

# ELEMENTS OF INVARIANT THEORY

T. R. RAMADAS

ABSTRACT. These are notes of lectures given at Mombasa during 4-14 July, 2005

## 1. GENERALITIES ON GROUP ACTIONS AND INVARIANTS

Let  $E$  be a set, and  $G$  a group. Recall that a *right action* of  $G$  on  $E$  is a map  $E \times G \rightarrow E$ , which, denoting by  $x \cdot g$  the image of  $(x, g)$ , satisfies  $x \cdot e = x$ , and  $(x \cdot g_1) \cdot g_2 = x \cdot (g_1 g_2)$ . A *left action* is a map  $G \times E \rightarrow E$ ; adopting the suggestive notation  $g \cdot x$  for the image of  $(g, x)$ , a left action satisfies  $e \cdot x = x$ , and  $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$ . We let  $E \curvearrowright G$  denote a right action, and  $G \curvearrowleft E$  a left action. (When  $G$  is commutative, as will be the case in our first three examples below, there is of course no distinction between a right and left action.)

A left action is the same as homomorphism  $g \mapsto \rho_g$  from  $G$  to the group of bijective maps  $E$  to  $E$ , the correspondence being  $g \cdot x = \rho_g(x)$ .

Let  $\mathbb{F}(E)$  denote the space of functions  $f : E \rightarrow \mathbb{C}$ . This is a  $\mathbb{C}$ -algebra, with addition and multiplication being defined respectively by

$$(1) \quad \begin{aligned} (f_1 + f_2)(x) &= f_1(x) + f_2(x) \\ (f_1 f_2)(x) &= f_1(x) f_2(x) \end{aligned}$$

If  $E \curvearrowright G$ , we can define a *left action* of  $G$  on  $\mathbb{F}(E)$ :

$$(g, f) \mapsto \rho_g(f)$$

defined by  $\rho_g(f)(x) = f(x \cdot g)$ . Check that this is a left action, and also that  $G$  acts by homomorphisms of the  $\mathbb{C}$ -algebras. In particular,

$$(2) \quad \begin{aligned} \rho_g(f_1 + f_2) &= \rho_g(f_1) + \rho_g(f_2) \\ \rho_g(f_1 f_2) &= \rho_g(f_1) \rho_g(f_2) \end{aligned}$$

If  $G$  acts on a set  $E$ , let  $E^G$  denote the subset of fixed points:  $E^G = \{x \in E \mid x \cdot g = x \ \forall g \in G\}$ . We have written the definition for a right action; clearly one can make a similar definition for a left action.

**Exercise:** Check that  $\mathbb{F}(E)^G$  is a subalgebra of  $\mathbb{F}(E)$ . The elements of  $\mathbb{F}(E)^G$  are called *invariant functions*.

We are interested in getting our hands on subalgebras of  $\mathbb{F}(E)^G$ . We will do this in two steps.

---

*Date:* August 8, 2005.

**Step 1:** Here is a good way to find subalgebras of  $\mathbb{F}(E)$ . Let  $\pi : E \rightarrow E'$  be a map, and define  $\pi^* : \mathbb{F}(E') \rightarrow \mathbb{F}(E)$  by  $\pi^*(f') = f' \circ \pi$ . The map  $\pi^*$  is a homomorphism of algebras, and so the image  $Im(\pi^*)$  is a subalgebra of  $\mathbb{F}(E)$ . If  $\pi$  is surjective, the map  $\pi^*$  will be *injective* (why?), and we can identify  $\mathbb{F}(E')$  with the image  $Im(\pi^*)$ .

**Step 2:** How do we make sure that  $Im(\pi^*)$  is a subalgebra of  $\mathbb{F}(E)^G$ ? Writing out this condition explicitly, what we require is:

$$f'(\pi(x \cdot g)) = f'(\pi(x)) \quad \forall x \in E, \quad g \in G, \quad \text{and} \quad f' \in \mathbb{F}(E')$$

Clearly this will be true if

$$\pi(x) = \pi(x \cdot g) \quad \forall x \in E, \quad g \in G$$

**Conclusion:** Given a surjective map  $\pi : E \rightarrow E'$  satisfying  $\pi(x \cdot g) = \pi(x) \quad \forall x, g$ , we obtain an algebra of invariant functions isomorphic to  $\mathbb{F}(E')$ .

## 2. SOME EXAMPLES

We will consider, in turn, three examples.

(1) The group with two elements,  $S_2 = \{e, \sigma\}$ , acting on  $\mathbb{C}^2$  as follows:

$$(x, y) \cdot \sigma = (y, x)$$

(2) The group  $\mathbb{C}^*$  of nonzero complex numbers acting on  $\mathbb{C}^2$ :

$$(x, y) \cdot \lambda = (x\lambda, y\lambda^{-1}), \quad \lambda \in \mathbb{C}^*$$

(3) The group  $\mathbb{C}^*$  of nonzero complex numbers acting on  $\mathbb{C}^3$ :

$$(x, y, z) \cdot \lambda = (x\lambda, y\lambda, z\lambda^{-2})$$

Note that in the above cases, the action is “polynomial”, that is, the induced action on the space of functions takes polynomial functions to polynomial functions. In each case we will be interested in describing the algebra of invariant polynomial functions.

We will do this in two steps as in §1, except that this time

- we will look for a *polynomial* map  $\pi$ ,
- we will consider the induced map on *polynomial* functions rather than *all* functions as in that section - we will however, continue to denote this map by  $\pi^*$ , and in fact we will only deal with the polynomial case from now on.
- we will, by choosing  $\pi$  carefully, ensure that the image of  $\pi^*$  is *all* invariant polynomial functions.

We use some standard notation to work with the algebra of polynomial functions. If  $(x_i)_{i=1, \dots, n}$  denotes a point of  $\mathbb{C}^n$ ,  $\mathbb{C}[X_1, \dots, X_n]$  will denote the space of polynomials. Here  $X_i$  are symbols (“indeterminates”) and a typical polynomial is a formal sum

$$P = \sum a_{\alpha_1, \dots, \alpha_n} X_1^{\alpha_1} \dots X_n^{\alpha_n}$$

where the  $a_{\alpha_1, \dots, \alpha_n}$  are complex numbers, which stands for the polynomial function  $P(x_1, \dots, x_n) = \sum a_{\alpha_1, \dots, \alpha_n} x_1^{\alpha_1} \dots x_n^{\alpha_n}$ . (We sometimes write  $P = \sum_{\alpha} a_{\alpha} X^{\alpha}$ , where  $\alpha$  is the “multi-index”  $(\alpha_1, \dots, \alpha_n)$  – a vector with non-negative integers – and by  $X^{\alpha}$  we mean the monomial  $X_1^{\alpha_1} \dots X_n^{\alpha_n}$ .) One uses interchangeably the notions of a polynomial as a formal sum as above, and a complex-valued function which is a sum of terms, each proportional to a product of powers of the co-ordinate functions  $x_i$ . Suppose a polynomial map  $Q : \mathbb{C}^n \rightarrow \mathbb{C}^m$  is given. By definition this is a map of the form

$$(x_1, \dots, x_n) \mapsto (z_1, \dots, z_m)$$

where the co-ordinates  $z_j$  are polynomial functions  $z_j = Q_j(x_1, \dots, x_n)$  of the co-ordinates  $x_i$ . This induces a map  $Q^*$  from the space of polynomial functions on  $\mathbb{C}^m$  to polynomial functions on  $\mathbb{C}^n$ :

$$Q^*(P) = P \circ Q$$

In terms of indeterminates, the map  $Q^* : \mathbb{C}[Y_1, \dots, Y_m] \rightarrow \mathbb{C}[X_1, \dots, X_n]$  is given by the “substitutions”  $Y_j \mapsto Q_j(X_1, \dots, X_n)$ .

Let us now look at the examples in turn.

**Example 1:** Consider the map  $\pi : \mathbb{C}^2 \rightarrow \mathbb{C}^2$ , defined by  $(x, y) \mapsto (e_1 = x + y, e_2 = xy)$ . (a) Clearly  $\pi$  satisfies  $\pi((x, y) \cdot \sigma) = \pi(y, x)$ . (b) We now check that  $\pi$  is surjective. To see this let  $e_1, e_2$  be given. Eliminate  $y$  from the two equations:

$$(3) \quad \begin{aligned} x + y &= e_1 \\ xy &= e_2 \end{aligned}$$

to get  $x^2 + e_2 = e_1x$ . This has (in general) two solutions, so that the above system of two equations also has two solutions. Note that  $\pi^* : \mathbb{C}[E_1, E_2] \rightarrow \mathbb{C}[X, Y]$  is given by  $E_1 \mapsto X + Y$ ,  $E_2 \mapsto XY$ ; (a) implies that  $Im \pi^* \subset \mathbb{C}[X, Y]^{S_2}$  and (b) implies  $\pi^*$  is injective.

We now prove:

**Proposition 2.1.**  *$Im \pi^* = \mathbb{C}[X, Y]^{S_2}$ . Thus (taking into account the injectivity statement above) every symmetric polynomial in two variables is a (unique) polynomial in the elementary symmetric polynomials.*

*Proof.* Let  $P = \sum a_{i,j} X^i Y^j$ ; then  $\rho_{\sigma} P = \sum a_{i,j} X^j Y^i$ , so that  $P$  is symmetric iff the coefficients satisfy  $a_{i,j} = a_{j,i}$ . In this case we can write  $P = \sum_{i>j} a_{i,j} (X^i Y^j + X^j Y^i) + \sum_i a_{i,i} (XY)^i = \sum_{i>j} a_{i,j} (XY)^j (X^{i-j} + Y^{i-j}) + \sum_i a_{i,i} (XY)^i$ , and it clearly suffices to prove: for every positive integer  $a$ ,  $X^a + Y^a$  is a polynomial in  $X + Y$  and  $XY$ . This is clearly true if  $a = 1$ , else note that  $X^a + Y^a - (X + Y)^a$  is a sum of terms of the form *coefficient*  $\times (XY)^c (X^b + Y^b)$ , with  $a > b > 0$ , and use induction.  $\square$

**Example 2:** Consider the map  $\pi : \mathbb{C}^2 \rightarrow \mathbb{C}$ , defined by  $(x, y) \mapsto t = xy$ . Check that (a)  $\pi$  satisfies  $\pi((x, y) \cdot \lambda) = \pi(x, y)$  and (b)  $\pi$  is surjective. Note that  $\pi^* : \mathbb{C}[T] \rightarrow \mathbb{C}[X, Y]$  is given by  $T \mapsto XY$ , and that (a) implies

that  $\text{Im } \pi^* \subset \mathbb{C}[X, Y]^{\mathbb{C}^*}$  and (b) implies  $\pi^*$  is injective. Check that in fact  $\text{Im } \pi^* = \mathbb{C}[X, Y]^{\mathbb{C}^*}$ .

**Example 3:** Consider the map  $\pi : \mathbb{C}^3 \rightarrow \mathbb{C}^3$ , defined by  $(x, y, z) \mapsto (u = x^2z, v = y^2z, w = xyz)$ . In this case,  $\pi$  is not surjective since the coordinates  $(u, v, w)$  of the image of  $(x, y, z)$  clearly satisfy  $uv = w^2$ . Let  $\mathcal{V} \subset \mathbb{C}^3$  be the closed subset defined by

$$\mathcal{V} = \{(u, v, w) \mid uv = w^2\}$$

This is an example of an *affine algebraic variety* - a subset of  $\mathbb{C}^n$  (for some  $n$ ) defined by algebraic equations. We will denote by  $\mathbb{C}[\mathcal{V}]$  the algebra of algebraic functions on  $\mathcal{V}$ . By definition, an algebraic function on  $\mathcal{V}$  is the restriction of a polynomial function on  $\mathbb{C}^3$ . More formally,  $\mathbb{C}[\mathcal{V}] = \mathbb{C}[U, V, W]/I_{\mathcal{V}}$ , where  $I_{\mathcal{V}}$  is the ideal of polynomials vanishing on  $\mathcal{V}$ . (In fact, it is a fact that  $I_{\mathcal{V}}$  is generated by  $UV - W^2$ .) See §4 for a summary of some elementary commutative algebra and algebraic geometry.

Let  $\iota$  denote the inclusion map  $\iota : \mathcal{V} \hookrightarrow \mathbb{C}^3$  and  $\pi_{\mathcal{V}}$  the map  $\pi$ , considered as a map to  $\mathcal{V}$ ; thus  $\pi = \iota \circ \pi_{\mathcal{V}}$ . Check that (a)  $\pi$  satisfies  $\pi((x, y, z) \cdot \lambda) = \pi(x, y, z)$  and (b)  $\pi_{\mathcal{V}} : \mathbb{C}^3 \rightarrow \mathcal{V}$  is surjective. Note that  $\pi^* : \mathbb{C}[U, V, W] \rightarrow \mathbb{C}[X, Y, Z]$  is given by  $U \mapsto X^2Z, V \mapsto Y^2Z, W \mapsto XYZ$ , (a) implies that  $\text{Im } \pi^* \subset \mathbb{C}[X, Y, Z]^{\mathbb{C}^*}$  and (b) implies that  $\pi_{\mathcal{V}}^*$  is injective. We claim that  $\text{Im } \pi_{\mathcal{V}}^* = \mathbb{C}[X, Y, Z]^{\mathbb{C}^*}$ . Thus we have, yet again, an explicit description of the algebra of invariant functions:  $\pi_{\mathcal{V}}^*$  gives an isomorphism  $\mathbb{C}[U, V, W]/(UV - W^2) = \mathbb{C}[X, Y, Z]^{\mathbb{C}^*}$ .

We prove the claim above. What remains to show is that every invariant polynomial can be written in terms of  $X^2Z, Y^2Z$  and  $XYZ$ . Let  $P = \sum a_{i,j,k} X^i Y^j Z^k$ ; then  $\rho_{\lambda}(P) = \sum a_{i,j,k} \lambda^{i+j-2k} X^i Y^j Z^k$ , so that  $P$  is invariant iff  $a_{i,j,k} = 0$  whenever  $i + j - 2k \neq 0$ . Thus it suffices to show that every monomial  $X^i Y^j Z^k$ , with  $i + j - 2k = 0$  belongs to the image of  $\pi^*$ . To see this, suppose  $i \geq j$  (else reverse the roles of  $i$  and  $j$  in the following argument). Then  $X^i Y^j Z^k = (XYZ)^j X^{i-j} Z^{k-j} = (XYZ)^j (X^2Z)^{k-j}$  where we have used the fact that  $i - j = 2(k - j) > 0$ . Thus  $X^i Y^j Z^k = \pi^*(W^j U^{k-j})$ .

### 3. (LINEAR) REPRESENTATIONS; REYNOLDS OPERATOR

Let  $G$  be a group, and  $W$  a vector space. A *representation* of  $G$  on  $W$  is a homomorphism  $\rho : G \rightarrow GL(W)$ , where  $GL(W)$  is the group of invertible linear transformations of  $W$ . We will use the notation  $\rho_g$  to denote the image by  $\rho$  of the element  $g \in G$ . Thus, for every  $g \in G$ , we are given a linear map  $\rho_g : W \rightarrow W$ , satisfying  $\rho_{g_1} \rho_{g_2} = \rho_{g_1 g_2}$ . Equivalently, The map  $G \times W \rightarrow W, (g, w) \mapsto \rho_g(w)$  defines a left action of  $G$  on  $W$  by linear maps.

Given a representation as above, one may ask if a nontrivial subspace  $W'$  exists which is invariant under the action, that is, such that if  $w' \in W'$  then  $\rho_g(w') \in W' \forall g \in G$ . By nontrivial one means  $W' \neq W$  and  $W' \neq \{0\}$ . If such a  $W'$  exists, we say that the representation is *reducible*. Suppose this

is the case, and  $W'$  is a nontrivial invariant subspace. One may further ask if  $W'$  possesses an “invariant supplement”  $W''$ . This means that

- (1)  $W = W' \oplus W''$  - in other words every vector  $w$  in  $W$  can be written uniquely as a sum  $w = w' + w''$ , with  $w' \in W'$  and  $w'' \in W''$ . (This is what is meant by saying that  $W''$  is a “supplement”.)
- (2)  $W''$  is invariant.

If such  $W', W''$  exist we say that the representation is *decomposable*. Clearly a decomposable representation is reducible, but the converse need not be true.

**Exercise:** Let  $\mathbb{R}$  be the additive group of real numbers, and consider the map  $\mathbb{R} \rightarrow GL_2(\mathbb{R})$ :

$$\mathbb{R} \ni a \mapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R})$$

Check that this gives a representation of  $\mathbb{R}$  on the vector space  $\mathbb{R}^2$  (which we think of as  $2 \times 1$  column vectors). Check that the subspace

$$\left\{ \begin{pmatrix} \lambda \\ 0 \end{pmatrix} \mid \lambda \in \mathbb{R} \right\}$$

is invariant, but admits no invariant supplement.

One last bit of terminology: if a representation is not reducible we say that it is *irreducible*, and if it is not decomposable, we call it *indecomposable*. Clearly an irreducible representation is indecomposable. The above example is not irreducible, but with a little more work you can prove that it is indecomposable.

Let a representation  $\rho : G \rightarrow GL(W)$  be given. Consider the subspace  $W^G = \{w \in W \mid \rho_g(w) = w\}$ . Clearly  $W^G$  is invariant. The following construction shows that  $W^G$  admits an invariant supplement when  $G$  is finite. Let  $|G|$  denote the cardinality of  $G$ .

**Proposition 3.1.** *Let  $\mathcal{R} = \frac{1}{|G|} \sum_{g \in G} \rho_g$ . This is a linear map  $W \rightarrow W$ , called the Reynolds operator. We have*

- (1)  $\mathcal{R} \circ \rho_g = \rho_g \circ \mathcal{R} \quad \forall g \in G$ .
- (2)  $\mathcal{R}(w) = w$  if  $w \in W^G$ .
- (3)  $\text{Im } \mathcal{R} = W^G$ .
- (4)  $\mathcal{R}^2 = \mathcal{R}$ .

*Proof.* We will write  $\mathcal{R} \circ \rho_g = \mathcal{R}\rho_g$  etc., omitting the ‘ $\circ$ ’. We have

$$\begin{aligned}
 \rho_g \mathcal{R} &= \rho_g \left[ \frac{1}{|G|} \sum_{g' \in G} \rho'_g \right] \rho_{g^{-1}} \rho_g \\
 &= \left[ \frac{1}{|G|} \sum_{g' \in G} \rho_g \rho'_g \rho_{g^{-1}} \right] \rho_g \\
 &= \left[ \frac{1}{|G|} \sum_{g' \in G} \rho_{gg'g^{-1}} \right] \rho_g \\
 &= \mathcal{R} \rho_g
 \end{aligned}
 \tag{4}$$

where we use the fact that (with  $g$  fixed)  $g' \mapsto gg'g^{-1}$  is a bijection  $G \rightarrow G$ . This proves (1). It is easy to check (2). To prove (3) note that (2) implies  $W^G \subset \text{Im } \mathcal{R}$ . Consider now an arbitrary vector  $\mathcal{R}(w)$  in  $\text{Im } \mathcal{R}$ . We have

$$\begin{aligned}
 \rho_g \mathcal{R}(w) &= \rho_g \left[ \frac{1}{|G|} \sum_{g' \in G} \rho'_g \right] (w) \\
 &= \left[ \frac{1}{|G|} \sum_{g' \in G} \rho_g \rho'_g \right] (w) \\
 &= \left[ \frac{1}{|G|} \sum_{g' \in G} \rho_{gg'} \right] (w) \\
 &= \mathcal{R}(w)
 \end{aligned}
 \tag{5}$$

where we use the fact that (with  $g$  fixed)  $g' \mapsto gg'$  is a bijection  $G \rightarrow G$ . This proves that  $\text{Im } \mathcal{R} \subset W^G$ . We leave (4) as an exercise.  $\square$

**Corollary 3.2.** *The kernel of the Reynolds operator,  $\text{Ker } \mathcal{R}$ , is a  $G$ -invariant supplement to  $W^G$ .*

*Proof.* Since  $\mathcal{R}^2 = \mathcal{R}$  – a linear map  $\mathcal{R}$  satisfying this equation is called a *projector* – we see that  $W = \text{Kernel } \mathcal{R} \oplus \text{Im } \mathcal{R}$ . That  $\text{Ker } \mathcal{R}$  is  $G$ -invariant follows from (1) above. On the other hand,  $\text{Im } \mathcal{R} = W^G$ .  $\square$

**Exercise** Show that  $W^G$  has a unique invariant supplement. (Warning: there exist representations of a group  $G$  on a vector space  $W$ , with  $W^G$  admitting *more than one supplement*. In the present case you will have to use the fact that  $G$  is finite.)

Suppose the representation of  $G$  is on a space of functions, and arises as in §1. In that case  $W$  is a  $\mathbb{C}$ -algebra  $\mathbb{F}(E)$ , and the following is true; the proof follows from the definitions.

**Proposition 3.3.** *Let  $f_1 \in \mathbb{F}(E)$  and  $f_2 \in \mathbb{F}(E)^G$ . Then*

$$\mathcal{R}(f_1 f_2) = \mathcal{R}(f_1) f_2$$

4. PRELIMINARIES FROM COMMUTATIVE ALGEBRA: HILBERT BASIS  
THEOREM

We recall some elementary commutative algebra. Let  $A$  be a commutative ring with unit. Given a subset  $S$ , the intersection of all ideals containing  $S$  is an ideal, denoted by  $\langle S \rangle$ , and called the *ideal generated by  $S$* . Check that

$$\langle S \rangle = \{ \text{finite sums } \sum a_i s_i \mid a_i \in A, s_i \in S \}$$

An ideal is said to be *finitely generated* if it contains a finite generating subset. The ring  $A$  is called *Noetherian* if every ideal is finitely generated.

**Theorem 4.1.** (*Hilbert*) *If  $A$  is Noetherian, so is the polynomial ring  $A[X]$ .*

Here we mean by  $A[X]$ , the ring of polynomials in the indeterminate  $X$ , with coefficients which belong to the ring  $A$ . For a proof, see any book on commutative algebra, for example, Atiyah-Macdonald or Eisenbud.

**Corollary 4.2.** *Let  $k$  be a field. The polynomial ring  $k[X_1, \dots, X_n]$  is Noetherian.*

Quotients of Noetherian rings are Noetherian. Thus, if  $\mathcal{V} \subset \mathbb{C}^n$  is an affine variety,  $\mathbb{C}[\mathcal{V}]$  is Noetherian since it is the quotient  $\mathbb{C}[X_1, \dots, X_n]/I_{\mathcal{V}}$ .

**Remark** Let  $A$  be a Noetherian ring and  $S$  any set of elements. We know that  $\langle S \rangle$  is finitely generated, but we can say more: *There exists a finite subset  $S' \subset S$  which generates  $\langle S \rangle$ .* To see this, let  $\{s'_i = \sum a_{i,j} s_j\} \in \langle S \rangle$  be a (finite) generating set, and take for  $S'$  the set of all elements  $s_j$  of  $S$  who appear in the above sums.

Finally, we quickly review the relation between complex affine varieties and finitely generated  $\mathbb{C}$ -algebras. An affine variety is a subset  $\mathcal{V} \subset \mathbb{C}^n$  (for some  $n$ ), defined as the set of (simultaneous) zeroes of a family of polynomials. An *algebraic function on  $\mathcal{V}$*  is the restriction of a polynomial function from  $\mathbb{C}^n$ . Let  $\mathbb{C}[\mathcal{V}]$  denote the algebra of algebraic functions - thus  $\mathbb{C}[\mathbb{C}^n] = \mathbb{C}[X_1, \dots, X_n]$ . By definition, the restriction map  $\mathbb{C}[X_1, \dots, X_n] \rightarrow \mathbb{C}[\mathcal{V}]$  is surjective, and the kernel is the ideal  $I_{\mathcal{V}}$  of polynomials vanishing on  $\mathcal{V}$ , so that we have the isomorphism  $\mathbb{C}[X_1, \dots, X_n]/I_{\mathcal{V}} \sim \mathbb{C}[\mathcal{V}]$ . Clearly, the algebra  $\mathbb{C}[\mathcal{V}]$  is generated by  $\bar{X}_i$  (the restriction to  $\mathcal{V}$  of the co-ordinate functions), so it is a *finitely generated algebra*.

Conversely, suppose that an algebra  $A$  is given, and it is finitely-generated by elements  $\bar{X}_i$ . By definition, this means that the map

$$\mathbb{C}[X_1, \dots, X_n] \rightarrow A$$

which sends  $X_i$  to  $\bar{X}_i$ , is surjective. Let  $I$  denote the kernel, and let  $\mathcal{V}$  be the subset of  $\mathbb{C}^n$  where the polynomials in  $I$  all vanish. Since  $A$  is a  $\mathbb{C}$ -algebra, and in particular has a unit,  $I \subsetneq \mathbb{C}[X_1, \dots, X_n]$ , and the (Hilbert) Nullstellensatz assures us that  $\mathcal{V}$  is nonempty. Then it is natural to ask if  $I = I_{\mathcal{V}}$  and  $A$  can be interpreted as  $\mathbb{C}[\mathcal{V}]$ . This is almost true, under one condition - if  $f \notin I$ , then  $f^m \notin I$  for any integer  $m > 1$ . (This is clearly a

necessary condition for the equality  $I = I_{\mathcal{V}}$ .) Translated into a condition on  $A$  this becomes if  $\bar{f} \in A$  and  $\bar{f} \neq 0$ , then  $\bar{f}^m \neq 0$  for any integer  $m > 1$ . An ideal  $I$  satisfying the above condition is called *radical*, and the condition on  $A$  is that it is *reduced*.

Summarising: affine varieties correspond to reduced, finitely generated algebras.

## 5. FINITE GENERATION OF INVARIANTS

**Theorem 5.1.** (*Hilbert*) *Let  $G$  be a finite group acting on  $\mathbb{C}^n$  by linear transformations. The subalgebra  $\mathbb{C}[X_1, \dots, X_n]^G$  is finitely generated.*

**Remark** (Quibble! quibble!) We assume that the group acts on  $\mathbb{C}^n$  on the *right* to keep faith with our convention that actions on spaces are on the right so that the induced (linear) action on functions is on the left.

*Proof.* To keep the notation simple, let us denote by  $A$  the algebra  $\mathbb{C}[X_1, \dots, X_n]$ . Let  $A_d$  denote the space of homogeneous polynomials of degree  $d$  (Recall that a homogeneous polynomial of degree  $d$  is one which is a sum of monomials, each of degree  $d$ .) Thus  $A = \sum_{d \geq 0} A_d$ ,  $A_0 = \mathbb{C}$ , and  $A_d A_{d'} \subset A_{d+d'}$  (where this last equality simply says that the product of a homogeneous polynomial of degree  $d$  and one of degree  $d'$  produces a third homogeneous polynomial of degree  $d + d'$ .)

Recall the definition of the induced action on  $A$ :

$$\rho_g(P)[x] = P(x \cdot g)$$

*Since the action of  $G$  is linear, this action preserves degrees, and takes each  $A_d$  to itself and  $A^G = \sum_{d \geq 0} A_d^G$ . Check this!*

Consider the invariant subalgebra  $A^G$ , and let  $J \equiv \sum_{d > 0} A_d^G$ . This is a (maximal) ideal of  $A^G$ , and if we knew that  $A^G$  is a finitely generated algebra,  $J$  would be a finitely generated ideal. The main step in the proof is to show directly that this is indeed the case. To see this consider the ideal  $I$  generated by  $J$  in  $A$  (Note that  $J$  is *not* an ideal in  $A$ !). Since  $A$  is Noetherian  $I$  is finitely generated as a  $A$ -ideal. Thus, by our Remark following Corollary 4.2, there exist homogeneous invariant elements  $b_1, \dots, b_N \in J$  such that any element  $b$  of  $I$  can be written

$$b = \sum_{k=1, \dots, N} a_k b_k$$

where  $a_k \in A$ . Applying the Reynolds operator and using Proposition 3.3 (or rather its analogue in the case of polynomial maps and polynomial functions), we get

$$b = \sum_{k=1, \dots, N} \mathcal{R}(a_k) b_k$$

This shows that  $J$  is generated as an  $A^G$ -ideal by the  $b_k$ .

Now it is easy to show that  $A^G$  is generated as a  $\mathbb{C}$ -algebra by the  $b_k$  - consider the subalgebra generated by these elements and, show inductively, that it contains each  $A_d^G$ .  $\square$

**Remark** In fact this result is true in much greater generality. First, the action of  $G$  need not be linear, *algebraic actions* are enough. In fact,  $\mathbb{C}^n$  can be replaced by an affine variety. The group  $G$  need not be finite, the theorem holds true provided  $G$  is reductive. (In particular, this includes  $\mathbb{C}^*$ ). The base field need not be  $\mathbb{C}$ , it can be any algebraically closed field, even of positive characteristic.

### 6. EXAMPLE 4: SYMMETRIC FUNCTIONS

We consider a final example, which is central to the subject of this school. Consider the right action of the symmetric group  $S_n$  on  $\mathbb{C}^n$ :

$$(x_i) \cdot \sigma = (x_{\sigma(i)})$$

Here  $S_n$  is regarded as the group of bijective maps  $\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ . As usual, this induces a left action on the algebra  $\mathbb{C}[X_1, \dots, X_n]$ . Polynomials invariant under this action are called *symmetric*. We are interested in the algebra  $\mathbb{C}[X_1, \dots, X_n]^{S_n}$  of symmetric polynomials.

Among these are the so-called *elementary symmetric polynomials*, defined as follows:

$$\begin{aligned} E_1 &= X_1 + X_2 + \dots + X_n \\ E_2 &= \sum_{1 \leq i < j \leq n} X^i X^j \\ \dots &= \dots \\ E_n &= X_1 X_2 \dots X_n \end{aligned} \tag{6}$$

Consider the map  $\pi : \mathbb{C}^n \rightarrow \mathbb{C}^n$ , given by  $(x_i) \mapsto e_j$ , where

$$e_j = E_j(x_1, \dots, x_n) \quad j = 1, \dots, n$$

Clearly  $\pi$  satisfies  $\pi((x_i) \cdot \sigma) = \pi(x_i)$ .

We now check that  $\pi$  is surjective. To see this, first define the functions  $\hat{E}_j$ ,  $j = 1, \dots, n - 1$  of variables  $x_1, \dots, x_{n-1}$  by:

$$\hat{E}_j = E_j(x_1, \dots, x_{n-1}, 0)$$

The functions  $E_j$  satisfy

$$\begin{aligned} E_1(x_1, \dots, x_n) &= \hat{E}_1(x_1, \dots, x_{n-1}) + x_n \\ E_2(x_1, \dots, x_n) &= \hat{E}_2(x_1, \dots, x_{n-1}) + \hat{E}_1(x_1, \dots, x_{n-1})x_n \\ \dots &= \dots \\ E_n(x_1, \dots, x_n) &= \hat{E}_n(x_1, \dots, x_{n-1})x_n \end{aligned} \tag{7}$$

To prove surjectivity, we will do an induction on  $n$ . We need (given  $e_j$ ) to first solve for  $x_n$  :

$$\begin{aligned}
 (8) \quad x_n^n &= e_1 x^{n-1} - \hat{E}_1(x_1, \dots, x_{n-1}) x^{n-1} \\
 &= e_1 x^{n-1} + e_2 x^{n-2} - \hat{E}_1(x_1, \dots, x_{n-1}) x^{n-2} \\
 &= \dots\dots\dots \\
 &= e_1 x^{n-1} + e_2 x^{n-2} + e_n
 \end{aligned}$$

Once a root  $x_n$  is chosen, we have to solve for  $x_1, \dots, x_{n-1}$  the equations

$$\begin{aligned}
 (9) \quad E_1(x_1, \dots, x_n) &= \hat{E}_1(x_1, \dots, x_{n-1}) + x_n \\
 E_2(x_1, \dots, x_n) &= \hat{E}_2(x_1, \dots, x_{n-1}) + \hat{E}_1(x_1, \dots, x_{n-1}) x_n \\
 \dots\dots\dots &= \dots\dots\dots \\
 E_n(x_1, \dots, x_n) &= \hat{E}_{n-1}(x_1, \dots, x_{n-1}) x_n
 \end{aligned}$$

That this can be done is an easy consequence of our inductive assumption.

As a consequence of the above, we get an injection  $\pi^* : \mathbb{C}[E_1, \dots, E_n] \rightarrow \mathbb{C}[X_1, \dots, X_n]^{S_n}$ .

*We will now show that  $\pi^*$  is surjective.* Let  $P$  be a symmetric polynomial of degree  $N$  in  $n$  variables. Our proof will be by induction on  $N$  and  $n$ . Set  $\hat{P}$  be the polynomial in  $n - 1$  variables:

$$\hat{P}(X_1, \dots, X_{n-1}) = P(X_1, \dots, X_{n-1}, 0)$$

The polynomial  $\hat{P}$  is clearly symmetric, and under our inductive hypothesis, can be written in terms of the elementary symmetric polynomials  $\hat{E}_i, i = 1, \dots, n - 1$  in the  $n - 1$  variables  $X_1, \dots, X_{n-1}$ :

$$\hat{P}(X_1, \dots, X_{n-1}) = \sum_{\alpha} \hat{E}^{\alpha}$$

Let  $\hat{P}'$  be the polynomial in  $n$  variables defined by

$$\hat{P}'(X_1, \dots, X_n) = \sum_{\alpha} E^{\alpha}$$

Clear  $\hat{P}'$  is symmetric, and also  $P_1 \equiv P - \hat{P}'$  vanishes on the hyperplane  $x_n = 0$ . Thus  $P_1$  is divisible by  $X_n$ , and by symmetry by all the  $X_i, i = 1, \dots, n$ . Since  $\mathbb{C}[X_1, \dots, X_n]$  is a UFD,  $P_1$  is divisible by the product  $E_n = X_1 X_2 \dots X_n$ , so we can write

$$P = \sum_{\alpha} E^{\alpha} + E_n P_2$$

Now  $P_2$  is a symmetric polynomial of degree  $N - n$ , so induction in  $N$  will do the trick.

In conclusion, we have proved:

**Proposition 6.1.** *The algebra of symmetric polynomials is isomorphic to the polynomial algebra  $\mathbb{C}[E_1, \dots, E_n]$ .*

In particular, the space of symmetric polynomials has as a basis the monomials  $E^\alpha$ , where  $\alpha$  runs over multi-indices  $(\alpha_1, \dots, \alpha_n)$ .

RAMADAS T. RAMAKRISHNAN, MATHEMATICS SECTION, ABDUS SALAM ICTP, TRIESTE 34014, ITALY

*E-mail address:* ramadas@ictp.trieste.it