field is realisable. We also prove, for any field, that any form produced by the algorithm of dimension at least 2 must have $\mathbb{H}$ as an orthogonal summand. Then we thoroughly explore the case of finite fields, and identify which isometry classes we can realise. We finish off with a small discussion of questions about this topic that can be studied in the future.

Chapter 2

Bilinear Forms

We start off with developing some of the theory of bilinear forms. We aim to develop techniques for doing computations with bilinear spaces. Also, the algorithm we are studying produces an element in the Grothendieck-Witt ring of a field k, $\mathrm{GW}(k)$, so we are also aiming to construct $\mathrm{GW}(k)$ and understand its structure.

Let k be a field with $\mathrm{char}(k) \neq 2$. We consider here vector spaces over k.

Definition 2.1. A *bilinear form* on a vector space V over k is a bilinear map $\beta\colon V \times V \to k$, so $\forall x, x', y, y' \in V$, $\forall a \in k$ we have

$$\begin{aligned} \beta(x + x', y) &= \beta(x, y) + \beta(x', y) \\ \beta(x, y + y') &= \beta(x, y) + \beta(x, y') \\ \beta(ax, y) &= a\beta(x, y) = \beta(x, ay). \end{aligned}$$

β is *symmetric* if $\beta(x, y) = \beta(y, x)\ \forall x, y \in V$.

We refer to the pair (V, β) as a *(symmetric) bilinear space* (over k).

The *transpose* of β is the bilinear form $\beta^T\colon V \times V \to k$, $\beta^T(x, y) = \beta(y, x)$.

We will primarily work with bilinear spaces that are symmetric, so if nothing else is specified then a given bilinear space can be assumed to be symmetric. We can see directly from the definitions that a bilinear space (V, β) is symmetric if and only if $\beta = \beta^T$.

Definition 2.2. A *quadratic form* on V is a map $q\colon V \to k$ such that $q(ax) = a^2 q(x)$ for all $x \in V$, $a \in k$ and such that $\forall x, y \in V$ the map

$$(x, y) \mapsto q(x + y) - q(x) - q(y)$$

is bilinear. We call (V, q) a *quadratic space*.

Using the bilinear map in this definition, we can associate to q a symmetric bilinear form given by

$$\beta_q(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y)).$$

And if β is a bilinear form on V, we can associate to it a quadratic form defined by

$$q_\beta(x) = \beta(x,x).$$

We then get $q_{\beta_q} = q$ and $\beta_{q_\beta} = \frac{1}{2}(\beta + \beta^T)$, and hence $\beta_{q_\beta} = \beta$ precisely when β is symmetric. So we get a one-to-one correspondence:

$$\begin{gathered}\{\text{symmetric bilinear spaces}\} \longleftrightarrow \{\text{quadratic spaces}\} \\ (V,\beta) \longmapsto (V, q_\beta) \\ (V,\beta_q) \longleftarrow\!\shortmid (V,q)\end{gathered}$$

And so the theory of symmetric bilinear forms on V and the theory of quadratic forms on V are equivalent. Note that this is only true when $\text{char}(k) \neq 2$.

Definition 2.3. Let (V,β) and (V',β') be bilinear spaces over k. We say that (V,β) and (V',β') are *isometric*, denoted $(V,\beta) \cong (V',\beta')$, if there is a bijective linear transformation $\sigma\colon V \to V'$ such that $\beta'(\sigma x, \sigma y) = \beta(x,y)$, $\forall x, y \in V$. Then σ is called an *isometry*.

Isometry of bilinear spaces can easily be shown to be an equivalence relation, and later on we will primarily be working with isometry classes of bilinear spaces instead of just the spaces themselves. Because of this we will want several properties for bilinear spaces to hold not just for the bilinear space, but also for its entire isometry class.

2.1 Bilinear spaces and matrices

As we will see, there is a close relationship between symmetric bilinear spaces and symmetric matrices, and we will use this relationship a lot when doing our computations. We will first observe that when we start with a bilinear space, we can produce a matrix associated to it.

Definition 2.4. Let (V,β) be a bilinear space and $\{b_1,\dots,b_n\}$ a basis of V. The *matrix of* β with respect to the basis $\{b_1,\dots,b_n\}$ is $B = (b_{ij}) = (\beta(b_i,b_j))$.

This definition necessitates that B is a square matrix, so we will assume that any matrices from here on are square. The definition also applies regardless of whether (V,β) is symmetric or not, but we are focusing on the symmetric case below. Note, however, that from the definition it follows that the matrix of

β^T with respect to the same basis will be B^T, and from there we see that β is symmetric exactly when B is symmetric.

Now we can use the matrix B with respect to $\{b_1, \ldots, b_n\}$ in order to evaluate β. Let $x, y \in V$ and write $x = \sum_{i=1}^n x_i b_i$, $y = \sum_{i=1}^n y_i b_i$ where $x_i, y_i \in k$. We identify x and y as column vectors by writing $x = [x_1, \ldots, x_n]^T$ and $y = [y_1, \ldots, y_n]^T$. Then:

$$\beta(x,y) = \begin{bmatrix} x_1 & \ldots & x_n \end{bmatrix} \begin{bmatrix} \beta(b_1,b_1) & \ldots & \beta(b_1,b_n) \\ \vdots & \ddots & \vdots \\ \beta(b_n,b_1) & \ldots & \beta(b_n,b_n) \end{bmatrix} \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = x^T B y.$$

Note that the matrix B depends on the choice of basis for V. But if $\{b'_1, \ldots, b'_n\}$ is another basis of V and $S = (s_{ij})$ is the change of basis matrix from $\{b_1, \ldots, b_n\}$ to $\{b'_1, \ldots, b'_n\}$, then we can compute the matrix of β with respect to the new basis as $B' = S^T B S$. Since S is invertible, the expression $B' = S^T B S$ tells us that B and B' are *congruent* matrices and we denote this by $B \cong B'$. Hence the matrix of a bilinear space is unique up to congruence.

We started with a symmetric bilinear space and produced a symmetric matrix. We can, in fact, go the other way and start with a symmetric matrix:

Let B be a symmetric $n \times n$-matrix over k. Consider the vector space k^n of column vectors over k, with the canonical basis

$$e_1 = \Big[1, 0, \ldots, 0\Big]^T, e_2 = \Big[0, 1, 0 \ldots, 0\Big]^T, \ldots, e_n = \Big[0, \ldots, 0, 1\Big]^T.$$

We define a symmetric bilinear form on k^n by

$$\beta_B \colon k^n \times k^n \to k,\ \beta_B(x,y) = x^T B y$$

and so we have produced a symmetric bilinear space $\langle B \rangle := (k^n, \beta_B)$. Also, if (V, β) is a symmetric bilinear space such that the matrix of β with respect to some basis $\{b_1, \ldots, b_n\}$ is exactly B, then $(V, \beta) \cong \langle B \rangle$ via $b_i \mapsto e_i$ for all i.

Now, both isometry of bilinear spaces and congruence of matrices can be shown to be equivalence relations. So the next thing we could hope for is that there is a relationship between isometry classes of symmetric bilinear spaces and congruence classes of symmetric matrices. As it turns out, that is the case:

Theorem 2.5. *Two symmetric bilinear spaces are isometric if and only if their associated symmetric matrices, with respect to some bases, are congruent.*

Proof. Let (V, β) and (V', β') be symmetric bilinear spaces with bases $\{b_1, \ldots, b_n\}$ and $\{b'_1, \ldots, b'_n\}$ respectively, and let B and B' be the matrices of β and β' that correspond to these bases.

If $\sigma\colon V \to V'$ is an isometry, then we can represent it with an $n \times n$-matrix $S = (s_{ij})$, meaning that for all j we have $\sigma(b_j) = \sum_{i=1}^{n} s_{ij} b'_i$. Then we have

$$x^T B y = \beta(x, y) = \beta'(\sigma x, \sigma y) = x^T S^T B' S y$$

for all $x, y \in V$. So $B = S^T B' S$ and hence $B \cong B'$.

Conversely, if B and B' are congruent, and so there is an invertible $n \times n$-matrix $S = (s_{ij})$ such that $B = S^T B' S$, then we define a bijective linear transformation $\sigma\colon V \to V'$ by $\sigma(b_j) = \sum_{i=1}^{n} s_{ij} b'_i$ and then we have

$$\beta(x, y) = x^T B y = x^T S^T B' S y = \beta'(\sigma x, \sigma y)$$

hence σ is an isometry. □

In the theorem we assumed that both bilinear spaces are symmetric. But in cases where we just know that one given bilinear space is symmetric, we have the following:

Lemma 2.6. *Let (V, β) and (V', β') be bilinear spaces, let (V, β) be symmetric. If $(V, \beta) \cong (V', \beta)$ then (V', β') is also symmetric.*

Proof. Let B and B' be the matrices of (V, β) and (V', β') respectively, with respect to some basis. B is clearly symmetric. Since $(V, \beta) \cong (V', \beta')$, we have that $B \cong B'$ so there is an invertible matrix S such that $B' = S^T B S$. Then

$$(B')^T = (S^T B S)^T = S^T B^T (S^T)^T = S^T B S = B'$$

so B' is symmetric. □

So if (V, β) is symmetric, we know that every bilinear space in the isometry class $[(V, \beta)]$ is symmetric. And so it makes sense for us for to consider symmetry at the level of isometry, not just with the bilinear spaces themselves.

To sum it up, we have the following one-to-one correspondence:

$$\left\{ \begin{array}{c} \text{isometry classes of} \\ \text{symmetric bilinear spaces} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{congruence classes of} \\ \text{symmetric matrices} \end{array} \right\}$$
$$[(V, \beta)] \longmapsto [B] = [(\beta(b_i, b_j))]$$
$$[\langle B \rangle] = [(k^n, \beta_B)] \longmapsto [B]$$

where $\{b_1, \ldots, b_n\}$ is a basis of V. So whenever we are studying a symmetric bilinear space up to isometry, we can do that by studying symmetric matrices up to congruence instead. When we do computations later on, we will precisely be working with isometry classes of symmetric bilinear spaces, and we will use this correspondence a lot.

2.2 Properties of the correspondence

We will now see what tools we have that make the correspondence from the previous section so useful.

If B is our symmetric matrix and we are working with its congruence class, we can freely change the matrix as long as the congruence class remains unchanged. Meaning, for any invertible matrix S we can also work with S^TBS. In practice, we will be doing this using elementary matrices.

Recall from linear algebra that the elementary matrices generate the general linear group, in particular they are invertible. Recall also that multiplying B with an elementary matrix corresponds to doing an elementary row or column operation on B.

So now, if E is an elementary matrix, then we are allowed to work with E^TBE instead of B, and the operation performed on B is both the column operation and the corresponding row operation determined by E. So whenever we want to do a certain operation on a matrix, say a row operation, then we also have to do the corresponding column operation in order to stay in the same congruence class.

We also have the following result [6], which will be very useful during our later computations:

Theorem 2.7. *Every symmetric matrix is congruent to a diagonal matrix.*

This allows us to introduce another notation: For $a_1, \dots, a_n \in k$, we define the bilinear space $\langle a_1, \dots, a_n \rangle$ as

$$\langle a_1, \dots, a_n \rangle := \langle A \rangle, \text{ where } A = \begin{bmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{bmatrix}$$

So then the theorem tells us, equivalently, that every symmetric bilinear space is isometric to a bilinear space $\langle a_1, \dots, a_n \rangle$.

Since we can change $\langle a_1, \dots, a_n \rangle$ using simultaneous row and column operations, it is not difficult to see that we have the following:

Corollary 2.8. *Let $\langle a_1, \dots, a_n \rangle$ be a bilinear space.*

(i) For any permutation $\pi \colon \{1, \dots, n\} \to \{1, \dots, n\}$, we have

$$\langle a_1, \dots, a_n \rangle \cong \langle a_{\pi(1)}, \dots, a_{\pi(n)} \rangle$$

(ii) For any $b_1, \dots, b_n \in k \backslash \{0\}$, we have

$$\langle a_1, \dots, a_n \rangle \cong \langle b_1^2 a_1, \dots, b_n^2 a_n \rangle$$

Like matrices, the theory of bilinear spaces also has the following notion:

Definition 2.9. A symmetric bilinear space (V, β) is *regular*, *non-degenerate*, or *non-singular* if $\forall x \in V,\ x \neq 0, \exists y \in V$ such that $\beta(x, y) \neq 0$.

If (V, β) is not regular, then it is called *degenerate* or *singular*.

Then using the correspondence with matrices we get that (V, β) is regular precisely when the matrix of β, with respect to any basis, is non-singular [6]. In the theory of matrices, invertibility and the determinant are closely related, and the determinant is also useful here. However, in the theory of bilinear forms we need to be a bit more careful when introducing the determinant.

If B is the matrix of (V, β) with respect to some basis, then we want to associate the determinant $\det(B)$ to (V, β) in some way. But doing this directly is not well-defined since B depends on the choice of basis of V, so we have to account for this. If B' is the matrix of β with respect to a different basis, then we know that $B \cong B'$. So $B = S^T B' S$ for some invertible matrix S. Then we get:

$$\det(B) = \det(S^T B' S) = \det(S^T) \det(B') \det(S) = \det(S)^2 \det(B').$$

So we get that $\det(B)$ is unique up to multiplication with squares, in other words as an element of $k^\times/(k^\times)^2$.

Definition 2.10. Let (V, β) be a symmetric bilinear space and let B be the matrix of β with respect to some basis. The *discriminant* of (V, β) is defined to be $\det(B) \in k^\times/(k^\times)^2$.

The above discussion shows that the discriminant of a symmetric bilinear space is well-defined. Furthermore, since the equation $\det(B) = a^2 \det(B')$ holds for any $a \in k^\times$ and for any congruent matrices B and B', we hence have that the discriminant is invariant under isometry. In particular, if two symmetric bilinear spaces have different discriminants then they cannot be isometric.

Using the bracket notation introduced in the previous section, it is easy to see that for $a_1, \ldots, a_n \in k$,

$$\det(\langle a_1, \ldots, a_n \rangle) = \prod_{i=1}^{n} a_i.$$

Lemma 2.11. *Let (V, β) and (V', β') be symmetric bilinear spaces, let (V, β) be regular. If $(V, \beta) \cong (V', \beta')$, then (V', β') is also regular.*

Proof. Let A and B be the matrices of (V, β) and (V', β') respectively, with respect to some bases. We have $\det(A) \neq 0$ since (V, β) is regular. And since $(V, \beta) \cong (V', \beta')$, there is an invertible matrix S, meaning $\det(S) \neq 0$, so that $B = S^T A S$. Then we have

$$\det(B) = \det(S^T) \det(A) \det(S) \neq 0.$$

So B is invertible and (V', β') is regular. $\square$

So like with symmetry, regularity is a property of bilinear spaces that we can consider at the level of isometry instead of just with the spaces.

Another value we can associate to a bilinear space (V, β) is dimension. And unlike the determinant, the dimension of (V, β) is straightforwardly defined as the dimension of the underlying vector space V, so $\dim_k(V, \beta) = \dim_k(V)$. We can also find the dimension of (V, β) by finding the rank of a matrix of (V, β).

The dimension of a bilinear space is unique up to isometry and congruence. For if $B \cong B'$ with $B' = C^T BC$ where C is invertible then, since multiplication by an invertible matrix does not change rank, we get

$$\dim(B') = \dim(C^T BC) = \dim(B).$$

2.3 Sums and products

In the previous section we saw things we can do to a symmetric bilinear space without changing its isometry class. We also have ways of combining different bilinear spaces, such as the following:

Definition 2.12. Let (V, β) and (V', β') be symmetric bilinear spaces over the same field k. The *(external) orthogonal sum* of (V, β) and (V', β') is the symmetric bilinear space $(V \oplus V', \beta \perp \beta')$ where the bilinear form is given by

$$\beta \perp \beta' \colon (V \oplus V') \times (V \oplus V') \to k$$
$$(\beta \perp \beta')((x, x'), (y, y')) = \beta(x, y) + \beta'(x', y')$$

The orthogonal sum of more than two spaces is defined similarly, and then the operation is associative. We have the following properties [6], presented without proof:

Lemma 2.13. *Let $(V, \beta), (V', \beta'), (V_1, \beta_1)$, and (V_1', β_1') be symmetric bilinear spaces.*

(i) $(V, \beta) \perp (V', \beta') \cong (V', \beta') \perp (V, \beta)$

(ii) *If* $(V, \beta) \cong (V_1, \beta_1)$ *and* $(V', \beta') \cong (V_1', \beta_1')$*, then we have* $(V, \beta) \perp (V', \beta') \cong (V_1, \beta_1) \perp (V_1', \beta_1')$

(iii) $(V, \beta) \perp (V', \beta')$ *is regular* $\iff$ (V, β) *and* (V', β') *are regular*

(iv) *If B and B' are matrices that represent β and β' respectively, then the matrix* $\begin{bmatrix} B & 0 \\ 0 & B' \end{bmatrix}$ *represents the bilinear form $\beta \perp \beta'$.*

By properties of the determinant, we get in (iv) that

$$\det \begin{bmatrix} B & 0 \\ 0 & B' \end{bmatrix} = \det(B) \det(B')$$

so it immediately follows that $\det((V, \beta) \perp (V', \beta')) = \det(V, \beta) \det(V', \beta')$.

Also notice in (iv), that if the matrices of β and β' are diagonal, then clearly the matrix of $\beta \perp \beta'$ will also be diagonal. Combining this with notation introduced earlier, then given $a_1, \ldots, a_n, b_1, \ldots, b_m, a \in k$, we write

$$\langle a_1, \ldots, a_n \rangle \perp \langle b_1, \ldots, b_m \rangle = \langle a_1, \ldots, a_n, b_1, \ldots, b_m \rangle$$
$$\overbrace{\langle a, \ldots, a \rangle}^{n \text{ times}} = \overbrace{\langle a \rangle \perp \ldots \perp \langle a \rangle}^{n \text{ times}} = n\langle a \rangle$$

Since any symmetric bilinear space is isometric to some $\langle a_1, \ldots, a_n \rangle$, then when we are working with isometry classes we can always express orthogonal sums using this notation.

Using the first three properties in Lemma 2.13, we can also say something more. Let $\mathrm{S}(k)$ denote denote the set of isometry classes of regular symmetric bilinear spaces over k. Then we have the following:

Theorem 2.14. $(\mathrm{S}(k), \perp)$ *is a commutative monoid.*

Proof. Lemma 2.13 (iii) ensures that $\perp \colon \mathrm{S}(k) \times \mathrm{S}(k) \to \mathrm{S}(k)$ really does map to $\mathrm{S}(k)$. Lemma 2.13 (ii) ensures that $\perp$ is independent of the choice of representative for the isometry classes. By construction, the orthogonal sum is associative. The identity is the zero bilinear space $(\{0\}, (0,0) \mapsto 0)$. And finally, $\perp$ is commutative by Lemma 2.13 (i). □

So the orthogonal sum is one example of an operation on bilinear spaces, and it even gives us structure when we focus on the isometry classes. We also have a product operation on bilinear spaces, which we will examine next.

Definition 2.15. Let (V, β) and (V', β') be bilinear spaces. The *tensor product* of (V, β) and (V', β') is the bilinear space

$$(V, \beta) \otimes (V', \beta') \coloneqq (V \otimes_k V', \beta \otimes \beta')$$

where the bilinear form is given by

$$\begin{aligned} \beta \otimes \beta' \colon (V \otimes_k V') \times (V \otimes_k V') &\to k \\ (x \otimes x', y \otimes y') &\mapsto \beta(x, y)\beta'(x', y') \end{aligned}$$

This definition does not require us to choose bases for V and V', and we will make use of this version of the tensor product for a proof below. But when we use bases, we have another way of defining tensor product, and it requires a small detour into matrices again.

Definition 2.16. Let $A = (a_{ij})$ be an $n \times n$ matrix and let $B = (b_{ij})$ be a $m \times m$ matrix. The *tensor product*, or *Kronecker product*, of A and B is the $mn \times mn$ matrix

$$A \otimes B = \begin{bmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \dots & a_{nn}B \end{bmatrix}$$

This definition uses square matrices, but in general the same definition works for matrices that are not square. In that case the Kronecker product of an $m \times n$ matrix and a $p \times q$ matrix will produce an $mp \times nq$ matrix.

We have some properties [6, 3], where we omit the proof:

Lemma 2.17. *Let A, A', B, B', and C be matrices over k. A and A' are $n \times n$ matrices, and B and B' are $m \times m$ matrices.*

(i) $(AA') \otimes (BB') = (A \otimes B)(A' \otimes B')$

(ii) $(A \otimes B)^T = A^T \otimes B^T$

(iii) *If A and B are symmetric, then so is $A \otimes B$*

(iv) $(A \otimes B) \otimes C = A \otimes (B \otimes C)$

(v) $\det(A \otimes B) = \det(A)^m \det(B)^n$

From (v) it immediately follows that if A and B are non-singular, then $A \otimes B$ is also non-singular.

Using the Kronecker product, we can now define a product on $\mathrm{S}(k)$

Definition 2.18. Let A and B be non-singular symmetric matrices over k. The *tensor product* of the symmetric bilinear spaces $\langle A \rangle$ and $\langle B \rangle$ is defined as

$$\langle A \rangle \otimes \langle B \rangle \coloneqq \langle A \otimes B \rangle.$$

For any isometry classes of some symmetric bilinear spaces $[(V, \beta)]$ and $[(V', \beta')]$, let A and B be matrices so that $(V, \beta) \cong \langle A \rangle$ and $(V', \beta') \cong \langle B \rangle$. Then the tensor product of $[(V, \beta)]$ and $[(V', \beta)]$ is defined as

$$[(V, \beta)] \otimes [(V', \beta')] \coloneqq [\langle A \otimes B \rangle].$$

This definition holds only for isometry classes of bilinear spaces, and not for just the bilinear spaces themselves. So Definition 2.15 is more general than this one, but we will primarily be working with isometry classes anyways, so this definition is mostly good enough for our purposes.

It can be also shown [6] that if A and B are the matrices of β and β' with respect to some bases, then the matrix of $\beta \otimes \beta'$ is precisely $A \otimes B$. In other words, when we choose a basis for the vector spaces, then we can use either of the definitions to get the tensor product and we will get the same one no matter which definition we use.

We can also see from Definition 2.18 that when we use the bracket notation for bilinear spaces corresponding to diagonal matrices, the tensor product becomes

$$\begin{aligned}\langle a_1, \ldots, a_n \rangle \otimes \langle b_1, \ldots, b_m \rangle &= \langle a_1 b_1, \ldots, a_1 b_m, \ldots, a_n b_1, \ldots, a_n b_m \rangle \\ &= \perp_{i,j} \langle a_i b_j \rangle\end{aligned}$$

Proposition 2.19. *Tensor product is a well-defined binary operation on* $\mathrm{S}(k)$.

Proof. Let $[(V, \beta)], [(V', \beta')] \in \mathrm{S}(k)$ be isometry classes of some regular symmetric bilinear spaces. Let A, A', B and B' be non-singular symmetric matrices over k so that $(V, \beta) \cong \langle A \rangle \cong \langle A' \rangle$ and $(V', \beta') \cong \langle B \rangle \cong \langle B' \rangle$.

Since $A \cong A'$ and $B \cong B'$, there are invertible matrices C and D such that $A' = C^T A C$ and $B' = D^T B D$. Then using Lemma 2.17 (i) and (ii), we have

$$\begin{aligned}A' \otimes B' &= (C^T A C) \otimes (D^T B D) \\ &= (C^T \otimes D^T)(A \otimes B)(C \otimes D) \\ &= (C \otimes D)^T (A \otimes B)(C \otimes D)\end{aligned}$$

and since it follows from Lemma 2.17 (v) that $C \otimes D$ is invertible, we get that $A \otimes B \cong A' \otimes B'$. Hence $[(V, \beta)] \otimes [(V', \beta')] = [\langle A \otimes B \rangle]$ is independent of the choices of A and B. Finally, since A and B are non-singular and symmetric, so is $A \otimes B$ by Lemma 2.17 (iii) and (v). And so by Lemma 2.6 and Lemma 2.11, $[(V, \beta)] \otimes [(V', \beta')]$ is regular and symmetric. □

Theorem 2.20. $(\mathrm{S}(k), \perp, \otimes)$ *is a commutative semiring.*

Proof. We have already seen in Theorem 2.14 that $(\mathrm{S}(k), \perp)$ is a commutative monoid. Also, the tensor product is associative by Lemma 2.17 (iv) and it has $\langle 1 \rangle$ as identity, so $(\mathrm{S}(k), \otimes)$ is a monoid.

To see that $(\mathrm{S}(k), \otimes)$ is commutative, let A be a symmetric $n \times n$ matrix and let B be a symmetric $m \times m$ matrix. Let e_{ij} denote the $m \times n$ matrix which

has 1 in the (i,j) position and 0 elsewhere. Then using the $mn \times mn$ matrix

$$C = \begin{bmatrix} e_{11} & e_{21} & \dots & e_{m1} \\ e_{12} & e_{22} & \dots & e_{m2} \\ \vdots & \vdots & \ddots & \vdots \\ e_{1n} & e_{2n} & \dots & e_{mn} \end{bmatrix}$$

we get that $A \otimes B = C^T(B \otimes A)C$, and so $[\langle A \rangle] \otimes [\langle B \rangle] = [\langle B \rangle] \otimes [\langle A \rangle]$ in $\mathrm{S}(k)$. Hence $(\mathrm{S}(k), \otimes)$ is a commutative monoid.

Let A, B and C be some matrices. Observe that we have

$$\begin{aligned} (A \perp B) \otimes C &= \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix} \otimes C \\ &= \begin{bmatrix} a_{11}C & \dots & a_{1n}C & 0C & \dots & 0C \\ \vdots & \dots & \vdots & \vdots & \ddots & \vdots \\ a_{n1}C & \dots & a_{nn}C & 0C & \dots & 0C \\ 0C & \dots & 0C & b_{11}C & \dots & b_{1m}C \\ \dots & \ddots & \dots & \dots & \ddots & \dots \\ 0C & \dots & 0C & b_{m1}C & \dots & b_{mm}C \end{bmatrix} \\ &= \begin{bmatrix} A \otimes C & 0 \\ 0 & B \otimes C \end{bmatrix} \\ &= (A \otimes C) \perp (B \otimes C) \end{aligned}$$

and similarly for $A \otimes (B \perp C)$, so the distribution laws hold.

Finally, we need to show that multiplication by the identity element of $(\mathrm{S}(k), \perp)$ annihilates $\mathrm{S}(k)$. Let $0_{\mathrm{S}(k)} = (\{0\}, (0,0) \mapsto 0)$ denote the identity of $(\mathrm{S}(k), \perp)$, and let $[(V, \beta)] \in \mathrm{S}(k)$. Here it is useful to use the version of tensor product from Definition 2.15. Because then we can see directly that the underlying vector space of $0_{\mathrm{S}(k)} \otimes (V, \beta)$ is $\{0\} \otimes_k V = \{0\}$, and so we necessarily need to have $0_{\mathrm{S}(k)} \otimes (V, \beta) = 0_{\mathrm{S}(k)}$.

Hence we get that $(\mathrm{S}(k), \perp, \otimes)$ is a commutative semiring. □

This semiring is very important, because later on we will turn it into the Grothendieck-Witt ring $\mathrm{GW}(k)$. Before we do that, however, there is another important topic we will cover first.

2.4 Hyperbolic space

The next type of space we want to examine is important to us because it will show up a lot in later computations, but it requires us to introduce a few more new terms:

Definition 2.21. Let (V, β) be a regular bilinear space. A non-zero vector $x \in V$ is called *isotropic* if $\beta(x, x) = 0$, otherwise it is called *anisotropic*. If (V, β) contains an isotropic vector, then (V, β) is called *isotropic*, otherwise it is called *anisotropic*.

Theorem 2.22. *Let (V, β) be a regular 2-dimensional bilinear space. Then the following are equivalent:*

(i) (V, β) *is isotropic*

(ii) $(V, \beta) \cong \langle 1, -1\rangle \cong \langle a, -a\rangle$ *for any* $a \neq 0$

(iii) $\det(V, \beta) = -1 \mod (k^\times)^2$

See [5] for proof.

Definition 2.23. Any bilinear space which satisfies the conditions in Theorem 2.22 is called a *hyperbolic plane*, and will be denoted by $\mathbb{H}$. An orthogonal sum of hyperbolic planes is called a *hyperbolic space*.

If we have a hyperbolic space that is the orthogonal sum of n hyperbolic planes, then we denote it by $n\mathbb{H}$.

Theorem 2.22, particularly part (ii), essentially tells us how we can recognise whether a given bilinear space is hyperbolic. Given the matrix of a 2-dimensional bilinear space, then if we use operations that respect congruence, then we can conclude that the bilinear space is hyperbolic if we can end up with $\langle 1, -1\rangle$. If the bilinear space has dimension that is even and larger than 2, then the goal would be to bring its matrix to $\langle 1, -1, \ldots, 1, -1\rangle \cong \langle 1, \ldots, 1, -1, \ldots, -1\rangle \cong n\mathbb{H}$.

If we are working with a bilinear space with odd dimension, then the whole space will not be hyperbolic, but there might be a hyperbolic space within the bilinear space. For instance, we could have something like $(V, \beta) \cong n\mathbb{H} \perp \langle a\rangle$ for some $a \in k$. So the notion of a hyperbolic space is still useful in odd dimensions.

But we do not even necessarily need to bring a matrix of a bilinear space all the way to $\langle 1, -1, \ldots, 1, -1\rangle$ in order to spot that it is hyperbolic. If (V, β) is $2n$-dimensional and $(V, \beta) \cong \langle B\rangle$, then [6, Thm. 4.5, p.12] tells us that (V, β) is a hyperbolic space if B has one of the following forms:

$$\begin{bmatrix} 0 & C \\ C^T & D \end{bmatrix} \qquad \begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix} \qquad \begin{bmatrix} C & 0 \\ 0 & -C \end{bmatrix}$$

where C and D are $n \times n$ matrices, C is invertible, and I_n is the $n \times n$ identity matrix.

It will also be useful to be able to spot when a bilinear space contains a hyperbolic plane at all, so we have the following.

Theorem 2.24. *Let (V, β) be a regular space over k of dimension ≥ 2. Then (V, β) is isotropic if and only if (V, β) has $\mathbb{H}$ as an orthogonal summand.*

See [5, Theorem 3.4, p. 13] for the proof. Clearly, Theorem 2.22 part (i) is just this theorem when the dimensions equals 2. So in total, if we have a bilinear space and we can find even just one isotropic vector in it, then we know that there is at least one hyperbolic plane in the space. This will be important for a proof in Chapter 4.

2.5 The Grothendieck-Witt ring $\mathrm{GW}(k)$

The Grothendieck construction is a procedure that constructs a ring from a semiring, or a group from a semigroup. Intuitively, the procedure is analogous to constructing the integers from the natural numbers (including 0), and this is indeed what happens if we apply the procedure to the natural numbers. We will use the construction with our commutative semiring $(\mathrm{S}(k), \perp, \otimes)$. But first we describe it in a general case, so let R be a commutative semiring.

Definition 2.25. The *Grothendieck ring* of R is the ring defined to be

$$\mathrm{Groth}(R) \coloneqq \frac{R \times R}{\sim}$$

where the equivalence relation is given by

$$(a, b) \sim (a', b') \iff \exists x \in R \text{ such that } a + b' + x = a' + b + x \in R$$

and where the addition and multiplication are defined by

$$\begin{aligned} [a, b] + [c, d] &= [a + c, b + d] \\ [a, b][c, d] &= [ac + bd, ad + bc]. \end{aligned}$$

It is easily shown that the equivalence described really is an equivalence relation, that the addition and multiplication on the equivalence classes are well-defined, and that $\mathrm{Groth}(R)$ satisfies the ring axioms. The zero in the ring is $[0, 0] = [a, a]$ for any $a \in R$, the unit is $[1, 0]$, and the additive inverse of $[a, b]$ is $[b, a]$.

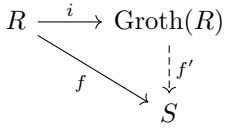
If R is a semigroup, then this definition without the multiplication produces the *Grothendieck group* of R, and many of the properties that follow also apply in this case.

Remark. Strictly speaking, the elements of $\mathrm{Groth}(R)$ are pairs $[a, b]$, but since $[a, b] = [a, 0] + [0, b] = [a, 0] + (-[b, 0])$, we can also think of the elements as formal differences. Additionally, the elements $[a, 0]$ are enough to generate all of $\mathrm{Groth}(R)$.

Proposition 2.26. *There is a canonical semiring homomorphism defined by*

$$i\colon R \to \mathrm{Groth}(R),\ a \mapsto [a, 0]$$

and this homomorphism has the universal property, meaning for any ring S and semiring homomorphism $f\colon R \to S$ there is a unique ring homomorphism $f'\colon \mathrm{Groth}(R) \to S$ such that the following diagram commutes



Proof. It is easily checked that i is a semiring homomorphism. Given S and $f\colon R \to S$, define $f'\colon \mathrm{Groth}(R) \to S$ by $f'([a, b]) = f(a) - f(b)$. It is easily checked that this is well-defined, that it is a ring homomorphism, and that $f'(i(a)) = f(a)$ for all $a \in R$. The remark before the proposition states that $\mathrm{Groth}(R)$ is generated by $\mathrm{Im}(i)$, so f' must be uniquely determined by f. □

In Definition 2.25 we need the $x \in R$ in the equation $a + b' + x = a' + b + x$ because not all semirings, specifically not all monoids, have the cancellation property. And if we do not have cancellation, then $\sim$ is not an equivalence relation because it then fails to have transitivity. Another reason cancellation is important is the following:

Lemma 2.27. *If R has the cancellation property, then i is injective.*

Proof. For $a, b \in R$ such that $i(a) = i(b)$, we have

$$\begin{aligned} i(a) = i(b) &\implies [a, 0] = [b, 0] \\ &\implies \exists x \in R \text{ such that } a + 0 + x = b + 0 + x \\ &\implies a = b \end{aligned}$$

where the last implication uses cancellation. Hence i is injective. □

So when R has cancellation, any $a \in R$ is sent by i to a unique element of $\mathrm{Groth}(R)$ and so by abuse of notation we can just think of this element as a.

Definition 2.28. The *Grothendieck-Witt ring* of k, denoted by $\mathrm{GW}(k)$, is the Grothendieck ring of $(\mathrm{S}(k), \perp, \otimes)$.

Witt's cancellation theorem [5, Thm. 4.2, p.15] shows that $(\mathrm{S}(k), \perp, \otimes)$ has the cancellation property. Hence $i\colon \mathrm{S}(k) \to \mathrm{GW}(k)$ is injective. So as the observation above notes, any isometry class $[(V,\beta)] \in \mathrm{S}(k)$ can be thought of as an element in $\mathrm{GW}(k)$ using i.

Later on we will be working exclusively in $\mathrm{GW}(k)$ and so to simplify the notation, we will just write (V,β) instead of $[(V,\beta)]$ and $(V,\beta) = (V',\beta')$ instead of $(V,\beta) \cong (V',\beta')$.

Although our focus later will be on $\mathrm{GW}(k)$, there is an interesting ring that is closely related. We first note the following:

Lemma 2.29. *The hyperbolic spaces form an ideal*

$$(\mathbb{H}) = \{n\mathbb{H} \mid n \in \mathbb{Z}\} \subseteq \mathrm{GW}(k).$$

Proof. For $n\mathbb{H}, m\mathbb{H} \in (\mathbb{H})$ we have $n\mathbb{H} \perp (-m\mathbb{H}) = (n-m)\mathbb{H} \in (\mathbb{H})$, so $(\mathbb{H}, \perp) \subseteq \mathrm{GW}(k)$ is a subgroup.

Let $\langle a_1, \ldots, a_n\rangle$ be an n-dimensional regular symmetric bilinear space. We show by induction on n that $\langle a_1, \ldots, a_n\rangle \otimes \mathbb{H} = \dim_k(\langle a_1, \ldots, a_n\rangle)\mathbb{H}$. For $n = 1$, we have $\langle a\rangle \otimes \mathbb{H} \cong \langle a\rangle \otimes \langle 1, -1\rangle = \langle a, -a\rangle \cong \mathbb{H} = 1\mathbb{H} = \dim_k(\langle a\rangle)\mathbb{H}$. Assume the statement holds for $n-1$. Then we have

$$\begin{aligned}
\langle a_1, \ldots, a_{n-1}, a_n\rangle \otimes \mathbb{H} &= (\langle a_1, \ldots, a_{n-1}\rangle \perp \langle a_n\rangle) \otimes \mathbb{H} \\
&= \langle a_1, \ldots, a_{n-1}\rangle \otimes \mathbb{H} \perp \langle a_n\rangle \otimes \mathbb{H} \\
&= \dim_k(\langle a_1, \ldots, a_{n-1}\rangle)\mathbb{H} \perp \mathbb{H} \\
&= (n-1)\mathbb{H} \perp 1\mathbb{H} \\
&= n\mathbb{H} \\
&= \dim_k(\langle a_1, \ldots, a_{n-1}\rangle)\mathbb{H}.
\end{aligned}$$

Then for any $\phi \coloneqq \langle a_1, \ldots, a_m\rangle \in \mathrm{GW}(k)$ and any $n\mathbb{H}$, we get

$$\begin{aligned}
\phi \otimes n\mathbb{H} &= \phi \otimes (\overbrace{\mathbb{H} \perp \ldots \perp \mathbb{H}}^{n \text{ times}}) \\
&= \overbrace{(\phi \otimes \mathbb{H}) \perp \ldots \perp (\phi \otimes \mathbb{H})}^{n \text{ times}} \\
&= \overbrace{\dim_k(\phi)\mathbb{H} \perp \ldots \perp \dim_k(\phi)\mathbb{H}}^{n \text{ times}} \\
&= \overbrace{m\mathbb{H} \perp \ldots \perp m\mathbb{H}}^{n \text{ times}} \\
&= nm\mathbb{H} \in (\mathbb{H}).
\end{aligned}$$

So $\langle a_1, \ldots, a_m\rangle \otimes n\mathbb{H} \in (\mathbb{H})$ and hence $(\mathbb{H})$ is an ideal of $\mathrm{GW}(k)$. □

Now that we have a particular ideal of $\mathrm{GW}(k)$, the next thing we could want to do is to consider the quotient ring. And this produces the ring of interest:

Definition 2.30. The *Witt ring* of k is defined as

$$\mathrm{W}(k) = \frac{\mathrm{GW}(k)}{(\mathbb{H})}.$$

The focus in this project is on computations in $\mathrm{GW}(k)$ rather than $\mathrm{W}(k)$. But generally speaking, in the theory of bilinear forms $\mathrm{W}(k)$ is just as important as $\mathrm{GW}(k)$.

Earlier we described the dimension of bilinear spaces, and it turns out it extends nicely to $\mathrm{GW}(k)$. Because as we can think of the dimension map $\mathrm{S}(k) \to \mathbb{Z}$ as a semiring homomorphism, the universal property of $i : \mathrm{S}(k) \to \mathrm{GW}(k)$ gives us a ring homomorphism $\dim : \mathrm{GW}(k) \to \mathbb{Z}$. We similarly get the discriminant as $\det : \mathrm{GW}(k) \to k^\times/(k^\times)^2$.

Since the dimension and discriminant of a bilinear space give us important information about the space's equivalence class in $\mathrm{GW}(k)$ and $\mathrm{W}(k)$, they can be useful for computing $\mathrm{GW}(k)$ or $\mathrm{W}(k)$ explicitly. See for example [6, Ch.2, §3].

We finish this chapter with a few results about finite fields. Later on, we will do computations over finite fields, and so the results will give us guidance that will be very important for how we attack the computations. See [6, p. 39] for the proofs.

Lemma 2.31. *Let $q = p^m$ where p is an odd prime. Then $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2$ consists of two elements.*

In the general $\mathbb{F}_q$ case, which is what we will cover later, we will denote the two elements by 1 and ε. Note that the set of square classes $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2$ is a group. So in the finite field case, multiplications with 1 and ε works like the multiplication in a group of order 2.

Theorem 2.32. *Let $k = \mathbb{F}_q$ where $q = p^m$ and p is an odd prime. Then:*

- *Every bilinear space over $\mathbb{F}_q$ of dimension ≥ 3 is isotropic.*
- *Two bilinear spaces over $\mathbb{F}_q$ are isometric if and only if they have the same dimension and discriminant.*
- *For each dimension n, there are exactly two isometry classes of regular bilinear spaces in dimension n.*

The last two points in particular are very important in our later computations, but we will save the details about that for later.

Chapter 3

Polynomial rings

We will now develop techniques for doing computations in the polynomial ring $k[x_1, \ldots, x_n]$ where k is a field. More specifically we need to be able to work with quotient rings and compute localisations.

First off, we are going to consider the quotient ring $k[x_1, \ldots, x_n]/I$ where the ideal $I = (f_1, \ldots, f_m) \subseteq k[x_1, \ldots, x_n]$ is generated by $f_i \in k[x_1, \ldots, x_n]$ for $i = 1, \ldots, m$. We want to know what the elements of this quotient ring are like, so we want to take any $h \in k[x_1, \ldots, x_n]$ and compute $h + I \in k[x_1, \ldots, x_n]/I$. More specifically, we mean that we want to find a representative r of the coset $h + I$ such that $r \notin I$ and write $h + I = r + I$.

It turns out that we need quite a bit of background work before we are able to do this in the case of multiple variables. In just one variable, however, this is not very complicated, so we will start with that case.

For $h \in k[x]$, we want to compute $h + I \in k[x]/I$ with $I = (f_1, \ldots, f_m) \subseteq k[x]$. Since $k[x]$ is a principal ideal domain, the ideal reduces to $I = (f_1, \ldots, f_m) = (f)$ for some $f \in k[x]$, so then we are computing $h + (f) \in k[x]/(f)$. Additionally, we have that the division algorithm for the integers extends very nicely to the polynomials in one variable:

Theorem 3.1. *Let $f \in k[x]$, $f(x) \neq 0$. Then for any $h \in k[x]$, we can write*

$$h = qf + r$$

for some $q, r \in k[x]$. If $r = 0$ or $\deg(r) < \deg(f)$, then q and r are unique. Furthermore, there is an algorithm for computing q and r.

Note first that for $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ where $a_n \neq 0$, the *leading term* of f is $\mathrm{LT}(f) = a_n x^n$, meaning the term of f with the highest degree.

Proof. The algorithm for computing q and r is shown in Algorithm 1.

Algorithm 1 Division Algorithm for $k[x]$

1: *Input:* h, f
2: $q \leftarrow 0$
3: $r \leftarrow h$
4: **while** $r \neq 0$ and $\mathrm{LT}(f) \mid \mathrm{LT}(r)$ **do**
5: $\quad q \leftarrow q + \mathrm{LT}(r)/\mathrm{LT}(f)$
6: $\quad r \leftarrow r - (\mathrm{LT}(r)/\mathrm{LT}(f))f$
7: **end while**
8: *Output:* q, r

Note first that the equation $h = qf + r$ clearly holds for the initial values of q and r. And because

$$qf + r = \left(q + \frac{\mathrm{LT}(r)}{\mathrm{LT}(f)}\right) f + \left(r - \frac{\mathrm{LT}(r)}{\mathrm{LT}(f)} f\right)$$

we get that $h = qf + r$ still holds at the end of each **while** loop. Additionally, the algorithm terminates if either $r = 0$ or if $\mathrm{LT}(f)$ does not divide $\mathrm{LT}(r)$, which would mean $\deg(r) < \deg(f)$. So provided the algorithm does terminate, we have that q and r have the desired properties.

To see that the algorithm does terminate, observe that the leading term of $(\mathrm{LT}(r)/\mathrm{LT}(f))f$ is precisely $\mathrm{LT}(r)$ and so line 6 in the algorithm will by design cancel out $\mathrm{LT}(r)$. Hence at at the end of each **while** loop the degree of r will strictly decrease. And since r at the start of the algorithm has finite degree, the algorithm will eventually terminate.

Finally, we need to prove that q and r are unique. Suppose $q, q', r, r' \in k[x]$ are such that $h = qf + r = q'f + r'$ and either $r = 0$ or $\deg(r) < \deg(f)$ and either $r' = 0$ or $\deg(r') < \deg(f)$. We have $(q' - q)f = r - r'$.

Let $r, r' \neq 0$ and so $\deg(r), \deg(r') < \deg(f)$. If we try to assume that $r \neq r'$, then we have $\deg(r - r') < \deg(f)$. And then

$$\deg(f) > \deg(r - r') = \deg((q' - q)f) = \deg(q' - q) + \deg(f) \geq \deg(f)$$

which is a contradiction, forcing $r = r'$. So then $(q' - q)f = r - r' = 0$ and as $k[x]$ is an integral domain and $f \neq 0$ by assumption, we hence get $q = q'$. If we let $r = r' = 0$, then we get $(q' - q)f = 0$ directly and again $q = q'$. If we assume $r \neq 0$ and $r' = 0$, then we get $(q' - q)f = r$ which again leads to the contradiction $\deg(f) < \deg(f)$. So $r \neq 0$, $r' = 0$, and similary $r = 0$, $r' \neq 0$, are impossible. Hence in all cases we get $q = q'$ and $r = r'$. □

The reason this algorithm is useful to us, is that if we have any non-zero polynomial $f \in k[x]$ and a polynomial $h \in k[x]$, then by using the division algorithm

we get

$$h + (f) = qf + r + (f) = r + (f) \in k[x]/(f)$$

which is what we want. In particular, $h \in (f) \iff r = 0$.

In order to compute $h + I \in k[x_1, \ldots, x_n]/I$ more generally, we want to extend the division algorithm to make it somehow work when we have more than one variable. By taking another look at Algorithm 2.25, we can see that the idea of the algorithm is essentially that each time we go through the **while** loop, we cancel out the term in h of highest degree. What we are left with we carry back with us through the loop and we do this until we end up with 0 or a polynomial where none of the terms can be canceled out by the loop.

Part of the reason this process works so nicely with one variable is that it is easy to determine what term of h has the highest degree. If ax^m and bx^n are terms in h, we just check which of m and n is the larger one. With multiple variables, this is less straightforward and we need to work out how to do it in order to to extend the division algorithm.

3.1 Monomial orderings

In one variable, we determine which of two monomials has the higher degree by comparing the exponents. We are also going do this in multiple variables, so observe first that we can express a monomial in $k[x_1, \ldots, x_n]$ as $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$, where the n-tuple $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$ consisting of the exponents of the monomial uniquely determines the monomial. This gives us a one-to-one correspondence between $\mathbb{Z}_{\geq 0}^n$ and the monomials of $k[x_1, \ldots, x_n]$, and it follows that by establishing a way to compare tuples in $\mathbb{Z}_{\geq 0}^n$ we can also compare the corresponding monomials in the same way. In other words, given $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$ if we have $\alpha > \beta$ then we can also say that $x^\alpha > x^\beta$.

The next thing to note is that, unlike in $k[x]$, there is not one unique way to define a way of comparing tuples in $\mathbb{Z}_{\geq 0}^n$ for $n > 1$. So instead of looking for one particular ordering, we need to define this notion a bit more generally:

Definition 3.2. A *monomial ordering* $>$ on $k[x_1, \ldots, x_n]$ is a relation on $\mathbb{Z}_{\geq 0}^n$ that satisfies the following:

(i) $>$ is a total ordering on $\mathbb{Z}_{\geq 0}^n$

(ii) $>$ is a well-ordering on $\mathbb{Z}_{\geq 0}^n$

(iii) For $\alpha, \beta, \gamma \in \mathbb{Z}_{\geq 0}^n$, if $\alpha > \beta$ then $\alpha + \gamma > \beta + \gamma$

If $\alpha > \beta$, then we will say that $x^\alpha > x^\beta$. Note that we could also define monomial ordering on the monomials directly, but we would be comparing the exponents as tuples of $\mathbb{Z}_{\geq 0}^n$ anyways.

The requirement that $>$ is a *total ordering* [2, p. 55] means that $>$ has the transitive property and that for any $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$, we have one of the following:

$$\alpha > \beta, \qquad \alpha = \beta, \qquad \beta > \alpha.$$

In particular, any two tuples in $\mathbb{Z}^n_{\geq 0}$ are comparable under $>$. The *well-ordering* requirement means that any non-empty subset of $\mathbb{Z}^n_{\geq 0}$ has a least element under $>$, so in a non-empty subset A there is some $\alpha \in A$ such that for any other $\beta \in A$ we have $\beta > \alpha$.

The third requirement ensures that $>$ is compatible with multiplication in $k[x_1, \ldots, x_n]$. In terms of monomials, it says that

$$x^\alpha > x^\beta \implies x^\alpha x^\gamma > x^\beta x^\gamma \implies x^{\alpha+\gamma} = x^{\beta+\gamma}.$$

So in particular, if we have written a polynomial $x^{\alpha_1} + x^{\alpha_2} + \ldots + x^{\alpha_n}$ such that the monomials are in decreasing order according to $>$, meaning $\alpha_1 > \alpha_2 > \ldots > \alpha_n$, then multiplying by any β will not mess up the ordering. We would get $x^{\alpha_1+\beta} + x^{\alpha_2+\beta} + \ldots + x^{\alpha_n+\beta}$ where the monomials are still in decreasing order. In other words, this condition ensures that nothing unpredictable happens with the monomials when we multiply polynomials together.

Now that we have a way of comparing the monomials, we can use monomial orderings to extend some old definitions:

Definition 3.3. Let $f = \sum_{\alpha \in A} a_\alpha x^\alpha$ be a non-zero polynomial in $k[x_1, \ldots, x_n]$ where $A \subseteq \mathbb{Z}^n_{\geq 0}$, let $>$ be a monomial ordering.

(i) The *multidegree* of f is $\text{multideg}(f) = \max\{\alpha \in A \mid a_\alpha \neq 0\}$ where the maximum is taken with respect to $>$.

(ii) The *leading term* of f is $\text{LT}(f) = a_{\text{multideg}(f)} x^{\text{multideg}(f)}$.

Now that we have talked about monomial orderings in general, we will describe some specific ones. There are many different monomial orderings, but not all of them are useful to us. We will mention two of them here.

Definition 3.4. The *lexicographic order*, or *lex order*, is denoted by $>_{lex}$ and defined as follows: for $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$ we have $\alpha >_{lex} \beta$ if the leftmost non-zero entry in $\alpha - \beta$ is positive. If $\alpha >_{lex} \beta$ then we say $x^\alpha >_{lex} x^\beta$.

In this ordering we have

$$(1, 0, \ldots, 0) >_{lex} (0, 1, 0, \ldots, 0) >_{lex} \ldots >_{lex} (0, \ldots, 0, 1)$$

which corresponds to $x_1 >_{lex} x_2 >_{lex} \ldots >_{lex} x_n$, so we essentially have a way of prioritising the variables. But note that this ordering of the variables is not unique. If we order the variables differently, for example $x_2, x_3, \ldots, x_n, x_1$ so

that $x_2 >_{lex} x_3 >_{lex} \ldots >_{lex} x_n >_{lex} x_1$, then we have a different lexicographic ordering. So in general we need to specify which ordering of the variables we are using. If nothing else is stated, however, we will use the standard one, $x_1 >_{lex} x_2 >_{lex} \ldots >_{lex} x_n$.

The name of this ordering comes from the fact that this monomial ordering is very similar to how words are ordered in the dictionary. We can see this by considering words as n-tuples and using the ordering $a >_{lex} b >_{lex} \ldots >_{lex} z$. Unlike the dictionary, however, the lexicographic order prioritises terms with more variables, for example $x_1x_2x_3x_4 >_{lex} x_1x_2$.

A feature of the lexicographic order is that a single variable will dominate any monomial that only contains variables deemed smaller, so $x_1 >_{lex} x_2^{m_2}x_3^{m_3}\cdots x_n^{m_n}$ no matter how large the m_i are. We might sometimes want to be able to take into account the size of the exponentials when ordering monomials. In other words, we would like to make use of the following:

Definition 3.5. The *total degree* of a monomial $x^\alpha \in \mathbb{Z}^n_{\geq 0}$ is

$$|\alpha| = \sum_{i=1}^{n} \alpha_i \in \mathbb{Z}_{\geq 0}.$$

There are multiple ways of using this to define monomial orderings, but we will use the following:

Definition 3.6. The *graded reverse lexicographic order*, or *grevlex order*, is denoted by $>_{grevlex}$ and is defined as follows: for $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$ we say $\alpha >_{grevlex} \beta$ if one of the following is satisfied

(i) $|\alpha| > |\beta| \in \mathbb{Z}_{\geq 0}$.

(ii) $|\alpha| = |\beta| \in \mathbb{Z}_{\geq 0}$ and the rightmost non-zero entry in $\alpha - \beta \in \mathbb{Z}^n$ is negative.

So this ordering priorities the largest total degrees first, and in the case of ties it compares the monomials in a manner that is similar to the lexicographic ordering. This idea might not seem very intuitive, but grevlex is an ordering which is considered to be very efficient for the kind of computations we will be doing [2].

It should also be noted that when using the canonical ordering of the variables, grevlex prioritises the variables the same way as the lex ordering, so by default we have $x_1 >_{grevlex} x_2 >_{grevlex} \ldots >_{grevlex} x_n$.

Now that we have developed a method of ordering multivariate monomials, we are ready to describe the division algorithm for $k[x_1, \ldots, x_n]$:

Theorem 3.7. *Let $>$ be a monomial ordering on $\mathbb{Z}^n_{\geq 0}$ and let $F = \{f_1, \ldots, f_s\}$ be an ordered s-tuple of polynomials in $k[x_1, \ldots, x_n]$. For any $h \in k[x_1, \ldots, x_n]$*

we can write

$$h = q_1 f_1 + q_2 f_2 + \ldots + q_s f_s + r$$

for some $q_1, \ldots, q_s, r \in k[x_1, \ldots, x_n]$ *where either* $r = 0$ *or* r *is a* k*-linear combination of monomials that are not divisible by any of* $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$. *And* r *is called the remainder of* h *on division by* F.

The proof is essentially a more general form of the proof for Theorem 3.1, see [2, Theorem 3, p. 64] for the full proof. The important thing for us here, is Algorithm 2, which describes how to construct $q_1, \ldots, q_s$, and r.

Algorithm 2 Division Algorithm for $k[x_1, \ldots, x_n]$

```
1:  Input: h, f_1, ..., f_s
2:  q_1 ← 0, ..., q_s ← 0, r ← 0
3:  p ← h
4:  while p ≠ 0 do
5:      i ← 0
6:      divisionoccured ← False
7:      while i ≤ s and divisionoccured = False do
8:          if LT(f_i) | LT(p) then
9:              q_i ← LT(p)/LT(f_i)
10:             p ← p − (LT(p)/LT(f_i))f_i
11:             divisionoccured ← True
12:         else
13:             i ← i + 1
14:         end if
15:     end while
16:     if divisionoccured = False then
17:         r ← r + LT(p)
18:         p ← p − LT(p)
19:     end if
20: end while
21: Output: q_1, ..., q_s, r
```

We will use this algorithm similarly as in the one variable case. So given $h \in k[x_1, \ldots, x_n]$ and an ideal $(f_1, \ldots, f_s)$ generated by polynomials $f_i \in k[x_1, \ldots, x_n]$, we can use Algorithm 2 to write $h = q_1 f_1 + \ldots + q_s f_s + r$ for some $q_1, \ldots, q_s, r \in k[x_1, \ldots, x_n]$. Then if $r = 0$ we have that $h \in (f_1 \ldots, f_s)$.

However, there is an important difference between Theorem 3.1 and Theorem 3.7. In Theorem 3.1 we have that q and r are unique, while in Theorem 3.7 we make no such claim for $q_1, \ldots, q_s$, and r. This is because they are not unique, and this actually raises a problem for us.

First off, we can find the reason why $q_1, \ldots, q_s$ and r are not unique by studying Algorithm 2. Looking at lines $7 - 15$ we see that in each **while** loop, we try to

perform a division by an f_i. If the division does not happen then we increment i and try again with f_{i+1}. We do this until a division happens or we run out of polynomials by which we want to divide.

The important thing here is that when we give the algorithms some polynomials $f_1, \ldots, f_s$ by which we want to perform the division, we need to order the polynomials and then the algorithm will use that order when testing if a division can be performed in each loop. So if the intermediate polynomial p is divisible by more than one f_i, we will only perform the division by the f_i that occurs first according to the order we picked. This then affects what the q_i and r we get at the end look like.

The reason this becomes a problem for us is that it is possible to have a division of h by some $f_1, \ldots, f_s$ which gives $r = 0$ with one ordering of the f_i and $r \neq 0$ with a different ordering. For example, in example 3 from [2, p. 68] we have that dividing $h = xy^2 - x$ by $f_1 = xy - 1$ and $f_2 = y^2 - 1$ in that order gives $r = -x + y$, while using the opposite order $\{f_2, f_1\}$ gives $r = 0$. The fact that we can get $r = 0$ means it is possible to write $h = q_1 f_1 + q_2 f_2$ and hence that $h \in (f_1, f_2)$. But if we only tried to check this using the order $\{f_1, f_2\}$ we could mistakenly believe that $h \notin (f_1, f_2)$. Clearly this is a big problem if we have many f_i and so many possible orders to consider.

So the next thing we want is a way to remedy this issue. If we can make the algorithm produce a unique r for any ordering of the divisors, then we would have solved how to determine if $h \in (f_1, \ldots, f_s)$. The solution will be to reconsider which polynomials by which we do the division.

3.2 Gröbner bases

Recall that what we want is being able to compute $h + I \in k[x_1, \ldots, x_n]/I$ where $I = (f_1, \ldots, f_s)$. Trying to write $h = q_1 f_1 + \ldots, q_s f_s + r$ is certainly one way of doing it, but we could also try to do it with a different set of generators for I. This is exactly the key to making Algorithm 2 produce a unique r, so we essentially want to find a good way of choosing generators for I. We first introduce the following:

Definition 3.8. Let $I \subseteq k[x_1, \ldots, x_n]$ be a non-zero ideal, fix some monomial ordering. The *leading term set* of I is defined as

$$\mathrm{LT}(I) = \{\mathrm{LT}(f) \mid f \in I \setminus \{0\}\}$$

and the *leading term ideal* of I is the ideal generated by the elements of $\mathrm{LT}(I)$, denoted $(\mathrm{LT}(I))$.

The leading term ideal $(\mathrm{LT}(I))$ is a monomial ideal, which means it is generated by monomials. It can also be shown that we can find finitely many polynomials

$g_1, \ldots, g_t \in I$ such that $(\mathrm{LT}(I)) = (\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t))$ [2, p. 77]. Another useful fact about monomial ideals is that a monomial x^α is contained in a monomial ideal I if and only if there is a monomial in I that divides x^α [2, p. 70].

Definition 3.9. Fix a monomial ordering on $k[x_1, \ldots, x_n]$ and let $I \subseteq k[x_1, \ldots, x_n]$ be a non-zero ideal. A finite subset $\mathcal{G} = \{g_1, \ldots, g_t\}$ of I is called a *Gröbner basis*, or *standard basis*, of I if

$$(\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)) = (\mathrm{LT}(I)).$$

It can be shown that a Gröbner basis of an ideal is indeed a basis of the ideal, and furthermore that any ideal in $k[x_1, \ldots, x_n]$ has a Gröbner basis [2, p. 78].

Proposition 3.10. *Let $I \subseteq k[x_1, \ldots, x_n]$ be a non-zero ideal, let $\mathcal{G} = \{g_1, \ldots, g_t\}$ be a Gröbner basis of I, and let $f \in k[x_1, \ldots, x_n]$ be any polynomial. Then the remainder r from dividing f by $\mathcal{G}$ is unique with respect to ordering the elements in $\mathcal{G}$.*

Proof. The division algorithm allows us to write $f = q_1 g_1 + \ldots + q_t g_t + r$ for some $q_i \in k[x_1, \ldots, x_n]$. To simplify notation we let $g = q_1 g_1 + \ldots + q_t g_t$ so that $f = g + r$. Let $g' \in I$ and $r' \in k[x_1, \ldots, x_n]$ be another pair of polynomials from the division algorithm such that $f = g + r = g' + r'$. Then we have $g' - g = r - r'$. Recall from Theorem 3.7 that either $r = 0$ or no term in r is divisible by any of the $\mathrm{LT}(g_i)$, and we have the same for r'.

Let $r, r' \neq 0$ and suppose that $r \neq r'$, then we have $r - r' \neq 0$ and since $g, g' \in I$ we get $r - r' = g' - g \in I = (\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t))$. Then any term in $r - r'$ is divisible by some $\mathrm{LT}(g_i)$, which contradicts that none of the terms in r and r' are divisible by any $\mathrm{LT}(g_i)$. So if $r, r' \neq 0$ then we need to have $r = r'$.

If $r \neq 0$ and $r' = 0$, then we get $r = r - r' = g' - g \in I$ which again contradicts that r is not divisible by any $\mathrm{LT}(g_i)$. Similarly for $r = 0$, $r' \neq 0$. Finally, if $r = r' = 0$ then we are directly done. □

So finally with this result we are capable of computing $f + I \in k[x_1, \ldots, x_n]/I$, as for any non-zero ideal $I \subseteq k[x_1, \ldots, x_n]$, any Gröbner basis $\mathcal{G}$ of I, and any polynomial $f \in k[x_1, \ldots, x_n]$, then $f + I$ is just the remainder of f divided by $\mathcal{G}$. And in particular $f \in I \iff$ the remainder is 0.

Note that the proposition only claims the uniqueness of r, not of the q_i. So by permuting the g_i in the division algorithm, we will get different values of the q_i. But this is not a problem for us, since the remainder is the important part when computing $f + I$.

What we have determined so far is that when we have a Gröbner basis $\mathcal{G}$ of an ideal I, then for any $f \in k[x_1, \ldots, x_n]$ we can compute $f + I$. But so far we

have not explored how we can find a Gröbner basis of I in the first place, so we will study that next.

First off we introduce some notation: When we divide a polynomial f by an ordered s-tuple $\mathcal{F} = (f_1, \ldots, f_s)$ then we will denote the remainder of this division by $\overline{f}^{\mathcal{F}}$. If $\mathcal{F}$ is a Gröbner basis of an ideal then we can just consider it as a set, without any particular ordering.

Definition 3.11. Let $f, g \in k[x_1, \ldots, x_n]$ be any non-zero polynomials. If $\text{multideg}(f) = \alpha = (\alpha_1, \ldots, \alpha_n)$ and $\text{multideg}(g) = \beta = (\beta_1, \ldots, \beta_n)$, then we let $\gamma = (\gamma_1, \ldots, \gamma_n)$ where for each i we have $\gamma_i = \max\{\alpha_i, \beta_i\}$. Then the *S-polynomial* of f and g is defined to be

$$S(f, g) = \frac{x^\gamma}{\text{LT}(f)} \cdot f - \frac{x^\gamma}{\text{LT}(g)} \cdot g.$$

Intuitively, we can think of the monomial x^γ is the least common multiple of the leading monomials of f and g.

The S-polynomial essentially combines f and g in a way that cancels out the leading terms of f and g. It is useful because of the following:

Theorem 3.12 (Buchberger's Criterion)**.** *Let $I \subseteq k[x_1, \ldots, x_n]$ be a non-zero ideal and let $\mathcal{G} = \{g_1, \ldots, g_t\}$ be a basis of I. Then $\mathcal{G}$ is a Gröbner basis of I if and only if $\overline{S(g_i, g_j)}^{\mathcal{G}} = 0$ for all pairs $i \neq j$.*

This result is also called the *S-polynomial criterion*.

The proof can be found in [2, Theorem 6, p. 86], but a notable thing about the proof is that it is non-constructive. So we can use this result to check whether a basis is Gröbner or not, but to construct a Gröbner basis we will need to make use of the following:

Theorem 3.13. *Let $I = (f_1, \ldots, f_s) \subseteq k[x_1, \ldots, x_n]$ be a non-zero ideal. Then a Gröbner basis for I can be constructed using Algorithm 3 in a finite number of steps.*

Sketch of proof. Show that $\mathcal{G} \subseteq I$ at each stage of the algorithm, so initially and after something is added to $\mathcal{G}$. The output $\mathcal{G}$ at the end contains $\mathcal{F}$ and so is a generating set for I. To show that the algorithm terminates, show that after each loop we have $(\text{LT}(\mathcal{G}')) \subseteq (\text{LT}(\mathcal{G}))$ with strict containment when $\mathcal{G}' \neq \mathcal{G}$. Then by going through the loop multiple times we get an ascending chain of ideals in $k[x_1, \ldots, x_n]$. And since $k[x_1, \ldots, x_n]$ is Noetherian, the chain stabilises after finitely many steps, hence the algorithm terminates in a finite number of steps. □

Algorithm 3 Buchberger's Algorithm

Input: $\mathcal{F} = (f_1, \ldots, f_s)$
$\mathcal{G} \leftarrow \mathcal{F}$
do
    $\mathcal{G}' \leftarrow \mathcal{G}$
    for all pairs $p \neq q$ in $\mathcal{G}'$ **do**
        $r \leftarrow \overline{S(p,q)}^{\mathcal{G}'}$
        if $r \neq 0$ **then**
            $\mathcal{G} \leftarrow \mathcal{G} \cup \{r\}$
        end if
    end for
while $\mathcal{G} \neq \mathcal{G}'$
Output: $\mathcal{G} = (g_1, \ldots, g_t)$

What essentially happens in this algorithm is that we have an ideal I and a set of generators $\{f_1, \ldots, f_s\}$, and we try Buchberger's criterion on $f_1, \ldots, f_s$. It fails whenever a remainder $\overline{S(f_i, f_j)}^{\mathcal{G}'}$ is non-zero, and in that case we just add that remainder to the generating set. At the end of the **do...while** loop the algorithm checks whether we added anything to $\mathcal{G}$ or not. It breaks the loop if we did not add anything to $\mathcal{G}$, meaning the current generating set passes Buchberger's criterion and so is a Gröbner basis.

It should be noted that this version of the algorithm is not as efficient as it could be. In particular, the **do...while** loop computes the remainder of all pairs of elements in the generating set. But if the remainder of two elements is zero in one iteration then it will still be zero in all the next iterations, so it is actually redundant to check this again. So when one new element f_j is added to the generating set $\{f_1, \ldots, f_{j-1}\}$, in the next iterations we only need to check the remainders $\overline{S(f_i, f_j)}^{\mathcal{G}'}$ for $i = 1, \ldots, j-1$. There are improvements on the algorithm that takes this into account, see for example Chapter 3, Section 10 in [2], but for our purposes the version presented here is good enough.

Another thing to note is that this algorithm constructs a Gröbner basis which may contain redundant elements. So the following may be useful:

Lemma 3.14. *Let $\mathcal{G}$ be a Gröbner basis of an ideal $I \subseteq k[x_1, \ldots, x_n]$. If $p \in \mathcal{G}$ is a polynomial such that $\mathrm{LT}(p) \in (\mathrm{LT}(\mathcal{G} \setminus \{p\}))$, then $(\mathrm{LT}(\mathcal{G} \setminus \{p\}))$ is also a Gröbner basis of I.*

Proof. By definition we have $(\mathrm{LT}(\mathcal{G})) = (\mathrm{LT}(I))$. And if $\mathrm{LT}(p) \in (\mathrm{LT}(\mathcal{G} \setminus \{p\}))$ then $(\mathrm{LT}(\mathcal{G} \setminus \{p\})) = (\mathrm{LT}(\mathcal{G})) = (\mathrm{LT}(I))$ and so by definition $\mathcal{G} \setminus \{p\}$ is a Gröbner basis of I. □

A Gröbner basis such that for all $p \in \mathcal{G}$ we have $\mathrm{LT}(p) \notin (\mathrm{LT}(\mathcal{G} \setminus \{p\}))$ and the

coefficient of $\mathrm{LT}(p)$ is 1 is called a *minimal Gröbner basis* of I.

Minimal Gröbner bases are unfortunately not unique, but we can single out a particular one with the following:

Definition 3.15. Let $\mathcal{G}$ be a Gröbner basis of an ideal $I \subseteq k[x_1, \ldots, x_n]$. $\mathcal{G}$ is called a *reduced Gröbner basis* of I if for all $p \in \mathcal{G}$ we have that the coefficient of $\mathrm{LT}(p)$ is 1 and no monomial in p is contained in $(\mathrm{LT}(\mathcal{G} \setminus \{p\}))$.

Theorem 3.16. *Let $I \subseteq k[x_1, \ldots, x_n]$ be a non-zero ideal. Then for a given monomial ordering, I has a unique reduced Gröbner basis.*

See [2, Theorem 3, p. 93] for proof. It then follows from this theorem that two ideals are equal if and only if their reduced Gröbner bases are equal. Similarly, we can check if two sets of polynomials $\{f_1, \ldots, f_s\}$ and $\{g_1, \ldots, g_t\}$ generate the same ideal by comparing their reduced Gröbner bases.

3.3 Quotients and localisations

So far in this chapter we have explored how to compute $h + I \in k[x_1, \ldots, x_n]/I$. In other words we have focused on taking elements in $k[x_1, \ldots, x_n]$ and studying how we turn them into elements of $k[x_1, \ldots, x_n]$. But we will also need some results about $k[x_1, \ldots, x_n]/I$ itself. In particular, we will see how we can find a basis of $k[x_1, \ldots, x_n]/I$ and we will also look at localisations of $k[x_1, \ldots, x_n]$.

First off note that the commutative quotient ring $k[x_1, \ldots, x_n]/I$ is also a k-vector space where the scalar multiplication comes from considering elements of k as constant polynomials and multiplying as usual. Then it is easy to see that $k[x_1, \ldots, x_n]/I$ is a k-algebra. But in particular, we have the following:

Theorem 3.17. *Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal. Then*

$$k[x_1, \ldots, x_n]/I \cong \mathrm{Span}_k\{x^\alpha \mid x^\alpha \notin (\mathrm{LT}(I))\}$$

where the isomorphism is as k-vector spaces.

Sketch of proof. The mapping

$$\begin{aligned} \Phi \colon k[x_1, \ldots, x_n]/I &\to \mathrm{Span}_k\{x^\alpha \mid x^\alpha \notin (\mathrm{LT}(I))\}, \\ f + I &\mapsto \overline{f}^G \end{aligned}$$

can be shown to be a vector space isomorphism. □

So then the monomials that are not in $(\mathrm{LT}(I))$ form a basis of $k[x_1, \ldots, x_n]/I$. Specifically, a monomial $x^\alpha \in k[x_1, \ldots, x_n]$ is in a basis of $k[x_1, \ldots, x_n]/I$ if and only if for each $x^\beta \in (\mathrm{LT}(I))$ there exists an $i \in \{1, 2, \ldots, n\}$ such that $\alpha_i < \beta_i$.

Since we are now considering the structure of $k[x_1, \ldots, x_n]/I$, the following will also be important:

Theorem 3.18. *Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal and fix a monomial ordering on $k[x_1, \ldots, x_n]$. Then $k[x_1, \ldots, x_n]/I$ is finite dimensional if and only if for each $i = 1, 2, \ldots, n$ there exists some $m_i \geq 0$ such that $x^{m_i} \in (\mathrm{LT}(I))$.*

Proof. If for each i, we have $x^{m_i} \in (\mathrm{LT}(I))$ for some $m_i \geq 0$, then any monomial $x^{\alpha_1} x^{\alpha_2} \cdots x^{\alpha_n}$ in the complement of $(\mathrm{LT}(I))$ must be such that $0 \leq \alpha_i \leq m_i - 1$. Hence the number of elements in $\mathrm{Span}_k\{x^\alpha \mid x^\alpha \notin (\mathrm{LT}(I))\}$, and hence the number of basis elements for $k[x_1, \ldots, x_n]$, is at most $m_1 m_2 \cdots m_n < \infty$.

Conversely, if $\dim_k k[x_1, \ldots, x_n]/I = N < \infty$, and so the complement of $(\mathrm{LT}(I))$ contains N elements, then for each i at least one of the $N + 1$ monomials $1, x_i, x_i^2, \ldots, x_n^N$ must lie in $(\mathrm{LT}(I))$. □

Later on we are primarily interested finite dimensional quotient rings, so this theorem provides us with a useful restriction on which ideals we can consider.

Finally for this chapter, we consider localisations of $k[x_1, \ldots, x_n]/I$. We first describe the construction for a general commutative ring R with unity.

A subset $S \subseteq R$ is a *multiplicatively closed subset* of R if $1 \in S$ and S is closed under multiplication. We define a relation on $R \times S$ by

$$(a, s) \sim (b, t) \iff \exists u \in S \text{ such that } (at - bs)u = 0.$$

One can easily show that this is an equivalence relation. We denote the equivalence classes of this relation by a/s for $a \in R$ and $s \in S$. The set of all such equivalence classes is called the *ring of fractions* of A with respect to S and it is denoted by $S^{-1}R$. This set gets a ring structure by defining addition and multiplication by

$$(a/s) + (b/t) = (at + bs)/st$$
$$(a/s)(b/t) = ab/st.$$

It can be verified that these operations do not depend on the choice of representatives for the equivalence classes and that $S^{-1}R$ is a commutative ring with unity. See [1, Chapter 3] for more details.

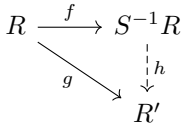
Looking at the equivalence relation here, we can see a distinct similarity with the Grothendieck construction described in section 2.5. Like the Grothendieck construction, the construction described here is essentially a way of introducing inverses to a ring. For example, using $R = \mathbb{Z}$ and $S = \mathbb{Z} \setminus \{0\}$, we get $S^{-1}R = \mathbb{Q}$.

And like the Grothendieck construction, the ring of fractions has a canonical map with the universal property:

Proposition 3.19. *There is a canonical ring homomorphism*

$$f\colon R \to S^{-1}R,\ x \mapsto x/1$$

which has the universal property, so if $g\colon R \to R'$ is a ring homomorphism such that for all $s \in S$ we have that $g(s)$ is a unit in R', then there exists a unique ring homomorphism $h\colon S^{-1}R \to R'$ such that $g = h \circ f$. So the following diagram commutes:



See [1, p. 37] for proof.

If $\mathfrak{p} \subseteq R$ is a prime ideal, then $S = R \setminus \mathfrak{p}$ is a multiplicatively closed set. This allows us to define the following:

Definition 3.20. If $\mathfrak{p}$ is a prime ideal of R and $S = R \setminus \mathfrak{p}$, then $S^{-1}R$ is called the *localisation* of R at $\mathfrak{p}$ and we denote it by $R_{\mathfrak{p}}$.

As the name suggest, $R_{\mathfrak{p}}$ is a local ring, where the unique maximal ideal is the ideal of $R_{\mathfrak{p}}$ generated by $\mathfrak{p}$, more specifically $S^{-1}\mathfrak{p} = \{a/s \in R_{\mathfrak{p}} \mid a \in \mathfrak{p}, s \in S\}$.

Intuitively, what happens when we localise R at $\mathfrak{p}$ is that we introduce inverses to all elements in $S = R \setminus \mathfrak{p}$. In other words, everything that is not in $\mathfrak{p}$ now has an inverse.

Consider now the polynomial ring $k[x_1, \ldots, x_n]$ and the ideal $(x_1, \ldots, x_n)$. This ideal consists of all polynomials with constant term zero. Trying to make the ideal larger requires us to introduce an element of k at which point the ideal blows up to all of $k[x_1, \ldots, x_n]$. So $(x_1, \ldots, x_n)$ is maximal and hence prime. So in other words, we can localise at it, and it is exactly this ideal our localisations later on will focus on. And intuitively, localising at $(x_1, \ldots, x_n)$ means that polynomials with a non-zero constant term gets an inverse.

However, our localisations will not be of the polynomial ring $k[x_1, \ldots, x_n]$, but rather the quotient ring $k[x_1, \ldots, x_n]/I$ for some ideal I. To make this process easier, we will make use of the following:

Proposition 3.21. *Let I be an ideal of the ring R, let S be a multiplicatively closed subset of R, and let $\overline{S}$ denote the image of S in R/I. Then $S^{-1}I$ is an ideal of $S^{-1}R$ and $S^{-1}R/S^{-1}I \cong \overline{S}^{-1}(R/I)$.*

In other words, localisation and taking quotients commutes under ring isomorphism.

Sketch of proof. $S^{-1}I$ being an ideal of $S^{-1}R$ is easily shown by using that I is an ideal of R. Define a map

$$f\colon S^{-1}R \to \overline{S}^{-1}(A/I),\ x/s \mapsto \overline{x}/\overline{s}$$

and show that it induces a map

$$\overline{f}\colon S^{-1}R/S^{-1}I \to \overline{S}^{-1}(A/I),\ \overline{x/s} \mapsto \overline{x}/\overline{s}.$$

Then use the map

$$R \to S^{-1}R/S^{-1}I,\ x \mapsto \overline{x/1}$$

to argue that we get a map

$$g\colon \overline{S}^{-1}(R/I) \to S^{-1}R/S^{-1}I,\ \overline{x}/\overline{s} \mapsto \overline{x/s}$$

and then observe that $\overline{f}$ and g are inverses of each other. □

See [7] for the whole proof.

So in our computations later we will use that

$$\left(\frac{k[x_1,\dots,x_n]}{I}\right)_{(x_1,\dots,x_n)} \cong \frac{k[x_1,\dots,x_n]_{(x_1,\dots,x_n)}}{I},$$

but note that the I on the right is not quite the same as the I on the left. Write $\tilde{I}$ for the I on the right side. $\tilde{I}$ is the ideal in the localisation $k[x_1,\dots,x_n]_{(x_1,\dots,x_n)}$ which is generated by $I \subseteq k[x_1,\dots,x_n]$, so

$$\tilde{I} = \{a/s \in k[x_1,\dots,x_n]_{(x_1,\dots,x_n)} \mid a \in I,\ s \in k[x_1,\dots,x_n] \setminus (x_1,\dots,x_n)\}.$$

Intuitively, since the localisation $k[x_1,\dots,x_n]_{(x_1,\dots,x_n)}$ can be understood as $k[x_1,\dots,x_n]$ with some additional inverse elements, $\tilde{I}$ can be thought of as I but in the localisation, so it must contain more elements to account for the extra elements in $k[x_1,\dots,x_n]_{(x_1,\dots,x_n)}$. Later on, we will drop the tilde in the notation, but we will have to keep track of which ring we are working in at any given time.

Chapter 4

Kass and Wickelgren's Method and Properties of it

Finally, we have the background theory needed to study the algorithm. We start this chapter with some definitions, then we present the method, and we go on to explore various properties of the algorithm. We continue by investigating which forms we can attain with the method in the case of finite fields, and finish with a few words about further questions regarding the method.

4.1 Definitions

Throughout this chapter we are considering polynomial functions $f\colon \mathbb{A}_k^n \to \mathbb{A}_k^n$. By $\mathbb{A}_k^n$ we mean the polynomial ring $k[x_1, \ldots, x_n]$ with the Zariski topology.

Definition 4.1. Let $f = (f_1, \ldots, f_n)\colon \mathbb{A}_k^n \to \mathbb{A}_k^n$ be a polynomial function, with component functions $f_1, \ldots, f_n \in k[x_1, \ldots, x_n]$. The *local algebra* of f at 0 is the k-algebra

$$Q_0(f) = \left(\frac{k[x_1, \ldots, x_n]}{(f_1, \ldots, f_n)} \right)_{(x_1, \ldots, x_n)}$$

where $(f_1, \ldots, f_n)$ is the ideal in $k[x_1, \ldots, x_n]$ generated by the f_i.

The 0 in the subscript of $Q_0(f)$ is due to the fact that we can more generally define the local algebra $Q_x(f)$ at any closed point $x \in \mathbb{A}_k^n$. Several of the other definitions in this section can also be extended to the general case $Q_x(f)$. But since we are only considering the local algebra at the origin here, we may simplify the notation by writing $Q \coloneqq Q_0(f)$ and will use a similar convention with other definitions in this section as well.

Note that Kass and Wickelgren define Q as

$$\frac{k[x_1,\dots,x_n]_{(x_1,\dots,x_n)}}{(f_1,\dots,f_n)}$$

but we already know from Proposition 3.21 that this expression is isomorphic to our definition. So since we will primarily work with Q by finding a basis for it and Theorem 3.17 gives us a basis via an isomorphism, it is clear that the two expressions for Q have the same basis up to isomorphism.

It should be noted, however, that Theorem 3.17 gives a basis of the quotient ring without the localisation. When we are searching for a basis and the localisation is included, it is not necessarily obvious that Theorem 3.17 still applies. It turns out it does still apply, but the proof is a bit lengthy. So we save it for a bit later, in order to get to the algorithm first.

Definition 4.2. Let $f\colon \mathbb{A}_k^n \to \mathbb{A}_k^n$ be a polynomial function with a zero at the origin. We say that the zero at 0 is *isolated* if the algebra Q has finite length.

Recall that the length of a finite chain of subspaces of Q of the form

$$0 = V_0 \subsetneq V_1 \subsetneq \dots \subsetneq V_n = Q$$

is n, and the length of Q is the maximum length among all such chains. If no such finite chain exists then Q has infinite length.

Note that if Q is not finitely generated and we try to build a chain

$$\mathrm{Span}_k\{v_1\} \subsetneq \mathrm{Span}_k\{v_1, v_2\} \subsetneq \dots$$

then we could never terminate the chain with $\mathrm{Span}_k\{v_1,\dots,v_n\} = Q$ for finitely many elements v_i, and so there are no finite chains of the above form. Hence if Q has finite length, then it must also be finitely generated and finite dimensional. And if Q is finite dimensional with basis $\{v_1,\dots,v_n\}$, then a maximal length chain is given by

$$0 \subsetneq \mathrm{Span}_k\{v_1,\} \subsetneq \mathrm{Span}_k\{v_1, v_2\} \subsetneq \dots \mathrm{Span}_k\{v_1,\dots,v_n\} = Q.$$

Hence Q has finite length if and only if it is finite dimensional. Since we are only considering polynomial functions with an isolated zero at 0, this guarantees that we are always working with a finite dimensional space and a finite basis.

Definition 4.3. Let $f = (f_1,\dots,f_n)\colon \mathbb{A}_k^n \to \mathbb{A}_k^n$ be a polynomial function. The *distinguished socle element* at the origin is

$$E = E_0(f) \coloneqq \det(a_{i,j}) \in Q$$

where the $a_{i,j} \in k[x_1,\dots,x_n]$ are polynomials such that for each $i = 1,\dots,n$ we have

$$f_i(x) = \sum_{j=1}^{n} a_{i,j}x_j$$

As the name implies, E is contained in the socle of Q and Lemma 4 in [4] tells us that E generates the socle when f has an isolated zero at the origin.

From the definition it is not very obvious that E is actually unique, since there can be multiple valid ways to write $f_i = \sum a_{ij}x_j$. However, we are considering E as an element of Q, and so a Gröbner basis division might be necessary to write E in terms of a basis of Q, and then it is unique.

Next up, if we have a k-linear function $\phi\colon Q \to k$, then

$$\beta_\phi\colon Q \times Q \to k,\ \beta_\phi(a_1, a_2) = \phi(a_1 \cdot a_2)$$

defines a symmetric bilinear form on Q. And Lemma 6 in [4] shows that β_ϕ is non-degenerate if $\phi(E) \neq 0$ and also that if ϕ_1 and ϕ_2 are two k-linear functions such that $\phi_1(E) = \phi_2(E)$ then $\beta_{\phi_1} \cong \beta_{\phi_2}$.

So once we know E, we can get an essentially unique bilinear form by just defining ϕ so that $\phi(E) \neq 0$. This motivates the final definition in this section:

Definition 4.4. The *Eisenbud-Khimshiashvili-Levine class*, or the *ELK class*, of f is the Grothendieck-Witt class

$$w = w_0(f) \coloneqq [(Q, \beta_\phi)] \in \mathrm{GW}(k)$$

where $\phi\colon Q \to k$ is any k-linear function such that $\phi(E) = 1$.

So for any $f\colon \mathbb{A}^n_k \to \mathbb{A}^n_k$ with an isolated zero at the origin, the resulting element $w \in \mathrm{GW}(k)$ is unique. In particular, since any valid choice of ϕ will do, we have a lot of freedom when deciding how to define ϕ. Since ϕ is going to be k-linear, it is enough to define ϕ on the elements of a basis of Q. And since we need $\phi(E) = 1$, it is only the basis elements that occur in E that give us any restrictions on what ϕ can be. Any basis elements that do not occur in E can be defined to be anything, and to make the computations as simple as possible we will favour having ϕ evaluate to 0 on as many basis elements as possible.

Immediately, there is an interesting observation we can make here. Kass and Wickelgren note that the socle is the annihilator of $(x_1, \ldots, x_n) \subseteq Q$ [4, Remark 2]. They further note that when f has an isolated zero at the origin, E generates the socle [4, Lemma 4]. So in our computations we always have that the socle of Q is the ideal $(E) = E \cdot Q$. In particular, this means that for all i we have $E \cdot x_i = 0$ in Q, which means $E \cdot x_i \in (f_1, \ldots, f_n) \subseteq k[x_1, \ldots, x_n]_{(x_1,\ldots,x_n)}$.

Now, if $E \in Q$ has a non-zero constant term, then it is a unit in Q and then for all i,

$$E \cdot x_i = 0 \in Q \implies x_i = 0 \in Q.$$

This means that $(x_1, \ldots, x_n) \subseteq (f_1, \ldots, f_n)$ in $k[x_1, \ldots, x_n]_{(x_1,\ldots,x_n)}$. And since $(x_1, \ldots, x_n)$ is a maximal ideal, we get $(x_1, \ldots, x_n) = (f_1, \ldots, f_n)$ in $k[x_1, \ldots, x_n]_{(x_1,\ldots,x_n)}$. The result is that Q is one-dimensional.

Now, using contrapositive, we get that if $\dim_k Q \geq 2$ then E must have constant term 0. So whenever the dimension of Q is at least 2, we are always free to map the basis element 1 to anything we want.

4.2 The method for computing the ELK class

Since the aim of the algorithm is to start with a polynomial $f\colon \mathbb{A}_k^n \to \mathbb{A}_k^n$ that has an isolated zero at 0 and end up with an element in $\mathrm{GW}(k)$, the definitions in the previous section actually provide a pretty good intuition for what should happen in the algorithm.

The method is as follows:

Computing the ELK class

Input: a polynomial $f\colon \mathbb{A}_k^n \to \mathbb{A}_k^n$ with an isolated zero at the origin:

(i) Compute a Gröbner basis for the ideal $I = (f_1, \ldots, f_n)$

(ii) Compute a k-basis $\mathcal{B} = \{b_1, \ldots, b_t\}$ for the vector space Q

(iii) Compute $E \in Q$ and express it in terms of the k-basis

(iv) Explicitly define a k-linear function $\phi : Q \to k$ such that $\phi(E) = 1$

(v) For each pair $b_i, b_j \in \mathcal{B}$, express $b_i \cdot b_j$ in terms of the k-basis, and then evaluate $\phi(b_i \cdot b_j)$

(vi) Construct the matrix

$$\begin{bmatrix} \phi(b_1 \cdot b_1) & \cdots & \phi(b_1 \cdot b_t) \\ \vdots & \ddots & \vdots \\ \phi(b_t \cdot b_1) & \cdots & \phi(b_t \cdot b_t) \end{bmatrix}$$

and use operations that respect isometry to bring it to a diagonal form $\langle a_1, \ldots, a_t \rangle$

Output: an element $w = \langle a_1, \ldots, a_t \rangle \in \mathrm{GW}(k)$

A useful thing we can notice immediately is that $\dim_k(Q) = \dim_k(w)$. Because, for example, if are trying to find a polynomial such that a given form has a certain dimension, then Q must have the same dimension. This gives us a restriction on what the polynomial can be.

Note also that to construct the matrix at the end, we need to choose an ordering on the basis of Q. But since we are working with isometry classes, we can use simultaneous row and column operations. Then by using swapping of rows, we

get that any ordering on the basis produces the same isometry class. Hence we can just choose whatever ordering on the basis that we want.

We now return to a point that we touched upon in the previous section, namely the issue of whether we can apply Theorem 3.17 to find a basis of Q, since there is a localisation involved. The solution turns out to be the following:

Theorem 4.5. *Let $f = (f_1, \ldots, f_n)\colon \mathbb{A}_k^n \to \mathbb{A}_k^n$ be a polyomial with an isolated zero at the origin. Then there is an ideal $(f_1, \ldots, f_n) \subseteq J \subseteq k[x_1, \ldots, x_n]$ such that*

$$\left(\frac{k[x_1, \ldots, x_n]}{(f_1, \ldots, f_n)}\right)_{(x_1,\ldots,x_n)} \cong \frac{k[x_1, \ldots, x_n]}{J}.$$

Proof. If $k[x_1, \ldots, x_n]/(f_1, \ldots, f_n)$ is a local ring, then just set $J = (f_1, \ldots, f_n)$. So suppose $k[x_1, \ldots, x_n]/(f_1, \ldots, f_n)$ is not local. Since f has an isolated zero at the origin, we know that $Q = (k[x_1, \ldots, x_n/(f_1, \ldots, x_n))_{(x_1,\ldots,x_n)}$ is finite dimensional. And since

$$\left(\frac{k[x_1, \ldots, x_n]}{(f_1, \ldots, f_n)}\right)_{(x_1,\ldots,x_n)} \cong \frac{k[x_1, \ldots, x_n]_{(x_1,\ldots,x_n)}}{(f_1, \ldots, f_n)}$$

we have that the RHS is also finite dimensional.

Using the finite dimensionality, we have that for each $i \in \{1, \ldots, n\}$ there must exist a large enough N such that $\{x_i, x_i^2, \ldots, x_i^N\}$ is a linearly dependent set in $k[x_1, \ldots, x_n]_{(x_1,\ldots,x_n)}/(f_1, \ldots, f_n)$. So there are some $a_1, a_2, \ldots, a_N \in k$, not all zero, such that

$$\begin{aligned} & a_1x_i + a_2x_i^2 + \ldots + a_Nx_i^N = 0 \text{ in } \frac{k[x_1, \ldots, x_n]_{(x_1,\ldots,x_n)}}{(f_1, \ldots, f_n)} \\ \implies & a_1x_i + a_2x_i^2 + \ldots + a_Nx_i^N \in (f_1, \ldots, f_n) \subseteq k[x_1, \ldots, x_n]_{(x_1,\ldots,x_n)}. \end{aligned}$$

Since not all of the coefficients are zero, there is a smallest m such that $a_m \neq 0$. Then write

$$a_mx_i^m + a_{m+1}x_i^{m+1} + \ldots + a_Nx_i^N = x_i^m(a_m + a_{m+1}x_i + \ldots + a_Nx_i^{N-m})$$

and since $a_m \neq 0$, we have that $a_m + a_{m+1}x_i + \ldots + a_Nx_i^{N-m}$ is a polynomial with a non-zero constant term. This means it is not in the ideal $(x_1, \ldots, x_n)$ and so it has an inverse in the localisation $k[x_1, \ldots, x_n]_{(x_1,\ldots,x_n)}$. Multipliying by this inverse we hence get that

$$x_i^m \in (f_1, \ldots, f_n) \subseteq k[x_1, \ldots, x_n]_{(x_1,\ldots,x_n)}.$$

Doing this for all $i \in \{1, \ldots, n\}$, we get integers $m_1, \ldots, m_n > 0$ such that

$$x_1^{m_1}, x_2^{m_2}, \ldots, x_n^{m_n} \in (f_1, \ldots, f_n) \subseteq k[x_1, \ldots, x_n]_{(x_1,\ldots,x_n)}$$

and then we have

$$\begin{aligned}\left(\frac{k[x_1,\ldots,x_n]}{(f_1,\ldots,f_n)}\right)_{(x_1,\ldots,x_n)} &\cong \frac{k[x_1,\ldots,x_n]_{(x_1,\ldots,x_n)}}{(f_1,\ldots,f_n)} \\ &= \frac{k[x_1,\ldots,x_n]_{(x_1,\ldots,x_n)}}{(f_1,\ldots,f_n,x_1^{m_1},\ldots,x_n^{m_n})} \\ &\cong \left(\frac{k[x_1,\ldots,x_n]}{(f_1,\ldots,f_n,x_1^{m_1},\ldots,x_n^{m_n})}\right)_{(x_1,\ldots,x_n)}\end{aligned}$$

and if now $k[x_1,\ldots,x_n]/(f_1,\ldots,f_n,x_1^{m_1},\ldots,x_n^{m_n})$ is a local ring, then we are done by setting $J=(f_1,\ldots,f_n,x_1^{m_1},\ldots,x_n^{m_n})$.

To simplify notation, write

$$R=\frac{k[x_1,\ldots,x_n]}{(f_1,\ldots,f_n,x_1^{m_1},\ldots,x_n^{m_n})}$$

and we now want to show that R is local. Note first that $(x_1,\ldots,x_n)$ is a maximal ideal of $k[x_1,\ldots,x_n]$ and it contains $(f_1,\ldots,f_n,x_1^{m_1},\ldots,x_n^{m_n})$. So $(x_1,\ldots,x_n)$ is also a maximal ideal of R.

Now let $\mathfrak{m}$ be any maximal ideal of R, so it is also maximal in $k[x_1,\ldots,x_n]$ and it contains $(f_1,\ldots,f_n,x_1^{m_1},\ldots,x_n^{m_n})$. In particular, we have $x_1^{m_1}\in\mathfrak{m}$ and since maximal ideals are also prime ideals, we get $x_1\in\mathfrak{m}$. We similiarly get $x_2,\ldots,x_n\in\mathfrak{m}$, and so $(x_1,\ldots,x_n)\subseteq\mathfrak{m}$. But since $(x_1,\ldots,x_n)$ is maximal we must have $\mathfrak{m}=(x_1,\ldots,x_n)$. Hence $(x_1,\ldots,x_n)$ is the only maximal ideal in R, so R is local. □

So Q is always isomorphic to a quotient ring without localisation, and so we can apply any of our techniques about polynomial quotient rings to Q, in particular finding a basis.

As for how we find the m_i, it is beneficial first to compute a Gröbner basis $\mathcal{G}$ of $(f_1,\ldots,f_n)\subseteq k[x_1,\ldots,x_n]$, meaning we do this before going through the isomorphism to $(f_1,\ldots,f_n)\subseteq k[x_1,\ldots,x_n]_{(x_1,\ldots,x_n)}$. Since Q is finite dimensional, we know that for each i, there is an integer $m_i\geq 0$ such that $x_i^{m_i}=\mathrm{LT}(g)$ for some $g\in\mathcal{G}$. Then when we use the isomorphism, we get $x_i^{m_i}\in(f_1,\ldots,f_n)\subseteq k[x_1,\ldots,x_n]_{(x_1,\ldots,x_n)}$.

But unfortunately, this is not a complete answer. Because even though we may have $x_i^{m_1}\in(f_1,\ldots,f_n)\subseteq k[x_1,\ldots,x_n]$, there are cases where we can find $m_i'<m_i$ such that $x_i^{m_i'}\in(f_1,\ldots,f_n)\subseteq k[x_1,\ldots,x_n]_{(x_1,\ldots,x_n)}$. If we just went with m_i, we would end up with the wrong dimension of Q.

This can happen if there is a polynomial in $(f_1,\ldots,f_n)$ that has a polynomial with non-zero constant term as a factor. For example,

$$x_1^5+x_1^3=x_1^3(x_1^2+1)$$

and in the localisation, $x_1^2 + 1$ is a unit. So if $x_1^5 + x_1^3 \in (f_1, \ldots, f_n)$ then we would get $x_1^3 \in (f_1, \ldots, x_n)$ and this would not necessarily be visible in the Gröbner basis that was computed earlier.

Unfortunately, we do not currently have a general technique for ensuring that we find the minimal m_i. But if we do end up with a basis of Q that is too large, then what seems to happen is that the bilinear form at the end is degenerate. So at least that should give a clue that there is a bit more work to be done in finding the correct basis. And the m_i we get from the Gröbner basis do give a baseline to work with, as we could play around with the ideal to see if we are able to find smaller values of m_i.

4.3 Properties of the method

Now we are ready to explore the algorithm and identify some properties. First, one thing we can ask is if there are some general types of polynomials $f\colon \mathbb{A}_k^n \to \mathbb{A}_k^n$ for which the computation of w follows a predictable pattern. We start with one example that builds off our observations from Section 4.1 about the element $E \in Q$:

Lemma 4.6. *Let $f = (f_1, \ldots, f_n)\colon \mathbb{A}_k^n \to \mathbb{A}_k^n$ be so that $f(0) = 0$ and so that for each i we have that $f_i \in k[x_1, \ldots, x_n]$ is a polynomial only in x_i,*

$$f_i = a_{i,m_i} x_i^{m_i} + a_{i,m_i-1} x_i^{m_i-1} + \ldots + a_{i,1} x_i.$$

Then Q is 1-dimensional and

$$w = \langle \prod_{i=1}^{n} a_{i,1} \rangle$$

Proof. Without even getting into Gröbner bases, we can immediately see that for each i we can write

$$f_i = (a_{i,m_i} x_i^{m_i-1} + a_{i,m_i-1} x_i^{m_i-2} + \ldots + a_{i,1}) \cdot x_i = b_i x_i$$

so then we get

$$\begin{aligned} E &= \det \begin{bmatrix} b_1 & 0 & \cdots & 0 \\ 0 & b_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & b_n \end{bmatrix} \\ &= \prod_{i=1}^{n} (a_{i,m_i} x_i^{m_i-1} + a_{i,m_i-1} x_i^{m_i-2} + \ldots + a_{i,1}). \end{aligned}$$

and when we expand the product one of the terms is $a \coloneqq \prod_{i=1}^n a_{i,1}$ which is a non-zero constant. So then Q is 1-dimensional and E reduces to $E = a$. Then define $\phi\colon Q \to k$ by $1 \mapsto 1/a$. Then

$$w = \langle \phi(1 \cdot 1) \rangle = \langle \phi(1) \rangle = \langle 1/a \rangle \cong \langle a \rangle = \langle \prod_{i=1}^n a_{i,1} \rangle.$$

□

Lemma 4.7. *Fix a monomial ordering. If $f = (f_1, \dots, f_n)\colon \mathbb{A}_k^n \to \mathbb{A}_k^n$ is such that*

- *f has an isolated zero at the origin*
- *$\{f_1, \dots, f_n\}$ is a Gröbner basis of the ideal $(f_1, \dots, f_n)$*
- *for each i, we have $x_i \mid f_i$*
- *the localisation in Q is trivial*
- *$\mathrm{LT}(f_i) = a_i x_i^{m_i}$*

then write $m = \prod_{i=1}^n m_i$ $a = \prod_{i=1}^n a_{i,m_i}$, and then

$$w = \begin{cases} \frac{m}{2}\mathbb{H} & \text{if } m \text{ is even} \\ \frac{m-1}{2}\mathbb{H} \perp \langle a \rangle & \text{if } m \text{ is odd} \end{cases}$$

Proof. We have

$$\begin{aligned} Q &\cong \frac{k[x_1, \dots, x_n]}{(f_1, \dots, f_n)} \\ &\cong \mathrm{Span}_k\{x^\alpha \mid x^\alpha \notin (\mathrm{LT}(f_1, \dots, f_n)\} \\ &= \mathrm{Span}_k\{x^\alpha \mid x^\alpha \notin (x_1^{m_1}, \dots, x_n^{m_n})\} \\ &= \mathrm{Span}_k\{x^\alpha \mid \alpha = (\alpha_1, \dots, \alpha_n) \text{ where } \alpha_i < m_i \text{ for all } i = 1, \dots, n\} \end{aligned}$$

and note that $\dim_k Q = \prod_{i=1}^n m_i = m < \infty$. Since $x_i \mid f_i$ for all i we can write $f_i = (a_{i,m_i} x_i^{m_i - 1} + \dots) \cdot x_i$. So then we get

$$\begin{aligned} E &= \det \begin{bmatrix} (a_{1,m_1} x_1^{m_1-1} + \dots) & 0 & \cdots & 0 \\ 0 & (a_{2,m_2} x_2^{m_2-1} + \dots) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & (a_{n,m_n} x_n^{m_n-1} + \dots) \end{bmatrix} \\ &= \prod_{i=1}^n (a_{i,m_i} x_i^{m_i-1} + \dots) = \prod_{i=1}^n a_{i,m_i} x_i^{m_i-1} + [\text{lower terms}] \end{aligned}$$

So this is a polynomial in Q with leading term

$$\prod_{i=1}^{n} a_{i,m_i} x_i^{m_i-1} = \prod_{i=1}^{n} a_{i,m_i} \prod_{i=1}^{n} x_i^{m_i-1} = a \cdot x_1^{m_1-1} x_2^{m_2-1} \cdots x_n^{m_n-1}.$$

We define a k-linear function $\phi\colon Q \to k$ by

$$\phi(x^\alpha) = \begin{cases} \frac{1}{a} & \text{if } \alpha = (m_1 - 1, m_2 - 1, \ldots, m_n - 1) \\ 0 & \text{otherwise} \end{cases}$$

and if we choose to order the basis of Q so that $x_1^{m_1-1} x_2^{m_2-1} \cdots x_n^{m_n-1}$ is last, the resulting $m \times m$ matrix corresponding to w is of the form

$$\begin{bmatrix} 0 & & 1/a \\ & \iddots & \\ 1/a & & 0 \end{bmatrix}$$

If m is even then by using simultaenous row and column operations and our knowledge about $\mathbb{H}$, we get

$$\begin{bmatrix} 0 & & & & & & 1/a \\ & & & & & \iddots & \\ & & & & 1/a & & \\ & & & 1/a & & & \\ & & \iddots & & & & \\ 1/a & & & & & & 0 \end{bmatrix} \cong \begin{bmatrix} 2/a & & & & & & 0 \\ & \ddots & & & & & \\ & & 2/a & & & & \\ & & & -1/2a & & & \\ & & & & & \ddots & \\ 0 & & & & & & -1/2a \end{bmatrix}$$
$$= \langle 2/a, \ldots, 2/a, -1/2a, \ldots, -1/2a \rangle$$
$$\cong \langle 2a, \ldots, 2a, -2a, \ldots, -2a \rangle$$
$$\cong \frac{m}{2}\mathbb{H}$$

If m is odd, then essentially the same operations will work, except for the fact that there is a term in the $(\frac{m+1}{2}, \frac{m+1}{2})$-th entry which will be unaffected while the rest of the matrix is brought to diagonal form. We hence end up with

$$\begin{aligned} \langle 2/a, \ldots, 2/a, 1/a, -1/2a, \ldots, -1/2a \rangle &\cong \langle 2a, \ldots, 2a, a, -2a, \ldots, -2a \rangle \\ &\cong \langle 2a, \ldots, 2a, -2a, \ldots, -2a, a \rangle \\ &\cong \langle 2a, \ldots, 2a, -2a, \ldots, -2a \rangle \perp \langle a \rangle \\ &\cong \frac{m-1}{2}\mathbb{H} \perp \langle a \rangle \end{aligned}$$

□

Singularity	g	$\text{grad}(g)$
A_n, n odd	$x_1^2 + x_2^{n+1}$	$(2x_1, (n+1)x_2^n)$
A_n, n even	$x_1^2 + x_2^{n+1}$	$(2x_1, (n+1)x_2^n)$
E_6	$x_1^3 + x_2^4$	$(3x_1^2,\ 4x_2^3)$
E_8	$x_1^3 + x_2^5$	$(3x_1^2,\ 5x_2^4)$

Singularity	Gröbner basis	w
A_n, n odd	$x_1,\ x_2^4$	$\frac{n-1}{2}\mathbb{H} \perp \langle 2(n+1) \rangle$
A_n, n even	$x_1,\ x_2^4$	$\frac{n}{2}\mathbb{H}$
E_6	$x_1^2,\ x_2^3$	$3\mathbb{H}$
E_8	$x_1^2,\ x_2^4$	$4\mathbb{H}$

Table 4.1: Some of the computations from [4]

This case may sound awfully specific, but interestingly this lemma actually covers several of the examples that Kass and Wickelgren did. In [4], they ran the algorithm with $f = \text{grad}(g)$ where g is a polynomial equation of the ADE singularities. Specifically, the results for A_n, E_6, and E_8 matches the description in this lemma. Table 4.1 shows some of the details from those computations.

We also have the following, which is a kind of variation on Lemma 4.7:

Lemma 4.8. *Suppose $k[x_1, \ldots, x_n]$ has the lexicographic ordering, and $f = (f_1, \ldots, f_n) \colon \mathbb{A}_k^n \to \mathbb{A}_k^n$ is so that*

- *f has an isolated zero at the origin*
- *$\{f_1, \ldots, f_n\}$ is a Gröbner basis of the ideal $(f_1, \ldots, f_n)$*
- *the localisation in Q is trivial*
- $\text{LT}(f_i) = a_i x_i^{m_i}$

then we get

$$w = \begin{cases} \frac{m}{2}\mathbb{H} & \text{if } m \text{ is even} \\ \frac{m-1}{2}\mathbb{H} \perp \langle a \rangle & \text{if } m \text{ is odd} \end{cases}$$

where $m = \prod_{i=1}^n m_i$ and $a = \prod_{i=1}^n a_i$.

Proof. This proof is very similar to the previous one. The only significant difference is the computation of E. For each i, we have

$$f_i = a_i x_i^{m_i} + [\text{lower terms}]$$

and recall that with the lex ordering, a variable completely dominates term that only contain "smaller" variables. Because of this, the assumption that

$\mathrm{LT}(f_i) = a_i x_i^{m_i}$ means that f_i can not contain any terms with any variables x_j such that $j < i$. This means that when we compute E, we get

$$E = \det \begin{bmatrix} (a_{1,m_1} x_1^{m_1-1} + \ldots) & \bullet & \cdots & \bullet \\ 0 & (a_{2,m_2} x_2^{m_2-1} + \ldots) & \cdots & \bullet \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & (a_{n,m_n} x_n^{m_n-1} + \ldots) \end{bmatrix}$$

where it does not matter what is in the entries over the diagonal. This E evaluates to essentially the same expression as in Lemma 4.7. The leading term is $a \cdot x_1^{m_1-1} x_2^{m_2-1} \cdots x_n^{m_n-1}$ where $a = \prod_{i=1}^{n} a_i$. The rest of the proof is exactly like Lemma 4.7. □

Up until now in this section we considered a few somewhat general polynomials and computed their associated bilinear forms generally. It seems likely that there could exist other generalisations for some choices of f.

But now we are interested in trying to go the other way. Namely if we start with a bilinear form, can we find a polynomial f so that applying the method to f yields the given bilinear form? Or more generally, which elements in $\mathrm{GW}(k)$ can we attain with the method by choosing f well?

This actually depends on the field k, and if k algebraically closed, this is easy:

Theorem 4.9. *Let k be algebraically closed. Then there is one isometry class of dimension n in $\mathrm{GW}(k)$, and we can attain this form with $f = x^n$.*

Proof. Every non-zero element in k is a square, so for all $a_i \in k^\times$ we have $\langle a_1, \ldots, a_n \rangle \cong \langle 1, \ldots, 1 \rangle \cong n\langle 1 \rangle$. So to attain this form, we just need any function that produces an n-dimensional form. It is easy to verify that $f = x^n$ accomplishes this. □

If k is not algebraically closed, then this problem immediately becomes much more complicated. For example, for $k = \mathbb{R}$, a non-zero number is either a positive square a^2 or a negative square $-a^2$. For 1-dimensional forms this is okay, as $f = x$ yields $\langle 1 \rangle$ and $f = -x$ yields $\langle -1 \rangle$. But for dimensions higher than 1, we have $\langle a_1, \ldots, a_n \rangle \cong p\langle 1 \rangle \perp q\langle -1 \rangle$ for some integers $0 \leq p, q \leq n$ such that $p + q = n$. Note that if, say, $p < q$, then $p\langle 1 \rangle \perp q\langle -1 \rangle \cong p\mathbb{H} \perp (q-p)\langle -1 \rangle$.

Over an algebraically closed field, we had $\mathbb{H} \cong \langle 1, 1 \rangle$. The moment k is not algebraically closed, $\mathbb{H}$ does not vanish quite as easily. As a matter of fact, for dimensions ≥ 2 we will always end up with at least one hyperbolic plane:

Theorem 4.10. *If $\dim_k(Q) \geq 2$, then w has $\mathbb{H}$ as an orthogonal summand.*

Proof. Recall from Theorem 2.24, that if w is isotropic, then it has $\mathbb{H}$ as an orthogonal summand. So we only need to show that there is a non-zero element $a \in Q$ such that $w(a, a) = 0$.

Pick 1 as a basis element and write $Q \cong \text{Span}_k\{1, b_2, \ldots, b_n\}$. We have

$$E = a_1 \cdot 1 + a_2 b_2 + \ldots + a_n b_n \in Q$$

for some $a_i \in k$. We earlier saw that $a_1 \neq 0$ implies that Q is 1-dimensional, but we have assumed that $\dim_k(Q) \geq 2$, and so we must have $a_1 = 0$. The basis element 1 does not appear in E and so when we define $\phi \colon Q \to k$, we can define $\phi(1)$ to be whatever we want. Let $\phi(1) = 0$. Then

$$w(1, 1) = \phi(1 \cdot 1) = \phi(1) = 0$$

hence w is isotropic. □

So in any field, if the dimension of Q is at least 2, then we have at least one hyperbolic plane in w. Interestingly, when $\dim_k(Q) = 2$ this theorem essentially tells us that we can only get $\mathbb{H}$. So any 2-dimensional form that is not isometric to $\mathbb{H}$ is unattainable.

But even with this result, determining more information about the attainability of forms over fields that are not algebraically closed is still a big task. For $k = \mathbb{R}$, this theorem really only tells us that the restriction on p and q has changed from $0 \leq p, q \leq n$ to $1 \leq p, q \leq n$. If we want a more complete answer we need a better overview of forms over k.

4.4 Finite fields $\mathbb{F}_q$

When $k = \mathbb{F}_q$ is a finite field, we have some results that can help us work out which of the bilinear forms can occur. Therefore, we are now going to determine completely which isometry classes of bilinear forms over $\mathbb{F}_q$ are attainable. We will also provide examples of polynomials that produce each of the forms when we run the algorithm on them.

Before we start, there are a couple of things to mention. First off, we are now considering $k = \mathbb{F}_q$ where $q = p^m$ and p is a prime number. But since we, as always, are not considering fields of characteristic 2, p will always be an odd prime.

The other thing to mention is that this section originally started out merely as a study of $\mathbb{F}_3$, with the hope of learning as much as we could about how the algorithm behaves here. But while working through the dimensions, we observed that the arguments and the polynomials were applicable more generally. Hence this section became what it is now.

Now, the first result that will help us is Lemma 2.31, which states that $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2$ consists of 2 elements, which we will denote by 1 and ε. Recall also that for any bilinear forms over a field, the discriminant of the form is an element of the field's group of square classes. So for any form over $\mathbb{F}_q$, its discriminant is either 1 or ε.

We are also going to make use of Theorem 2.32, which tells us a few things. The first part of the theorem says that any bilinear space over $\mathbb{F}_q$ of dimension ≥ 3 is isotropic. This is exactly what Theorem 4.10 tells us for a general field k, so this confirms that from dimension 2 and onwards we will always expect to see $\mathbb{H}$.

Theorem 2.32 also states that two bilinear forms over $\mathbb{F}_q$ are isometric if and only if they have the same dimension and the same discriminant. And the last part of the theorem says that there are precisely two isometry classes of regular n-dimensional bilinear spaces over $\mathbb{F}_q$. These two points essentially gives us a strategy to follow in our computations. Namely that we will consider one dimension at a time, and in each dimension we are looking for two isometry classes.

If we fix the dimension, then two bilinear forms are isometric if and only if they have the same discriminant. So since we have two possible values for the discriminant, this is where we get that there are two isometry classes per dimension. In other words, in each dimension there is one isometry class corresponding to the discriminant 1 and one class corresponding to ε.

Now we are ready to do the computations. Let $n = \dim_k w$.

$\underline{n=1}$: $f = ax \in \mathbb{F}_q[x]$ yields $\langle a \rangle$ so choosing $a = 1$ or $a = \varepsilon$ we can get either class. Note that this polynomial works over any field, as no matter how many isometry classes there are you can just choose a appropriately to get each of them.

$\underline{n=2}$: We have already shown that any 2-dimensional bilinear form acquired through the algorithm must have $\mathbb{H}$ as summand. Then as $\langle 1,1\rangle \ncong \langle 1,\varepsilon\rangle$, it is not possible to obtain $\langle 1,1\rangle$ through the algorithm. On the other hand, this also means that any polynomial will result in $\langle 1,\varepsilon\rangle \cong \mathbb{H}$. But to provide an explicit example, $f = x^2 \in \mathbb{F}_q[x]$ gets the job done.

$\underline{n=3}$: Take $f = ax^3 \in \mathbb{F}_q[x]$ and then since there is no need to search for Gröbner bases when there is only one variable, we get immediately that $Q \cong \mathrm{Span}_k\{1, x, x^2\}$ and $E = ax^2$. So we define

$$\phi\colon Q \to \mathbb{F}_q,\ \phi(x^s) = \begin{cases} 1/a & s = 2 \\ 0 & \text{otherwise} \end{cases}$$

Then we get

$$w = \begin{bmatrix} 0 & & 1/a \\ & 1/a & \\ 1/a & & 0 \end{bmatrix} \cong \langle 2/a, 1/a, -1/2a \rangle \cong \langle 2a, -2a, a \rangle \cong \mathbb{H} \perp \langle a \rangle$$

and as expected we get a hyperbolic plane here. Like the $n = 1$ case, we get the isometry classes by choosing $a = 1$ or $a = \varepsilon$. Note, however, that $a = 1$ makes the resulting isometry class have discriminant ε and $a = \varepsilon$ gives the class discriminant 1.

$\underline{n = 4}$: Let $f = (xy, x^2 + by^2) \in \mathbb{F}_q[x, y]$. With respect to the lexicographic ordering, a Gröbner basis of $(xy, x^2 + by^2)$ is given by $\{xy, x^2 + by^2, y^3\}$. Then we get $Q \cong \mathrm{Span}_k\{1, y, y^2, x\}$ and

$$E = \det \begin{bmatrix} y & 0 \\ x & by \end{bmatrix} = by^2.$$

So define $\phi\colon Q \to \mathbb{F}_q$ by letting $\phi(y^2) = 1/b$ and by letting ϕ evaluate to 0 on the other basis elements. Note that $\phi(x^2) = \phi(-by^2) = -b\phi(y^2) = -b\frac{1}{b} = -1$. Then we get

$$\begin{aligned} w = \begin{bmatrix} 0 & 0 & 1/b & 0 \\ 0 & 1/b & 0 & 0 \\ 1/b & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} &\cong \langle 2/b, 1/b, -1/2b, -1 \rangle \\ &\cong \langle 2b, -2b, -1, b \rangle \\ &\cong \mathbb{H} \perp \langle -1, b \rangle. \end{aligned}$$

In this case we get discriminant 1 by setting $b = 1$ and we get ε by setting $b = \varepsilon$.

As we will see next, the computations for $n = 3$ and $n = 4$ can actually be generalised, so with just two more computations we can cover all the remaining dimensions.

$\underline{n \geq 3 \text{ odd}}$: We want to extend the computation from $n = 3$ so that it works for all odd numbers ≥ 3. So let $f = ax^n \in k[x]$. We get $Q \cong \mathrm{Span}_k\{1, x, x_2 \ldots, x_{n-1}\}$ and $E = ax^{n-1}$, so define

$$\phi\colon Q \to \mathbb{F}_3,\ \phi(x^s) = \begin{cases} 1/a & s = n - 1 \\ 0 & \text{otherwise} \end{cases}$$

and then we get

$$w = \begin{bmatrix} 0 & & 1/a \\ & \iddots & \\ 1/a & & 0 \end{bmatrix} \cong \langle 2/a, \dots, 2/a, 1/a, -1/2a, \dots, -1/2a \rangle$$
$$\cong \langle 2a, \dots, 2a, -2a, \dots, -2a, a \rangle$$
$$\cong \frac{n-1}{2}\mathbb{H} \perp \langle a \rangle$$

and once again $a = 1$ and $a = \varepsilon$ produce each of the isometry classes. Which discriminant the forms have, though, depends on n. If $\frac{n-1}{2}$ is even, then $a = 1$ gives the form discriminant 1 and $a = \varepsilon$ gives discriminant ε. If $\frac{n-1}{2}$ is odd, then it is just the other way around.

$\underline{n \geq 4 \text{ even:}}$ Similarly to the previous case, we want to use a more general version of the $n = 4$ case, so let $f = (xy, x^2 + by^{n-2})$. Again using the lexicographic ordering, we get that a Gröbner basis of $(xy, x^2 + by^{n-2})$ is given by $\{xy, x^2 + by^{n-2}, y^{n-1}\}$. Then $Q \cong \text{Span}_k\{1, y, y^2, \dots, y^{n-2}, x\}$ and $E = by^{n-2}$, so we define

$$\phi \colon Q \to \mathbb{F}_q,\ \phi(x) = 0 \text{ and } \phi(y^s) = \begin{cases} 1/b & s = n-2 \\ 0 & \text{otherwise} \end{cases}$$

and then we get

$$w = \begin{bmatrix} 0 & \cdots & 1/b & 0 \\ \vdots & \iddots & \iddots & \vdots \\ 1/b & \iddots & 0 & 0 \\ 0 & \cdots & 0 & -1 \end{bmatrix} \cong \langle 2/b, \dots, 2/b, 1/b, -1/2b, \dots, -1/2b, -1 \rangle$$
$$\cong \langle 2b, \dots, 2b, -2b, \dots, -2b, -1, b \rangle$$
$$\cong \frac{n-2}{2}\mathbb{H} \perp \langle -1, b \rangle$$

and once again choosing $b = 1$ or $b = \varepsilon$ produces the isometry classes. If $\frac{n-2}{2}$ is even, then $b = 1$ gives discriminant ε and $b = \varepsilon$ gives discriminant 1. If $\frac{n-2}{2}$ is odd, then it is the other way around.

And with that we now have an overview over which isometry classes over $\mathbb{F}_q$ can be attained using the algorithm, and we also have some polynomials that produce each class. Table 4.2 demonstrates the first ten dimensions of this with the polynomials written out explicitly.

We have investigated the attainability of the isometry classes of bilinear forms over $\mathbb{F}_k$ using the algorithm. But we could also ask about attainability of just the bilinear forms directly. For example, in dimension 1 we used ax to get the form $\langle a \rangle$. We only needed $a = 1$ and $a = \varepsilon$ above to know that both isometry

$\dim_k(w)$	1	ε	$\dim_k(w)$	1	ε
1	x	εx	2	n/a	x^2
3	εx^3	x^3	4	$(xy, x^2 + y^2)$	$(xy, x^2 + \varepsilon y^2)$
5	x^5	εx^5	6	$(xy, x^2 + \varepsilon y^4)$	$(xy, x^2 + y^4)$
7	εx^7	x^7	8	$(xy, x^2 + y^6)$	$(xy, x^2 + \varepsilon y^6)$
9	x^9	εx^9	10	$(xy, x^2 + \varepsilon y^8)$	$(xy, x^2 + y^8)$

Table 4.2: Table of polynomials that produce forms of discriminant 1 and ε

classes are covered. But since we can just choose any non-zero value of $a \in \mathbb{F}_q$, we can explicitly get every 1-dimensional form over $\mathbb{F}_q$ via choices of a.

Since a bilinear form over $\mathbb{F}_q$ will be contained in one of the two isometry classes, we can naturally get the form by using a polynomial that lands in the correct isometry class and then just reach the form through isometry. But it still seems like an interesting question to explore.

In dimension 2 there is not much to do. We know that we need a hyperbolic space as an orthogonal summand, but in 2 dimensions we do not have room for anything else after that. So this case is very much done.

For 3 dimensions we used ax^3 to get $\mathbb{H} \perp \langle a \rangle$. Now even though we are in 3 dimensions now, we must have the hyperbolic plane and it occupies two of the coordinates. So we only have one slot to experiment with, and clearly this functions just like the 1-dimensional case. Once again, making choices on a will again allow us to get any form. More precicely, any form with $\mathbb{H}$ as a summand.

At a glance, it might seem like we are in trouble in 4 dimensions. We used $(xy, x^2 + by^2)$ to get $\mathbb{H} \perp \langle -1, b \rangle$. A hyperbolic plane will occupy two of the entries, but that should leave us with two entries that we would want to be free to explore. So currently, the -1 seems like a bit of an obstruction to this. Fortunately, we only need to do a slight modification in this case. If we instead use $f = (xy, ax^2 + by^2)$, then a similar calculation as earlier will yield $\mathbb{H} \perp \langle -a, b \rangle$. Then we are once again free to put in any non-zero field elements that we want so we can get any form here.

In dimensions 5 and higher, however, we really are in trouble. The computation in dimension 5 will give us $2\mathbb{H} \perp \langle a \rangle$. As before, the last entry a can be anything non-zero and we know that we must have a copy of $\mathbb{H}$. But currently we have two hyperbolic planes, and we do not know if we can get rid of one of them by choosing a polynomial in a clever way and then doing the algorithm with it. So we do not know if we are able to free up two of the entries, and so we are presently not able to say if any 5-dimensional form (with one $\mathbb{H}$ as summand) can be realised directly from the choice of polynomial. This problem clearly extends to dimensions higher than 5, too.

Instead, we finish this section with a different observation. In our computations in odd dimensions we used the polynomial ax^n and we ended up with as many copies of $\mathbb{H}$ as we can fit in the form, and the last entry was determined by a. If we also use the method on ax^n in even dimensions we get only copies of $\mathbb{H}$. So interestingly, ax^n will fill up the associated bilinear form with as many hyperbolic planes as we are allowed. So while the above discussion, in a way, explored how to free up as many entries as possible, it is also neat to know that we are also able to go the other way and occupy as much space as possible.

4.5 Further questions

This thesis has really explored quite a few different things surrounding Kass and Wickelgren's method. But it is only natural that there are still things to explore. We mention just a few of them here.

In the previous section we looked a bit at which bilinear forms we can achieve directly through the method by choosing the polynomial wisely, and we already covered dimensions 1-4. As we also explained there, from dimension 5 and onwards we do not yet have complete answers. This is naturally something that can be explored in the future. We can note that here we primarily stuck with polynomials in one or two variables. It is certainly possible that there are more answers in polynomial rings of more than two variables. This also risks the computations becoming much more complicated, but it might be what is necessary to get somewhere.

A bit related to this, we could also ask if there are more results about the presence of hyperbolic planes in bilinear forms produced by the algorithm. We have determined that we always get at least one copy of $\mathbb{H}$ when we use the algorithm. But are there, for example, situations where the number of hyperbolic planes in a form is strictly larger than 1? Recall also that when we proved that $\mathbb{H}$ is always an orthogonal summand, we did this by finding an isotropic vector in Q. Maybe exploring isotropic vectors a bit more could yield interesting results.

We also mentioned in the previous section how ax^n fills up a form with as many copies of $\mathbb{H}$ as the bilinear form can contain. There could very well be other polynomials with some interesting behaviour like that. Considering how ubiquitous the hyperbolic plane has been here it would be interesting to have more results on it.

Finally, recall that in Theorem 4.5 we wanted to find integers m_i so that $x_i^{m_i} \in (f_1, \ldots, f_n)$. After the proof, we discussed some potential hurdles in trying to find the minimal values of m_i. It is fair to say that it would be very nice to determine an algorithm or criterion or something that would make that computation easier.

Bibliography

[1] Michael F. Atiyah and Ian G. MacDonald, *Introduction to commutative algebra*, Westview Press, 1969.

[2] David A. Cox, John Little, and Donal O'Shea, *Ideals, varieties, and algorithms: An introduction to computational algebraic geometry and commutative algebra*, 4th ed., Springer Publishing Company, Incorporated, 2015.

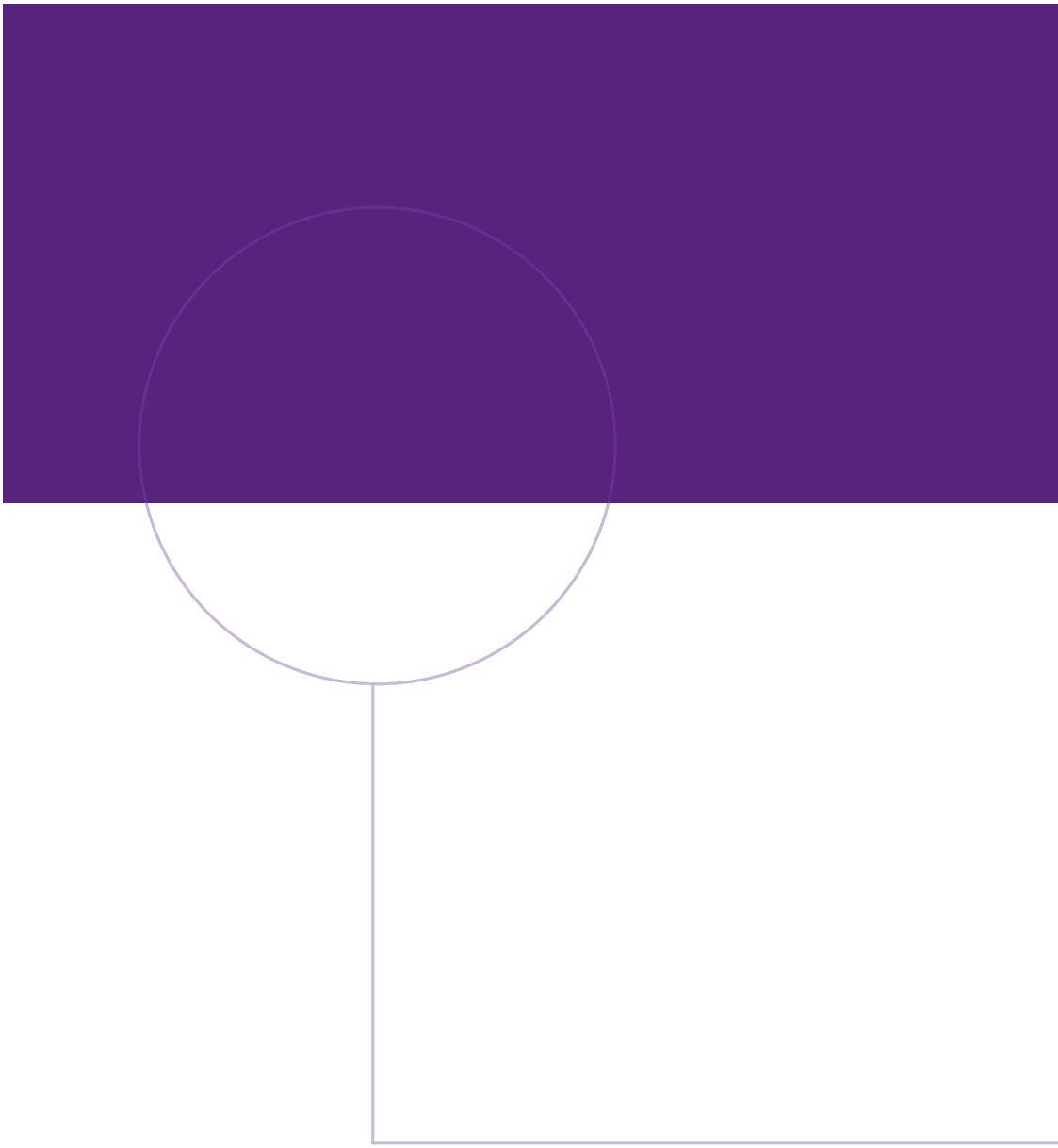
[3] Roger A. Horn and Charles R. Johnson, *Topics in matrix analysis*, Cambridge University Press, 1991.

[4] Jesse L. Kass and Kirsten Wickelgren, *The class of Eisenbud–Khimshiashvili–Levine is the local* $\mathbf{A}^1$*-Brouwer degree*, Duke Math. J. **168** (2019), no. 3, 429–469.

[5] Tsit Y. Lam, *The algebraic theory of quadratic forms*, W. A. Benjamin, Inc., 1973.

[6] Winfried Scharlau, *Quadratic and hermitian forms*, Springer-Verlag, 1985.

[7] The Stacks project authors, *The Stacks project*, `https://stacks.math.columbia.edu/tag/00CT`, Accessed: 25/05/2020.



NTNU

Kunnskap for en bedre verden