Polynomial Invariant Theory of the Classical Groups

Quinton Westrich

April 17, 2006

Abstract

The goal of invariant theory is to find all the generators for the algebra of representations of a group that leave the group invariant. Such generators will be called *basic invariants*. In particular, we set out to find the set of basic invariants for the classical groups $\mathrm{GL}(V)$, $\mathrm{O}(n)$, and $\mathrm{Sp}(n)$ for n even. In the first half of the paper we set up relevant definitions and theorems for our search for the set of basic invariants, starting with linear algebraic groups and then discussing associative algebras. We then state and prove a monumental theorem that will allow us to proceed with hope: it says that the set of basic invariants is finite if G is reductive. Finally we state without proof the First Fundamental Theorems, which aim to list explicitly the relevant sets of basic invariants, for the classical groups above. We end by commenting on some applications of invariant theory, on the history of its development, and stating a useful theorem in the appendix whose proof lies beyond the scope of this work.

Contents

1 Linear Algebraic Groups and their Representations

1.1 Linear Algebraic Groups

First we shall establish some notations. We denote by $\mathrm{GL}(n,\mathbb{C})$ the group of invertible $n \times n$ complex matrices. By $M_n(\mathbb{C})$ we mean the space of all $n \times n$ complex matrices. We write the i,j entry of a matrix $y \in M_n(\mathbb{C})$ with $1 \leq i,j \leq n$ as $x_{ij}(y)$. The ring of complex polynomials in n variables will be denoted $\mathbb{C}[x_1,\ldots,x_n]$. Now we may state the following definitions:

Definition 1.1 *A function $f : M_n(\mathbb{C}) \to \mathbb{C}$ is a* **polynomial function** *on $M_n(\mathbb{C})$ if there exists $p \in \mathbb{C}[x_{11}(y), x_{12}(y), \ldots, x_{nn}(y)]$ such that*

$$f(y) = p(x_{11}(y), x_{12}(y), \ldots, x_{nn}(y)).$$

Definition 1.2 *A subgroup $G \leq \mathrm{GL}(n,\mathbb{C})$ is a* **linear algebraic group** *if there exists a set A of polynomial functions on $M_n(\mathbb{C})$ such that*

$$G = \{g \in G \mid f(g) = 0 \text{ for all } f \in A\}.$$

A consequence of the *Hilbert basis theorem* (App.A) is that any linear algebraic group can be defined by a *finite* number of polynomial equations [4]. As an example of a linear algebraic group, consider the subgroup $D_n \leq \mathrm{GL}(n,\mathbb{C})$ of diagonal invertible matrices. The defining equations for D_n are $x_{ij} = 0$ for $i \neq j$. So D_n is a linear algebraic group.

1.2 Regular Functions

Definition 1.3 *The ring of* **regular functions** *for the linear algebraic group $\mathrm{GL}(n,\mathbb{C})$ is defined as*

$$\mathrm{Aff}(\mathrm{GL}(n,\mathbb{C})) := \mathbb{C}[x_{11}(y), x_{12}(y), \ldots, x_{nn}(y), (\det(y))^{-1}].$$

This is just the complex algebra generated by the matrix entry functions x_{ij} and the function $(\det(y))^{-1}$.

We must now state a few more notational conventions. We shall denote a vector space by V, the algebra of all linear transformations on V by $\mathrm{End}(V)$, and the group of all invertible linear transformations on V by $\mathrm{GL}(V)$.

Definition 1.4 *Suppose $\dim V = n$ and $\{e_i\}$ is a basis for V. Let $g \in \mathrm{GL}(V)$ and $\phi(g)$ be the matrix $[g_{ij}]$ such that*

$$ge_j = \sum_{i=1}^{n} g_{ij} e_i.$$

Then the map $g \mapsto \phi(g)$ gives an isomorphism

$$\phi : \mathrm{GL}(V) \xrightarrow{\cong} \mathrm{GL}(n,\mathbb{C}).$$

We define the **regular functions** *on $\mathrm{GL}(V)$ to be those of the form $f \circ \phi$, where f is a regular function on $\mathrm{GL}(n,\mathbb{C})$.*

This definition just says that it only makes sense to move into a basis before we can talk about a regular function on $\mathrm{GL}(V)$. To denote the algebra of regular functions on $\mathrm{GL}(V)$, we use the symbol $\mathrm{Aff}(\mathrm{GL}(V))$. Note, however, that $\mathrm{Aff}(\mathrm{GL}(V))$ is independent on the particular choice of basis of V.

Definition 1.5 *Let $G \leq \mathrm{GL}(V)$ be a linear algebraic group. Let $f : \mathrm{GL}(V) \to \mathbb{C}$ be a regular function on $\mathrm{GL}(V)$. Then the restriction $f|_G : G \to \mathbb{C}$ is called a* **regular function** *on G.*

The set $\mathrm{Aff}(G)$ of regular functions on G is a commutative algebra over $\mathbb{C}$ under pointwise multiplication.

Definition 1.6 *Let G and H both be linear algebraic groups. Then a* **regular homomorphism** *is a group homomorphism $\phi : G \to H$ such that $\phi^*(\mathrm{Aff}(H)) \subseteq \mathrm{Aff}(G)$, where for $f \in \mathrm{Aff}(H)$,*

$$\phi^*(f)(g) := f(\phi(g)).$$

Definition 1.7 *Let G and H both be linear algebraic groups. We say that G and H are* **isomorphic** *as linear algebraic groups if there exists a regular homomorphism $\phi : G \to H$ such that ϕ^{-1} is also a regular homomorphism.*

1.3 Representations of Linear Algebraic Groups

Definition 1.8 *A* **representation** *of a linear algebraic group G is a pair (ρ, V), where V is a complex finite- or infinite-dimensional vector space and $\rho : G \to \mathrm{GL}(V)$ is a group homomorphism.*

Definition 1.9 *A* **regular representation** *of a linear algebraic group G is a representation (ρ, V) for which $\dim(V)$ is finite and $\rho : G \to \mathrm{GL}(V)$ is a regular homomorphism.*

This means that if we fix a basis and write out the matrix for $\rho(g)$ in this basis, then the elements $\rho_{ij}(g)$ are all regular functions on G.

Definition 1.10 *If (ρ, V) is a regular representation of the linear algebraic group G and $W \subseteq V$ is a vector subspace of V, then we say that W is* **G-invariant** *if $\rho(g)w \in W$ for all $g \in G$, $w \in W$.*

Definition 1.11 *A representation (ρ, V) with $V \neq \{0\}$ is* **reducible** *if there is a non-trivial G-invariant subspace $W \subseteq V$. A representation is* **irreducible** *if it is not reducible.*

As an example, let (ρ, V) and (σ, W) be regular representations of a linear algebraic group G. Define the *tensor product representation* $\rho \otimes \sigma$ on $V \otimes W$ by

$$(\rho \otimes \sigma)(g)(v \otimes w) := \rho(g)v \otimes \sigma(g)w$$

for $g \in G$, $v \in V$, and $w \in W$. Then $\rho \otimes \sigma$ is a regular representation.

Definition 1.12 *A regular representation (ρ, V) of a linear algebraic group G is* **completely reducible** *if for every G-invariant subspace $W \subseteq V$ there exists another G-invariant subspace $U \subseteq V$ such that $V = W \oplus U$.*

In terms of matrices, this means that any basis $\{w_1, \ldots, w_p\}$ for W can be completed to a basis $\{w_1, \ldots, w_p, u_1, \ldots, u_q\}$ for V so that the subspace $U = \text{span}_{\mathbb{C}}\{u_1, \ldots, u_q\}$ is invariant under $\rho(g)$ for all $g \in G$. Thus, the matrix of $\rho(g)$ relative to this basis has the block-diagonal form

$$\begin{pmatrix} \sigma(g) & 0 \\ 0 & \tau(g) \end{pmatrix}$$

where $\sigma(g) = \rho(g)|_W$ and $\tau(g) = \rho(g)|_U$.

Definition 1.13 *We say that a linear algebraic group G is* **reductive** *if every regular representation (ρ, V) of G is completely reducible.*

In particular, it can be shown that all finite groups and the classical groups are reductive [4].

2 Associative Algebras and their Representations

In this section we introduce some of the basic terminology to describe the space $\mathcal{P}(V)$ of polynomials of elements of a vector space V. To understand what one means by a polynomial function on a vector space we need the concept of an *algebra*.

2.1 Associative Algebras

Definition 2.1 *An* **associative algebra** *over the complex field $\mathbb{C}$ is a pair $(\mathcal{A}, \mu)$ with $\mathcal{A}$ a vector space over $\mathbb{C}$ and μ a bilinear associative map on $\mathcal{A}$, i.e.*

$$\mu : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$$

with

$$(x, y) \mapsto \mu(x, y) \equiv xy$$

such that

$$(xy)z = x(yz)$$

for all $x, y, z \in \mathcal{A}$. If the algebra possesses a unit element, it is called a **unital algebra**.

When speaking of an algebra $(\mathcal{A}, \mu)$, it is customary to only write the vector space $\mathcal{A}$ and omit mentioning explicitly the bilinear map μ. Also, we note that it is easy to see that for a vector space V the space of linear maps $\text{End}(V)$ is an associative algebra with composition taken as the algebra multiplication.

Definition 2.2 *Let $\mathcal{J}$ be a vector subspace of the algebra $\mathcal{A}$. Then if $\mu|_{\mathcal{J}}$ is closed in $\mathcal{J}$, we call $\mathcal{J}$ a* **subalgebra** *of $\mathcal{A}$ with respect to the bilinear map $\mu|_{\mathcal{J}}$.*

Definition 2.3 *Let $\mathcal{A}$ be an associative algebra and $\mathcal{I}$ be a subalgebra of $\mathcal{A}$. Then $\mathcal{I}$ is called a* **two-sided ideal** *of the algebra $\mathcal{A}$ if, $\forall(x \in \mathcal{I})$, $\forall(y \in \mathcal{A})$, $xy \in \mathcal{I}$ and $yx \in \mathcal{I}$.*

Definition 2.4 *Let $\mathcal{A}$ and $\mathcal{C}$ be associative algebras. An* **algebra homomorphism** *is a map $\varphi : \mathcal{A} \to \mathcal{C}$ such that for all $x, y \in \mathcal{A}$,*

$$\varphi(xy) = \varphi(x)\varphi(y). \tag{1}$$

Definition 2.5 *An* **algebra isomorphism** *is a bijective algebra homomorphism.*

2.2 Representations of Associative Algebras

Definition 2.6 *A* **representation** *of an associative algebra $\mathcal{A}$ is a pair (ρ, V) with V a vector space and $\rho : \mathcal{A} \to \mathrm{End}(V)$ an algebra homomorphism. Here we call V an* **$\mathcal{A}$-module**.

Let $\mathcal{A}$ be an associative algebra and U be a finite-dimensional irreducible $\mathcal{A}$-module. Denote by $[U]$ the equivalence class of all $\mathcal{A}$-modules isomorphic to U. Denote by $\widehat{\mathcal{A}}$ the set of all equivalence classes of finite-dimensional irreducible $\mathcal{A}$-modules.

Definition 2.7 *Let $\mathcal{A}$ be an associative algebra and V be a completely reducible $\mathcal{A}$-module. Then for $\xi \in \widehat{\mathcal{A}}$, we define the* **$\xi$-isotypic subspace** *$V_{(\xi)}$ of V to be*

$$V_{(\xi)} := \sum_{\substack{U \subseteq V \\ [U]=\xi}} U \tag{2}$$

where the U are invariant and irreducible.

Let V be a completely reducible $\mathcal{A}$-module and

$$V = \bigoplus_{i=1}^{d} V_i \tag{3}$$

be any decomposition such that all the V_i are invariant and irreducible. Then it can be shown that $\forall(\xi \in \widehat{\mathcal{A}})$,

$$V_{(\xi)} = \bigoplus_{[V_j]=\xi} V_j \tag{4}$$

and so

$$V = \bigoplus_{\xi \in \widehat{\mathcal{A}}} V_{(\xi)}. \tag{5}$$

We have now developed a sufficient amount of theory to begin our development of invariant theory.

3 The Ring of Polynomial Invariants

Let G be a reductive linear algebraic group and (π, V) be a regular representation of G. Define a representation ρ of G on the algebra $\mathcal{P}(V)$ by

$$\rho(g)f(v) := f(\pi(g^{-1})v) \equiv f(g^{-1}v) \tag{6}$$

for $f \in \mathcal{P}(V)$, $g \in G$, and $v \in V$, where in the last equality we have suppressed the π notation as convention dictates. Note that $\mathcal{P}(V)$ contains polynomials of all orders. We'll need to be more specific so we introduce the notation:

$$\mathcal{P}^k(V) := \{f \in \mathcal{P}(V) \mid f(zv) = z^k f(v) \text{ for } z \in \mathbb{C}^\times\}, \tag{7}$$

the (finite-dimensional) space of *homogeneous polynomials of degree* k for $k \in \mathbb{N}$. In particular, $\mathcal{P}^k(V)$ is G-invariant and $\rho|_{\mathcal{P}^k(V)} \equiv \rho_k$ is a regular representation of G.

Definition 3.1 *The* **algebra of G-invariants** *is the space of G-invariant polynomials on a vector space V. We shall denote this algebra by $\mathcal{P}(V)^G$.*

Theorem 3.1 *Suppose G is a reductive linear algebraic group which has a regular representation on a vector space V. Then the algebra $\mathcal{P}(V)^G$ of G-invariant polynomials on V is finitely generated as an algebra over $\mathbb{C}$.*

Proof. Since G is reductive we have that $\mathbb{C}[\rho_k(G)]$ is semisimple. Hence, we can write

$$\mathcal{P}^k(V) = \bigoplus_{\sigma \in \widehat{G}} W_{(\sigma)}, \tag{8}$$

the decomposition into G-isotypic subspaces.

Consider some polynomial function $f \in \mathcal{P}(V)$ of arbitrary order. We can decompose f as

$$f = \sum_{k=0}^{d} f_k \tag{9}$$

with the f_k homogeneous of degree k so that we have d polynomials each in some $\mathcal{P}^k(V)$. Decompose further every f_k by (8), collect like σ's, and write

$$f = \sum_{\sigma \in \widehat{G}} f_{(\sigma)} \tag{10}$$

where $f_{(\sigma)} \in W_{(\sigma)}$ is the *σ-isotypic component of f*.

Denote by $f_{(1)} = f^\natural$ the trivial representation. Let φ be a G-invariant function, i.e. $\varphi \in \mathcal{P}(V)^G$ and $f \in \mathcal{P}(V)$ as above. Then, since multiplication by a G-invariant function leaves isotypic subspaces invariant,

$$(\varphi f)^\natural = \varphi f^\natural. \tag{11}$$

So, taking $\mathcal{P}(V)$ as a module of $\mathcal{P}(V)^G$, the $\mathcal{P}(V)^G$-module map $f \mapsto f^\natural$ is a projection operator.

Now, by the Hilbert basis theorem (App.A), every ideal of $\mathcal{P}(V)$ is finitely generated. Also if $\mathcal{I}$ is an ideal of $\mathcal{P}(V)$, then $\mathcal{P}(V)/\mathcal{I}$ is finitely generated too. Denote by $\mathcal{P}(V)^G_+$ the space of invariant polynomials in which the zeroth order term vanishes. We claim that $\mathcal{P}(V)^G_+$ is an ideal of $\mathcal{P}(V)$. Indeed, let $x \in \mathcal{P}(V)^G_+$ and $y \in \mathcal{P}(V)$. Then we can write y as $y = w + z$ with $\deg w \geq 1$ and $\deg z = 0$, i.e. $w \in \mathcal{P}(V)^G_+$ and $z \in \mathbb{C}$. Then

$$xy = x(w + z) = xw + xz. \tag{12}$$

Obviously, $\deg(xw) \geq 1$. But we also have $\deg(xz) \geq 1$ since for any polynomials $a, b \in \mathcal{P}(V)$, $\deg(ab) = \deg(a) + \deg(b)$. The proof that $yx \in \mathcal{P}(V)^G_+$ is completely symmetric. It follows that $\mathcal{P}(V)^G_+$ is finitely generated.

Suppose the set $\{\phi_i\}_{i=1}^n$ generates $\mathcal{P}(V)^G_+$. We claim now that $\{\phi_i\}_{i=1}^n$ must also generate $\mathcal{P}(V)^G$ as an algebra over $\mathbb{C}$. Let $\phi \in \mathcal{P}(V)^G$. Then there exists a set of polynomials $\{f_i\}_{i=1}^n$ with $f_i \in \mathcal{P}(V)$ for every i such that

$$\phi = \sum_{i=1}^n f_i \phi_i. \tag{13}$$

If we now project out $\phi^\natural$ so that

$$\phi^\natural = \sum_{i=1}^n (f_i \phi_i)^\natural = \sum_{i=1}^n f_i^\natural \phi_i, \tag{14}$$

we may assume, since $\deg f_i^\natural \leq \deg f_i \leq \deg \phi$, that $f_i^\natural$ is in the algebra generated by the set $\{\phi_i\}_{i=1}^n$, and, hence, so is ϕ. $\square$

Thm. 3.1 motivates the following definition.

Definition 3.2 *The smallest set $\{f_i\}_{i=1}^n$ that generates $\mathcal{P}(V)^G$ is called the set of* **basic invariants**.

The goal of invariant theory is to find this set. In the following we shall state without proof the sets of basic invariants for the classical groups. It should be noted that while the above theorem states the necessary existence of such a set for reductive groups, these sets are not unique in general. However if we order the set of degrees of each of the generators, that set is unique [4].

4 Polynomial Invariants of the Classical Groups

4.1 Polynomial Invariants of $\mathbf{GL}(V)$

Given a vector space V, there exist *natural isomorphisms*

$$(V^*)^{\oplus k} \cong \mathrm{Hom}(V, \mathbb{C}^k) \tag{15}$$

given by

$$v \mapsto [\langle v_1^*, v\rangle, \ldots, \langle v_k^*, v\rangle]$$

and

$$V^{\oplus m} \cong \mathrm{Hom}(\mathbb{C}^m, V) \tag{16}$$

given by

$$[c_1, \ldots, c_m] \mapsto c_1 v_1 + \cdots + c_m v_m.$$

From this, we can write the *algebra* isomorphism

$$\mathcal{P}((V^*)^{\oplus k} \times V^{\oplus m}) \cong \mathcal{P}(\mathrm{Hom}(V, \mathbb{C}^k) \times \mathrm{Hom}(\mathbb{C}^m, V)) \tag{17}$$

Suppose $f \in \mathcal{P}(\mathrm{Hom}(V, \mathbb{C}^k) \times \mathrm{Hom}(\mathbb{C}^m, V))$ and $g \in \mathrm{GL}(V)$. We define the *action of g on f* by

$$g \cdot f(x, y) = f(x\rho(g^{-1}), \rho(g)y). \tag{18}$$

Denoting by $M_{k,m}$ the (vector) space of all $k \times m$ complex matrices we can also define the function

$$\mu : \mathrm{Hom}(V, \mathbb{C}^k) \times \mathrm{Hom}(\mathbb{C}^m, V) \to M_{k,m}$$

by

$$\mu(x, y) := xy,$$

in which by juxtaposition we mean ordinary composition of linear maps. Then $\forall(g \in \mathrm{GL}(V))$,

$$\begin{aligned} g \cdot \mu(x, y) &= \mu(x\rho(g^{-1}), \rho(g)y) \\ &= x\rho(g^{-1})\rho(g)y \\ &= xy \\ &= \mu(x, y). \end{aligned} \tag{19}$$

Now, define

$$\mu^* : \mathcal{P}(M_{k,m}) \to \mathcal{P}(\mathrm{Hom}(V, \mathbb{C}^k) \times \mathrm{Hom}(\mathbb{C}^m, V))^{\mathrm{GL}(V)}$$

such that $\forall(f \in \mathcal{P}(M_{k,m}))$, $f \mapsto f \circ \mu$. Finally, define the *matrix entry function* on $M_{k,m}$:

$$z_{ij} := \mu^*(x_{ij}). \tag{20}$$

Then z_{ij} is the *contraction* of the ith dual vector and the jth vector position, i.e.

$$z_{ij}(v_1^*, \ldots, v_k^*, v_1, \ldots, v_m) = \langle v_i^*, v_j\rangle. \tag{21}$$

Theorem 4.1 (Polynomial FFT for $\mathrm{GL}(V)$)
The map μ^* is surjective and, hence, $\mathcal{P}((V^*)^{\oplus k} \times V^{\oplus m})^{\mathrm{GL}(V)}$ is generated by the contractions

$$\{\langle v_i^*, v_j\rangle \mid i = 1, \ldots, k; j = 1, \ldots, m\}.$$

4.2 Polynomial Invariants of $\mathbf{O}(n)$

Let $V = \mathbb{C}^n$ and define a nondegenerate symmetric bilinear form on on V by

$$(x, y) := \sum_{i=1}^{n} x_i y_i \tag{22}$$

for $x, y \in \mathbb{C}^n$. Denote by $\mathrm{O}(n)$ the *orthogonal group* for $(\cdot\,,\cdot)$ so that

$$g \in \mathrm{O}(n) \;:\Leftrightarrow\; g^T g = \mathbf{1}_{n\times n}. \tag{23}$$

Denote also the space of all $k \times k$ symmetric matrices over $\mathbb{C}$ by SM_k so that

$$B \in SM_k \Rightarrow B = B^T.$$

Define the map $\tau : M_{n,k} \to SM_k$ such that $X \mapsto X^T X$ for all $X \in M_{n,k}$. Then for all $g \in \mathrm{O}(n)$ and $X \in M_{n,k}$,

$$\begin{aligned} \tau(gX) &= (gX)^T gX \\ &= X^T g^T gX \\ &= X^T X \\ &= \tau(X). \end{aligned} \tag{24}$$

For $f \in \mathcal{P}(SM_k)$, define $\tau^* : \mathcal{P}(SM_k) \to \mathcal{P}(V^k)^{\mathrm{O}(n)}$ by $f \mapsto f \circ \tau$. From this definition, it follows that

$$\tau^*(f)(gX) = \tau^*(f)(X) \tag{25}$$

and τ is an algebra isomorphism. For example, if $v_1, \ldots, v_k \in \mathbb{C}^n$, then there exists $X = [v_1, \ldots, v_k] \in M_{n,k}$ so that

$$x_{ij}(X^T X) = (v_i, v_j). \tag{26}$$

Now, by Eqs.(25) and (26), we have on $(\mathbb{C}^n)^{\oplus m}$:

$$\tau^*(x_{ij})(v_1, \ldots, v_k) = (v_i, v_j), \tag{27}$$

the contraction of the i, jth vector using $(\cdot\,,\cdot)$.

Theorem 4.2 (Polynomial FFT for $\mathrm{O}(n)$)
The map $\tau^* \in \mathrm{Hom}(\mathcal{P}(SM_k), \mathcal{P}((\mathbb{C}^n)^{\oplus k})^{\mathrm{O}(n)})$ is surjective, and, hence, $\mathcal{P}((\mathbb{C}^n)^{\oplus k})^{\mathrm{O}(n)}$ is generated by the orthogonal contractions

$$\{(v_i, v_j) \,|\, 1 \le i \le j \le k\}.$$

4.3 Polynomial Invariants of $\mathbf{Sp}(n)$

Define the matrices

$$\kappa := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad J_n := \begin{pmatrix} \kappa & 0 & \cdots & 0 \\ 0 & \kappa & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \kappa \end{pmatrix}$$

(where J_n is block-diagonal) and the antisymmetric form

$$\omega(x, y) := (x, J_n y) \tag{28}$$

for $x, y \in \mathbb{C}^n$. Obviously, if we mean by the subscript n the dimension of J_n, then $n \in 2\mathbb{N}$. Denote by $\mathrm{Sp}(n)$ the *symplectic group* for $\omega(\cdot\,,\cdot)$ so that

$$g \in \mathrm{Sp}(n) \;:\Leftrightarrow\; g^T J_n g = J_n. \tag{29}$$

For the space of $k \times k$ antisymmetric matrices we write AM_k. Now, define $\gamma : M_{n,k} \to AM_k$ by $X \mapsto X^T J_n X$ for all $X \in M_{n,k}$. We can define further, for $f \in \mathcal{P}(AM_k)$, the map

$$\gamma^* := f \circ \gamma. \tag{30}$$

It follows that $\gamma^* \in \mathrm{Hom}(\mathcal{P}(AM_k), \mathcal{P}(V^{\oplus k})^{\mathrm{Sp}(n)})$ since

$$\gamma^*(f)(gX) = \gamma^*(f)(X). \tag{31}$$

Now,

$$X \in M_{n,k} \;\Rightarrow\; X^T J_n X \in AM_k \tag{32}$$

and

$$x_{ij}(X^T J_n X) = (v_i, J_n v_j) \;\Rightarrow\; \gamma^*(x_{ij})(v_1, \ldots, v_k) = \omega(v_i, v_j), \tag{33}$$

the contraction of the i, jth position with $i < j$ using the $\omega(\cdot\,,\cdot)$.

Theorem 4.3 (Polynomial FFT for $\mathrm{Sp}(n)$)
Let $n \in 2\mathbb{N}$. Then the map $\gamma^* \in \mathrm{Hom}(\mathcal{P}(AM_k), \mathcal{P}((\mathbb{C}^n)^{\oplus k})^{\mathrm{Sp}(n)})$ is surjective, and, hence, $\mathcal{P}((\mathbb{C}^n)^{\oplus k})^{\mathrm{Sp}(n)}$ is generated by the symplectic contractions

$$\{\omega(v_i, v_j) \,|\, 1 \leq i < j \leq k\}.$$

5 Afterword

5.1 Applications

There are a plethora of applications which use the results of the invariant theory of the classical groups. Here we state just a few. Polynomial and tensor invariants have been used most explicitly in quantum computing [8], but have also appeared in works on classical mechanics [7]. They also provide a method of describing quantum entanglement [9] and quantum information [1]. However, the results of invariant theory are most often assumed in most all work in special and general relativity where the invariants of $\mathrm{SO}(3, 1)$ play a leading role.

5.2 Comments

The proof of Theorem 3.1 is due to Hurwitz and follows that presented in [4]. The terminology *First Fundamental Theorem* is due to H. Weyl (1946). Also, in his landmark book *The Classical Groups, their Invariants and Representations,* Weyl proved the polynomial form of the FFT using the *Capelli identity* and "polarization operators". For a sketch of this method see [3]. Also it may be noted that although invariant theory is well-established, ongoing research into novel proofs that may give insight into other fields of mathematics are continuing to be sought after. For example, see [5] and [6].

A The Hilbert Basis Theorem

Since there are two references to this theorem in the body of the paper, it seems necessary to at least state this deep theorem from algebraic geometry. For details and a proof see [4].

Theorem A.1 (Hilbert basis theorem)
Let $\mathcal{I} \subseteq \mathcal{P}(V)$ be an ideal. Then $\mathcal{I}$ is finitely generated. That is, there is a finite set of polynomials $f_1, \ldots, f_d$ in $\mathcal{I}$ so that every $g \in \mathcal{I}$ can be written as

$$g = g_1 f_1 + \cdots + g_d f_d \tag{34}$$

for some choice of $g_1, \ldots, g_d \in \mathcal{P}(V)$.

References

[1] Brylinski, J. and Brylinski, R. *Invariant Polynomial Functions on k qubits.* e-print: quant-ph/0010101 (2000)

[2] Fuchs, J. and Schweigert, C. *Symmetries, Lie Algebras, and Representations: A graduate course for physicists.* Cambridge University Press, 1997.

[3] Fulton, W. and Harris, J. *Representation Theory, a First Course.* Springer Verlag, New York, 1991.

[4] Goodman, R. and Wallach, N. *Representations and Invariants of the Classical Groups.* Cambridge University Press, 1998.

[5] Mihailovs, A. *Symplectic tensor invariants, wave graphs, and S-tris.* eprint: math/9803102 (1998)

[6] Mihailovs, A. *Tensor invariants of $SL(n)$, wave graphs, and L-tris.* e-print: math/9802119 (1998)

[7] Morrison, P. and Narayanan, V. *Rank change in Poisson dynamical systems.* http://www.ma.utexas.edu/users/narayana/Academics/Publications/pap1.pdf (2003)

[8] Rodríguez-Carbonell, E. *Applications of Polynomial Invariants.* http://www.lsi.upc.es/∼erodri/webpage/papers/parma2.pdf

[9] Sudbery, A. *Polynomial entanglement invariants.* http://www.imaph.tu-bs.de/qi/problems/3.pdf (2001)