INVARIANT THEORY

RAJIV NELAKANTI

1. Introduction

As one might imagine, invariants deal with quantities that do not change under some algebraic transformations, such as polynomial discriminants. We will consider invariants under two lights: first with the more concrete manner to gain some footing, and then with more abstraction to prove some results.

2. Invariants Basics

In order to understand invariants, we need to understand what invariants pertain to.

Definition 2.1. A **form** of degree r in n variables is a polynomial in n variables such that each term has degree r: $f(x_1,\ldots,x_n) = \sum_{i_1+\ldots+i_n=r}(a_{i_1\ldots i_n}\cdot x_1^{i_1}\ldots x_n^{i_n})$

Furthermore, we need to pinpoint under what circumstances these invariants remain the same.

Definition 2.2. A **linear change of variables** upon form $f(x_1,\ldots,x_n)$ redefines every variable as $x_i \to \sum_{j=1}^{n}\alpha_{ij}x_j$ from $i=1$ to $i=n$ to create the new form $f'(x_1,\ldots,x_n) = \sum_{i_1+\ldots+i_n=r}(a'_{i_1\ldots i_n}\cdot x_1^{i_1}\ldots x_n^{i_n})$ such that $a_{i_1\ldots i_n}\to a'_{i_1\ldots i_n}$ according to the matrix α.

Finally, we have enough material to properly define an invariant: a polynomial on the coefficients of forms that does not change (up to a multiple of the determinant of the matrix α) despite linear changes of variables.

Definition 2.3. The polynomial $\phi(\ldots,a_{i_1\ldots i_n},\ldots)$ in coefficients of the form $f(x_1,\ldots,x_n)$ is called an **invariant** if, after a linear change of variables into $f'(x_1,\ldots,x_n)$, $\phi(\ldots,a'_{i_1\ldots i_n},\ldots) = \left|\alpha\right|^q\cdot\phi(\ldots,a_{i_1\ldots i_n},\ldots)$.

We call q the weight of the invariant, where $q=0$ implies that the invariant is an absolute invariant. As an example, the discriminant $D=b^2-4ac$ of the binary quadratic form $ax^2+bxy+cy^2$ remains constant under linear transformations of x and y, with weight 0.

It is interesting to wonder how many invariants can be described given a form. In the case of the binary quadratic form, just the determinant is enough to generate every other invariant. In general, the algebra of invariants is finitely generated; that is, it only takes polynomials $\phi_1,\ldots,\phi_m$ to express any invariant of a form. As it turns out, this marvelous result is the first fundamental theorem of invariant theory, and we will grapple with its proof after familiarizing ourselves with a more abstract algebra-oriented approach.

Date: June 30, 2017.

3. First Fundamental Theorem of Invariant Theory

We now address invariants in terms of group theory to outline Hilbert's proof of the FFT of Invariant Theory.

Consider vector space V, which we can think of as $\mathbb{C}^n$, along with group G that acts linearly on V. Under this context, V/G is the space of G-orbits of V. A typical element would be an equivalence class of elements of V such that $v \in V$ generates the class $gv : g \in G$.

We can think of a polynomial function on V as a polynomial in n variables. We say that polynomial $f \in \mathbb{C}[x_1, \ldots, x_n]$ is **G-invariant** if $f(gv) = f(v)$ for all $g \in G$. The G-invariant functions form a ring, which we call $\mathbb{C}[V/G]$ - also known as the polynomials on the orbit space V/G. These special kinds of polynomials have values over V/G because they remain constant over each respective equivalence class. Note that this is similar to our use of homogeneous functions in $\mathbb{P}^n$ to make things make sense.

As an example, consider the vector space $V = \mathbb{C}^2$ acted on by group $G = \mathbb{Z}/2\mathbb{Z}$ by $(x, y) \to (-x, -y)$. Then, $\mathbb{C}[V/G] = \{f(x, y) : f(x, y) = f(-x, -y)\} = \mathbb{C}[x^2, y^2, xy]$.

Theorem 3.1. *(Hilbert's Proof of the FFT) $\mathbb{C}[V/G]$ is finitely generated if G is linearly reductive.*

Proof. In order to prove this result, Hilbert defined the Reynolds operator $R : \mathbb{C}[V] \to \mathbb{C}[V/G]$, which was essentially a linear projection acting as the identity on $\mathbb{C}[V/G]$. By definition, given $h \in \mathbb{C}[V/G]$ and $f \in \mathbb{C}[V]$, $R(hf) = hR(f)$. This implies that for every ideal $\mathfrak{a} \subset \mathbb{C}[V/G]$, we have $R(\mathbb{C}[V]\mathfrak{a}) = \mathbb{C}[V]\mathfrak{a} \cap \mathbb{C}[V/G] = \mathfrak{a}$. Now, take the homogeneous maximal ideal $\mathfrak{m}_0$ of $\mathbb{C}[V]$. By Hilbert's Basis Theorem, the ideal is finitely generated by some $f_1, \ldots, f_s$. Since $\mathfrak{m}_0 = R(\mathbb{C}[V]\mathfrak{m}_0)$, the ideal of $\mathbb{C}[V/G]$ is also generated by $f_1, \ldots, f_s$. Any homogeneous system of generators of $\mathfrak{m}_0$ is also a system of generators for $\mathbb{C}[V/G]$, thus proving the theorem and showing that $\mathbb{C}[V/G]$ is Noetherian. ■