Separating Invariants

by

Emilie Sonia Dufresne

A thesis submitted to the
Department of Mathematics and Statistics
in conformity with the requirements for
the degree of Doctor of Philosophy

Queen's University
Kingston, Ontario, Canada
August 2008

Abstract

Roughly speaking, a separating algebra is a subalgebra of the ring of invariants whose elements distinguish between any two orbits that can be distinguished using invariants. In this thesis, we introduce the notion of a geometric separating algebra, a more geometric notion of a separating algebra. We find two geometric formulations for the notion of separating algebra which allow us to prove, for geometric separating algebras, the results found in the literature for separating algebras, generally removing the hypothesis that the base field be algebraically closed. Using results from algebraic geometry allows us to prove that, for finite groups, when a polynomial separating algebra exists, the group is generated by reflections, and when a complete intersection separating algebra exists, the group is generated by bireflections. We also consider geometric separating algebras having a small number of generators, giving an upper bound on the number of generators required for a geometric separating algebra. We end with a discussion of two methods for obtaining new separating sets from old. Interesting, and relevant examples are presented throughout the text. Some of these examples provide answers to questions which previously appeared in print.

Acknowledgements

Sur le plan académique, je remercie tout d'abord David Wehlau, mon superviseur. Je remercie aussi Greg Smith et Mike Roth, et le reste du groupe d'algèbre commutative et de géométrie algébrique. Je remercie Jennifer Read, et l'administration du département en général. Je remercie le CRSNG pour son généreux soutient financier.

Sur le plan personel, je remercie mes parents, mon frère et John, mais aussi mes amis de Kingston et d'ailleurs.

Statement of Originality

I hereby certify that, unless otherwise indicated, the results contained in this document are mine. Whenever other people's ideas and results been used, I have given due credit, and references when applicable.

Emilie Dufresne

Table of Contents

Chapter 1

Introduction

Suppose we want to decide if two polygons are the same, how do we do this? First, of course, we need to precisely define what “the same” means. We could take the same to mean congruent, that is, one polygon can be obtained from the other by translations, reflections and rotations; the idea being that a polygon remains the same if we move it around the plane, or reflect it with respect to a line. We have just described a group action on a set. The set in question is the set of polygons, and the group is the group generated by translations, reflections, and rotations of the plane. Elements of the group will be transformations of the plane that are built up from translations, rotations, and reflections, and a group element sends a polygon to its image under the transformation. This group action partitions the set of polygons into equivalence classes. Saying that two polygons are the same corresponds exactly to saying that they belong to the same equivalence class, or in other words they belong to the same group orbit.

In order to decide if two polygons are in the same equivalence class, we need to find properties that are common to all elements belonging to the same equivalence class. There are various objects and numbers we may associate to a polygon: for example, the number of sides, the length of the sides, the length of the diagonals, the area, the angles between sides, etc. One may consider this association as a function: a function from the set of polygons to the set of objects (or numbers). Such a function will be called invariant if it takes the same value on all elements in each equivalence class. Clearly, if two polygons do not have the same number of sides, or the same area, or sides of the same length, then they are not the same. A square and a triangle are not the same because they do not have the same number of sides. But two polygons may have the same number of sides and still not be the same. So the invariant "number of sides" is not sufficient to decide if two polygons are the same. Let us add another invariant, say the length of the sides. For the triangles, this is enough. Indeed congruent triangles are a staple of high school planar geometry. Also knowing 2 angles and the side between them, or knowing two sides and the angle between them, are also valid criteria to decide if two triangles are the same. These are other separating sets. For polygons in general, however this is not enough. It is not too hard to find two quadrilaterals having sides of the same length, but which are not the same.

We need more invariants. What if we throw in the distance between any two points? This might work for quadrilaterals. But the length of the sides must be distinguished from the length of the diagonals. Indeed, Boutin and Kemper [3] give an example of two sets of 4 points in the plane, which have the same distribution of distance between any two points, but which are not the same, meaning that you can not get one by moving around the other one, or reflecting it. But if we know which 4 of the distances are the length of the sides, can we separate quadrilaterals? Certainly, if we know 3 angles, and the length of the sides between them, we can separate quadrilaterals. In general, we can separate n-sided polygons using $n-1$ angles, and the length of the sides between them. But do we really need all this information?

Let us consider another example, one which is closer to our setting. We consider the problem of deciding if two square matrices represent the same linear transformation. For one thing, they should be of the same size. Let us assume they are, then Linear Algebra tells us that two matrices will represent the same linear transformation if they are conjugate, that is, A and B correspond to the same linear transformation if there exists an invertible matrix P such that $A = P^{-1}BP$. As in the previous example, two matrices will be "the same" if they are in the same equivalence class for a group action. The group here is the group of invertible $n \times n$ matrices, usually called the general linear group. It acts via conjugation on the set of $n \times n$ matrices. If we view the $n \times n$ matrices as a n^2-dimensional vector space, then this action is linear. A first invariant to consider would be the characteristic polynomial (or the eigenvalues). This invariant alone is not enough to decide if two matrices represent the same linear transformation. For example,

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \text{ and } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

do not correspond to the same linear transformation, but they have the same characteristic polynomial. If we also include the geometric multiplicities of the eigenvalues, then we have a separating set.

This second examples fits within the general setting in which we will be working throughout this text. We consider algebraic groups acting linearly on vector spaces. We are interested in the actions of any group, not just general linear group, but also finite groups and other infinite groups, and we work over any field, of any characteristic, algebraically closed or not. The functions we are interested in are polynomials, and the invariants are polynomials which take the same value on all elements of each orbit. In the previous example, the characteristic polynomial, or more exactly its coefficients, is a polynomial invariant, but the geometric multiplicities are not. Ideally, we would like to say a set is a separating set if it separates the equivalence classes. Usually, however, even with all the polynomial invariants, there usually are orbits which cannot be separated. The previous example is in that category: polynomial invariants alone are not enough to decide if two matrices represent the same linear transformation. Therefore, we must be satisfied with calling a set a *separating set*, if it separates the orbits that can be separated using polynomial invariants.

Here is an outline of the content of this text:

Chapter 2 tells the (short) story of the study of separating invariants through reviews of the published, and not yet published papers and book chapters written about separating invariants.

Chapter 3 sets up the scene. We describe the general setting of Invariant Theory, and quickly move on to define the notions of separating algebra and introduce the notion of geometric separating algebra. The core of the chapter consists of the two geometric formulations of our new definition, and some of their consequences.

In Chapter 4, we consider nice separating algebras. We provide a number of interesting, and informative examples, but more importantly, we prove general results linking the existence of particularly nice separating algebras to the geometry of the representation. These are the central results of this text. We show that only reflection groups may have polynomial separating algebras, only bireflection groups may have graded complete intersection separating algebras.

Chapter 5 consists mostly of examples, but also we give an upper bound on the minimal size of a separating set which depends only on the dimension of the representation.

In Chapter 6, we discuss two methods for obtaining separating sets from other separating sets. Our main input is to highlight, via examples, the close relationship between polarization and separating invariants.

Chapter 7 concludes this text with a discussion of possible future work.

Chapter 2

Literature Review

The study of separating invariants is a new trend in invariant theory, initiated by Derksen and Kemper in their 2003 book *Computational Invariant Theory* [11]. In this book, which is an excellent reference book on invariant theory, there are two sections dedicated to separating invariants: Section 2.3, and Section 3.9. They give a definition and obtain some interesting results: they show finite separating sets always exist; they show separating invariants of finite groups satisfy Noether's bound, that is, they show that the invariants of degree at most $|G|$ form a separating set; they show that for reductive groups over algebraically closed fields, separating algebras are very closely related to the ring of invariants: the extension is finite, and the extension of fields of fractions is purely inseparable.

In his 2003 paper *Computing Invariants for Reductive Groups in Positive Characteristic* [28], Kemper gives an algorithm which computes a separating set as an intermediate step to computing the ring of invariants. To do this, he gives an alternate criterion for being a separating set which relies on a Gröbner basis computation, and exploits the close relationship between graded separating algebras and the ring of invariants.

In their 2008 paper *Polarization of Separating Invariants* [14], Draisma, Kemper, and Wehlau reconsider a classical tool, polarization, from the point of view of separating invariants. They show that the polarization of separating invariants yields separating invariants. They introduce a computationally cheaper version of polarization which also yields separating invariants. Note that the 2007 paper *Vector Invariants in Arbitrary Characteristic* [16] of Grosshans contains similar results concerning polarization, although the step where one recognises his result is about separating invariants is missing.

In his 2007 paper *Typical Separating Invariants* [13], Domokos introduces a weaker polarization, and shows that it sends separating sets to separating sets, but more importantly he shows that when polarizing, one only needs to consider polarized invariants involving a restricted number of copies.

In *Separating Invariants* [29], Kemper generalizes the notion of separating set, and separating subalgebra to more general rings of functions. He also shows that some of the earlier results still hold. For example, there is still a finite separating set.

In their recent preprint *Characterizing Separating Invariants* [32] Neusel and Sezer consider separating sets of two important classes of groups: finite abelian groups, and p-groups in characteristic p. They exhibit a small separating set for abelian groups, whose size depends only on the dimension of the representation.

My recent preprint *Separating Invariants and Finite Reflection Groups* [15], contains some of the main results from this thesis. Namely, the main results of Chapters 3 and 4.

Although not the main focus of that paper, Derksen and Kemper mention separating invariants in their 2008 paper *Computing Invariants of Algebraic Groups in Arbitrary Characteristic* [12]. An interesting result characterizing separating algebras in positive characteristic appears in a remark.

Chapter 3

Orbit Separation, Separation, Geometric Separation

We start by establishing the setting and the notation with which we will be working throughout this text. We consider a linear algebraic group G, and V, a n-dimensional representation of G over a field $\Bbbk$ of characteristic $p \geq 0$. We write $\Bbbk[V]$ for the symmetric algebra on the vector space dual V^* of V. If $x_1, \ldots, x_n$ is a basis for V^*, then $\Bbbk[V] = \Bbbk[x_1, \ldots, x_n]$ is a polynomial ring in the n variables $x_1, \ldots, x_n$. The polynomial ring $\Bbbk[V]$ is a standard graded $\Bbbk$-algebra, graded bydegree.

The action of G on V induces an action on $\Bbbk[V]$ via by extending the following action of G on V^*

$$(\sigma \cdot f)(v) = f(\sigma^{-1} \cdot v),$$

where σ is an element of G, f is in $\Bbbk[V]$, and v is in V. The *ring of invariants*, denoted $\Bbbk[V]^G$, is the ring formed by the elements of $\Bbbk[V]$ left fixed by the action of G. Since the G-action preserves degree, $\Bbbk[V]^G$ is a graded subalgebra of $\Bbbk[V]$.

3.1 Separation

Elements of $\Bbbk[V]$ are functions from V to $\Bbbk$, and elements of $\Bbbk[V]^G$ are constant on the G-orbits. Indeed, if f is an invariant, σ is an element of G, and u belongs to V, then $f(\sigma \cdot u) = (\sigma^{-1} \cdot f)(u) = f(u)$. Thus, for u and v in V, if there is an invariant f such that $f(u) \neq f(v)$, then we may conclude that u and v belong to distinct orbits. In this situation, we say that f *separates* u and v. A natural definition for a separating set would be to require that it separates elements u and v whenever they belong to distinct orbits. The ring of invariants, however, generally does not distinguish the orbits (see Example 3.1.1). Hence, this natural definition of separating set is not very useful.

Example 3.1.1 (Example 2.3.1 in [11]) Let $G = \mathbb{C}^*$ be the multiplicative group of $\mathbb{C}$ acting on a 2-dimensional vector space V over $\mathbb{C}$ via scalar multiplication. The ring of invariants is $\mathbb{C}$. Indeed, if f is an homogeneous polynomial of degree d, then for any t in $\mathbb{C}^*$, $t \cdot f = t^d f$. Hence f is invariant if and only if $d = 0$ or $f = 0$, that is, if and only if f is constant. The invariants do not separate any points of V. In contrast, there are infinitely many orbits: one is the origin, the others are the lines through the origin minus the origin. $\triangleleft$

Derksen and Kemper [11, 28] define a *separating set* as a set E such that whenever two points of V can be separated by an invariant, they can be separated by an element of E. More formally, they make the following definition:

Definition 3.1.1 (Derksen and Kemper [11, 28])**.** A subset E of $\Bbbk[V]^G$ is a *separating set* if and only if, for all u, v in V, if there exists f in $\Bbbk[V]^G$ such that $f(u) \neq f(v)$, then there exists h in E such that $h(u) \neq h(v)$. A subalgebra $A \subset \Bbbk[V]^G$ satisfying this condition is called a *separating algebra*. Note that if a subalgebra of $\Bbbk[V]^G$ is generated by a separating set, then it is a separating algebra.

We now consider a simple example which shall accompany us throughout this text.

Example 3.1.2 Let $C_3 = \langle \sigma \rangle$ be the cyclic group of order 3 acting on $\mathbb{C}^2$ via

$$\sigma \mapsto \begin{pmatrix} \zeta_3 & 0 \\ 0 & \zeta_3 \end{pmatrix},$$

where ζ_3 is a primitive third root of unity. If x_1, x_2 form the dual basis to the usual basis for $\mathbb{C}^2$, then

$$\mathbb{C}[V]^{C_3} = \mathbb{C}[x_1^3, x_1^2x_2, x_1x_2^2, x_2^3],$$

where $\{x_1^3, x_1^2x_2, x_1x_2^2, x_2^3\}$ forms a minimal set of generators. On points where x_1 is zero, $x_1x_2^2$ is also zero, and on other points

$$x_1x_2^2 = \frac{(x_1^2x_2)^2}{x_1^3}.$$

Thus, the value of $x_1x_2^2$ at a point is entirely determined by the value of the three other generators. Therefore, $x_1x_2^2$ does not separate additional points, and $\{x_1^3, x_1^2x_2, x_2\}$ is a separating set. $\triangleleft$

This example illustrates that the notion of separating set is distinct from the notion of generating set. Since generating sets separate, following Kemper [29], we may say that separating sets are generalised generating sets. Moreover, this example shows how separating algebras can have a much nicer structure than the ring of invariants. In the example, we get a hypersurface separating algebra when the ring of invariants is not even a complete intersection.

Example 3.1.3 (Separating the Points on a Line)

The purpose of this example is to study the notion of separating set in a simple situation: the 1-dimensional representation of the trivial group over $\mathbb{C}$. We will see that, while separating sets are fairly easy to find, it is hard to describe general separating sets precisely.

If V is the 1-dimensional representation of the trivial group over $\mathbb{C}$, then the ring of invariants is $\mathbb{C}[V] = \mathbb{C}[x]$, a polynomial ring in one variable. The orbits of the group action are just the points of $\mathbb{C}$. By definition, the set $\{f_1, \ldots, f_r\}$ is a separating set if for any two distinct elements a and b of $\mathbb{C}$, there is an i such that $f_i(a) \neq f_i(b)$.

We will consider more closely separating sets of size 1 and 2. We start with separating sets of size one. Suppose the polynomial $f = \alpha_m x^m + \alpha_{m-1}x^{m-1} + \ldots + \alpha_0$ forms a separating set. In particular, f separates non-zero elements from zero. Thus, for any $a \neq 0$ in $\mathbb{C}$, $f(a) \neq f(0)$, that is, the only linear factor in $\mathbb{C}[x]$, of

$$f - f(0) = \alpha_m x^m + \alpha_{m-1}x^{m-1} + \ldots + \alpha_1 x$$

is x. Thus, $f = \alpha_m x^m + \alpha_0$. Now, take b to be any nonzero element of $\mathbb{C}$. If $a \neq b$, since f separates points, $f(a) \neq f(b)$. In other words, the only root of $f - f(b)$ is b. But $f - f(b) = \alpha_m(x^m - b^m)$, thus $(x^m - b^m) = (x - b)^m$. As b is nonzero, m must be 1, and $f = \alpha_1 x + \alpha_0$ is a linear polynomial. On the other hand, if f is a linear polynomial, then it will take distinct values on distinct points, and so it will separate points.

We now consider geometric separating sets of size 2. Suppose $\{f_1 = \alpha_m x^m + \ldots + \alpha_0, f_2 = \beta_n x^n + \ldots + \beta_0\}$, where $m \leq n$, is a separating set. We will consider fixed values of m successively. First, if f_1 has degree 1, then it separates, and there are no restrictions on f_2.

Suppose f_1 has degree 2. The first step is to replace f_1 with a simpler polynomial which separates the same points. We have

$$\begin{aligned} f_1 &= \alpha_2 x^2 + \alpha_1 x + c \\ &= \alpha_2 \left(x^2 + \tfrac{\alpha_1}{\alpha_2} x + \tfrac{\alpha_0}{\alpha_2} \right) \\ &= \alpha_2 \left(\left(x + \tfrac{\alpha_1}{2\alpha_2} \right)^2 + \tfrac{\alpha_0}{\alpha_2} - \tfrac{\alpha_1^2}{4\alpha_2^2} \right). \end{aligned}$$

After the change of variable $y = x + \frac{\alpha_1}{2\alpha_2}$, the polynomial f_1 is now given by $f_1 = \alpha_2\left(y^2 + \frac{\alpha_0}{\alpha_2} - \frac{\alpha_1^2}{4\alpha_2^2}\right)$. Note that for any polynomial h, and any nonzero constant γ, the polynomials $h + \gamma$ and γh will separate exactly the same points as h. Indeed, if a and b are elements of $\mathbb{C}$, then $h(a) \neq h(b)$ if and only if $h(a) + \gamma \neq h(b) + \gamma$ if and only $\gamma h(a) \neq \gamma h(b)$. Thus, $f_1' = \frac{1}{\alpha_2}\left(f_1 - \frac{\alpha_0}{\alpha_2} + \frac{\alpha_1^2}{4\alpha_2^2}\right) = y^2$ will separate exactly the same points as f_1, and so $\{f_1, f_2\}$ is a separating set if and only if $\{f_1', f_2\}$ is a separating set. Thinking of f_2 as a polynomial in y, we form f_2' by subtracting from f_2 the constant term and powers of f_1' to remove all terms of even degree. Then, $\{f_1', f_2\}$ is a separating set if and only if $\{f_1', f_2'\}$ is a separating set. Indeed, if f_1' separates a and b, then both sets separate a and b, if not, then f_1' takes the same value on a and b, and $(f_2 - f_2')(a) = (f_2 - f_2')(b)$. Thus, f_2 separates a and b if and only if f_2' separates a and b. $\{f_1', f_2'\}$ is a separating set if and only if for any point a in $\mathbb{C}$, the only b in $\mathbb{C}$ such that both $f_1'(a) = f_1'(b)$ and $f_2'(a) = f_2'(b)$ is a. In other words, $\{f_1', f_2'\}$ is a separating set if and only if, for all a in $\mathbb{C}$, the only common root of $f_1' - f_1'(a)$ and $f_2' - f_2'(a)$ is a. But $f_1' - f_1'(a) = y^2 - a^2 = (y - a)(y + a)$. Note that if $a = 0$, then the only root of $f_1' - f_1'(a)$ is 0, and so by default the only common root of $f_1' - f_1'(a)$ and $f_2' - f_2'(a)$ is $a = 0$. Thus $\{f_1', f_2'\}$ is a separating set if and only if, for all nonzero a in $\mathbb{C}$, $f_2'(a) \neq f_2'(-a)$. As f_2' only has terms of odd degree, $f_2'(-a) = -f_2'(a)$. Therefore, $\{f_1', f_2'\}$ is a separating set if and only if f_2' has no nonzero roots, i.e., as a polynomial in y, f_2' is of the form $f_2' = \beta_{2k+1}y^{2k+1}$ for some $k \geq 1$. We conclude that, as polynomials in the original variable x, a separating set of size 2 where f_1 has degree 2 will be of the form:

$$\begin{aligned}
&f_1 = \alpha_2 x^2 + \alpha_1 x + \alpha_0 \\
&f_2 = \beta_{2k+1}\left(x + \tfrac{\alpha_1}{2\alpha_2}\right)^{2k+1} + h\left(\left(x + \tfrac{\alpha_1}{2\alpha_2}\right)^2\right),
\end{aligned}$$

where α_i and β_{2k+1} belong to $\mathbb{C}$, and α_2 and β_{2k+1} are nonzero, $k \geq 1$, and h is a polynomial in one variable. Generally, a pair of polynomials of this form will be a separating set.

Next, we consider separating sets of size 2 where f_1 has degree 3. Again, we want to find a simpler polynomial which separates the same points as f_1. We have

$$\begin{aligned} f_1 &= \alpha_3 x^3 + \alpha_2 x^2 + \alpha_1 x + \alpha_0 \\ &= \alpha_3 \left(\left(x - \tfrac{\alpha_2}{3\alpha_3} \right)^3 + \left(\frac{\alpha_1}{\alpha_3 - \frac{\alpha_2^2}{3\alpha_3^2}} \right) x + \tfrac{\alpha_2^3}{27\alpha_3^3} + \tfrac{\alpha_0}{\alpha_3} \right) \\ &= \alpha_3 \left(\left(x - \tfrac{\alpha_2}{3\alpha_3} \right)^3 + \left(\tfrac{\alpha_1}{\alpha_3} - \tfrac{\alpha_2^2}{3\alpha_3^2} \right) \left(x - \tfrac{\alpha_2}{3\alpha_3} \right) + \tfrac{\alpha_2}{3\alpha_3} \left(\tfrac{\alpha_1}{\alpha_3} - \tfrac{\alpha_2^2}{3\alpha_3^2} \right) + \tfrac{\alpha_2^3}{27\alpha_3^3} + \tfrac{\alpha_0}{\alpha_3} \right). \end{aligned}$$

After the change of variable $y = x - \frac{\alpha_2}{3\alpha_3}$, we form f_1' by multiplying f_1 by an α_3^{-1} and subtracting the constant term. Thus, $f_1' = y^3 + \gamma y$, where $\gamma = \left(\frac{\alpha_1}{\alpha_3} - \frac{\alpha_2^2}{3\alpha_3^2} \right)$. As before, $\{f_1, f_2\}$ is a separating set if and only if either $\{f_1', f_2\}$ is a separating set. For a in $\mathbb{C}$, f_1 and f_2 separate an arbitrary b from a if and only if $f_1'(a) \neq f_1'(b)$ or $f_2(a) \neq f_2(b)$, that is, the only common root of $f_1' - f_1'(a)$ and $f_2 - f_2(a)$ is a. We have

$$f_1' - f_1'(a) = y^3 + \gamma y - a^3 - \gamma a = (y - a)(y^2 + ay + a^2 - \gamma^2).$$

For each a, the linear factor $(y - a)$ can have multiplicity 1, 2, or 3 in $f_1' - f_1'(a)$. We will treat these 3 cases separately. First, let us consider the points a where $(x - a)$ has multiplicity 1 in $f_1' - f_1'(a)$. In this situation, f_1' and f_2 separate points from a if and only if, $f_1' - f_1'(a)$ and $f_2 - f_2(a)$ have no other common root than a, that is, as polynomials in y, $gcd(y^2 + ax + a^2 - \gamma^2, f_2 - f_2(a)) = 1$. We can answer this question for all a's at once by considering $y^2 + ay + y^2 - \gamma^2$ and $f_2 - f_2(a)$ as polynomials in y and a and asking if the multivariate resultant is nonzero everywhere.

Suppose, now, that $y - a$ is a multiple root. We have that

$$y^2 + ay + a^2 - \gamma^2 = (y - a)(y + 2a) + 3a^2 - \gamma^2.$$

Thus, $(y - a)$ divides $y^2 + ay + a^2 - \gamma^2$ if and only if $3a^2 - \gamma^2 = 0$, i.e., when $a = \pm\frac{\gamma}{\sqrt{3}}$. Note that the only way $(y - a)$ can be a triple root is if $\gamma = a = 0$. When

$\gamma \neq 0$, then $y-a$ is a double root if and only if $a = \pm\frac{\gamma}{\sqrt{3}}$, and for those values of a, $y^2+ay+a^2-\gamma^2 = (y-a)(y+2a)$, and so f_1', f_2 separate other points b of $\mathbb{C}$ from $\pm\frac{\gamma}{\sqrt{3}}$ if and only if $f_2\left(2\frac{\gamma}{\sqrt{3}}\right) \neq f_2\left(-\frac{\gamma}{\sqrt{3}}\right)$, and $f_2\left(-2\frac{\gamma}{\sqrt{3}}\right) \neq f_2\left(\frac{\gamma}{\sqrt{3}}\right)$.

The next case to consider is when $\gamma = 0$, i.e., $f_1' = y^3$. We form f_2' by subtracting the constant term of f_2, and powers of f_1' so that the resulting polynomial only has terms of degree coprime to 3. The set $\{f_1', f_2'\}$ separates the same points as $\{f_1', f_2\}$. $\{f_1', f_2'\}$ will be a separating set if and only if f_2' has no nonzero roots (specialize the argument of Proposition 3.1.1). This forces f_2' to be a monomial. Thus, when f_1, f_2 is a geometric separating set, where $f_1 = \alpha_3x^3+\alpha_2x^2+\alpha_1x+\alpha_0$ and $0 = \gamma = \left(\frac{\alpha_1}{\alpha_3} - \frac{\alpha_2^2}{3\alpha_3^2}\right)$, f_2 will be of the form: $f_2 = \beta_k\left(x - \frac{b}{3a}\right)^k + h\left(\left(x-\frac{b}{3a}\right)^3\right)$, where β_k is in $\mathbb{C}$, $k \geq 1$ is not divisible by 3, and h is a polynomial in one variable over $\mathbb{C}$.

Already, our method does not yield a general formula for separating sets of size 2 with f_1 of degree 3: what we get is an "easy" to check criterion to decide if a given pair of polynomials forms a separating set. We could follow the same process, to obtain easy to check criteria for deciding if two polynomials form a separaing set when f_1 has degree 4, or 5. But our method can not take us any further. Indeed, if f_1 has degree m, finding those points u for which $(x-u)$ may have multiplicity more that 1 in $f_1 - f_1(u)$, requires factoring a polynomial of degree $m-1$. If we do not assume f_1 is in any special form, the polynomial we want to factor will be general. This example shows how quickly things get rather complicated.

There is, however, one case which we can describe fully for all m:

Proposition 3.1.1 *Let V be the 1-dimensional representation of the trivial group over an algebraically closed field $\Bbbk$ of characteristic $p \geq 0$. Let $f_1 = x^m$, where $m > 1$ and $p \nmid m$, and let f_2 be a polynomial with degree at least m. Suppose $\{f_1, f_2\}$ is a separating set, then f_2 is of the form $f_2 = \beta x^k + h(f_1)$, where $m \nmid k$, β is in $\Bbbk$, and h is in $\Bbbk[z]$.*

Proof. Suppose $\{f_1 = x^m, f_2\}$ is a separating set. We form f_2' by substracting the constant and all terms with degree a multiple of m. We obtain $f_2 = f_2' + h(f_1)$, where all terms in f_2' have degree not divisible by m and h is a polynomial in one variable over $\Bbbk$. We can then write $f_2' = g_1 + \ldots + g_{m-1}$, where all terms in g_i have degree congruent to i modulo m. Note that $\{f_1, f_2\}$ is a separating set if and only if $\{f_1, f_2'\}$ is a separating set. For all u in $\Bbbk$,

$$f_1 - f_1(u) = x^m - u^m = \prod_{j=0}^{m-1} (x - \zeta_m^j u),$$

where $\zeta_m \in \Bbbk$ is a primitive m-th root of unity. Thus, f_1, f_2' is a separating set if and only if, for all nonzero u in $\Bbbk$ and $j = 1, \ldots, m-1$, $f_2'(u) \neq f_2'(\zeta_m^j u)$. For all nonzero u in $\Bbbk$ and $j = 1, \ldots, m-1$, we have

$$f_2'(\zeta_m^j u) = g_1(\zeta_m^j u) + \ldots + g_{m-1}(\zeta_m^j u) = \zeta_m^j g_1(u) + \ldots + \zeta_m^{(m-1)j} g_{m-1}(u),$$

and $f_2'(u) = g_1(u) + \ldots + g_{m-1}(u)$. Thus,

$$f_2'(u) - f_2'(\zeta_m^j u) = (1 - \zeta_m^j) g_1(u) + \ldots + (1 - \zeta_m^{(m-1)j}) g_{m-1}(u).$$

As f_1, f_2' separate, it follows that $f_2'(u) - f_2'(\zeta_m^j u)$ is non-zero for all $0 \neq u \in \Bbbk$, and so of the form βu^k for some $k \geq 1$ and $\beta \in \Bbbk$. As the g_i's are linearly independent, and their coefficients are all nonzero whenever ζ_m^j is still a primitive m-th root of unity, it follows that all but one of the g_i's are zero. Therefore, f_2 is of the form $f_2 = \beta x^k + h(f_1)$, where $m \nmid k$, $\beta \in \Bbbk$ and h is a polynomial in one variable over $\Bbbk$. □

◁

3.2 Geometric Separation

In this section we introduce the notion of geometric separating set, a new notion of separating invariants which has the advantage of being stable under algebraic extensions of the base field. We give two geometric formulations of this notion in which lies the strength of our new definition.

The notion of separating invariants introduced by Derksen and Kemper has proven itself to be quite interesting. It does, however have its limitations: many of the results in the literature require the base field to be algebraically closed. Indeed, the notion of separating set behaves rather differently over non-algebraically closed fields, and its behavior over finite fields diverges even more from the situation over algebraically closed fields. For example, Kemper proved that over algebraically closed fields, graded separating algebras have the same dimension as the ring of invariants, but this result does not always hold over finite fields (Example 3.2.1).

Let $\overline{\mathbb{k}}$ be an algebraic closure of $\mathbb{k}$ and let $\overline{V} = V \otimes_{\mathbb{k}} \overline{\mathbb{k}}$. Then $\mathbb{k}[V] \subset \overline{\mathbb{k}}[\overline{V}]$ and so any element $f \in \mathbb{k}[V]$ can be considered as a function $\overline{V} \to \overline{\mathbb{k}}$. Moreover, the action of G on V extends to an action on $\overline{V}$, and so $\mathbb{k}[V]^G \subset \overline{\mathbb{k}}[\overline{V}]^G$.

Definition 3.2.1. A subset E of $\mathbb{k}[V]^G$ is a *geometric separating set* if and only if, for all u and v in $\overline{V}$, if there exists f in $\mathbb{k}[V]^G$ such that $f(u) \neq f(v)$, then there exists h in S such that $h(u) \neq h(v)$. If $A \subset \mathbb{k}[V]^G$ is a subalgebra satisfying this property, then A is a *geometric separating algebra.* Note that a subalgebra generated by a geometric separating set is a geometric separating algebra.

Clearly, over algebraically closed fields, separating sets and geometric separating sets coincide, hence, the separting set obtained in Example 3.1.2 is a geometric separating set. But separating sets are not always geometric separating sets:

Example 3.2.1 Let $G = C_3$ be the cyclic group of order 3 acting on a 2-dimensional vector space V over the field $\mathbb{F}_2$ as follows:

$$G := \langle \sigma \rangle = \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle .$$

If x, y form a basis for V^* dual to the usual basis for V, then by Example (i) in Annex B of [1], the ring of invariants is minimally generated by

$$\begin{aligned} f_1 &= x^2 + xy + y^2, \\ f_2 &= x^3 + x^2y + y^3, \text{ and} \\ f_3 &= x^3 + xy^2 + y^3. \end{aligned}$$

As functions on V, however, f_1,f_2, and f_3 coincide (just check the value of the 3 polynomials on the 4 points of V). Thus, only one is needed to separate the orbits, and despite the ring of invariants being 2-dimensional, there are 1-dimensional separating algebras.

In contrast, on $\overline{V}$, f_1, f_2, and f_3 do not correspond to the same function, and taking f_1 alone does not yield a geometric separating set. $\triangleleft$

It is easy to see that our modification of Derksen and Kemper's definition avoids many problems. Its real strentgh, however, lies in the two geometric formulations presented later in this section. In fact, throughout this text they will let us recover most of the results found in the literature, often removing the requirement that $\Bbbk$ be algebraically closed.

3.2.1 The Separating Scheme

In this subsection, we give a first geometric formulation of the definition of a geometric separating algebra. We start by defining the *separating scheme*, a geometric object which can be used to detect when a subalgebra is a geometric separating algebra. The separating scheme is an extension to general groups and fields of some ideas of Kemper [28] for reductive groups over algebraically closed fields. We let V denote the affine scheme $\mathrm{Spec}(\Bbbk[V])$; when writing V, whether we mean the affine scheme or the vector space should be clear from the context. We also write $V /\!\!/ G$ for the affine scheme corresponding to $\Bbbk[V]^G$.

Definition 3.2.2. The *separating scheme* $\mathcal{S}_G$ is the unique reduced scheme having the same underlying topological space as the product $V \times_{V/\!\!/G} V$, i.e., $\mathcal{S}_G := (V \times_{V/\!\!/G} V)_{\mathrm{red}}$.

Since all the schemes involved are affine,

$$V \times_{V/\!\!/G} V = \operatorname{Spec}\left(\Bbbk[V] \otimes_{\Bbbk[V]^G} \Bbbk[V]\right).$$

If $\delta : \Bbbk[V] \to \Bbbk[V] \otimes_{\Bbbk} \Bbbk[V]$ is the map which sends $f \in \Bbbk[V]$ to $\delta(f) = f \otimes 1 - 1 \otimes f$, then, for any subalgebra $B \subset \Bbbk[V]$,

$$\Bbbk[V] \otimes_B \Bbbk[V] \cong \frac{\Bbbk[V] \otimes_{\Bbbk} \Bbbk[V]}{(\delta(B))}.$$

Hence, we have the identity

$$\Bbbk[V] \otimes_{\Bbbk[V]^G} \Bbbk[V] \cong \frac{\Bbbk[V] \otimes_{\Bbbk} \Bbbk[V]}{(\delta(\Bbbk[V]^G))},$$

and the separating scheme may be viewed as the closed subscheme of $V \times V$ with ideal $\sqrt{\delta(\Bbbk[V]^G)}$.

Theorem 3.2.1 *If $A \subset \Bbbk[V]^G$ is a subalgebra, then the following statements are equivalent.*

1. *A is a geometric separating algebra;*

2. *if $W = \operatorname{Spec}(A)$, then the natural morphism $\mathcal{S}_G \to (V \times_W V)_{\mathrm{red}}$ is an isomorphism;*

3. *the ideals $(\delta(A))$ and $(\delta(\Bbbk[V]^G))$ have the same radical in the ring $\Bbbk[V] \otimes_{\Bbbk} \Bbbk[V]$, that is, $\sqrt{(\delta(A))} = \sqrt{(\delta(\Bbbk[V]^G))}$.*

Proof. First, we prove (3) and (2) are equivalent. As V, $V/\!\!/G$, and W are affine schemes, $V \times_{V/\!\!/G} V = \operatorname{Spec}(\Bbbk[V] \otimes_{\Bbbk[V]^G} \Bbbk[V])$, and

$$V \times_W V = \operatorname{Spec}(\Bbbk[V] \otimes_A \Bbbk[V]).$$

Thus, (2) is equivalent to saying the $\Bbbk$-algebra homomorphism

$$\frac{\Bbbk[V]\otimes_{\Bbbk}\Bbbk[V]}{\sqrt{\delta(A)}}\to\frac{\Bbbk[V]\otimes_{\Bbbk}\Bbbk[V]}{\sqrt{\delta(\Bbbk[V]^G)}}$$

is an isomorphism, that is, $\sqrt{\delta(A)}=\sqrt{\delta(\Bbbk[V]^G)}$.

We now prove (3) and (1) are equivalent. If A is a geometric separating algebra, then for any u and v in $\overline{V}$, $f(u)=f(v)$ for all f in $\Bbbk[V]^G$ if and only if $h(u)=h(v)$ for all h in A. We can rewrite this statement as:

$$\mathcal{I}_{\overline{V}^2}(u,v)\cap(\Bbbk[V]\otimes_{\Bbbk}\Bbbk[V])\supset\delta(\Bbbk[V]^G)$$

if and only if

$$\mathcal{I}_{\overline{V}^2}(u,v)\cap(\Bbbk[V]\otimes_{\Bbbk}\Bbbk[V])\supset\delta(A),$$

where $\mathcal{I}_{\overline{V}^2}(u,v)$ denotes the maximal ideal of $\overline{\Bbbk}[\overline{V}]\otimes_{\overline{\Bbbk}}\overline{\Bbbk}[\overline{V}]$ corresponding to the point (u,v) of $\overline{V}\times\overline{V}$.

Since the maximal ideals of $\Bbbk[V]\otimes_{\Bbbk}\Bbbk[V]$ are in bijection with Galois orbits of the maximal ideals of $\overline{\Bbbk}[\overline{V}]\otimes_{\overline{\Bbbk}}\overline{\Bbbk}[\overline{V}]$, the maximal ideals of $\Bbbk[V]\otimes_{\Bbbk}\Bbbk[V]$ are exactly the primes of the form

$$\mathcal{I}_{\overline{V}^2}(u,v)\cap(\Bbbk[V]\otimes_{\Bbbk}\Bbbk[V])\,.$$

As $\Bbbk[V]\otimes_{\Bbbk}\Bbbk[V]$ is a finitely generated $\Bbbk$-algebra, by Theorem 5.5 of [31], the radical of an ideal I is given by the intersection of all maximal ideals containing I. Therefore, $\sqrt{\delta(\Bbbk[V]^G)}=\sqrt{\delta(A)}$. □

Remark 3.2.1. The proof of Theorem 3.2.1 implies that a subset $E\subset\Bbbk[V]^G$ is a geometric separating set if and only if $\sqrt{\delta(\Bbbk[V]^G)}=\sqrt{\delta(E)}$.

As a consequence of Theorem 3.2.1 every representation of any linear algebraic group admits a finitely generated geometric separating algebra. Our proof, however, is essentially the same as the proof of Theorem 2.3.15 of [11].

Proposition 3.2.2 *There always exists a finite geometric separating set.*

Proof. As the ring $\Bbbk[V] \otimes_{\Bbbk} \Bbbk[V]$ is Noetherian, there exist $f_1, \ldots, f_m \in \Bbbk[V]^G$ such that

$$(\delta(\Bbbk[V]^G) = (\delta(f_1), \ldots, \delta(f_m)).$$

By Remark 3.2.1, $\{f_1, \ldots, f_m \in \Bbbk[V]^G\}$ is a separating set. □

This result is particularly interesting because rings of invariants are not always finitely generated (see Example 2.1.4 in [11]).

The following theorem is a generalization of Proposition 2.3.10 of [11], the proof, however, is rather different. In fact, we obtain this result as a special case of Theorem 3.1 of [23].

Theorem 3.2.3 *Suppose that $A \subset \Bbbk[V]^G$ is a geometric separating algebra, and suppose $\Bbbk$ has characteristic $p \geq 0$. If $p > 0$, then $Q(A) \subset Q(\Bbbk[V]^G)$ is a purely inseparable field extension, and if $p = 0$, $Q(A) = Q(\Bbbk[V]^G)$. Here, $Q(A)$ and $Q(\Bbbk[V]^G)$ denote the fields of fractions of A, and $\Bbbk[V]^G$, respectively (See Appendix A).*

Proof. Suppose that $A \subset \Bbbk[V]^G$ is a separating algebra, then by Theorem 3.2.1

$$\sqrt{\delta(A)} = \sqrt{\delta(\Bbbk[V]^G)}.$$

Take $b \in Q(\Bbbk[V]^G)$, then $b = f/g$, where $f, g \in \Bbbk[V]^G$ and $g \neq 0$. In the tensor product $\Bbbk(V) \otimes_{\Bbbk} \Bbbk(V)$,

$$\begin{aligned}(g \otimes g)(f/g \otimes 1 - 1 \otimes f/g) &= f \otimes g - g \otimes f \\ &= (1 \otimes g)(f \otimes 1 - 1 \otimes f) - (1 \otimes f)(g \otimes 1 - 1 \otimes g).\end{aligned}$$

In the tensor product $\Bbbk[V] \otimes_{\Bbbk} \Bbbk[V]$,

$$(1 \otimes f)(g \otimes 1 - 1 \otimes g) + (1 \otimes g)(f \otimes 1 - 1 \otimes f) \in (\delta(\Bbbk[V]^G)).$$

Thus there exists an $N \geq 0$ such that

$$((1 \otimes f)(g \otimes 1 - 1 \otimes g) + (1 \otimes g)(f \otimes 1 - 1 \otimes f))^N \in (\delta(A)).$$

As $g \otimes g$ is not a zero divisor in the tensor product $\Bbbk(V) \otimes_{\Bbbk} \Bbbk(V)$, it follows that in that ring, $((f/g \otimes 1 - 1 \otimes f/g))^N$ in the ideal $(\delta(Q(A)))$, and so $((b \otimes 1 - 1 \otimes b))^N = 0$ in the tensor product $\Bbbk(V) \otimes_{Q(A)} \Bbbk(V)$.

Suppose $p > 0$. For k large enough, we will have

$$0 = ((b \otimes 1 - 1 \otimes b))^{p^k} = b^{p^k} \otimes 1 - 1 \otimes b^{p^k}.$$

As $Q(A)$ is a field, this implies that $b^{p^k} \in Q(A)$(see Lemma A.0.2).

On the other hand, when $\Bbbk$ has characteristic zero, so does $Q(A)$. It is a perfect field and so does not have any purely inseparable extensions (finite or not). Moreover, as $\Bbbk(V)$ is a field, it is reduced, and so its prime spectrum $\mathrm{Spec}(\Bbbk(V))$ is reduced. It follows that for all finite purely inseparable extension L of $Q(A)$,

$$\mathrm{Spec}(\Bbbk(V)) \otimes_{Q(A)} L = \mathrm{Spec}(\Bbbk(V)) \otimes_{Q(A)} Q(A) = \mathrm{Spec}(\Bbbk(V))$$

is reduced, and so by Proposition 4.6.1 in [17], $\mathrm{Spec}(\Bbbk(V)) \times_{\mathrm{Spec}(Q(A))} \mathrm{Spec}(\Bbbk(V))$ is also reduced. Thus, the ring $\Bbbk(V) \otimes_{Q(A)} \Bbbk(V)$ is reduced, and as such does not have any nonzero nilpotent elements. Thus $b \otimes 1 - 1 \otimes b = 0$ in the tensor product $\Bbbk(V) \otimes_{Q(A)} \Bbbk(V)$, and by Lemma A.0.2, $b \in Q(A)$. □

3.2.2 Reductive Groups

For reductive groups, we obtain a second geometric formulation for the definition of geometric separating algebra, which calls on the notion of *radicial* morphism. Recall that, a morphism of schemes $f : X \to Y$ is said to be radicial (or universally injective) if for all fields $\mathbb{F}$, the corresponding map of $\mathbb{F}$-points is injective (Definition 3.5.4 in [17]).

Theorem 3.2.4 *If G is reductive, then a finitely generated $\Bbbk$-algebra A is a geometric separating algebra if and only if the morphism of schemes $\theta : V/\!\!/G \to W = \mathrm{Spec}(A)$ corresponding to the inclusion $A \subset \Bbbk[V]^G$ is a radicial morphism.*

Proof. We write γ for the morphism of schemes corresponding to the inclusion of $\Bbbk[V]$ inside of $\overline{\Bbbk}[\overline{V}]$. By definition, a subalgebra $A \subset \Bbbk[V]^G$ is a geometric separating algebra if and only if for u, v in $\overline{V}$, $\theta(\pi(\gamma(u))) = \theta(\pi(\gamma(v)))$ implies $\pi(\gamma(u)) = \pi(\gamma(v))$, that is, A is a geometric seprating algebra if and only if θ is injective on $\overline{\Bbbk}$-points in the image of $\overline{V}$.

On the other hand, since G is reductive, π is surjective (Lemma 1.3 in [26]), and any map $\mathrm{Spec}(\overline{\Bbbk}) \to V/\!\!/G$ factors through V. Since $\overline{V} \to V$ is also surjective, $\mathrm{Spec}(\overline{\Bbbk}) \to V$ factors through $\overline{V}$. Thus, all $\overline{\Bbbk}$-points of $V/\!\!/G$ are in the image of $\overline{V}$. Therefore, A is a geometric separating algebra if and only if θ is injective on $\overline{\Bbbk}$-points.

Clearly, if θ is radicial, it is injectective on $\overline{\Bbbk}$-points. On the other hand, if θ is injective on $\overline{\Bbbk}$-points, then the corresponding diagonal map $V/\!\!/G \to V/\!\!/G \times_W V/\!\!/G$ is surjective on $\overline{\Bbbk}$-points (see argument of 1.8.7.1, [20]). That is, as $V/\!\!/G$ and W are of finite type over $\Bbbk$, the image of the diagonal morphism contains all the closed points. The product $V/\!\!/G \times_W V/\!\!/G$ is also of finite type over $\Bbbk$. Thus by Theorem 1.8.4 of [20], the image of the diagonal morphism closed points. is the whole underlying topological space. Hence, the diagonal morphism is surjective, and by Proposition 1.8.7.1 in [20], the morphism θ is radicial. □

Corollary 3.2.5 *If G is reductive, and A is a geometric separating algebra, then* $\dim A = \dim \Bbbk[V]^G$. *In particular, a geometric separating set must contains at least n elements.*

3.2.3 Graded Geometric Separating Algebras for Reductive Groups

When G is reductive, the relationship between grade separating algebras and the ring of invariants is very close.

Proposition 3.2.6 *Let $A \subset \Bbbk[V]^G$ be a graded subalgebra. If the map of schemes $\theta : V/\!\!/G \to W = \operatorname{Spec}(A)$ is injective, then the extension $A \subset \Bbbk[V]^G$ is integral.*

Proof. Let A_+ and $\Bbbk[V]^G_+$ denote the maximal graded ideal of A, and of $\Bbbk[V]^G$ respectively. Let $\mathfrak{p}$ be a proper prime ideal of $\Bbbk[V]^G$ containing $A_+\Bbbk[V]^G$. It follows that

$$A_+ \subset \left(A_+\Bbbk[V]^G \cap A\right) \subset (\mathfrak{p} \cap A) \subset A.$$

As A_+ is maximal, $\mathfrak{p} \cap A = A_+$.

On the other hand, $A_+ = \Bbbk[V]^G_+ \cap A$. Therefore, the injectivity of θ implies that $\mathfrak{p} = \Bbbk[V]^G_+$, and the radical of $A_+\Bbbk[V]^G$ in $\Bbbk[V]^G$ is $\Bbbk[V]^G_+$. It follows that

$$\frac{\Bbbk[V]^G}{A_+\Bbbk[V]^G}$$

has Krull dimension 0, i.e., it is a finite dimensional $\Bbbk$-vector space. By the graded version of Nakayama's Lemma (Lemma 3.5.1 in [11]), $\Bbbk[V]^G$ is a finite A-module, and so the extension $A \subset \Bbbk[V]^G$ is integral. □

Corollary 3.2.7 *If G is reductive, and if $A \subset \Bbbk[V]^G$ is a graded geometric separating algebra, then the extension $A \subset \Bbbk[V]^G$ is integral.*

Proof. By Theorem 3.2.4, the morphism of schemes $\theta : V/\!\!/G \to W$ is radicial. As radicial morphisms of schemes are injective (Proposition 3.5.8 in [17]), and as A is graded, the conclusion follows directly from Proposition 3.2.6. □

Following [11, 28] we get an even more precise description of the relationship between graded geometric separating subalgebras and the ring of invariants. We obtain an analog to Theorem 1.6 of [28] and Theorem 2.3.12 in [11].

Theorem 3.2.8 *If G is reductive, and if $A \subset \Bbbk[V]^G$ is a graded geometric separating algebra, then $\hat{\tilde{A}} = \Bbbk[V]^G$, that is, the purely inseparable closure in $\Bbbk[V]$ of the normalization of A is equal to the ring of invariants (See Definitions A.0.4 and A.0.5 in Appendix A).*

Proof.
$\subset$: As $\Bbbk[V]^G$ is integrally closed (Proposition 2.3.11 in [11]), $\tilde{A} \subset \Bbbk[V]^G$, And so the desired inclusion holds in characteristic zero. Suppose $p > 0$, and take f in the purely inseparable closure of $\tilde{A}$ in $\Bbbk[V]$. There exist an $m \geq 0$ such that $f^{p^m} \in \tilde{A}$. For $\sigma \in G$, we have $(\sigma \cdot f - f)^{p^m} = \sigma \cdot f^{p^m} - f^{p^m} = 0$. Thus, $\sigma \cdot f - f = 0$, and so $f \in \Bbbk[V]^G$. $\supset$: Take $f \in \Bbbk[V]^G$. As the extension $Q(A) \subset Q(\Bbbk[V]^G)$ is purely inseparable, there exist a m such that $f^{p^m} \in Q(A)$. But f is integral over A, thus so is f^{p^m}, and as it is also in $Q(A)$, it follows that $f^{p^m} \in \tilde{A}$. Hence, $f \in \hat{\tilde{A}}$, and we are done. □

Although the converse of Theorem 3.2.8 does not hold in general, in positive characteristic, following Derksen and Kemper [12] (Remark 1.3), we obtain a similar characterization of geometric separating algebra. We use a slight variation of Sublemma A.5.1 of Wilbert van der Kallen [39]. Our proof is also essentially his.

Proposition 3.2.9 *Let $A \subset B$ be a finite extension of finitely generated algebras over a field $\Bbbk$ of characteristic $p > 0$. Set $Y = \operatorname{Spec}(A)$, and $X = \operatorname{Spec}(B)$, and suppose that the map of schemes corresponding to the inclusion is radicial. Then for all $b \in B$ there exists an m such that $b^{p^m} \in A$.*

Proof. We will argue by induction on the dimension of A.

As the extension $A \subset B$ is finite, B is finitely generated over A as an A-module, say by $b_1, \ldots, b_d$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be the minimal primes (A is a finitely generated $\Bbbk$-algebra, so there is a finite number of minimal primes).

Suppose we can show that for every i, j, we have $m_{i,j}$ such that $b_j^{p^{m_{i,j}}} \in A + \mathfrak{p}_i B$. Then for every i, we have m_i such that $b^{p^{m_i}} \in A + \mathfrak{p}_i B$ for all $b \in B$ (every b is a A-linear combinaison of the b_i's, so we can just take m_i to be the maximum of the $m_{i,j}$'s). Then, for all $b \in B$, $b^{p^{m_1 + \ldots + m_s}} \in A + \mathfrak{p}_1 \ldots \mathfrak{p}_s B$. Since

$$\mathfrak{p}_1 \ldots \mathfrak{p}_s \subset \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_s \subset \bigcap_{\mathfrak{p} \text{ is prime}} \mathfrak{p} = \sqrt{0},$$

(every ideal contains a minimal ideal) the ideal $\mathfrak{p}_1 \dots \mathfrak{p}_s$ is nilpotent, and so we can find a m such that for all $b \in B$, $b^{p^m} \in A$. As the extension $A \subset B$ is finite, for each $\mathfrak{p}_i$ there exists a prime ideal $\mathfrak{q}_i$ such that $\mathfrak{p}_i = \mathfrak{q}_i \cap A$, and thus the map $A/\mathfrak{p}_i \to B/\mathfrak{p}_i B$ into an inclusion. Moreover, the corresponding map of schemes is radicial. Indeed, given a homomorphism $f : A/\mathfrak{p}_i \to \mathbb{F}$ where $\mathbb{F}$ is any field, we get a homomorphism $A \to \mathbb{F}$. In turn, as the inclusion $A \subset B$ is radicial, we get a map $B \to \mathbb{F}$ which must factor through $B/\mathfrak{p}_i B$. It follows that it will suffice to show the proposition holds for the extensions $A/\mathfrak{p}_i \subset B/\mathfrak{p}_i B$. Therefore we can assume A is a domain.

Let $\mathfrak{r}$ denote the nilradical of B. Suppose we can show that for all $b \in B$, there is a m such that $b^{p^m} \in A + \mathfrak{r}$, then we can also find a u such that $b^{p^u} \in A$. So it will suffice to prove the proposition for the extension $A \subset B/\mathfrak{r}$. Note that the inclusion will remain radicial. Thus we may assume that B is reduced. But then one of the components of X must map onto Y, so bijectivity implies there is only one component. In other words B is also a domain.

Choose t so that the field extension $Q(A) \subset Q(AB^{p^t})$ is separable (so it is the separable closure of $Q(A)$ in $Q(B)$). Clearly the inclusion $A \subset AB^{p^t}$ is still radicial. If we suppose the proposition holds for the extension $A \subset AB^{p^t}$, then for all $b \in B$ there exists a m such that $b^{p^{t+m}} = (b^{p^t})^{p^m} \in A$, i.e., the proposition holds for $A \subset B$. Thus we may assume that the extension $Q(A) \subset Q(B)$ is separable. The fact that the homomorphism is radicial, however, implies that this same extension $Q(A) \subset Q(B)$ is purely inseparable, thus $Q(A) = Q(B)$.

We now consider the case where $Q(A) = Q(B)$. Let $\mathfrak{c}$ be the conductor of $A \subset B$. So $\mathfrak{c} = \{b \in B \mid bB \subset A\}$. We know it is non-zero (because B is a finite A-module, and $Q(A) = Q(B)$). If it is the unit ideal, then $B \subset A$ and we are done. Suppose it is not. By induction applied to $A/\mathfrak{c} \subset B/\mathfrak{c}$, we have that for each $b \in B$ there is a m such that $b^{p^m} \in A + \mathfrak{c} = A$. We are now done. □

We then obtain the following characterisation of geometrically separating algebras in characteristic $p > 0$ (when $\Bbbk[V]^G$ is finitely generated):

Corollary 3.2.10 *Suppose $\Bbbk$ has positive characteristic. If G is reductive, and if $A \subset \Bbbk[V]^G$ is a graded subalgebra, then $A \subset \Bbbk[V]^G$ is a geometric separating algebra if and only if $\widehat{A} = \Bbbk[V]^G$.*

Proof. Suppose that $\hat{A} = \Bbbk[V]^G$, and take $u, v \in \overline{V}$ such that $f(u) = f(v)$ for all $f \in A$. For each $h \in \Bbbk[V]^G$ there exists $r \in \mathbb{N}$ such that $h^{p^r} \in A$, hence, $h^{p^r}(u) = h^{p^r}(v)$. Furthermore,

$$\begin{aligned} h^{p^r}(u) \neq h^{p^r}(v) &\Rightarrow h^{p^r}(u) - h^{p^r}(v) \neq 0 \\ &\Rightarrow (h(u) - h(v))^{p^r} \neq 0 \\ &\Rightarrow h(u) - h(v) \neq 0 \\ &\Rightarrow h(u) \neq h(v). \end{aligned}$$

Thus, A is a geometric separating algebra.

On the other hand, suppose $A \subset \Bbbk[V]^G$ is a graded geometric separating algebra. Theorem 3.2.4 implies the map of schemes $V /\!\!/ G \to W$ is radicial, and Corollary 3.2.7 implies the extension $A \subset \Bbbk[V]^G$ is finite. Thus, by Propostion 3.2.9 every element of $\Bbbk[V]^G$ is a p-th power of an element of A, and so $\widehat{A} \supset \Bbbk[V]^G$. If h is in $\widehat{A}$, then there exists r in $\mathbb{N}$ such that h^{p^r} is in A. Let σ be any element of G, then

$$\begin{aligned} \sigma \cdot h^{p^r} = h^{p^r} &\Rightarrow (\sigma \cdot h)^{p^r} - h^{p^r} = 0 \\ &\Rightarrow (\sigma \cdot h - h)^{p^r} = 0 \quad , \\ &\Rightarrow \sigma \cdot h - h = 0. \end{aligned}$$

and so, $\widehat{A} \subset \Bbbk[V]^G$. □

3.2.4 Finite Groups

In this subsection, we concentrate on finite groups. As the ring of invariants separate orbits, we obtain a more concrete description of the separating scheme, which we exploit in Chapter 2.

We start with a proof that the ring of invariants separate orbits.

Definition 3.2.3. Let G be a finite group acting linearly on the n-dimensional $\Bbbk$-vector space V. We define $F_{T,U}$ as follows

$$F_{T,U} = \prod_{\sigma \in G} \left(T - \sum_{i=1}^{n} U^{i-1} \sigma \cdot x_i \right),$$

Where T, U are formal variables. Let $\Bbbk[\operatorname{coeff} F_{T,U}]$ be the subalgebra of $\Bbbk[V]$ generated by the coefficients of $F_{T,U}$ as a polynomial in T and U.

Proposition 3.2.11 (Lemma 2.1 in [14]) *If G is a finite group, then, $\Bbbk[\operatorname{coeff} F_{T,U}]$ is a geometric separating algebra. In particular, $\Bbbk[\operatorname{coeff} F_{T,U}]$ separates the G-orbits.*

Proof. Let G act trivially on T and U, then we see that elements of G act on F by permuting the factors. Thus F, and its coefficients, are invariant.

Take $u, v \in \overline{V}$ such that the coefficients of F agree on u and v, then $F(u) = F(v)$, and since $\overline{\Bbbk}[T, U]$ is factorial, ,

$$F(u) = \prod_{\sigma \in G} \left(T - \sum_{i=1}^{n} U^{i-1} \sigma \cdot u_i \right), \text{ and } F(v) = \prod_{\sigma \in G} \left(T - \sum_{i=1}^{n} U^{i-1} \sigma \cdot v_i \right)$$

have the same factors. In particular, for some $\tau \in G$,

$$T - \sum_{i=1}^{n} U^{i-1} u_i = T - \sum_{i=1}^{n} U^{i-1} \tau \cdot v_i.$$

Hence, for $i = 1, \ldots, n$, $u_i = \tau \cdot v_i$, that is, $u = \tau \cdot v$. It follows that u and v are in the same orbit, and so $f(u) = f(v)$ for any $f \in \Bbbk[V]^G$, and so the coefficients of $F_{T,U}$ for a geometric separating set. □

As the coefficients of F all have degree at most $|G|$, we obtain:

Corollary 3.2.12 (Lemma 2.1 in [14] and Corollary 3.9.14[11]) *If G is a finite group, then the $\Bbbk$-algebra generated by the invariants of degree at most $|G|$ is a geometric separating algebra.*

Proposition 3.2.13 *If G is a finite group, then the separating scheme is a union of $|G|$ linear subspaces, each of dimension n. There is a natural correspondence between these linear spaces and the elements of G. Moreover, if H_σ and H_τ denote the subspaces corresponding to the elements σ and τ of G, respectively, then the dimension of the intersection $H_\sigma \cap H_\tau$ is equal to the dimension of the subspace fixed by $\tau^{-1}\sigma$ in V.*

Proof. For each $\sigma \in G$, let H_σ be the graph of σ, that is

$$H_\sigma = \{(u, \sigma \cdot u) \in V \times V \mid u \in V\}.$$

H_σ is a linear space of dimension n. For elements σ and τ of G, the intersection $H_\sigma \cap H_\tau$ is

$$\{(u, v) \in V \times V \mid u \in V \text{ and } v = \sigma \cdot u = \tau \cdot u\}.$$

Hence, $H_\sigma \cap H_\tau$ is isomorphic to the fixed space of $\tau^{-1}\sigma$. Next, we show that

$$\mathcal{S}_G = \bigcup_{\sigma \in G} H_\sigma.$$

For each $\sigma \in G$, H_σ is given as a closed subscheme of $V \times V$ by the ideal $(f \otimes 1 - 1 \otimes \sigma^{-1} f \mid f \in \Bbbk[V])$. Thus, in algebraic terms, we want to show that

$$\frac{\Bbbk[V] \otimes_{\Bbbk} \Bbbk[V]}{\sqrt{(\delta(\Bbbk[V]^G))}} = \frac{\Bbbk[V] \otimes_{\Bbbk} \Bbbk[V]}{\cap_{\sigma \in G}(f \otimes 1 - 1 \otimes \sigma^{-1} f \mid f \in \Bbbk[V])}.$$

As G is finite, the ring of invariants separates orbits in $\overline{V}$ (Proposition 3.2.11), thus for u and v in $\overline{V}$, $f(u) = f(v)$, for all f in $\Bbbk[V]^G$, if and only if there exists σ in G such that $u = \sigma v$. In other words, $\delta(\Bbbk[V]^G) \subset \mathcal{I}_{\overline{V}^2}(u, v) \cap (\Bbbk[V] \otimes_{\Bbbk} \Bbbk[V])$, if and only if

$$\cap_{\sigma \in G}(f \otimes 1 - 1 \otimes \sigma^{-1} f \mid f \in \Bbbk[V]) \subset \mathcal{I}_{\overline{V}^2}(u, v) \cap (\Bbbk[V] \otimes_{\Bbbk} \Bbbk[V]).$$

Therefore, $\sqrt{(\delta(\Bbbk[V]^G))} = \cap_{\sigma \in G}(f \otimes 1 - 1 \otimes \sigma^{-1} f \mid f \in \Bbbk[V])$. □

Example 3.2.2 We now revisit Example 3.1.2. By Proposition 3.2.13 we know that the separating schemes consist of three 2-dimensional linear subspaces. They are given by

$$H_1 : \{(a, b, a, b) \mid a, b \in \mathbb{C}\},$$

$$H_\sigma : \{(a, b, \zeta_3 a, \zeta_3 b) \mid a, b \in \mathbb{C}\},$$

and

$$H_{\sigma^2} : \{(a, b, \zeta_3^2 a, \zeta_3^2 b) \mid a, b \in \mathbb{C}\}.$$

Thus the 3 planes intersect in exactly 1 point, the origin. ◁

Example 3.2.3 We reconsider the easy example of the trivial group acting on a 1-dimensional representation which we visited in Example 3.1.3. But this time, we allow more general fields. Theorem 3.2.1 and Proposition 3.2.13 provide us with a computational criterion for geometric separability.

By Proposition 3.2.13, the separating scheme is given by the ideal $\mathcal{I}(\mathcal{S}_G) = (x-y)$, thus $\{f_1, \ldots, f_r\}$ is a geometric separating set if and only if

$$\sqrt{(\delta(f_1), \ldots, \delta(f_r))} = (x - y),$$

which is equivalent to saying

$$(\delta(f_1), \ldots, \delta(f_r)) = (x - y)^k \mathbb{C}[x, y],$$

for some $k \geq 1$. As reduced Gröbner Bases are unique (for a fixed monomial order), and since $\{(x - y)^k\}$ is a reduced Gröbner basis for the ideal $(x - y)^k \mathbb{C}[x, y]$ for the monomial ordering grevlex with $x > y$ (for example), we have:

Proposition 3.2.14 *Let V be the 1-dimensional representation of the trivial group over an algebraically closed field $\mathbb{k}$. The subset $f_1, \ldots, f_r \in \mathbb{k}[x]$ is a geometric separating set if and only if the reduced grevlex Gröbner basis of the ideal $(\delta(f_1), \ldots, \delta(f_r))$ is $(x - y)^k$, for some $k \geq 1$*

◁

Chapter 4

Well-Behaved Geometric Separating Algebras

This chapter concentrates on well-behaved separating algebras. One can often find geometric separating algebras that are better behaved than the ring of invariants. For example, in Example 3.1.2, there is a hypersurface separating algebra when the ring of invariants is not even a complete intersection. More impressively, recall that there always is a finitely generated separating algebra (Proposition 3.2.2), even when the ring of invariants is not finitely generated.

In the following, we give more examples where very nice geometric separating algebras can be found, and we discuss limitations to how nice separating algebras can be given a representation of a group G. These limitations are consequences of the strong relationship between geometric separating algebras and the ring of invariants for reductive groups.

4.1 Polynomial Geometric Separating Algebras

The simplest structure a finitely generated $\Bbbk$-algebra may have is that of a polynomial ring. The question of when the ring of invariants is a polynomial ring has been central in the Invariant Theory of finite groups. In characteristic zero, and in the non-modular case in general, there is a characterization of representations for which the ring of invariants is polynomial, but in the modular case the question is still open. In this section, we generalize the existing results to geometric separating algebras, and obtain both a characterization of the representations for which a polynomial geometric separating algebra exists in the non-modular case, and a necessary condition in the modular case.

Recall that an element σ of G acts as a reflection on V if it fixes a codimension one subspace in V.

Theorem 4.1.1 *Let G be a finite group. If there exists a geometric separating algebra which is a polynomial ring, then the action of G on V is generated by reflections.*

Proof. Suppose a separating algebra A is a polynomial ring. By Corollary 3.2.5, A is n-dimensional, thus A is generated by n elements. It follows that the ideal $(\delta(A))$ is also generated by n elements. Indeed, if f and g are elements of A, then $\delta(fg) = (f \otimes 1)\delta(g) + (1 \otimes g)\delta(f)$, thus generators for A are generators for $\delta(A)$. Therefore, $V \times_W V$ is a complete intersection, and in particular, it is Cohen-Macaulay. As $V \times_W V$ is Noetherian, Hartshorne's Connectedness Theorem (Corollary 2.4 in [21]) implies that $V \times_W V$ is connected in codimension 1, and thus so is $\mathcal{S}_G = (V \times_W V)_{\text{red}}$.

Consider the irreducible components H_1 and H_σ of $\mathcal{S}_G$ corresponding to the identity and an arbitrary element σ of G, respectively. As $\mathcal{S}_G$ is connected in codimension 1, there is a sequence of irreducible components

$$H_1 = H_{\sigma_0}, \cdots, H_{\sigma_r} = H_\sigma,$$

such that $H_{\sigma_i} \cap H_{\sigma_{i+1}}$ has codimension 1. By Proposition 3.2.13, $\sigma_i^{-1}\sigma_{i+1}$ fixes a subspace of codimension 1, and so acts as a reflection on V. Thus,

$$\sigma = 1^{-1}\sigma = \sigma_0^{-1}\sigma_r = (\sigma_0^{-1}\sigma_1)(\sigma_1^{-1}\sigma_2)\cdots(\sigma_{r-1}^{-1}\sigma_r)$$

is a product of reflections on V. Therefore, the action of G on V is generated by reflections. □

As the ring of invariants is a geometric separating algebra, Theorem 4.1.1 is a generalization of the following result of Serre. Moreover, our method provides a new proof for this result.

Theorem 4.1.2 (Serre [36]) *Let G be a finite group. If $\Bbbk[V]^G$ is polynomial, then G acts on V as a reflection group.*

In the non-modular case, the converse holds:

Theorem 4.1.3 (Shephard and Todd [37], Chevalley [9], Serre, Clark and Ewing [10]) *Let G be a finite group, and suppose $|G|$ is invertible in $\Bbbk$. The ring of invariants is polynomial if and only if the action of G on V is generated by reflections.*

As a corollary to Theorem 4.1.1 and the more classical Theorem 4.1.3, we get a characterization of the existence of separating algebras which are polynomial rings which generalizes Theorem 4.1.3.

Theorem 4.1.4 *Let G be a finite group and let V be a finite dimensional representation of G over the field $\Bbbk$. Suppose further that the characteristic of $\Bbbk$ does not divide the order of G. There exists a geometric separating algebra which is a polynomial ring if and only if the action of G on V is generated by reflections.*

Proof. One direction is given by Theorem 4.1.1, and as the ring of invariants is a geometric separating algebra, the other is an immediate consequence of the part of the result of Shephard and Todd [37], Chevalley [9], Serre, and Clark and Ewing [10] which establishes that reflection groups have polynomial ring of invariants. □

Note that Theorem 4.1.4 implies that, in the non-modular case, there exists a polynomial separating algebra if and only if the ring of invariants in polynomial. A consequence of Theorem 3.2.8 is that in characteristic zero, graded separating algebras which are polynomial rings are the ring of invariants. This, however, does not hold in positive characteristic:

Example 4.1.1 Let $\Bbbk$ be a field of characteristic $p > 0$. Let V be the 1-dimensional representation of the trivial group over $\Bbbk$. Then $\Bbbk[V] = \Bbbk[V]^G = \Bbbk[x]$, hence the ring of invariants is polynomial. The subalgebra $\Bbbk[x^p]$ is a polynomial ring, and a separating algebra, but it is strictly included in $\Bbbk[x]$, the ring of invariants.

Another related remark is that Theorem 4.1.4 is new even in characteristic zero, because the statement does not include the assumption that the separating algebra be graded.

In the following examples, we find nontrivial polynomial separating algebras. They show that Theorem 4.1.1 is a strict generalization of Serre's result: there are cases where Serre's result does not apply, but where Theorem 4.1.1 does.

Example 4.1.2 Let $\Bbbk$ be a field of characteristic p, containing a root z of the polynomial $Z^p - Z - 1$. First, note that this polynomial is irreducible over $\mathbb{F}_p$. Let $G \leq GL(V)$ be the group given by

$$G = \langle r, s, t \rangle = \left\langle \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & z \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\rangle.$$

Let $\{y_2, x_2, y_1, x_1\}$ be the dual basis for V^*.

First, we prove that the ring of invariants of G, $\Bbbk[V]^G$, is generated minimally by x_1, x_2, M_1, M_2, and h, where

$$\begin{aligned} M_1 &= (y_1^p - x_1^{p-1}y_1)^p - (x_1^p)^{p-1}(y_1^p - x_1^{p-1}y_1), \\ M_2 &= (y_2^p - x_2^{p-1}y_2)^p - (x_1^p - x_2^{p-1}x_1)^{p-1}(y_2^p - x_2^{p-1}y_2), \\ h &= (x_1^{p-1} - x_2^{p-1})(y_1^p - x_1^{p-1}y_1) - x_1^{p-1}(y_2^p - x_2^{p-1}y_2). \end{aligned}$$

Let $H = \langle r, s\rangle$, and $L = \langle r, s, t_1, t_2\rangle$, where

$$t = t_1t_2 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & z \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The representation V, when restricted to the group $H \cong C_p \times C_p$, is the direct sum of two copies of the 2-dimensional representation of the cyclic group C_p. Therefore, the ring of invariants of H is

$$\Bbbk[V]^H = \Bbbk[x_1, Y_1 = y_1^p - x_1^{p-1}y_1, x_2, Y_2 = y_2^p - x_2^{p-1}y_2].$$

Now, we consider the group L. We will show that

$$\Bbbk[V]^L = \Bbbk[x_1, M_1 = Y_1^p - X_1^{p-1}Y_1, x_2, M_2 = Y_2^p - X_2^{p-1}Y_2],$$

where $X_1 = x_1^p$, and $X_2 = x_1^p - x_2^{p-1}x_1$. M_1 and M_2 are the norm under the action of L of y_1 and y_2 respectively. Thus M_1 and M_2 are L-invariant. Next, consider the zero set in V corresponding to the ideal $J = (x_1, M_1, x_2, M_2)$ in $\Bbbk[V]$. By Proposition 5.3.7 in [38], showing that the zero set of J is the origin will show that $\{x_1, M_1, x_2, M_2\}$ forms an homogeneous system of parameters in $\Bbbk[V]$, and hence, also in $\Bbbk[V]^L$. Take $v \in V$ in the zero set of J. If we write

$$v = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix},$$

then $x_1(v) = x_2(v) = 0$ implies that $b = d = 0$. Thus, $M_1(v) = c^{p^2}$ and $M_2(v) = a^{p^2}$. Therefore, $M_1(v) = M_2(v) = 0$ implies that $a = c = 0$, and so v is the origin. Since the product of the degrees of $\{x_1, M_1, x_2, M_2\}$ is $1 \cdot p^2 \cdot 1 \cdot p^2 = p^4 = |L|$, by Theorem 3.7.5 in [11], it follows that $\{x_1, M_1, x_2, M_2\}$ generates the ring of invariants of L as desired. Writing M_1 and M_2 the way we did highlights the connection between the invariants of G and those of two copies of the 2-dimensional representation of C_p. We will follow the computation of the ring of invariants of two copies of the 2-dimensional representation of C_p as in [4]. As in [4], there is an extra G-invariant $U = X_2Y_1 - X_1Y_2$, related to the previous ones by the relation:

$$U^p - X_2^p M_1 + X_1^p M_2 - (X_1X_2)^{p-1}U = 0.$$

But here, X_1 and X_2 are not irreducible invariants. Their greatest common divisor in $\Bbbk[V]^G$ is x_1, hence,

$$h = U/x_1 = (x_1^{p-1} - x_2^{p-1})Y_1 - x_1^{p-1}Y_2$$

is also G-invariant (and thus H-invariant).

We will show that $G \leq L$ together with the H-invariant h satisfy the hypothesis of Proposition 3.1 of [6]. The first step is to note that G has index p in L. Next, since $L = \langle G, t_1 \rangle$, we consider $(t_1 - 1)(h)$. Note that

$$\begin{aligned} t_1(Y_1) &= Y_1, \\ t_1(Y_2) &= Y_2 - X_2, \\ t_2^{-1}(Y_1) &= Y_1 + X_1, \text{ and} \\ t_2^{-1}(Y_2) &= Y_2. \end{aligned}$$

We have:

$$\begin{aligned} t_1(h) &= t_1(x_1^{p-1}Y_1 - (x_1^{p-1} - x_2^{p-1})Y_2) \\ &= x - 1^{p-1}Y_1 - (x_1^{p-1} - x_2^{p-1})(Y_2 - X_2) \\ &= h + (x_1^{p-1} - x_2^{p-1})X_2 \\ &= h + (x_1^{p-1} - x_2^{p-1})x_1^{p-1}, \end{aligned}$$

and so, $(t_1 - 1)h = (x_1^{p-1} - x_2^{p-1})x_1^{p-1}$ is G-invariant. The elements of $\Bbbk[V]^H$ are linear combinaisions of polynomials of the form $x_1^a x_2^b Y_1^c Y_2^d$, where a, b, c, d are nonnegative integers. We have:

$$t_1(x_1^a x_2^b Y_1^c Y_2^d) = x_1^a x_2^b Y_1^c (Y_2 - X_2)^d = x_1^a x_2^b Y_1^c (Y_2^d + X_2 A),$$

where A is a polynomial in X_2 and Y_2. We also have:

$$t_2^{-1}(x_1^a x_2^b Y_1^c Y_2^d) = x_1^a x_2^b (Y_1 + X_1)^c Y_2^d = x_1^a x_2^b (Y_1^c + X_1 B) Y_2^d,$$

where B is a polynomial in X_1 and Y_1. It follows that X_1 divides $(t_2^{-1} - 1)(x_1^a x_2^b Y_1^c Y_2^d)$, and X_2 divides $(t_1 - 1)(x_1^a x_2^b Y_1^c Y_2^d)$. If $c \in \Bbbk[V]^G$ is any G-invariant, then

$$t_1(c) = t_1 t_2 t_2^{-1}(c) = t_2^{-1} t(c) = t_2^{-1}(c),$$

hence, both X_1 and X_2 divide $(t_1 - 1)(c) = (t_2^{-1} - 1)(c)$, and so

$$(t_1 - 1)(h) = (x_1^{p-1} - x_2^{p-1})x_1^{p-1} = \mathrm{lcm}(X_1, X_2)$$

divides $(t_1 - 1)(c)$. Therefore, the hypotheses of Proposition 3.1 of [6] are verified, and so $\Bbbk[V]^G = \Bbbk[V]^L[h]$, as desired.

Thus, $\Bbbk[V]^G$ is an hypersurface. A generating relation is given by

$$h^p - (x_1^{p-1} - x_2^{p-1})^p M_1 + x_1^{p^2-p} M_2 - (x_1^p(x_1^{p-1} - x_2^{p-1}))^{p-1} h = 0,$$

which we can rewrite as

$$h^p = (x_1^{p-1} - x_2^{p-1})^p M_1 - x_1^{p^2-p}(M_2 - (x_1^{p-1} - x_2^{p-1})^{p-1} h).$$

Hence, h is in the purely inseparable closure of

$$\Bbbk[x_1, x_2, M_1, M_2' = (M_2 - (x_1^{p-1} - x_2^{p-1})^{p-1} h)],$$

and so, by Corollary 3.2.10, $S = \{x_1, x_2, M_1, M_2'\}$ is a geometric separating set which generates a polynomial geometric separating algebra. ◁

The following example arose in [7] as an example of rigid group with a non-polynomial ring of invariant.

Example 4.1.3 Let $\Bbbk$ be a field of characteristic p. Let G be the subgroup of $GL_4(\Bbbk)$ given by

$$G = \langle r, s, t \rangle = \left\langle \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\rangle .$$

Let y_2, y_1, x_2, x_1 be the dual basis for V^*. By Theorem 4.4 of [6], if $\Bbbk = \mathbb{F}_p$, the ring of invariants $\Bbbk[V]^G$ is a hypersurface minimally generated by x_1, x_2, M_1, M_2, and h, where

$$\begin{aligned} M_1 &= (y_1^p - x_1^{p-1}y_1)^p - (x_2^p - x_1^{p-1}x_2)^{p-1}(y_1^p - x_1^{p-1}y_1), \\ M_2 &= (y_2^p - x_2^{p-1}y_2)^p - (x_1^p - x_2^{p-1}x_1)^{p-1}(y_2^p - x_2^{p-1}y_2), \\ h &= x_1(y_1^p - x_1^{p-1}y_1) + x_2(y_2^p - x_2^{p-1}y_2), \end{aligned}$$

with the relation $h^p - x_1^p M_1 - x_2^p M_2 - (x_1 x_2(x_1^{p-1} - x_2^{p-1}))^{p-1}h = 0$.

In fact, this result holds over any field of characteristic p. A proof could be obtained by the same method as in Example 4.1.2.

We can rewrite the relation as

$$h^p = x_1^p M_1 + x_2^p M_2 + (x_1 x_2(x_1^{p-1} - x_2^{p-1}))^{p-1}h$$

As in Example 4.1.2 we change our generators to eliminate the h on the right hand side, however, this time there are infinitely many ways of doing so. Indeed, in

$$\begin{aligned}(x_1x_2(x_1^{p-1}-x_2^{p-1}))^{p-1} &= \textstyle\sum_{i=0}^{p-1}\binom{p-1}{i}(-1)^{p-1-i}x_1^{(i+1)(p-1)}x_2^{(p-i)(p-1)} \\ &= (-1)^{p-1}\textstyle\sum_{i=0}^{p-1}x_1^{(i+1)(p-1)}x_2^{(p-i)(p-1)} \\ & \quad \left(\text{since } \tbinom{p-1}{i}=(-1)^i\right)\end{aligned}$$

x_1^p divides all but the first term and x_2^{p-1} divide all but the last. Thus for each $(p-2)$-tuple $a \in \mathbb{k}^{p-2}$, we can rewrite the relation as

$$\begin{aligned}&h^p = x_1^p\left(M_1+\left(x_1^{(p-1)^2}x_2^{p-1}+(-1)^{p-1}\textstyle\sum_{i=1}^{p-2}a_ix_1^{i(p-1)-1}x_2^{(p-i)(p-1)}\right)h\right)+ \\ &x_2^p\left(M_2+\left(x_2^{(p-1)^2}x_1^{p-1}-(-1)^{p-1}\textstyle\sum_{i=1}^{p-2}(a_i-1)x_1^{(i+1)(p-1)}x_2^{(p-i)(p-1)-p}\right)h\right),\end{aligned}$$

Thus, for each $a=(a_1,\ldots,a_{p-2})\in\mathbb{k}^{p-2}$, setting

$$M_{1,a}=M_1+\left(x_1^{(p-1)^2}x_2^{p-1}+(-1)^{p-1}\sum_{i=1}^{p-2}a_ix_1^{i(p-1)-1}x_2^{(p-i)(p-1)}\right)h,$$

and

$$M_{2,a}=M_2+\left(x_2^{(p-1)^2}x_1^{p-1}-(-1)^{p-1}\sum_{i=1}^{p-2}(a_i-1)x_1^{i+1)(p-1)}x_2^{(p-i)(p-1)-p}\right)h,$$

yields a polynomial geometric separating algebra: $\mathbb{k}[x_1,x_2,M_{1,a},M_{2,a}]$. $\triangleleft$

4.2 Complete Intersection and Hypersurface Geometric Separating Algebras

In this section, we give a necessary condition on a representation of a finite group for the existence of a complete insersection separating algebra. We also include an example of Harm Derksen which shows that such nice separating algebras do not always exist. Our proof extends the argument used by Kac and Watanabe to prove their Theorem A in [25]. Moreover, it exploits the second geometric formulation of the notion of geometric separating algebra.

Theorem 4.2.1 *Let G be a finite group. If there exists a graded geometric separating algebra which is a complete intersection, then the action of G on V is generated by bireflections.*

Proof. Without loss of generality, we may assume that the base field is algebraically closed. Indeed, if A is a complete intersection graded geometric separating algebra inside of $\Bbbk[V]^G$, then $A \otimes_{\Bbbk} \overline{\Bbbk}$ is a complete intersection and a graded geometric separating algebra inside of $\overline{\Bbbk}[\overline{V}]^G$. Assuming the theorem holds over algebraically closed fields, it follows that G is generated by bireflection on $\overline{V}$. Thus, the action of G on V is also generated by bireflections.

Since G is finite, it is reductive, and so Theorem 3.2.4 implies that θ is a radicial morphism. As A is graded, Corollary 3.2.7 implies θ is finite. Finally, since θ is dominant and finite it is also surjective.

Now, let $\widehat{\Bbbk[V]}$, $\widehat{\Bbbk[V]^G}$, and $\widehat{A}$ be the completions of $\Bbbk[V]$, $\Bbbk[V]^G$, and A at their maximal graded ideal $\Bbbk[V]_+$, $\Bbbk[V]^G_+$, and A_+, respectively. A scheme is *simply connected* if and only if there are no nontrivial étale coverings ([22], Example 2.5.3). Hence, taking completions yields simply connected objects. The G-action on $\Bbbk[V]$ extends to a G-action on $\widehat{\Bbbk[V]}$, and $\widehat{\Bbbk[V]^G} = (\widehat{\Bbbk[V]})^G$. Thus $\operatorname{Spec}(\widehat{\Bbbk[V]^G}) = \widehat{V}/\!\!/G$, and the finite morphism π lifts to the quotient morphism $\widehat{\pi} : \widehat{V} \to \widehat{V}/\!\!/G$, which remains finite. Since $\widehat{\Bbbk[V]^G} = \Bbbk[V]^G \otimes_A \widehat{A}$ (Theorem 9.3A in [22]), taking the the completion corresponds to doing a base change. Hence, θ lifts to a morphism $\widehat{\theta}$ which is radicial, surjective, and finite, since all three properties are preserved by base changes: see Propositions 3.5.2 and 3.5.7 in [17], and 6.1.5 in [18].

For σ in G we let $\widehat{V}^{\sigma}$ denote the subscheme of fixed points of σ on $\widehat{V}$. Let L be the union of all the $\widehat{V}^{\sigma}$'s with codimension at least 3, and put $M = \widehat{\pi}(L)$, and $N = \widehat{\theta}(M)$.

Since W is a complete intersection, Proposition 3.2 of [21] implies $\widehat{W} = \mathrm{Spec}(\widehat{A})$ is also a complete intersection. Since $\widehat{\pi}$ and $\widehat{\theta}$ are finite, N has codimension 3 in $\widehat{W}$. Hence, by Lemma 1 from [25], $\widehat{W} \setminus N$ is simply connected. As the restriction of $\widehat{\theta}$ to $\widehat{V}/\!\!/G \setminus M$ is radicial, surjective, and finite, by Theorem 4.10 of [19] it follows that $(\widehat{V}/\!\!/G) \setminus M$ is also simply connected.

The scheme $X = \widehat{V} \setminus L$ is integral (see 2.1.8, [17]). Indeed, X is irreducible, and the local rings at points of X are localisations of the local rings at points of $\widehat{V}$, thus integral domains. Furthermore, X has an induced G-action, and $(\widehat{V}/\!\!/G) \setminus N = X/\!\!/G$. Since $X/\!\!/G$ is simply connected, Lemma 2 from [25] implies that G is generated by the set $\{G_x \mid x \in X = \widehat{V} \setminus L\}$, where G_x is the subgroup of G fixing x. But by the definition of $\widehat{V} \setminus L$, an element σ belongs to G_x for some $x \in \widehat{V} \setminus L$ if and only if $\mathrm{codim}(\widehat{V}^{\sigma}) \leq 2$. Hence, G is generated by bireflections. □

Nice properties of invariant rings are generally inherited by the invariant rings of isotropy subgroups. In [27], Kemper brings together all these results. Is the same true of separating algebras? If $\Bbbk[V]^G$ has a nice separating algebra will $\Bbbk[V]^{G_U}$ have an equally nice separating algebra? At the moment this remains unknown. However, using a result found in [27], which relates the two invariant rings, and using an argument similar to the one of Theorem 4.2.1, we can show that when there is a complete intersection geometric separating algebra, not only is G generated by bireflections, but so is every isotropy subgroup of the form G_u, where u is a closed point in V.

Theorem 4.2.2 *Let G be a finite group. If there exists a graded geometric separating algebra which is a complete intersection, then all the isotropy subgroups of points of the action of G on V are generated by bireflections.*

Proof. Without loss of generality, we may assume that the base field is algebraically closed. Indeed, if A is a complete intersection graded geometric separating algebra in

$\Bbbk[V]^G$, then $A \otimes_{\Bbbk} \overline{\Bbbk}$ is a complete intersection graded geometric separating algebra in $\overline{\Bbbk}[\overline{V}]^G$. If u is a closed point in V, then it is a closed point in $\overline{V}$. Assuming the theorem holds over algebraically closed fields, it follows that the action of G_u is generated by bireflection over $\overline{V}$. Thus, the action of G_u on V is also generated by bireflections.

Since G is finite, it is reductive, and so Theorem 3.2.4 implies that θ is a radicial morphism. As A is graded, Corollary 3.2.7 implies θ is finite. Finally, since θ is also dominant and finite morphisms are closed, θ is surjective.

Take u to be a closed point of V. Write π_G for the quotient morphism $V \to V/\!\!/G$, and write π_{G_u} for the quotient morphism $V \to V/\!\!/G_u$. Let $\widehat{\Bbbk[V]^G}_{\pi_G(u)}$, and $\widehat{A}_{\theta(\pi_G(u))}$ be the localization of $\Bbbk[V]^G$ and A, at the maximal ideals corresponding to $\pi_G(u)$, and $\theta(\pi_G(u))$, respectively. Let $\widehat{\Bbbk[V]}_0$, and $\widehat{\Bbbk[V]^{G_u}_{\pi_{G_u}(0)}}$ be the completion of $\Bbbk[V]$ and $\Bbbk[V]^{G_u}_{\pi_{G_u}(0)}$ at their maximal graded ideal.

A scheme is *simply connected* if and only if it there are no nontrivial étale coverings (see Example 2.5.3 in [22]). Hence, as complete local rings satisfy Hensel's Lemma , taking completions yields simply connected objects. The action of G_u on $\Bbbk[V]$ extend to an action of G_u on $\widehat{\Bbbk[V]}_0$. Moreover, $\widehat{\Bbbk[V]^{G_u}_{\pi_{G_u}(0)}} = \widehat{\Bbbk[V]}_0^{G_u}$. Thus $\operatorname{Spec}(\widehat{\Bbbk[V]^{G_u}_{\pi_{G_u}(0)}}) = \widehat{V_0}/\!\!/G_u$. Hence, the finite morphism π_{G_u} lifts to the quotient morphism $\widehat{\pi}_{G_u} : \widehat{V_0} \to \widehat{V_0}/\!\!/G_u$, which remains finite. Since $\widehat{\Bbbk[V]^G}_{\pi_G(u)} = \Bbbk[V]^G \otimes_A \widehat{A}_{\theta(\pi_G(u))}$ (Theorem 9.3A in [22]), taking the completion corresponds to doing a base change. Hence, θ lifts to a morphism $\widehat{\theta}$ which is radicial, surjective, and finite, since all three properties are preserved by base changes: see Propositions 3.5.2 and 3.5.7 in [17], and 6.1.5 in [18].

For σ in G_u we let $\widehat{V_0}^{\sigma}$ denote the subscheme of fixed points of σ on $\widehat{V_0}$. Let L be the union of all the V^{σ}'s with codimension at least 3, and put $M = \widehat{\pi_{G_u}}(L)$. By Proposition 1.3 of [27], $\widehat{\Bbbk[V]^G}_{\pi_G(u)}$ and $\widehat{\Bbbk[V]^{G_u}_{\pi_{G_u}(0)}}_0$ are isomorphic. Let N be the image in $\widehat{\Bbbk[V]^G}_{\pi_G(u)}$ of M under this isomorphism, and let $O = \widehat{\theta}(M)$. Since W is a complete intersection, Proposition 3.2 of [21] implies $\widehat{W} = \operatorname{Spec}(\widehat{A})$ is also a complete intersection. Since $\widehat{\pi_{G_u}}$, and $\widehat{\theta}$ are finite, N has codimension 3 in $\widehat{W}$. By Lemma 1 from [25], $\widehat{W} \setminus N$ is simply connected. As the restriction of $\widehat{\theta}$ to $\widehat{W} \setminus N$ is radicial, surjective, and finite, by Theorem 4.10 of [19] it follows that $(\widehat{V}/\!\!/G) \setminus N$ is simply connected. Since $\widehat{\Bbbk[V]^G}_{\pi_G(u)}$ and $\widehat{\Bbbk[V]^{G_u}}_{\pi_{G_u}(0)}$ are isomorphic, so are $\widehat{\Bbbk[V]^G}_{\pi_G(u)} \setminus M$ and $\widehat{\Bbbk[V]^{G_u}}_{\pi_{G_u}(0)} \setminus N$, and so $\widehat{\Bbbk[V]^{G_u}}_{\pi_{G_u}(0)} \setminus N$ is also simply connected.

Furthermore, $\widehat{V}_0 \setminus L$ is an integral scheme with an induced G_u-action. Furthermore, $(\widehat{V}_0/\!\!/G_u) \setminus N = (\widehat{V}_0 \setminus L)/\!\!/G_u$. Since $(\widehat{V}_0/\!\!/G_u) \setminus N$ is simply connected, Lemma 2 in [25] implies that G_u is generated by the set $\{G_x \mid x \in \widehat{V} \setminus L\}$. But by the definition of $\widehat{V} \setminus L$, an element σ belongs to G_x for some $x \in \widehat{V}_0 \setminus L$ if and only if $\operatorname{codim}(\widehat{V}_0^{\sigma}) \leq 2$. Hence, G_u is generated by bireflections. □

It would be interesting to see if this result could be extended to more general isotropy subgroups. Perhaps considering actions of algebraic groups on more general geometric objects would put us on the right track.

The following example, which precedes our results, shows that separating hypersurfaces cannot always be found. But it is a representation of an infinite group, and the method used does not appear to be adaptable to build a similar example of a finite group. This example motivated our interest in hypersurface, and complete intersection separating algebras for finite groups.

Example 4.2.1 (Harm Derksen) Let the element t of $G = \mathbb{C}^*$ act on the polynomial ring $\mathbb{C}[x_1, x_2, x_3, y_1, y_2]$, as

$$\begin{pmatrix} t & 0 & 0 & 0 & 0 \\ 0 & t & 0 & 0 & 0 \\ 0 & 0 & t & 0 & 0 \\ 0 & 0 & 0 & t^{-1} & 0 \\ 0 & 0 & 0 & 0 & t^{-1} \end{pmatrix}.$$

Monomials are sent to scalar multiples of themselves, and so the ring of invariants is generated by monomials. In fact,

$$\mathbb{C}[V]^{\mathbb{C}^*} = \mathbb{C}[x_1y_1, x_2y_1, x_3y_1, x_1y_2, x_2y_2, x_3y_2].$$

The dimension of $\mathbb{C}[V]^{\mathbb{C}^*}$ is equal to its transcendence degree (i.e., the maximal number of algebraically independent elements). The set $\{x_1y_1, x_3y_1, x_1y_2, x_2y_2\}$ forms a transcendence basis for $\mathbb{C}[V]^{\mathbb{C}^*}$. Indeed, they are clearly algebraically independent, and we have the relations

$$(x_1y_1)(x_3y_2) = (x_3y_1)(x_1y_2) \text{ and } (x_2y_2)(x_1y_1) = (x_2y_1)(x_1y_2),$$

which give x_3y_2 and x_2y_2 as roots of polynomials in the other generators. Thus, $\mathbb{C}[V]^{\mathbb{C}^*}$ has dimension 4.

As $\mathbb{C}^*$ is reductive, by Corollary 3.2.5, geometric separating algebras have dimension 4. Thus, a geometric separating algebra is a hypersurface if it is generated by 5 elements. We will prove that there are no geometric separating sets of 5 elements.

Suppose, by way of contradiction, that f_1, f_2, f_3, f_4, f_5 is a geometric separating set. As the f_i's are invariant, we can write:

$$f_i = F_i(x_1y_1, x_2y_1, x_3y_1, x_1y_2, x_2y_2, x_3y_2),$$

where each F_i is a polynomial in $\mathbb{C}[z_1, z_2, z_3, z_4, z_5, z_6]$. The ideal generated by the 5 polynomials

$$F_i(z_1, z_2, z_3, 0, 0, 0) - F_i(0, 0, 0, z_4, z_5, z_6), \ i = 1, \ldots, 5$$

corresponds to a subvariety of $\mathbb{C}^6$ which is either empty or has dimension at least 1. As the point $(0, 0, 0, 0, 0, 0)$ is a common zero, there are infinitely many solutions. In particular there is a non-zero solution (a, b, c, d, e, f). Put

$$u = (a, b, c, 1, 0) \text{ and } v = (d, e, f, 0, 1) \in V.$$

Then for all $i = 1, \ldots, 5$

$$f_i(u) = F_i(a, b, c, 0, 0, 0) = F_i(0, 0, 0, d, e, f) = f_i(v),$$

that is, the f_i's do not separate u and v. However, we have

$$\begin{aligned} x_1y_1(u) &= a, & x_1y_1(v) &= 0,\\ x_2y_1(u) &= b, & x_2y_1(v) &= 0,\\ x_3y_1(u) &= c, & x_3y_1(v) &= 0,\\ x_1y_2(u) &= 0, & x_1y_2(v) &= d,\\ x_2y_2(u) &= 0, & x_2y_2(v) &= e,\\ x_3y_2(u) &= 0, & x_3y_2(v) &= f, \end{aligned}$$

and as (a, b, c, d, e, f) is non zero, this is a contradiction. We conclude that no geometric separating algebra is a hypersurface. ◁

4.3 Cohen-Macaulay Geometric Separating Algebras

In characteristic zero, and in the non-modular case in general, the ring of invariants is always Cohen-Macaulay, thus Cohen-Macaulay separating algebras always exist. In the modular case, the ring of invariants is not Cohen-Macaulay in general. In fact, for almost all modular representations of a group G, the ring of invariants is not Cohen-Macaulay. Is there always a Cohen-Macaulay geometric separating algebra? This is certainly a hard question. It is not clear how it should be attacked. The result we have related to this question is an example where there is a Cohen-Macaulay separating algebra, but where the ring of invariants is not Cohen-Macaulay.

Example 4.3.1 Let G act on a 7-dimensional vector space V over $\mathbb{F}_2$ as follows:

$$\left\{ \left(\begin{array}{cccc|c} \multicolumn{4}{c|}{I_4} & 0 \\ \hline \alpha & 0 & 0 & \delta & \\ 0 & \beta & 0 & \delta & I_3 \\ 0 & 0 & \gamma & \delta & \end{array} \right) \mid \alpha, \beta, \gamma, \delta \in \mathbb{k} \right\}$$

Proposition 4.3.1 (Example 9.0.8, [8]) *If G is as above, then $\mathbb{F}_2[V]^G$ is not Cohen-Macaulay.*

Proposition 4.3.2 *Let G be as above, and suppose that $p = 2$, then there exists a Cohen-Macaulay separating algebra.*

Proof. Let $x_1, x_2, x_3, x_4, y_1, y_2, y_3$ be the dual basis for V^*. We start by showing that $E = \{x_1, x_2, x_3, x_4, n_1, n_2, n_3, n_{1,2}, n_{1,3}\}$, where

$$\begin{aligned} n_1 &= y_1(y_1 + x_1)(y_1 + x_4)(y_1 + x_1 + x_4), \\ n_2 &= y_2(y_2 + x_2)(y_2 + x_4)(y_2 + x_2 + x_4), \\ n_3 &= y_3(y_3 + x_3)(y_3 + x_4)(y_3 + x_3 + x_4), \\ n_{1,2} &= (y_1 + y_2)(y_1 + y_2 + x_1)(y_1 + y_2 + x_2)(y_1 + y_2 + x_1 + x_2), \\ n_{1,3} &= (y_1 + y_3)(y_1 + y_3 + x_3)(y_1 + y_3 + x_3)(y_1 + y_3 + x_1 + x_3)\}, \end{aligned}$$

forms a separating set. Note that n_1, n_2, n_3 are linear in the y_i variables, and $n_{1,2}, n_{1,3}$ are linear in the sums $(y_1 + y_i)$. Suppose that all the elements of E take the same value on the elements u and v of $\overline{V}$. The first thing to notice is that we will have $u = (w_1, w_2, w_3, w_4, u_1, u_2, u_3)$ and $v = (w_1, w_2, w_3, w_4, v_1, v_2, v_3)$, then $n_1(u) = n_1(v)$ implies $n_1(u_1 - v_1) = 0$, that is, either $u_1 = v_1$, $u_1 = v_1 + w_1$, $u_1 = v_1 + w_4$, or $u_1 = v_1 + w_4$. Similarly $n_1(u) = n_1(v)$ implies either $u_2 = v_2$, $u_2 = v_2 + w_2$, $u_2 = v_2 + w_4$, or $u_2 = v_2 + w_4$, and $n_3(u) = n_3(v)$ implies either $u_3 = v_3$, $u_3 = v_3 + w_3$,

$u_3 = v_3 + w_4$, or $u_3 = v_3 + w_4$. Thus,

$$u = \left(\begin{array}{cccc|c} & I_4 & & & 0 \\ \hline \alpha & 0 & 0 & \delta_1 & \\ 0 & \beta & 0 & \delta_2 & I_3 \\ 0 & 0 & \gamma & \delta_3 & \end{array}\right) v,$$

where $\alpha, \beta, \gamma, \delta_1, \delta_2, \delta_2 \in \mathbb{F}_2$.

Now, if we suppose $n_{1,2}(u) = n_{1,2}(v)$, then $n_{1_2}(u_1 + u_2 - v_1 - v_2) = 0$, and so either $u_1 + u_2 = v_1 + v_2$, $u_1 + u_2 = v_1 + v_2 + w_1$, $u_1 + u_2 = v_1 + v_2 + w_2$, or $u_1 + u_2 = v_1 + v_2 + w_1 + w_2$. But $u_1 + u_2 = v_1 + v_2 + \alpha w_1 + \beta w_2 + (\delta_1 + \delta_2) w_4$, thus $\delta_1 = \delta_2$. Similarly, we obtain that $\delta_1 = \delta_3$. Therefore, u and v are in the same orbit. Note that, unlike many of the other examples presented in this text, we found a separating set without computing the ring of invariants.

In the rest of the argument, we will be using the computational algebra software Magma [2] for our computations, and for verifying that polynomials belong to certain ideals. Taking $x_1, x_2, x_3, x_4, n_1, n_2, n_3$ as primary invariants, we get 4 secondary invariants which we denote by h_1, h_2, h_3, h_4. As $n_{1,2} = n_1 + n_2 + (x_1 + x_2 + x_4)h_1$, and $n_{1,3} = n_1 + n_3 + (x_1 + x_3 + x_4)h_2$, the set $\{x_1, x_2, x_3, x_4, n_1, n_2, n_3, h_1, h_2\}$ is a separting set, and $A = \mathbb{F}_2[x_1, x_2, x_3, x_4, n_1, n_2, n_3, h_1, h_2]$ is a separating algebra. We shall show that A is Cohen-Macaulay. We do this by proving that $x_4, n_2, n_1, x_1, x_2, x_3, n_3$ forms a regular sequence. To obtain the ideal of relations between x_1 ,x_2, x_3, x_4, n_1, n_2, n_3, h_1, and h_2, we take the relation ideal of the ring of invariants and eliminate the variables h_3 and h_4. This ends up getting rid of the "bad" relations, the ones that cause the ring of invariants not to be Cohen-Macaulay. If we view $x_1, x_2, x_3, x_4, n_1, n_2, n_3, h_1, h_2$ as variables, then we get A as a quotient of the polynomial ring $S = \mathbb{F}_2[x_1, x_2, x_3, x_4, n_1, n_2, n_3, h_1, h_2]$, that is, $A \cong S/I$. As A is a domain, I is prime, and any element not contained in I is regular in $A \cong S/I$. In particular, x_4 is regular sequence. The ideal (I, x_4), is again prime. Since n_2 does not belong to

(I, x_4), n_2 is regular in $A/(x_4) \cong S/(I, x_4)$. The ideal (I, x_4, n_2) is again prime, and since it does not contain n_1, n_1 is regular in $A/(x_4, n_2) \cong S/(I, x_4, n_2)$. The ideal (I, x_4, n_2) is not prime, but it is primary, and so elements taken outside its radical are regular in the quotient $A/(x_4, n_2, n_1) \cong S/(I, x_4, n_2, n_1)$. In particular, x_1 is not in the radical of (I, x_4, n_2, n_1), and so x_1 is regular in $A/(x_4, n_2, n_1) \cong S/(I, x_4, n_2, n_1)$. The ideal (I, x_4, n_2, n_1, x_1) is again primary, and its radical does not contain x_2. The ideal $(I, x_4, n_2, n_1, x_1, x_2)$ is also primary, and its radical does not contain x_3. Finally, the ideal $(I, x_4, n_2, n_1, x_1, x_2, x_3)$ is primary as well, and its radical does not contain n_3. We conclude that $x_4, n_2, n_1, x_1, x_2, x_3, n_3$ forms a regular sequence as desired, and so A is Cohen-Macaulay. □

◁

Chapter 5

Small Separating Sets

This chapter is all about geometric separating sets, and especially small ones. We give a bound on the minimal size possible for a separating set over algebraically closed fields, and compute some separating sets explicitely.

5.1 A bound on the size of Small Separating Sets

For reductive groups, Corollary 3.2.5 says separating sets must have at least n elements. In this section, we give an upper bound on the size of small separating sets depending only on the dimension of the representation. Our result, however, holds only over algebraically closed fields.

Proposition 5.1.1 [1] *If V is a n-dimensional representation of G, then a separating set of size $2n + 1$ exists.*

Proof. Suppose $\{f_1, \ldots, f_s\}$ is a finite separating set (we know such a set exists by

[1] *This approach was suggested by Corrado De Concini and Friedrich Knop at a conference at the Fields Institute in summer 2006 . Antonio Laface, then a postdoctoral fellow at Queen's University also provided some help in fixing up the details. It now appears that Gregor Kemper and Harm Derksen were aware of this bound as early as 2004. Kemper did not appear to be aware of this bound in his later publications on separating invariants.*

Proposition 3.2.2). We have the following commutative diagram

$$\begin{tikzcd} V = \Bbbk^n \arrow[r, "\phi"] \arrow[d, "i"'] & \Bbbk^s \arrow[d, "j"] \\ \mathbb{P}^n \arrow[r, "\psi"] & \mathbb{P}^s \end{tikzcd}$$

with

$$\begin{array}{rrcl} \phi : & (x_1, \ldots, x_n) & \longmapsto & (f_1(x_1, \ldots, x_n), \ldots, f_s(x_1, \ldots, x_n)), \\ i : & (x_1, \ldots, x_n) & \longmapsto & [1 : x_1 : \ldots : x_n], \\ j : & (y_1, \ldots, y_s) & \longmapsto & [1 : y_1 : \ldots : y_s], \\ \psi : & [x_0 : x_1 : \ldots : x_n] & \longmapsto & [x_0^d : F_1(x_0, x_1, \ldots, x_n) : \ldots : F_s(x_1, \ldots, x_n)], \end{array}$$

where $d = \max_i\{\deg f_i\}$, and F_i is the result of the homogenization (using x_0) of f_i to an homogeneous polynomial of degree d for all i.

Let H be an hyperplane in $\mathbb{P}^s$. Given $q \notin H$ we can project $\mathbb{P}^s \setminus \{q\}$ on H from q, and so get a map:

$$\pi_q : \mathbb{P}^s \setminus \{q\} \to H = \mathbb{P}^{s-1}.$$

Suppose this map is defined and injective on $\overline{\psi(\mathbb{P}^n)}$. The image of the open affine $j(k^s)$ is contained in an open affine $U \subset \mathbb{P}^{s-1}$ and so the restriction of π to $j(\Bbbk^s)$ gives a map

$$\tau : \Bbbk^s \longrightarrow U = \Bbbk^{s-1}.$$

As π_q is injective on $\overline{\psi(\mathbb{P}^n)}$, τ is injective on $\phi(\Bbbk^n)$. The map τ is given by

$$\tau : (y_1, \ldots, y_s) \mapsto (\tau_1(y_1, \ldots, y_s), \ldots, \tau_{s-1}(y_1, \ldots, y_s)),$$

where the τ_i's are polynomials

Then $\{h_i = \tau_i(f_1, \ldots, f_s) \mid 1 \leq i \leq s-1\}$ separates. Indeed, take $u, v \in V = \Bbbk^n$ and suppose that $h_i(u) = h_i(v)$ for each i, then as τ is injective on the image of $\phi = (f_1, \ldots, f_s)$, it follows that $f_j(u) = f_j(v)$ for all $1 \geq j \geq s$. Finally, since the f_j's separate, $f(u) = f(v)$ for all $f \in \Bbbk[V]^G$.

So whenever we can choose q such that the projection π from q onto H is injective we can get a finite separating with one less element. The projection π_q will be injective on $\overline{\psi(\mathbb{P}^n)}$ when any line going through q intersects $\overline{\psi(\mathbb{P}^n)}$ in at most one point, i.e., when no secant of $\overline{\psi(\mathbb{P}^n)}$ contains q. So picking a point q in

$$(\mathbb{P}^s \setminus H) \cap (\mathbb{P}^s \setminus sec(\overline{\psi(\mathbb{P}^n)})$$

will make the projection π injective on $\overline{\psi(\mathbb{P}^n)}$. As long as neither of these sets is empty, their intersection is nonempty (they are open sets). Thus, the intersection will be empty if and only

$$\dim(sec(\overline{\psi(\mathbb{P}^n)})) = s.$$

But,

$$\dim(sec(\overline{\psi(\mathbb{P}^n)})) \leq 2\dim(\overline{\psi(\mathbb{P}^n)}) + 1 \leq 2n + 1.$$

Indeed, $\overline{\psi(\mathbb{P}^n)}$ has the same dimension as the ring of invariants, which, in turn, has dimension less than n.

So when $2n+1 < s$, we can get a separating set of size $s-1$. This guarantees the existence of a separating set of size at most $2n+1$. □

5.2 Small Separating Sets

In this section, we construct small separating sets for various families of examples. We start with finite dimensional representations of cyclic groups, then consider abelian subgroups of $GL(2, \mathbb{C})$, and finally non-abelian subgroups of $GL(2, \mathbb{C})$ with monomial action.

5.2.1 Finite Dimensional Representations of Finite Cyclic Groups

Another interesting class of examples in invariant theory are the invariants of the representations of finite cyclic groups. They are some of the best understood examples.

Proposition 5.2.1 *If V is a n-dimensional representation of the cyclic group of order m over a field $\Bbbk$ containing a primitive m-th root of unity, then there is a separating set consisting of $n + \binom{n}{2}$ monomials.*

Proof. If V is a n-dimensional representation of the cyclic group of order m over a field containing a primitive m-th root of unity, then there is a basis for which it is given by:

$$\sigma \mapsto \begin{pmatrix} \zeta_{m_1} & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & \zeta_{m_{n-1}} & 0 \\ 0 & \cdots & 0 & \zeta_{m_n} \end{pmatrix},$$

where $m_i | m$, and ζ_{m_i} is a primitive m_i-th root of unity. We will show that the set

$$E = \{x_i^{m_i}, x_j^{a_{j,k}} x_k^{b_{j,k}} \mid i = 1, \cdots, n, \text{ and } 1 \leq j < k \leq n\},$$

where $a_{j,k}$ is minimal such that there exist $b_{j,k} < m_k$ with $x_j^{a_{j,k}} x_k^{b_{j,k}}$ invariant, is a geometric separating set.

If the $x_i^{m_i}$ agree on u and v, then we know that $u_i = \zeta_{m_i}^{\alpha_i} v_i$. Since by Proposition 5.2.3, for each pair (i, j), $E_{i,j} = \{x_i^{m_i}, x_i^{a_{i,j}} x_j^{b_{i,j}}, x_j^{m_j}\}$ is a geometric separating set for the corresponding subrepresentation, we get that all the α's are equal by looking at each 2-dimensional subrepresentation corresponding to (x_i, x_j). Note that when $v_i = 0$, we already know that $u_i = 0$, and putting any value for α_i will do. □

Proposition 5.2.2 *Let $G = \langle\sigma\rangle$ be the cyclic group of order m, and consider the n-dimensional representation*

$$\sigma \mapsto \begin{pmatrix} \zeta_m^{d_1} & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & \zeta_m^{d_{n-1}} & 0 \\ 0 & \cdots & 0 & \zeta_m \end{pmatrix},$$

where ζ_m is a primitive mth root of unity, and $d_{n-1}|d_{n-2}|\dots|d_1|m$. Then there exists a separating set of size $2n-1$.

Proof. For $k = 2, \cdots, 2n$, for k odd, set

$$f_k = \sum_{\substack{1 \le i \le j \le n \\ i+j=k}} x_i x_j^{\frac{d_i}{d_j}(\frac{m}{d_i}-1)},$$

and for k even, set

$$f_k = x_{k/2}^{m/d_i} + \sum_{\substack{1 \le i \le j \le n \\ i+j=k}} x_i x_j^{\frac{d_i}{d_j}(\frac{m}{d_i}-1)},$$

This coresponds to adding the terms on the diagonal of the following triangle:

$$\begin{array}{cccccc}
x_1^{\frac{m}{d_1}} & x_1x_2^{\frac{d_1}{d_2}(\frac{m}{d_1}-1)} & x_1x_3^{\frac{d_1}{d_3}(\frac{m}{d_1}-1)} & \cdots & x_1x_{n-1}^{\frac{d_1}{d_{n-1}}(\frac{m}{d_1}-1)} & x_1x_n^{d_1(\frac{m}{d_1}-1)} \\
 & x_2^{\frac{m}{d_2}} & x_2x_3^{\frac{d_2}{d_3}(\frac{m}{d_2}-1)} & \cdots & x_2x_{n-1}^{\frac{d_2}{d_{n-1}}(\frac{m}{d_2}-1)} & x_2x_n^{d_2(\frac{m}{d_2}-1)} \\
 & & x_3^{\frac{m}{d_3}} & \cdots & x_3x_{n-1}^{\frac{d_3}{d_{n-1}}(\frac{m}{d_3}-1)} & x_3x_n^{d_3(\frac{m}{d_3}-1)} \\
 & & & \ddots & \vdots & \vdots \\
 & & & & x_{n-1}^{\frac{m}{d_{n-1}}} & x_{n-1}x_n^{d_{n-1}(\frac{m}{d_{n-1}}-1)} \\
 & & & & & x_n^m
\end{array}$$

By Proposition 5.2.1 the terms in the triangle form a separating set. We will prove by induction on n that $f_2, \ldots, f_{2n}$ forms a geometric separating set. It suffices to show that we can express all the terms of the triangle in terms of the diagonal sums f_i. If $x_n = 0$, then the whole last column is zero, $f_n = 0$, and by the induction hypothesis, $f_2, \ldots, f_{n-1}$ form a geometric separating set. Suppose $x_n \neq 0$, then we may divide by $x_n^{\frac{m}{d_n}}$. We express the terms in the first $n-1$ colums using elements of the last colum that lie on the same line, or below, and we get elements of the last column by substracting all the other terms of the appropriate f_i. Doing this, diagonal, by diagonal, starting at the bottom, will ensure that at each step we are using only terms we already know. We have

$$x_i^{\frac{m}{d_i}} = \frac{\left(x_i x_n^{\frac{d_i}{d_n}(\frac{m}{d_i}-1)}\right)^{\frac{m}{d_i}}}{(x_n^m)^{\left(\frac{m}{d_i}-1\right)}},$$

and

$$x_i x_j^{\frac{d_i}{d_j}(\frac{m}{d_i}-1)} = \frac{x_i x_n^{d_i(\frac{m}{d_i}-1)} \left(x_j x_n^{d_j\left(\frac{m}{d_j}-1\right)}\right)^{\frac{d_i}{d_j}\left(\frac{m}{d_i}-1\right)}}{(x_n^m)^{\left(\frac{m}{d_i}-1\right)}}.$$

and so we are done. □

Although we cannot provide a proof, we believe that this “triangle trick” will work in general. The problems we encounter when trying to come up with a proof is, on one hand, that whether the trick works or not depends on how we order the primitive roots of unity on the diagonal, on the other hand, it is a bit hard to find the correct notation. Here is an example not covered by the proposition, for which we can make the trick work.

Example 5.2.1 Let G be the cylic group of order 12, and let $\Bbbk$ be a field containing a primitive 12-th root of unity ζ_{12}. We consider the representation given by

$$\sigma \mapsto \begin{pmatrix} \zeta_{12}^6 & 0 & 0 & 0 & 0 \\ 0 & \zeta_{12}^3 & 0 & 0 & 0 \\ 0 & 0 & \zeta_{12}^4 & 0 & 0 \\ 0 & 0 & 0 & \zeta_{12}^2 & 0 \\ 0 & 0 & 0 & 0 & \zeta_{12}^2 \end{pmatrix}.$$

Then by Proposition 5.2.1 the terms in the following triangle form a separating set:

$$\begin{array}{ccccc} x_1^2 & x_1x_2^2 & & x_1x_4^3 & x_1x_5^3 \\ & x_2^4 & & x_2^2x_4^3 & x_2^2x_5^3 \\ & & x_3^3 & x_3x_4^4 & x_3x_5^4 \\ & & & x_4^6 & x_4x_5^5 \\ & & & & x_5^6 \end{array}$$

The empty spots correspond to the 2-dimensional representations which have polynomial invariants. We will prove that x_5^6, $x_4x_5^5$, $x_4^6+x_3x_5^4$, $x_3x_4^4+x_2^2x_5^3$, $x_3^3+x_2^2x_4^3+x_1x_5^3$, $x_1x_4^3$, $x_1x_2^2$, and x_1^2 form a separating set. We have

$$x_4^6 = \frac{\left(x_4x_5^5\right)^6}{\left(x_5^6\right)^5},$$

and so $x_3x_5^4 = (x_4^6 + x_3x_5^4) - x_4^6$. Next,

$$x_3x_4^4 = \frac{x_3x_5^4\left(x_4x_5^5\right)^4}{\left(x_5^6\right)^4},$$

and so $x_2^2x_5^3 = (x_3x_4^4 + x_2^2x_5^3) - x_3x_4^4$. Next,

$$x_3^3 = \frac{\left(x_3x_5^4\right)^3}{\left(x_5^6\right)^2},$$

and

$$x_2^2x_4^3 = \frac{x_2^2x_5^3\left(x_4x_5^5\right)^3}{\left(x_5^6\right)^3},$$

and so $x_1x_5^3 = (x_3^3 + x_2^2x_4^3 + x_1x_5^3) - x_3^3 - x_2^2x_4^3$. ◁

5.2.2 Finite Subgroups of $GL(2, \mathbb{C})$

Example 5.2.2 (Finite abelian subgroups of $GL(2, \mathbb{C})$) Note that the results presented here are a special case of the result presented by Neusel and Sezer for representations of abelian groups. The separating sets we find here are of size 3, which is the minimum possible for groups that are not reflection groups.

Following Huffman [24], if G is a finite abelian subgroup of $GL(2, \mathbb{C})$ of exponent e, then $G \cong \mathbb{Z}_e \times \mathbb{Z}_f$, where $g = e/f \in \mathbb{Z}$. Let ζ_e be a primitive e-th root of unity. Furthermore,

$$G = \left\langle \begin{pmatrix} \zeta_e^{v_1} & 0 \\ 0 & \zeta_e^{v_2} \end{pmatrix}, \begin{pmatrix} \zeta_e^{g} & 0 \\ 0 & \zeta_e^{gd} \end{pmatrix} \right\rangle,$$

with $(j, e) = 1$, $v_1|e$, $v_2|ej$, $(v_1, v_2) = 1$, $d|e$, and $(d, v_1) = (d, v_2) = 1$ (see Lemma 2.1 in [24]).

Set $m = e/v_1$ and $n = ej/v_2$, then Huffman (Theorem 3.1 in [24]) proves that the ring of invariants $\mathbb{C}[V]^G$ is generated by

$$\{x^m, y^n\} \cup \{x^{lfv_2+k(l)m}y^{lfv_1} \mid 0 \leq lfv_1 < n \text{ and } 0 \leq lfv_2 + k(l)m < m\}.$$

Note that for each l there is a unique $k(l)$ satisfying the given property. Also, if the ring of invariants is polynomial, there will be no l satisfying the condition. Furthermore, in this case, we know automatically that there is a polynomial separating algebra (as the ring of invariants separates).

Proposition 5.2.3 *Suppose the ring of invariants is not polynomial, then the set $\{x^m, y^m, x^{fv_2+k(1)m}y^{fv_1}\}$ separates.*

Proof. First recall that as

$$\{x^m, y^n, x^{lfv_2+k(l)m}y^{lfv_1} | 0 < lfv_1 < n,\ 0 < lfv_2 + k(l)m < m\}$$

generates the ring of invariants, it also separates. Thus, it will suffice to express these invariants in terms of x^m, y^n, and $x^{fv_2+k(1)m}y^{fv_1}$. If $x^m = 0$ at a point, then $x = 0$

and so $x^{lfv_2+k(l)m}y^{lfv_1} = 0$ for all l. Note that y^n is not determined when $x = 0$, and so we really need it. For points where $x^m \neq 0$, we have

$$x^{lfv_2+k(l)m}y^{lfv_1} = \frac{(x^{fv_2+k(1)m}y^{fv_1})^l}{(x^m)^{lk(1)-k(l)}}$$

□

◁

Example 5.2.3 (Finite Non-abelian monomial subgroups of $GL(2,\mathbb{C})$*)* The separating sets we construct here are of size 3 or 4. We do not know if the separating sets of size 4 generate complete intersection rings. In any case 4 is smaller than $2n+1$, the bound we get in Proposition 5.1.1.

Consider finite non-abelian subgroups of $GL(2,\mathbb{C})$ which have monomial action, that is, each group element sends monomials to monomials. These groups corresponds to type 2 of Huffman's classification of finite subgroups of $GL(2,\mathbb{C})$ ([24], Lemma 2.2). Following Huffman, if G is a non-abelian finite subgroup of $GL(2,\mathbb{C})$ with monomial action, then

$$G = \left\langle \begin{pmatrix} \zeta_e & 0 \\ 0 & \zeta_e^j \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & \zeta_e^g \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ \alpha & 0 \end{pmatrix} \right\rangle,$$

where ζ_e is a primitive e-th root of unity and α, a primitive 2^b-th root of unity. Moreover, the integers, e, g, $f = e/g$, b, and j satisfy the following four relations:

1. $(e,j) = 1$
2. $g|(j^2-1)$
3. $2^b|e$
4. $\frac{2^b}{(2^b,f)}|(j-1)$

Invariants are linear combinations of polynomials of the form x^ly^l and $x^ky^l+\beta x^ly^k$. Furthermore, Huffman shows:

Lemma 5.2.4 (Lemma 3.2 in [24])
If $m = lcm\left(\frac{g}{(g,j+1)}, \frac{2^b}{(2^b,f)}\right)$, then,

1. *$x^l y^l \in \Bbbk[V]^G$ if and only $mf|l$;*

2. *if $k \neq l$, then $x^k y^l + \beta x^l y^k \in \Bbbk[V]^G$ if and only if $e|(k+jl)$, $f|l$, $f|k$, and $\beta = \alpha^l$;*

3. *moreover if $k \neq l$ and $x^k y^l + \beta x^l y^k \in \Bbbk[V]^G$, then $2^b|(k+l)$;*

It follows that the invariants are linear combinations of polynomials in the set $E = E_1 \cup E_2$, where $E_1 = \left\{x^{lmf} y^{lmf} \mid l \in \mathbb{N}\right\}$, and

$$E_2 = \left\{x^{kf} y^{lf} + \alpha^{lf} x^{lf} y^{kf} \mid g|(k+jl), \text{ where } k \neq l \in \mathbb{N}\right\}.$$

Note that if $x^{kf} y^{lf} + \alpha^{lf} x^{lf} y^{kf}$ is in E_2, then part 3 of the lemma implies that $2^b/(2^b, f)$ divides $k + jl$.

We can, in fact, give a more precise description of the invariants in E_2. But first, we recall a well known result from number theory. We refer to [30], although this result can be found in any book on elementary number theory.

Theorem 5.2.5 (Theorem 6.3 in [30]) *If a, b, and c are integers, and set $d = (a, b)$, then the diophantine equation $aw + bu = c$ admits integer solutions if and only if $d|c$, in which case the solutions are given by $w = w_0 - t\frac{b}{d}$, and $u = u_0 + t\frac{a}{d}$,where t is any integer and $w = w_0$, $u = u_0$ gives a particular solution to the diophantine equation.*

We now go back to our situation.

Proposition 5.2.6 *Let u_0 be minimal among the positive integers for which there exists an integer w_0 such that $gw_0 - (j+1)u_0 = (g, j+1)$. The invariants in E_2 are given by $x^{kf} y^{lf} + \alpha^{lf} x^{lf} y^{kf}$, where $l = u_0 a + t\frac{g}{(g,j+i)}$, and $k = u_0 a + t\frac{g}{(g,j+i)} + a(g, j+1)$, where a and t are integers such that $u_0 a + t\frac{g}{(g,j+i)} \geq 0$.*

Proof. On one hand, we show that if l and k are as above, then $x^{kf}y^{lf} + \alpha^{lf}x^{lf}y^{kf}$ is invariant. It suffices to show that $g|(k + jl)$. We have

$$\begin{aligned} k + jl = & \quad u_0a + t\tfrac{g}{(g,j+1)} + a(g, j + 1) + j\left(u_0a + t\tfrac{g}{(g,j+i)}\right) \\ = & \quad (j + 1)u_0a + (j + 1)t\tfrac{g}{(g,j+i)} + a(g, j + 1) \\ = & \quad (gw_0 - (g, j + 1))a + tg\tfrac{(j+1)}{(g,j+1)} + a(g, j + 1) \\ = & \quad gw_0 + tg\tfrac{(j+1)}{(g,j+1)} \equiv 0 \pmod{g}. \end{aligned}$$

On the other hand, suppose that k and l satisfy $g|(k+jl)$, that is, $x^{kf}y^{lf}+\alpha^{lf}x^{lf}y^{kf}$ is invariant. First, since $k - l = k + jl - (j + 1)l$, $(g, g + 1)$ divides $k - l$. Hence, $k = l + a(g, j + 1)$, where a is an integer. Thus, $g|(k + jl)$ translates to

$$gx = l + a(g, j + 1) + jl = (j + 1)l + a(g, j + 1),$$

for some integer x, and equivalently, $gx - (j + 1)l = a(g, j + 1)$. By Theorem 5.2.5, it follows that $l = u_1 + t\frac{ag}{(g,j+1)}$, where $\{w_1,u_1\}$ is a particular solution to the diophantine equation $gw - (j + 1)u = ga$. Finally, we note that $w = aw_0$ and $u = au_0$ give a solution to the diophantine equation $gw - (j + 1)u = ag$, thus, $l = au_0 + t\frac{ag}{(g,j+1)}$, and $k = l + a(g, j + 1) = au_0 + t\frac{ag}{(g,j+1)} + a(g, j + 1)$, for some integer t. □

To make the following easier to read (or at least faster to write), let us introduce a shorthand notation for invariants of the form $x^{kf}y^{lf} + \alpha^{lf}x^{lf}y^{kf}$. We will denote the invariant $x^{kf}y^{lf} + \alpha^{lf}x^{lf}y^{kf}$ by $[k, l]$. As

$$\begin{aligned} &(x^{kf}y^{lf} + \alpha^{lf}x^{lf}y^{kf})(x^{k'f}y^{l'f} + \alpha^{l'f}x^{l'f}y^{k'f}) = \\ &\qquad x^{(k+k')f}y^{(l+l')f} + \alpha^{(l+l')f}x^{(l+l')f}y^{(k+k')f} \\ &\qquad\qquad + \alpha^{l'f}\left(x^{(k+l')f}y^{(l+k')f} + \alpha^{(l+k')f}x^{(l+k')f}y^{(k+l')f}\right), \end{aligned}$$

we have

$$[k, l][k', l'] = [k + k', l + l'] + \alpha^{l'f}[k + l', l + k'].$$

What if $k + l' = l + k'$ or $k + k' = l + l'$? Well, first note that since $k \neq l$ and $k' \neq l'$, these two equalities cannot be both satisfied at the same time. The term where we do not have equality will be invariant, indeed,

$$k + k' + j(l + l') = k + jl + k' + jl' \cong 0 \pmod g,$$

and

$$k + l' + j(l + k') = k + jl + l' + jk' \cong l' + j(-jl') \cong 0 \pmod g.$$

It follows that even for the term where there is equality, the corresponding element is invariant, and so it is either zero or 2 times a power of $x^{mf}y^{mf}$. In this new notation, elements of E_2 are of the form:

$$[au_0 + a(g, j + 1) + t\frac{g}{(g, j + 1)}, au_0 + t\frac{g}{(g, j + 1)}].$$

We can extend the new notation to elements of E_1 by observing that $x^{mf}y^{mf}$ corresponds to $\frac{1}{2}[m, m]$.

Proposition 5.2.7 *Put*

$$\begin{aligned} h_1 = &\ \tfrac{1}{2}[m, m], \\ h_2 = &\ [g, 0], \\ h_3 = &\ [u_0 + (g, j + 1), u_0], \text{ and} \\ h_4 = &\ \left[u_0 + (g, j + 1) + \tfrac{g}{(g,j+1)}, u_0 + \tfrac{g}{(g,j+1)}\right]. \end{aligned}$$

Then, $\{h_1, h_2, h_3, h_4\}$ is a separating set. If $m = g/(g, j + 1)$, then $h_4 = h_1h_3$, and so $\{h_1, h_2, h_3\}$ is a separating set. Furthermore, if g divides $j + 1$, then only one of h_3 or h_4 is needed to separate

Proof. We will express all the elements of E in terms of h_1, h_2, h_3, and h_4. Clearly, elements of E_1 are powers of h_1. Before we consider elements of E_2, note that since $e = fg$ and $2^b|e$, then $\frac{2^b}{(2^b,f)}|g$, and so $m|g$.

On the points where $h_1 = 0$, one of x or y must be zero and so all the elements of E are zero except for those of the form $x^{kf} + y^{kf}$ or $y^{lf} + \alpha^{lf}x^{lf}$. Let us see how the conditions given in the lemma translate in these cases. For invariants of the form $x^{kf}+y^{kf}$ we get $g|k$. On the other hand, for invariants of the form $y^{lf}+\alpha^{lf}x^{lf}$, we get $g|jl$, which implies that $g|l$, and so $\alpha^{lf}=1$. Therefore, the only non-zero elements of E are of the form $x^{ke}+y^{ke}$, for some $k\in\mathbb{N}$. As one of x or y must be zero, these are clearly powers of f_2.

Before considering points where $h_1\neq 0$, we establish a few facts. First, we show that if $[k,l]$ is in E_2, then $m|(k+l)$. Indeed, as $g|(k+jl)$, $k=ga-jl$ for some $a\in\mathbb{Z}$ and so

$$l+kj=l+j(ga-jl)=(1-j^2)l+jga\equiv 0 \pmod{g},$$

i.e., $g|(j+kl)$. It follows that g divides $k+jl+l+jk=(j+1)(k+l)$, and so that $g/(g,j+1)$ divides $k+l$. But $2^b/(2^b,f)$ divides $k+l$, therefore, $m|(k+l)$.

Now, we prove that $m|2g/(g,j+1)$. Suppose $[k_1,l_1]$ and $[k_2,l_2]$ denote invariants such that $k_1-k_2=l_1-l_2=g/(g,j+1)$, this is possible because of the previous proposition and (in particular the two invariants will correspond to the same a), then

$$\begin{aligned}2\tfrac{g}{(g,j+1)} &= 2(k_1-k_2)=k_1-k_2+l_1-l_2\\ &= k_1+l_1-(k_2+l_2)\equiv 0 \pmod{m}.\end{aligned}$$

As $g/(g,j+1)$ divides m, this leaves only two possibilities, either $m=g/(g,j+1)$ or $m=2g/(g,j+1)$.

As $[k,l]=\alpha^l[l,k]$, it is enough to consider the cases where $k>l$. For any invariant $[k,l]$ in E_2, we will prove that one can express $[k,l]$ in terms of h_1, h_2, h_3, h_4 by (strong) induction on the difference $k-l$. Suppose $k-l=(g,j+1)$, then $k=u_0+(g,j+1)+t\frac{g}{(g,j+1)}$ and $l=u_0+t\frac{g}{(g,j+1)}$ for some $t\in\mathbb{Z}$. If $m=\frac{g}{(g,j+1)}$, then $[k,l]=h_1^th_3$. If $m=2\frac{g}{(g,j+1)}$ and $t=2s$, $[k,l]=h_1^sh_3$, but if $t=2s+1$, then $[k,l]=h_1^sh_4$.

Now, assume the result holds for invariants such that $k-l<a(g,j+1)$. Suppose that $k-l=a(g,j+1)$, then $k=au_0+a(g,j+1)+t\frac{g}{(g,j+1)}$ and $l=au_0+t\frac{g}{(g,j+1)}$ for

some $t \in \mathbb{Z}$. If $m = \frac{g}{(g,j+1)}$, then

$$\begin{aligned}[k,l] = \; & h_1^t([(a-1)u_0 + (a-1)(g,j+1), (a-1)u_0]h_3 \\ & - [au_0 + (a-1)(g,j+1), au_0 + (g,j+1)]).\end{aligned}$$

As $au_0 + (a-1)(g,j+1) - (au_0 + (g,j+1)) = (a-2)(g,j+1)$, by the induction hypothesis, we are done. Note that if $a = 2$ by a previous remark the last element is either zero or the double of a power of h_1. If $m = 2\frac{g}{(g,j+1)}$ and $t = 2s$, then

$$\begin{aligned}[k,l] = \; & h_1^s([(a-1)u_0 + (a-1)(g,j+1), (a-1)u_0]h_3 \\ & - [au_0 + (a-1)(g,j+1), au_0 + (g,j+1)]).\end{aligned}$$

Conversely, if $m = 2\frac{g}{(g,j+1)}$ and $t = 2s+1$, then

$$\begin{aligned}[k,l] = \; & h_1^s([(a-1)u_0 + (a-1)(g,j+1), (a-1)u_0]h_4 \\ & - [au_0 + (a-1)(g,j+1) + \tfrac{g}{(g,j+1)}, au_0 + (g,j+1)\tfrac{g}{(g,j+1)}]).\end{aligned}$$

Hence, by the principle of induction, we are done, and $\{h_1, h_2, h_3, h_4\}$ separates.

Now, suppose g divides $j+1$. Then

$$m = lcm\left(\frac{g}{(g,j+1)}, \frac{2^b}{(2^b,f)}\right) = lcm\left(1, \frac{2^b}{(2^b,f)}\right) = \frac{2^b}{(2^b,f)}$$

But m divides $2g/(g,j+1)$, i.e., $m|2$. It follows that $2^b/(2^b,f)$ divides 2, which means that $2^b|2f$. Therefore, 2^b divides either $u_0 f$ or $(u_0+1)f = (u_0 + \frac{g}{(g,j+1)})f$, i.e.,

$$\alpha^{u_0 f} = 1 \text{ or } \alpha^{(u_0 + \frac{g}{(g,j+1)})f} = 1.$$

If $m = 1 = \frac{g}{(g,j+1)}$, then $h_4 = h_3 h_1$, and so $\{h_1, h_2, h_3\}$ separates.

If $m = 2$, then $h_1 = \frac{1}{2}[2,2]$, and there are two cases to consider. If u_0 is even,

$$h_3 = [u_0 + (g,j+1), u_0] = [u_0 + g, u_0] = h_1^{\frac{u_0}{2}} h_2,$$

and so $\{h_1, h_2, h_4\}$ separates. If u_0 is odd,

$$h_4 = [u_0 + \frac{g}{(g,j+1)} + (g,j+1), u_0 + \frac{g}{(g,j+1)}] = [u_0 + 1 + g, u_0 + 1] = h_1^{\frac{u_0+1}{2}} h_2,$$

and so $\{h_1, h_2, h_3\}$ separates. □

◁

A next step could be to find separating sets, preferably of minimal size, for the remaining types of finite subgroups of $GL(2, \mathbb{C})$.

Chapter 6

New Separating Sets From Old Separating Sets

6.1 Polarization

The purpose of this section is to present methods for obtaining new separating sets from known separatings sets. We discuss polarization and the Noether map.

Classically, polarization is a method for obtaining vector invariants. In characteristic zero, and in the non-modular case in general, one obtains a generating set for the invariants of a certain number of copies of a representation V, from the invariants of a smaller number of copies of the same representation V. But in the modular case, the polarization of a generating set does not generate the ring of invariants in general. However, Draisma, Kemper, and Wehlau [14], as well as Domokos [13] showed that the polarization of separating invariants, or some weaker version of polarization, yields separating invariants. We adapt their results to our new notion of separating algebra, and highlight the relation between geometric separating invariants and polarization.

We start with the definition of polarization.

Definition 6.1.1. Let V and W be finite dimensional vector spaces over any field $\Bbbk$, and write V^m for the direct sum of m copies of V. $\Bbbk[V^m \oplus W]$ denotes the ring of functions on $V^m \oplus W$. If $\{x_1, \ldots, x_k\}$ is a basis for V^* and $\{y_1, \ldots, y_l\}$ is a basis for W^*, then we obtain a basis $\{x_{i,\nu} \mid i = 1, \ldots, m, \nu = 1, \ldots, k\} \cup \{y_1, \ldots, y_l\}$ of $(V^m \oplus W)^*$ by defining $x_{i,\nu}(v_1, \ldots, v_m, w) = x_\nu(v_i)$, and $y_i(v_1, \ldots, v_m, w) = y_i(w)$. Then

$$\Bbbk[V^m \oplus W] = \Bbbk[x_{i,\nu}, y_j \mid i = 1, \ldots, m, \nu = 1, \ldots, k, i = 1 \ldots, l].$$

Let n be another positive integer, and for $i = 1, \ldots, m$ and $j = 1, \ldots, n$, let $a_{i,j}$ be indeterminates. Define a homomorphism

$$\begin{array}{rccc} \Phi: & \Bbbk[V^m \oplus W] & \longrightarrow & \Bbbk[V^n \oplus W][a_{1,1}, \ldots, a_{m,n}] \\ & x_{i,\nu} & \longmapsto & \sum_{j=1}^{n} a_{i,j} x_{j,\nu} \\ & y_i & \longmapsto & y_i \end{array} .$$

For any $f \in \Bbbk[V^m \oplus W]$ the *polarization of* f, $\mathrm{Pol}_m^n(f)$ is the set of all non-zero coefficients of $\Phi(f)$ seen as a polynomial in the $a_{i,j}$'s.

The following theorem of Weyl, and especially the fact that it does not hold in the modular case (See Example 0.2 in [14]), motivated the investigation of polarization from the point of view of separating invariants.

Theorem 6.1.1 (Weyl, Theorem 2.5A in [40]) *Let G be a group acting linearly on two finite dimensional vector spaces V and W over a field $\Bbbk$ of characteristic zero. Let n and m be positive integers such that $m \geq \min\{\dim_{\Bbbk}(V), n\}$. If $S \subset \Bbbk[V^m \oplus W]^G$ is a generating set of invariants, then $\mathrm{Pol}_m^n(S) \subset \Bbbk[V^n \oplus W]^G$ is also generating.*

Switching our focus to geometric separating invariants yields a separating invariants version of Weyl's result.

Theorem 6.1.2 (c.f. Theorem 1.4 in [14]) *Let G be a group acting linearly on two finite dimensional vector space V and W over a field $\Bbbk$. Let n and m be positive* *integers such that* $m \geq \min\{\dim_{\Bbbk}(V), n\}$*. If* $S \subset \Bbbk[V^m \oplus W]$ *is a geometric separating set of invariants, then* $\mathrm{Pol}^n_m(S) \subset \Bbbk[V^n \oplus W]$ *is also a geometric separating set.*

Proof. If $S \subset \Bbbk[V^m \oplus W]^G$ is a geometric separating set, then it also is a geometric separating set in $\overline{\Bbbk}[\overline{V}^m \oplus \overline{W}]^G$, applying Theorem 1.4 of [14], we get that $Pol^n_m(S)$ is a geometric separating set in $\overline{\Bbbk}[\overline{V}^n \oplus \overline{W}]^G$. But $\mathrm{Pol}^n_m(S) \subset \Bbbk[V^n \oplus W]$, thus $\mathrm{Pol}^n_m(S)$ is a geometric separating set in $\Bbbk[V^n \oplus W]$. □

In the case of finite groups, we can get away with a computationally "cheaper" alternative to polarization.

Definition 6.1.2. As before, let V and W be finite dimensional vector spaces over any field $\Bbbk$. The set $\{x_i \mid i = 1, \ldots, k\} \cup \{y_1, \ldots, y_l\}$ of $V^m \oplus W$ is a basis for $(V \oplus W)^*$, and

$$\Bbbk[V \oplus W] = \Bbbk[x_i, y_j \mid i = 1, \ldots, k, i = 1 \ldots, l].$$

Let n be a positive integer, and U be an indeterminate. Define an homomorphism

$$\begin{array}{cccc} \Phi: & \Bbbk[V \oplus W] & \longrightarrow & \Bbbk[V^n \oplus W][U] \\ & x_i & \longmapsto & \sum_{j=1}^n U^{j-1} x_{i,j} \\ & y_i & \longmapsto & y_i \end{array} .$$

For any $f \in \Bbbk[V \oplus W]$ the *cheap polarization of* f, $\mathrm{Pol}^n_{\mathrm{cheap}}(f)$, is the set of all non-zero coeffincients of $\Phi(f)$ seen a a polynomial in a.

Theorem 6.1.3 (c.f. Theorem 2.4 in [14]) *Let* G *be a finite group, and let* V *and* W*, be finite dimensional representations of* G*. Suppose* $S \subset \Bbbk[V \oplus W]$ *is a geometric separating set, then* $\mathrm{Pol}^n_{\mathrm{cheap}}(S) \subset \Bbbk[V^n \oplus W]^G$ *is also a geometric separating set.*

Proof. We prove this result as a consequence of Theorem 2.4 in [14] in the same way as was done for the previous result.

If $S \subset \Bbbk[V \oplus W]^G$ is a geometric separating set, then it also is a geometric separating set in $\overline{\Bbbk}[\overline{V} \oplus \overline{W}]^G$. As $\overline{\Bbbk}$ is infinite, we apply Theorem 2.4 of [14], and obtain that $\mathrm{Pol}^n_{\mathrm{cheap}}(S)$ is a geometric separating set in $\overline{\Bbbk}[\overline{V}^n \oplus \overline{W}]^G$. But $\mathrm{Pol}^n_{\mathrm{cheap}}(S) \subset \Bbbk[V^n \oplus W]$, thus $\mathrm{Pol}^n_{\mathrm{cheap}}(S)$ is a geometric separating set in $\Bbbk[V^n \oplus W]$.

□

In contrast with Theorem 2.4 of [14], we do not have to assume that either S generates $\Bbbk[V \oplus W]^G$ as a $\Bbbk$-algebra, or S is a (geometric) separating set and $\Bbbk$ large enough. The following example illustrates that this requirement is unavoidable when considering separating sets rather than geometric separating sets:

Example 6.1.1 (Example 3.2.1 continued) We revisit Example 3.2.1 once more. Recall that G was the cyclic group of order 3 acting on a two dimensional vector space over $\mathbb{F}_2$ via

$$\sigma \mapsto \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Then the ring of invariants $\mathbb{F}_2[V]^{C_3}$ is minimally generated by 3 polynomials f_1, f_2, and f_3. Since all three correspond to the same function over V, picking any one gives a separating set. Say we pick $f_1 = x^2+xy+y^2$. We will see that the cheap polarization of f_1 does not yield a separating set in $\mathbb{F}_2[2V]^{C_3}$. If x_1, y_1 are the coordinates for the first copy of V, and x_2, y_2 the coordinates for the second copy, then the cheap polarization of f_1 is the set of coefficients of the following polynomial in the indeterminate U:

$$\begin{gathered}(x_1 + Ux_2)^2 + (x_1 + Ux_2)(y_1 + Uy_2) + (y_1 + Uy_2) = \\ (x_1^2 + x_1y_1 + y_1^2) + (x_1y_2 + y_1x_2)U + (x_2^2 + x_2y_2 + y_2^2)U^2,\end{gathered}$$

i.e., $\mathrm{Pol}^n_{\mathrm{cheap}}(f_1) = \{x_1^2 + x_1y_1 + y_1^2, x_1y_2 + y_1x_2, x_2^2 + x_2y_2 + y_2^2\}$. The two points $(1, 1, 1, 1)$, and $(1, 1, 1, 0)$ in V^2 clearly belong to distinct orbits, but all 3 polynomials in $\mathrm{Pol}^n_{\mathrm{cheap}}(f_1)$ take the same value on both points. Since for finite groups the ring of invariants distinguishes the orbits, we conclude that $\mathrm{Pol}^n_{\mathrm{cheap}}(f_1)$ is not a separating set. ◁

In the case of the action of a cyclic group of order 2 acting via multiplication on a n-dimensional vector space, the separating set obtained via cheap polarization corresponds to the separating set obtained from the "triangle trick" from Section 5.2.1:

Example 6.1.2 (c.f. Section 5.2.1) Let $\Bbbk$ be a field of characteristic not 2. Let G be the cyclic group of order 2. Suppose the representation V consist of n copies of the non-trivial faithful 1-dimensional representation W of G. $\Bbbk[W]^G = \Bbbk[x^2]$. $\mathrm{Pol}^n_{\mathrm{cheap}}(x^2)$ is the set of coefficients of

$$\left(\sum_{i=1}^{n} x_i U^{i-1}\right)^2 = \sum_{\substack{0 \le k \le 2(n-1) \\ 2|k}} x^2_{\frac{k+2}{2}} + \sum_{k=0}^{2(n-1)} \left(\sum_{i+j=k+2} x_i x_j\right) U^k.$$

The coefficients of the various powers of U correspond to the sum of the terms on the diagonals of the triangle. The set of elements of the following triangle correspond to the full polarization of x^2.

$$\begin{array}{cccccc}
x_1^2 & x_1x_2 & x_1x_3 & \cdots & x_1x_{n-1} & x_1x_n \\
 & x_2^2 & x_2x_3 & \cdots & x_2x_{n-1} & x_2x_n \\
 & & x_3^2 & \cdots & x_3x_{n-1} & x_3x_n \\
 & & & \ddots & \vdots & \vdots \\
 & & & & x_{n-1}^2 & x_{n-1}x_n \\
 & & & & & x_n^2
\end{array}$$

◁

6.2 The Noether Map

In this section we consider the relationship between geometric separating invariants and the Noether map, which was introduced by Emmy Noether herself in her 1915 paper [35]. We became interested in the Noether map (in the context of separating invariants) while reading [33]. We eventually realised that related results had been proved in a previous paper by Campbell, Hughes, and Pollack [5]. We will present a hybrid of the approaches suggested by the two papers.

We start by defining the Noether map. Let G be a finite group acting on the n-dimensional vector space V over the field $\Bbbk$. Let $\{e_i\}$ be a basis for V, and $\{x_i\}$ be the dual basis for V^*. Let $\Bbbk G$ be the group algebra. Set $V(G) = \Bbbk G \otimes V$, then

$$V(G) = \bigoplus_{\sigma \in G} \bigoplus_{i=1}^{n} \sigma \otimes e_i,$$

that is, $\{\sigma \otimes e_i \mid \sigma \in G,\ i = 1, \dots, n\}$ forms a basis for $V(G)$. Let $\{x_{\sigma,i}\}$ be the dual basis for $V(G)^*$. The group $\Sigma_{|G|}$ of permutations on the $|G|$ elements elements of G acts on $V(G)$ in the following way: if τ is in $\Sigma_{|G|}$ and, σ in G, then, for $1 \leq i \leq n$,

$$\tau \cdot (\sigma \otimes e_i) = (\tau(\sigma)) \otimes e_i.$$

The induced action on $V(G)^*$ is given as follows

$$(\tau \cdot x_{\sigma,i})(\upsilon \otimes x_j) = x_{\sigma,i}((\tau^{-1}(\upsilon)) \otimes x_j) = \begin{cases} 1 & \text{if } \tau^{-1}(\upsilon) = \sigma \text{ and } i = j, \\ 0 & \text{otherwise,} \end{cases}$$

that is, $\tau \cdot x_{\sigma,i} = x_{\tau(\sigma),i}$.

Define a map $\eta_G : \Bbbk[V(G)] \to \Bbbk[V]$ of $\Bbbk$-algebras by $\eta_G(x_{\sigma,i}) = \sigma \cdot x_i$. Let G act on $V(G)$ via $\gamma \cdot (\sigma \otimes e_i) = (\gamma\sigma) \otimes e_i$, where γ and σ are elements of G, and $1 \leq i \leq n$. This gives an embedding of G into $\Sigma_{|G|}$. The map η_G is G-equivariant, as for γ and σ in G, and $1 \leq i \leq n$,

$$\eta_G(\gamma \cdot x_{\sigma,i}) = \eta_G(x_{\gamma\sigma,i}) = (\gamma\sigma) \cdot x_i = \gamma \cdot (\sigma \cdot x_i) = \gamma \cdot \eta_G(x_{\sigma,i}).$$

As invariants under $\Sigma_{|G|}$ are, in particular, invariants under G, we can define the Noether map $\eta_G^{\Sigma_{|G|}} : \Bbbk[V(G)]^{\Sigma_{|G|}} \to \Bbbk[V]^G$ as the restriction of η_G to the ring of invariants $\Bbbk[V(G)]^{\Sigma_{|G|}}$. This is the definition found in [5]. In [33], the Noether map $\eta_G^G : \Bbbk[V(G)]^G \to \Bbbk[V]^G$ is the restriction of η_G to the invariants of G.

We can now prove the following proposition, Proposition 4 in [5]. In that paper, the hypotheses are stronger, but the proof provided actually requires only what we include here.

Proposition 6.2.1 (Proposition 4 in [5]) *If G is a finite group, then*

1. $\widehat{\mathrm{Im}(\eta_G^{\Sigma_{|G|}})} \subset \Bbbk[V]^G$,
2. $\forall f \in \Bbbk[V]^G,\ f^{|G|} \in \mathrm{Im}(\eta_G^{\Sigma_{|G|}})$.

Proof. The first part follows from Corollary 3.2.10 since $\mathrm{Im}(\eta_G^{\Sigma_{|G|}}) \subset \Bbbk[V]^G$.

Now, take $f \in \Bbbk[V]^G$. Define $h = \prod_{\sigma\in G} f(x_{\sigma,1}, \ldots, x_{\sigma,n}) \in \Bbbk[V(G)]$. Then h is $\Sigma_{|G|}$-invariant, and $\eta_G^{\Sigma_{|G|}}(h) = f^{|G|}$. □

Before we give our new proof of Proposition 1.2 of [33], we recall the definition of the transfer and a result concerning it.

Definition 6.2.1. Let G be a finite group. The *transfer* Tr^G is defined as the map

$$\begin{array}{rccc} \mathrm{Tr}^G: & \Bbbk[V] & \longrightarrow & \Bbbk[V]^G \\ & f & \longmapsto & \sum_{\sigma\in G} \sigma \cdot f. \end{array}$$

Lemma 6.2.2 (See [33] and [34]) *Let G be a finite group. If $\mathrm{Tr}^G$is the transfer, then,*

1. $\mathrm{Im}(\mathrm{Tr}^G) \subset \mathrm{Im}(\eta_G^{\Sigma_{|G|}})$, *and*
2. $\mathrm{Q}(\Bbbk[\mathrm{Im}(\mathrm{Tr}^G)]) = \Bbbk(V)^G$. *Therefore,* $\mathrm{Q}(\mathrm{Im}(\eta_G^G)) = \Bbbk(V)^G$.

Proof. 1. If $h \in \mathrm{Im}(\mathrm{Tr}^G)$, then there exists a $f \in \Bbbk[V]$ such that

$$h = \mathrm{Tr}^G(f) = \sum_{\sigma\in G} \sigma \cdot f.$$

The element

$$H = \sum_{\sigma\in G} \sigma \cdot f(x_{1,1}, \ldots, x_{1,n}) \in \Bbbk[V(G)]$$

of $\Bbbk[V(G)]$ is $\Sigma_{|G|}$-invariant, and so $h = \eta_G(H) = \eta_G^{\Sigma_{|G|}}(H)$.

2. By 1, we have the inclusion $\mathrm{Q}(\Bbbk[\mathrm{Im}(\mathrm{Tr}^G)]) \subset \Bbbk(V)^G$. Take $f \in \Bbbk[V]^G$, and take $h \in \Bbbk[V]$ such that $\mathrm{Tr}^G(h) \neq 0$ (such a h exists, by Lemma 3.7.2 in [1]), then
$$f = \frac{f\mathrm{Tr}^G(h)}{\mathrm{Tr}^G(h)} = \frac{\mathrm{Tr}^G(fh)}{\mathrm{Tr}^G(h)} \in \mathrm{Q}(\Bbbk[\mathrm{Im}(\mathrm{Tr}^G)]).$$
Taking fields of quotient on each side gives the second inclusion.

□

Corollary 6.2.3 (Proposition 1.2 in [33]) *If G is a finite group,then,* $\widetilde{\mathrm{Im}(\eta_G^{\Sigma_{|G|}})} = \Bbbk[V]^G$.

Proof. By part 2 of Lemma 6.2.2, $\mathrm{Im}(\eta_G^{\Sigma_{|G|}})$ and $\Bbbk[V]^G$ have the same field of fractions, and by 2 of Proposition 6.2.1 the extension $\mathrm{Im}(\eta_G^{\Sigma_{|G|}}) \subset \Bbbk[V]^G$ is integral, thus we obtain the desired conclusion. □

In the case of p-groups we get the following easy corollary to Proposition 6.2.1.

Corollary 6.2.4 *If G is a p-group, and $\Bbbk$ has characteristic $p > 0$, then* $\mathrm{Im}(\eta_G^{\Sigma_{|G|}})$ *is a geometric separating algebra.*

Proof. Since $|G|$ is a power of p, Proposition 6.2.1 implies that $\widehat{\mathrm{Im}(\eta_G^{\Sigma_{|G|}})} = \Bbbk[V]^G$, and then Lemma 3.2.10 implies $\mathrm{Im}(\eta_G^{\Sigma_{|G|}})$ separates. □

In fact, this result holds for finite groups in general:

Proposition 6.2.5 *If G is a finite group, then* $\mathrm{Im}(\eta_G^{\Sigma_{|G|}})$ *contains the coefficients of the polynomial $F_{T,U}$. In particular,* $\mathrm{Im}(\eta_G^{\Sigma_{|G|}})$ *is a geometric separating algebra.*

Proof. Consider the polynomial H defined as follows
$$H = \prod_{\sigma \in G} \left(T - \sum_{i=1}^{n} U^{i-1} x_{\sigma,i} \right),$$

where T and U are formal variables. Its coefficients are $\Sigma_{|G|}$-invariants. Taking the image of these coefficients under the Noether map, we get the coefficients of

$$F_{T,U} = \prod_{\sigma \in G} \left(T - \sum_{i=1}^{n} U^{i-1} \sigma \cdot x_i \right).$$

□

Remark 6.2.1. An alternate proof of this result is found in the example ending the introduction of Neusel and Sezer's recent paper [32]. They make use of Proposition 2.2 of [33], where they show that the purely inseparable closure of the image of the Noether map is the ring of invariants. Of course, their Noether map has a slightly bigger image (there are more G-invariants than $\Sigma_{|G|}$-invariants).

Proposition 6.2.5 can be extended further:

Proposition 6.2.6 *Let G be a finite group. The Noether map sends geometric separating sets to geometric separating sets.*

Proof. Take $V(G)/\!\!/\Sigma_{|G|} = \operatorname{Spec}(\Bbbk[V(G)]^{\Sigma_{|G|}})$. By Proposition 6.2.5, the image of the transfer is a geometric separating algebra. Equivalently, the morphism of schemes $\phi : V/\!\!/G \to V(G)/\!\!/\Sigma_{|G|}$ corresponding to the Noether map $\eta_G^{\Sigma_{|G|}}$ is radicial. Indeed, as G is finite, the ring of invariants is finitely generated, and we may use the second geometric formulation of separation.

If $B \subset \Bbbk[V(G)]^{\Sigma_{|G|}}$ is a geometric separating algebra, and $A = \eta_G^{\Sigma_{|G|}}(B)$, then the following diagram commutes:

$$\begin{tikzcd}
\Bbbk[V(G)]^{\Sigma_{|G|}} \arrow[r, "\eta_G^{\Sigma_{|G|}}"] & \Bbbk[V]^G \\
B \arrow[u, "\iota_1"] \arrow[r, "\eta_G^{\Sigma_{|G|}} \circ \iota_1"'] & A, \arrow[u, "\iota_2"']
\end{tikzcd}$$

where ι_1, and ι_2 are the inclusion morphism. Taking $W = \mathrm{Spec}(A)$, and $X = \mathrm{Spec}(B)$, it follows that the corresponding diagram commutes as well:

$$\begin{tikzcd}
V(G)/\!\!/\Sigma_{|G|} \arrow[d, "\pi_1"'] & V/\!\!/G \arrow[l, "\phi"'] \arrow[d, "\pi_2"] \\
X & W. \arrow[l, "\psi"]
\end{tikzcd}$$

As B is a geometric separating algebra, π_1 is radicial. As ϕ is also radicial, Proposition 3.5.6 of [17] implies that $\pi_1 \circ \phi = \psi \circ \pi_2$ is also radicial, and then so is π_2. Hence, we conclude that A is a geometric separating algebra, and so the Noether map sends geometric separating separating sets to geometric separating sets. □

6.3 The Relationship between $\Bbbk[\mathrm{coeff}\, F_{T,U}]$, the Image of the Noether Map, and Cheap Polarization

In this section we explore the relationship between $\Bbbk[\mathrm{coeff}\, F_{T,U}]$, the Image of the Noether map and Cheap Polarization. Recall that we proved that the image of the Noether map is a geometric separating algebra by showing that it contains the coefficients of $F_{T,U}$, and thus $\Bbbk[\mathrm{coeff}\, F_{T,U}] \subset \mathrm{Im}(\eta_G^{\Sigma_{|G|}})$. How close are $\Bbbk[\mathrm{coeff}\, F_{T,U}]$ and $\mathrm{Im}(\eta_G^{\Sigma_{|G|}})$ in general? We consider a few examples.

Example 6.3.1 (Example 1 in [33]) Let $\Bbbk$ be a field of characteristic 2. Set

$$G = \langle \sigma \rangle = \left\langle \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\rangle,$$

then the ring of invariants is $\Bbbk[V]^G = \Bbbk[x_1 + x_2, x_1x_2, x_3]$ and

$$\mathrm{Im}(\eta_G^{\Sigma_{|G|}}) = \Bbbk[x_1 + x_2, x_1x_2, x_3^2, (x_1 + x_2)x_3].$$

In [33] they are interested in a slightly different Noether map η_G^G, but in the present case $G = C_2 = \Sigma_2$, and so a new computation is not required. We consider the separating algebra $\Bbbk[\operatorname{coeff} F_{T,U}]$. It is generated by the coefficients of

$$\begin{aligned} F_{T,U} = {} & \left(T - \textstyle\sum_{i=1}^{3} U^{i-1}x_i\right)\left(T - \textstyle\sum_{i=1}^{3} U^{i-1}\sigma\cdot x_i\right) \\ \\ = {} & T^2 - T\left[(x-1+x_2) + U(x_1+x_2)\right] + x_1x_2 + U(x_2^2 + x_1^2) \\ & \quad + U^2(x_3(x_1+x_2) + x_1x_2) + U^3(x_3(x_1+x_2)) + U^4x_3^2. \end{aligned}$$

Thus,

$$\Bbbk[\operatorname{coeff} F_{T,U}] = \Bbbk[x_1+x_2, x_1x_2, x_3^3, (x_1+x_2)x_3] = \operatorname{Im}(\eta_G^{\Sigma_{|G|}}).$$

◁

Example 6.3.2 Let $\Bbbk$ be a field of characteristic 3. Let G be the cyclic group of order 3, and let V be the 2-dimensional irreducible representation, i.e.,

$$G = \langle\sigma\rangle = \left\langle\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}\right\rangle \in GL(V).$$

The ring of invariants is $\Bbbk[V]^G = \Bbbk[x_2, x_1^3 + 2x_1x_2^2]$. Consider the polynomial $F_{T,U}$ given by

$$\begin{aligned} F_{T,U} &= (T-(x_1+Ux_2))(T-((x_1+x_2)+Ux_2)(T-((x_1+2x_2)+Ux_2) \\ &= T^3 + T(2x_2^2) + (x_1^3 + 2x_1x_2^2) + U(2x_3) + U^3(x-2^3), \end{aligned}$$

and so $\Bbbk[\operatorname{coeff} F_{T,U}] = \Bbbk[x_2^2, x_2^3, x_1^3 + 2x_1x_2^2]$. Clearly $\mathrm{Q}(\Bbbk[\operatorname{coeff} F_{T,U}]) = \Bbbk(V)^G$, but $\Bbbk[\operatorname{coeff} F_{T,U}] \neq \Bbbk[V]^G$.

Now, let's look at the image of the Noether map. For this purpose, we need to compute $\Bbbk[V(G)]^{\Sigma_{|G|}}$.

Using Magma [2], we find that the ring of invariants $\Bbbk[V(G)]^{\Sigma_{|G|}}$ is generated minimally by 10 polynomials which we omit here for space.

Their image under the Noether map $\eta_G^{\Sigma_{|G|}}$, is

$$\{2x_2^2, x_2^3, x_1^3 + 2x_1x_2^2, x_2^4 + 2x_1x_2^3 + 2x_1^3x_2\},$$

and so the image of the Noether map is $\Bbbk[x_2^2, x_2^3, x_1^3 + 2x_1x_2^2] = \Bbbk[\operatorname{coeff} F_{T,U}]$. ◁

In the last two examples, the image of the Noether map coincided with $\Bbbk[\operatorname{coeff} F_{T,U}]$, but this is not true in general.

Example 6.3.3 Let $\Bbbk$ be a field of characteristic 5, and let G be the eighth group of the Shephard-Todd classification of reflection groups. When acting on a 2-dimensional vector space over $\Bbbk$ it is given by

$$G = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 3 \\ 3 & 4 \end{pmatrix} \right\rangle \subset GL(V).$$

This is a non-modular reflection group, and so its ring of invariants is polynomial. On the other hand, if we compute the coefficients of $F_{T,U}$, using Magma [2], we find that the $\Bbbk$-algebra they generate, $\Bbbk[\operatorname{coeff} F_{T,U}]$, is minimally generated by 5 invariants. ◁

Combined with cheap polarization, the Noether map gives us a method to obtain separating invariants for any finite dimensional representation of any finite group. Indeed, if V is a n-dimensional representation of a finite group G, start with generators for the symmetric polynomials in $|G|$ variables, i.e., generators for the invariants of the permutation representation of the symmetric group on $|G|$ elements. Then, cheap-polarize them to n copies of the permutation representation of $\Sigma_{|G|}$ to obtain a separating set for the action of $\Sigma_{|G|}$ on $V(G)$. Finally, apply the Noether map.

Example 6.3.4 Let G be as in Example 6.3.2. Let W be the permutation representation of $\Sigma_{|G|} = \Sigma_3$,where $\{x_1, x_\sigma, x_{\sigma^2}\}$ is the dual basis for U^*. Then, by Theorem 3.10.1 of [11], the ring of invariants $\Bbbk[U]^{\Sigma_3}$ is given by

$$\Bbbk[U]^{\Sigma_3} = \Bbbk[x_1 + x_\sigma + x_{\sigma^2}, x_1x_\sigma + x_1x_{\sigma^2} + x_\sigma x_{\sigma^2}, x_1x_\sigma x_{\sigma^2}].$$

The cheap polarization of the generators give us

$$\mathrm{Pol}^2_{\text{cheap}}(x_1 + x_\sigma + x_{\sigma^2}) = \{x_{1,1} + x_{\sigma,1} + x_{\sigma^2,1}, x_{1,2} + x_{\sigma,2} + x_{\sigma^2,2}\},$$

$$\begin{aligned}&\mathrm{Pol}^2_{\text{cheap}}(x_1x_\sigma + x_1x_{\sigma^2} + x_\sigma x_{\sigma^2}) =\\ &\{x_{1,1}x_{\sigma,1} + x_{1,1}x_{\sigma^2,1} + x_{\sigma,1}x_{\sigma^2,1}, x_{1,2}x_{\sigma,1} + x_{1,2}x_{\sigma^2,1} + x_{\sigma,2}x_{\sigma^2,1}\\ &\quad + x_{1,1}x_{\sigma,2} + x_{1,1}x_{\sigma^2,2} + x_{\sigma,1}x_{\sigma^2,2}, x_{1,2}x_{\sigma,2} + x_{1,2}x_{\sigma^2,2} + x_{\sigma,2}x_{\sigma^2,2}\},\end{aligned}$$

and

$$\begin{aligned}&\mathrm{Pol}^2_{\text{cheap}}(x_1x_\sigma x_{\sigma^2}) =\\ &\quad\{x_{1,1}x_{\sigma,1}x_{\sigma^2,1}, x_{1,2}x_{\sigma,1}x_{\sigma^2,1} + x_{1,1}x_{\sigma,2}x_{\sigma^2,1} + x_{1,1}x_{\sigma,1}x_{\sigma^2,2},\\ &\quad\ x_{1,1}x_{\sigma,2}x_{\sigma^2,2} + x_{1,2}x_{\sigma,1}x_{\sigma^2,2} + x_{1,2}x_{\sigma,2}x_{\sigma^2,1}, x_{1,2}x_{\sigma,2}x_{\sigma^2,2}\}.\end{aligned}$$

Applying the Noether map we obtain

$$\begin{array}{lcl}\eta_G^{\Sigma_{|G|}}(\mathrm{Pol}^2_{\text{cheap}}(x_1 + x_\sigma + x_{\sigma^2})) & = & \{0, 0\}\\ \eta_G^{\Sigma_{|G|}}(\mathrm{Pol}^2_{\text{cheap}}(x_1x_\sigma + x_1x_{\sigma^2} + x_\sigma x_{\sigma^2})) & = & \{2x_2^2, 0, 0\}\\ \eta_G^{\Sigma_{|G|}}(\mathrm{Pol}^2_{\text{cheap}}(x_1x_\sigma x_{\sigma^2})) & = & \{x_1^3 - x_2^2x_1, 2x_2^3, 0, x_2^3\}\end{array}$$

This corresponds exactly to the coefficients of $F_{T,U}$.

In the previous example the process of polarizing the elementary symmetric polynomials and then applying the Noether map gives us the coefficients of the T, U-separating polynomial. This is not a coincidence:

Proposition 6.3.1 *Let G be a finite group, and let V be a n-dimensional representation over $\Bbbk$. The process of cheap-polarizing the elementary symmetric polynomial on $|G|$ variables to n copies, and then applying the Noether map yields the coefficients of the T, U-separating polynomial $F_{T,U}$.*

Proof. Let W be the permutation representation of $\Sigma_{|G|}$, and let $\{x_\sigma \mid \sigma \in G\}$ be the dual basis for W^*. Also, as before, $\{x_{\sigma,i} \mid \sigma \in G,\ 1 \geq i \geq n\}$ is the basis for

$V(G)^*$. We assume here, that the Noether map does not affect T and U, and that cheap-polarization does not affect T. Then since both maps are multiplicative, we have:

$$\begin{aligned}
F_{T,U} &= \textstyle\prod_{\sigma \in G} \left(T - \sum_{i=1}^n U^{i-1} \sigma \cdot x_i\right) \\
&= \textstyle\prod_{\sigma \in G} \left(T - \sum_{i=1}^n U^{i-1} \eta_G^{\Sigma_{|G|}}(x_{\sigma,i})\right) \\
&= \eta_G^{\Sigma_{|G|}} \left(\textstyle\prod_{\sigma \in G} \left(T - \sum_{i=1}^n U^{i-1} x_{\sigma,i}\right)\right) \\
&= \eta_G^{\Sigma_{|G|}} \left(\textstyle\prod_{\sigma \in G} \left(T - \mathrm{Pol}_{\mathrm{cheap}}^n(x_\sigma)\right)\right) \\
&= \eta_G^{\Sigma_{|G|}} \left(\mathrm{Pol}_{\mathrm{cheap}}^n \left(\textstyle\prod_{\sigma \in G} (T - x_\sigma)\right)\right)
\end{aligned}$$

Finally, as the coefficients of $\prod_{\sigma \in G} (T - x_\sigma)$ are the elementary symmetric polynomials in the x_σ's, which are, by Theorem 3.10.1 of [11], the generators of the ring of invariants of the permutation representation of $\Sigma_{|G|}$. Thus, we are done. □

Chapter 7

Concluding Remarks

The main results of this thesis are found in Chapters 3 and 4. They are the geometric formulations of the notion of geometric separating algebra, and the results linking the existence of nice geometric separating algebras to the geometry of the representation.

The results presented in this text shed light on many avenues for future work. Although the focus of this text has been mostly on finite groups, the two formulations for the notion of a geometric separating algebra, presented in Chapter 3, make sense for reductive groups in general. It would be interesting to study more general reductive groups. It may be that we could get a good enough handle of the separating scheme to link its geometry to the geometry of the representation.

Another interesting avenue would be to consider actions of algebraic groups on more general geometric objects. It may be that our definitions still make sense, and we may be able to reproduce, or even extend some of our results.

More concretely, it has not yet been established if the converses of the main results of Chapter 4 hold. Also, a proof that there is a separating set of size $2n-1$, for any diagonal representation still escapes us.

Bibliography

[1] David J. Benson. *Polynomial Invariants of Finite Groups.* Number 190 in London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 1993.

[2] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] Mireille Boutin and Gregor Kemper. On reconstructing configurations of points in $\mathbb{P}^2$ from a joint distribution of invariants. *Appl. Algebra Engrg. Comm. Comput.*, 15(6):361–391, 2005.

[4] H. E. A. Campbell and I. P. Hughes. 2-Dimensional Vector Invariants of Parabolic Subgroups of $Gl_2(\mathbb{F}_p)$ over the Field $\mathbb{F}_p$. *J. Pure and Applied Algebra*, 112:1–12, 1996.

[5] H. E. A. Campbell, I. P. Hughes, and R. D. Pollack. Rings of Invariants and p-Sylow Subgroups. *Can. Math. Bull.*, 34(1):42–47, 1991.

[6] H. E. A. Campbell and I.P. Hughes. Rings of Invariants of Certain p-Groups over the Field $\mathbb{F}_p$. *J. Algebra*, 211:549–561, 1998.

[7] H. E. A. Campbell, I.P. Hughes, and R. J. Shank. Preliminary Notes on Rigid Reflection Groups. Preprint, 1996.

[8] H.E.A. Campbell and David Wehlau. *Modular Invariant Theory*. Encyclopædia of Mathematical Sciences. Springer-Verlag, Berlin, Heidelberg, New York, to appear.

[9] Claude Chevalley. Invariants of Finite Groups Generated by Reflections. *Amer. J. Math.*, 77:778–782, 1955.

[10] Allan Clark and John Ewing. The Realization of Polynomial Algebras as Cohomology Rings. *Pacific J. Math.*, 50:425–434, 1974.

[11] Harm Derksen and Gregor Kemper. *Computational Invariant Theory*. Number 130 in Encyclopædia of Mathematical Sciences. Springer-Verlag, Berlin, Heidelberg, New York, 2002.

[12] Harm Derksen and Gregor Kemper. Computing Invariants of Algebraic Groups in Arbitrary Characteristic. *Adv. Math.*, 217(5):2089–2129, 2008. arXiv:math.AC/0704.2594.

[13] Mátyás Domokos. Typical separating invariants. *Transform. Groups*, 12(1):49–63, 2007.

[14] Jan Draisma, Gregor Kemper, and David Wehlau. Polarization of Separating Invariants. *Can. J. Math.*, 60(3):556–571, 2008.

[15] Emlie Dufresne. Separating Invariants and Finite Reflection Groups. arXiv:math.AC/0805.2605, 2008.

[16] Frank D. Grosshans. Vector Invariants in Arbitrary Characteristic. *Transform. Groups*, 12(3), 2007.

[17] Alexander Grothendieck. Éléments de géométrie algébrique. I. Le langage des schémas. *Inst. Hautes Études Sci. Publ. Math.*, (4):228, 1960.

[18] Alexander Grothendieck. Éléments de géométrie algébrique. II. Étude globale élémentaire de quelques classes de morphismes. *Inst. Hautes Études Sci. Publ. Math.*, (8):222, 1961.

[19] Alexander Grothendieck. *Revêtements étales et groupe fondamental. Fasc. II: Exposés 6, 8 à 11*, volume 1960/61 of *Séminaire de Géométrie Algébrique.* Institut des Hautes Études Scientifiques, Paris, 1963.

[20] Alexander Grothendieck. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. I. *Inst. Hautes Études Sci. Publ. Math.*, (20):259, 1964.

[21] Robin Hartshorne. Complete Intersection and Connectedness. *Amer. J. Math.*, 84.

[22] Robin Hartshorne. *Algebraic geometry.* Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[23] Albert Holleman. Inseparable algebras. *J. Algebra*, 46(2):415–429, 1977.

[24] W. Cary Huffman. Polynomial Invariants of Finite Linear Groups of Degree Two. *Can. J. Math.*, XXXII(2):317–330, 1980.

[25] Victor Kac and Kei-Ichi Watanabe. Finite Linear Groups whose Ring of Invariants is a Complete Intersection. *Bull. (New Series) of the AMS*, 6(2).

[26] Gregor Kemper. A Characterization of Linear Reductive Groups by their Invariants. *Transformation Groups*, 5(1):85–92, 2000.

[27] Gregor Kemper. Loci in quotients by finite groups, pointwise stabilizers and the Buchsbaum property. *J. Reine Angew. Math.*, 547:69–96, 2002.

[28] Gregor Kemper. Computing Invariants of Reductive Groups in Positive characteristic. *Transformation Groups*, 8(2):158–176, 2003.

[29] Gregor Kemper. Separating Invariants. *J. Symbolic Computation*, to appear.

[30] Jean-Marie De Koninck and Armel Mercier. *Introduction à la Théorie des Nombres.* Modulo, Mont-Royal (Québec), 1994.

[31] Hideyuki Matsumura. *Commutative ring theory*, volume 8 of *Cambridge Studies in Advanced Mathematics.* Cambridge University Press, Cambridge, second edition, 1989. Translated from the Japanese by M. Reid.

[32] Mara D. Neusel and Müfit Sezer. Characterizing Separating Invariants. Preprint, 2008.

[33] Mara D. Neusel and Müfit Sezer. The Noether Map I. *Forum Mathematicum,*, to appear.

[34] Mara D. Neusel and Larry Smith. *Invariant Theory of Finite Groups*, volume 94 of *Mathematical Surveys and Monographs.* American Mathematical Society, Providence (Rhode Island), 2002.

[35] Emmy Noether. Der Endlichkeitssatz der Invarianten endlicher Gruppen. *Math. Ann.*, 77(1):89–92, 1915.

[36] Jean-Pierre Serre. Groupes finis d'automorphismes d'anneaux locaux réguliers. In *Colloque d'Algèbre (Paris, 1967), Exp. 8*, page 11. Secrétariat mathématique, Paris, 1968.

[37] G. C. Shephard and J. A. Todd. Finite Unitary Reflection Groups. *Canadian J. Math.*, 6:274–304, 1954.

[38] Larry Smith. *Polynomial Invariants of Finite Groups.* A K Peters, Wellesley, Massachusetts, 1995.

[39] Wilberd van der Kallen. *Lectures on Frobenius splittings and B-modules.* Published for the Tata Institute of Fundamental Research, Bombay, 1993. Notes by S. P. Inamdar.

[40] Hermann Weyl. *The Classical Groups. Their Invariants and Representations.* Princeton University Press, Princeton, NJ., 1939.

Appendix A

Commutative Algebra: Some Definitions, Results and Notation

Definition A.0.1. Let A be a comutative ring, and let S be a multiplicative subset (i.e. a set closed under multiplication), We define the *localization* $S^{-1}A$ as the quotient of $A \times S$ by the equivalence relation $\backsim$ defined as follows:

$$(a, s) \backsim (a', s') \Leftrightarrow as' - a's \text{ is a zero divisor,}$$

for any $(a, s), (a', s') \in A \times S$.

Definition A.0.2. Let A be an integral domain, then $Q(A)$ denotes its field of fractions, namely the localization $S^{-1}A$, where $S = \{s \in A \mid s \neq 0\}$.

The construction given in this definition is exactly the construction used to obtain the rational numbers from the integers. In this light, for convenience we will use the following notation, analogous to the notation of rational numbers, for the field of fractions of any domain A:

$$Q(A) = \left\{ \frac{f}{g} \mid f, g \in A \ , g \neq 0 \right\}.$$

Lemma A.0.2 (known) *Let $\Bbbk \subset \mathcal{F}$ be an extension of fields of characteristic $p \geq 0$, and consider the tensor product $\mathcal{F} \otimes_{\Bbbk} \mathcal{F}$. If for $f \in \mathcal{F}$,*

$$f \otimes 1 - 1 \otimes f = 0$$

in the tensor product $\mathcal{F} \otimes_{\Bbbk} \mathcal{F}$, then $f \in \Bbbk$.

Proof. Let $\{f_\alpha\}_{\alpha \in A}$ be a basis for $\mathcal{F}$ over $\Bbbk$. Then $\{f_\alpha \otimes f_\beta\}_{(\alpha,\beta) \in A \times A}$ is a basis for the tensor product $\mathcal{F} \otimes_{\Bbbk} \mathcal{F}$ over $\Bbbk$. Suppose

$$f \otimes 1 - 1 \otimes f = 0,$$

and assume $f = \sum_{\alpha \in A} a_\alpha f_\alpha$, then

$$\begin{aligned} 0 &= \left(\textstyle\sum_{\alpha \in A} a_\alpha f_\alpha\right) \otimes 1 - 1 \otimes \left(\textstyle\sum_{\alpha \in A} a_\alpha f_\alpha\right) = \\ &= \textstyle\sum_{\alpha \in A} a_\alpha (f_\alpha \otimes 1) - \textstyle\sum_{\alpha \in A} a_\alpha (1 \otimes f_\alpha) \end{aligned}$$

Let α_0 be the only $\alpha \in A$ such that $f_\alpha \in \Bbbk$, then $a_{\alpha_0}(f_{\alpha_0} \otimes 1 - 1 \otimes f_{\alpha_0}) = 0$ and all the remaining terms are distinct basis elements. It follows that $a_\alpha = 0$ for all $\alpha \neq \alpha_0$, and so $f \in \Bbbk$. □

Definition A.0.3. Let B be a $\Bbbk$-algebra. We define a map δ:

$$\begin{aligned} \delta : \quad B &\rightarrow B \otimes_{\Bbbk} B \\ b &\mapsto b \otimes 1 - 1 \otimes b. \end{aligned}$$

Within this document we will call any such map δ. Which one we refer to should be clear from the context.

Proposition A.0.3 *Let B be a $\Bbbk$-algebra, and let $A \subset B$ be a subalgebra. Then*

$$B \otimes_A B \cong \frac{B \otimes_{\Bbbk} B}{(\delta(A))}.$$

Proof. It will suffice to show that $\frac{B\otimes_{\Bbbk}B}{(\delta(A))}$ satisfies the universal property defining the tensor product $B\otimes_A B$. Define

$$\begin{array}{rccc} \theta: & B\times B & \longrightarrow & \frac{B\otimes_{\Bbbk}B}{(\delta(A))} \\ & (b_1,b_2) & \longmapsto & b_1\otimes b_2+(\delta(A)) \end{array}.$$

The $\Bbbk$-bilinearity of the tensor product insures that θ is a well defined $\Bbbk$-bilinear map. Take $a\in A$, and $(b_1,b_2)\in B\times B$, then

$$\begin{aligned} \theta(ab_1,b_2) &= (ab_1)\otimes b_2+(\delta(A)) \\ &= (a\otimes 1)(b_1\otimes b_2)+(1\otimes a-a\otimes 1)(b_1\otimes b_2)+(\delta(A)) \\ &= (1\otimes a)(b_1\otimes b_2)+(\delta(A)) \\ &= b_1\otimes(ab_2)+(\delta(A)) \end{aligned},$$

thus, θ is A-linear.

Let C be any A-algebra and let $f: B\times B\to C$ be a A-linear map. We can then define a map $\tilde{f}:\frac{B\otimes_{\Bbbk}B}{(\delta(A))}\to C$ by setting

$$b_1\otimes b_2+(\delta(A))\mapsto f(b_1,b_2),$$

and extending linearly. This map is well defined since

$$\tilde{f}(1\otimes a-a\otimes 1+(\delta(A)))=f(1,a)-f(a,1)=af(1,1)-af(1,1)=0,$$

and $f=\tilde{f}\circ\theta$ by construction. □

Definition A.0.4. Let A be a domain. We define the *normalization* $\tilde{A}$ of A to be the integral closure of A in its field of fractions $Q(A)$. If $\tilde{A}=A$, the we say that A is a *normal domain.*

Definition A.0.5. Let $A\subset B$ be domains of characteristic $p>0$, then the *purely inseparable closure* of A in B is defined to be

$$\hat{A}=\{f\in B\mid \exists r\in\mathbb{N},\ f^{p^r}\in A\}.$$

If A and B have characteristic zero, we set $\hat{A}=A$.