Chapter 1

Finite Generation of Invariants

1.1 The basic object of study

Let G be a finite group, K a field of coefficients and V a finite dimensional K-vector space on which G acts by linear substitutions (or equivalently a finitely generated KG-module). We write $K[V]$ for the ring of polynomial functions on V. In other words, if V has dimension n as a vector space, and $x_1, \ldots, x_n$ is a basis for the dual space $V^* = \mathrm{Hom}_K(V, K)$, then

$$K[V] = K[x_1, \ldots, x_n] = K \oplus V^* \oplus S^2(V^*) \oplus S^3(V^*) \oplus \cdots$$

Here, $S^m(V^*)$ denotes the symmetric mth power of V^*, which consists of the homogeneous polynomials of degree m in $x_1, \ldots, x_n$. Thus for example $S^2(V^*)$ has a basis consisting of the monomials $x_i x_j$ for the $\binom{n+1}{2}$ choices of i and j. In general, the dimension of $S^m(V^*)$ as a vector space is $\binom{n+m-1}{m} = \binom{n+m-1}{n-1}$. We regard $K[V]$ as a graded ring by putting each x_i in degree one. (If you are a topologist, then you may wish to double all the degrees.) The group G acts on $K[V]$ via $(gf)(v) = f(g^{-1}v)$, and the basic object of study of invariant theory is the set of all fixed points of this action, the **ring of invariants** $K[V]^G$.

Warning If K is a finite field F_q, then we should not really regard $K[V]$ as a ring of functions on V, since for example x_i and x_i^q take the same value at all points of V. Rather, we regard $K[V]$ as a ring of functions on $\bar{K} \otimes_K V$ fixed by the Galois automorphisms $\mathrm{Gal}(\bar{K}/K)$, where $\bar{K}$ is an algebraic closure of K.

If $\chi : G \to K^\times$ is a 1–dimensional representation of G, the module of χ–relative invariants, denoted by $K[V]^G_\chi$ is defined by

$$K[V]^G_\chi = \{f \in K[V] \mid g(f) = \chi(g)f \forall g \in G\}.$$

More generally, if S is a simple KG-module, we set

$$K[V]_S^G = S \otimes_{\mathrm{End}_{KG}(S)} \mathrm{Hom}_{KG}(S, K[V])$$

(note that if K is algebraically closed then $\mathrm{End}_{KG}(S) = K$). The evaluation map

$$S \otimes_{\mathrm{End}_{KG}(S)} \mathrm{Hom}_{KG}(S, K[V]) \to K[V]$$

is injective, and identifies $K[V]_S^G$ with the largest subspace of $K[V]$ consisting of a direct sum of copies of S. Multiplication in $K[V]$ gives a map

$$K[V]^G \times K[V]_S^G \to K[V]_S^G$$

making $K[V]_S^G$ into a $K[V]^G$-module.

At a coarser level, we could look at the action of G on the field of fractions $K(V)$ of $K[V]$. This may be regarded as the field of rational functions on V. The action of G is given by $g(f_1/f_2) = g(f_1)/g(f_2)$.

Recall that if we are given an extension of commutative rings $B \supseteq A$, we say that an element of B is **integral** over A if it satisfies a monic polynomial (i.e., a polynomial whose leading coefficient is one) with coefficients in A. This is the same as saying that the element lies in a subring of B which contains A and is finitely generated as an A-module. So the sum and product of integral elements is again integral. We say that B is an integral extension of A if every element of B is integral over A. If B is an integral extension of A and finitely generated over A as a ring, then it is finitely generated over A as a module. In this case, we say that B is a **finite** extension of A. Finally, we say an integral domain A is **integrally closed** if every element of the field of fractions of A which is integral over A is in A. For example, a unique factorization domain is always integrally closed.

Proposition 1.1.1 *Suppose that V is a finite dimensional faithful representation of a finite group G over a field K. Then $K(V)$ is a Galois (i.e., normal and separable) extension of $K(V)^G$ with Galois group G. The field $K(V)^G$ is the field of fractions of $K[V]^G$, and $K[V]^G$ is integrally closed in $K(V)^G$.*

Proof Since G acts as field automorphisms on $K(V)$, it is clear that $K(V)$ is a Galois extension of $K(V)^G$ with Galois group G.

Every element of $K(V)$ may be written in the form f_1/f_2 with f_2 G-invariant, just by multiplying the top and bottom by the distinct images of f_2. It follows from this that $K(V)^G$ is the field of fractions of $K[V]^G$.

Any element $f \in K(V)^G$ which is integral over $K[V]^G$ is also integral over $K[V]$. Since $K[V]$ is integrally closed in $K(V)$, this means that $f \in K[V]$. Since f is G-invariant, this means that $f \in K[V]^G$. □

The question of whether $K(V)^G$ is pure transcendental over K is a hard one in general. For a nilpotent group in coprime characteristic, the answer is affirmative, Morikawa [62]. The first examples where $K(V)^G$ is not pure transcendental with $K = \mathbf{Q}$ were produced by Swan [104], and with $K = \mathbf{C}$ by Saltman [85]. See also the survey article of Kervaire and Vust [54].

Example Let G be the symmetric group Σ_n, acting as permutations on a basis $v_1, \ldots, v_n$ of V. If $x_1, \ldots, x_n$ is the dual basis of V^*, then the elements of

$$K[V]^{\Sigma_n} = K[x_1, \ldots, x_n]^{\Sigma_n}$$

are called **symmetric functions**. The "fundamental theorem on symmetric functions" says that they form a polynomial ring in generators $e_i(x_1, \ldots, x_n)$ $(1 \leq i \leq n)$ called the **elementary symmetric functions** defined by

$$f(X) = \prod_{i=1}^{n}(X - x_i) = X^n + \sum_{i=1}^{n}(-1)^i e_i(x_1, \ldots, x_n)X^{n-i},$$

where X is an indeterminate. To prove that $K[V]^{\Sigma_n} = K[e_1, \ldots, e_n]$, we argue as follows. First of all, Σ_n acts as Galois automorphisms of $K(V)$ fixing $K(e_1, \ldots, e_n)$. Now $K(V)$ is the splitting field of f over $K(e_1, \ldots, e_n)$, and $df/dX \neq 0$, so the extension is Galois. Any Galois automorphism must permute the roots of $f(X)$, namely $x_1, \ldots, x_n$, and is determined by this permutation, and so Σ_n is precisely the Galois group, and $K(V)^{\Sigma_n} = K(e_1, \ldots, e_n)$. Now $K[V]$ is integral over $K[e_1, \ldots, e_n]$, and hence so is $K[V]^{\Sigma_n} = K(V)^{\Sigma_n} \cap K[V]$. Since $K[e_1, \ldots, e_n]$ is integrally closed, this completes the proof.

For a more direct proof, see Macdonald [56], §I.2.

1.2 Noetherian rings and modules

Let G be a finite group, K a field and V a finite dimensional KG-module. The fact that $K[V]^G$ is finitely generated as a K-algebra follows from the work of Hilbert in the case where $|G|$ is coprime to the characteristic of K, and was proved by Noether [78, 79] in the general case. We shall present three proofs, each with its advantages and disadvantages (Theorem 1.3.1, Corollary 1.5.3 and Theorem 1.6.3).

The first proof depends on a certain amount of commutative algebra, and we begin with some comments. Classically, one of the main motivations for the development of commutative algebra was to put algebraic geometry on a firm foundation. Two topics which provided impetus are intersection theory (various forms of Bézout's theorem and generalizations) and invariant theory, the topic of this book. In the course of this book, we shall need to make use of a considerable amount of commutative algebra, which we introduce as we need it. Good general references for commutative algebra are Matsumura [59] and Serre [90].

A module M over a commutative ring A is said to be Noetherian if every ascending chain of submodules is eventually constant. Clearly, every finite direct sum of Noetherian modules, as well as every submodule and quotient of a Noetherian module is again Noetherian. The ring A itself is said to be Noetherian if it is so as a module over itself; in other words, if every ascending chain of ideals is eventually constant.

Proposition 1.2.1 *A module M over a Noetherian ring A is Noetherian if and only if it is finitely generated.*

Proof If M is finitely generated, then it is a quotient of a finite direct sum of copies of A, and hence Noetherian. Conversely, if M is Noetherian, we choose a sequence of elements $x_1, x_2, \ldots$ in M with each x_i not in the submodule generated by $x_1, \ldots, x_{i-1}$. Since M is Noetherian, such a sequence must terminate, and so M is finitely generated. □

Corollary 1.2.2 *A submodule of a finitely generated module over a Noetherian ring is again finitely generated.* □

Lemma 1.2.3 *A commutative ring A is Noetherian if and only if every ideal is finitely generated.*

Proof If A is Noetherian then by the corollary, every ideal is finitely generated. Conversely, suppose that every ideal of A is finitely generated. Given an ascending chain of ideals of A, the union is an ideal in A, and hence finitely generated. But any finite subset of the union lies in one of the ideals, and so the chain is constant from that ideal onwards. □

Theorem 1.2.4 (Hilbert's basis theorem) *If A is a commutative Noetherian ring, then so is the polynomial ring $A[x]$.*

Proof By the lemma, it suffices to prove that if I is an ideal in $A[x]$ then I is finitely generated. Let I' be the ideal in A generated by the leading coefficients of the polynomials in I. Since A is Noetherian, I' is finitely generated, say by $a_1, \ldots, a_n$. Choose polynomials $f_1, \ldots, f_n \in I$ with these leading coefficients, let t be the maximum of the degrees of the f_i, and write I_0 for the ideal in $A[x]$ generated by $f_1, \ldots, f_n$. If f is any polynomial in I of degree at least t, then the leading coefficient of f is in I', so that we may subtract off an A-linear combination of products of f_i's with powers of x, in order to get rid of the leading coefficient and hence decrease the degree. Eventually the degree is less than t, and so we have

$$I = I_0 + (I \cap (A \oplus Ax \oplus \cdots \oplus Ax^{t-1})).$$

It follows that I is finitely generated. □

Corollary 1.2.5 *If A is a finitely generated commutative algebra over a field K, then A is Noetherian.*

Proof A is a quotient of some polynomial ring over K, which is Noetherian by the theorem. □

1.3 Finite groups in arbitrary characteristic

The first proof we present of the finite generation of the invariants is as follows.

Theorem 1.3.1 (Hilbert–Noether) *Suppose that K is a field, and G is a finite group acting as automorphisms of a finitely generated commutative K-algebra A (for example $A = K[V]$). Then A^G is also a finitely generated commutative K-algebra and A is finitely generated as a module over A^G.*

Proof If $a \in A$ then a satisfies the monic polynomial

$$\prod_{g \in G} (X - g(a)) \in A^G[X]$$

and so A is an integral extension of A^G. Let A' be the subalgebra of A^G generated by the coefficients of the monic polynomials satisfied by a finite set of K-algebra generators of A. Then A' is a finitely generated K-algebra, and hence Noetherian. A is a finitely generated A'-module, and hence so is A^G by Corollary 1.2.2. Thus A^G is a finitely generated K-algebra. □

Corollary 1.3.2 *Suppose that G is a finite group, K is a field and V is a finite dimensional KG-module. Then $K[V]^G$ is a finitely generated K-algebra. If S is a simple KG-module then $K[V]^G_S$ is a finitely generated $K[V]^G$-module.* □

1.4 Krull dimension and going up and down

Having seen that $K[V]$ is a finite extension of the finitely generated K-algebra $K[V]^G$, we can use this to describe the relationship between the prime ideals of $K[V]$ and $K[V]^G$.

We first discuss Krull dimension. The **Krull dimension** of a commutative ring A is the maximum length n of a chain of proper inclusions of prime ideals $\mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_n$, or ∞ if there are such chains of unbounded length. If M is an A-module, we define the Krull dimension of M to be the Krull dimension of the ring $A/\mathrm{Ann}_A(M)$, where $\mathrm{Ann}_A(M) = \{a \in A \mid \forall m \in M,\ am = 0\}$ is the **annihilator** in A of M.

We write $\dim(A)$ and $\dim(M)$, with no subscript, to denote the Krull dimension of A and M. Whenever we wish to denote the dimension of a vector space, we keep the field as a subscript, to avoid confusion.

Proposition 1.4.1 *The Krull dimension of $K[V]$ is equal to* $\dim_K(V)$.

Proof Suppose that $K[V] = K[x_1, \ldots, x_n]$. The chain of prime ideals

$$(x_1, \ldots, x_n) \supset (x_2, \ldots, x_n) \supset \cdots \supset (x_n) \supset 0$$

shows that the Krull dimension is at least n. To prove that it is at most n, it suffices to show that if $\mathfrak{p} \subset \mathfrak{p}'$ are prime ideals then the transcendence degree over K of (the field of fractions of) $K[V]/\mathfrak{p}'$ is strictly less than that of $K[V]/\mathfrak{p}$. If this is not the case, since $K[V]/\mathfrak{p}$ surjects onto $K[V]/\mathfrak{p}'$, then the transcendence degrees are equal. Reorder the x_j so that $x_1, \ldots, x_r$ form a transcendence base for $K[V]/\mathfrak{p}'$ and hence also for $K[V]/\mathfrak{p}$. Let $K' = K(x_1, \ldots, x_r)$, so that we may extend $\mathfrak{p}$ and $\mathfrak{p}'$ to ideals $\mathfrak{P} \subset \mathfrak{P}'$ in $K'[x_{r+1}, \ldots, x_n]$. Each of $x_{r+1}, \ldots, x_n$ is algebraic in $K'[x_{r+1}, \ldots, x_n]/\mathfrak{P}$, and so this is already a field, which contradicts the proper inclusion of $\mathfrak{P}$ in $\mathfrak{P}'$. □

We relate the prime ideals in $K[V]$ and $K[V]^G$ using Theorem 1.4.4. Before discussing this, we introduce localization, which is a way of turning prime ideal into maximal ideals.

If A is an integral domain, and $\mathfrak{p}$ is a prime ideal in A, we write $A_{\mathfrak{p}}$ for the subring of the field of fractions of A consisting of elements xy^{-1} with $x, y \in A$ and $y \notin \mathfrak{p}$. More generally, if A is a commutative ring, we write $A_{\mathfrak{p}}$ for the ring whose elements are expressions of the form x/y with $x, y \in A$ and $y \notin \mathfrak{p}$. We regard x/y and x'/y' as equal if for some $z \in A$, $z \notin \mathfrak{p}$ we have $z(xy' - x'y) = 0$.

If M is an A-module then $M_{\mathfrak{p}} = A_{\mathfrak{p}} \otimes_A M$ is an $A_{\mathfrak{p}}$-module. The kernel of the map $M \to M_{\mathfrak{p}}$ consists of the elements which are annihilated by some element of A not in $\mathfrak{p}$. A short exact sequence $0 \to M_1 \to M_2 \to M_3 \to 0$ of A-modules gives rise to a short exact sequence

$$0 \to (M_1)_{\mathfrak{p}} \to (M_2)_{\mathfrak{p}} \to (M_3)_{\mathfrak{p}} \to 0$$

of $A_{\mathfrak{p}}$-modules (i.e., $A_{\mathfrak{p}}$ is flat over A). To see this, it suffices to see that the first map is injective. This is clear, because whether an element of M_1 is annihilated by an element of A not in $\mathfrak{p}$ does not depend on whether we view it as an element of M_1 or M_2.

If I is an ideal in $A_{\mathfrak{p}}$ then $I \cap A$ is an ideal in A contained in $\mathfrak{p}$ (because if it contains an element outside $\mathfrak{p}$ then it contains the identity element). Conversely, if I' is an ideal in A contained in $\mathfrak{p}$ then $I'_{\mathfrak{p}}$ is an ideal in $A_{\mathfrak{p}}$. These processes set up a one–one correspondence between ideals in $A_{\mathfrak{p}}$ and ideals in A contained in $\mathfrak{p}$. In particular, $\mathfrak{p}_{\mathfrak{p}}$ is the unique maximal ideal of $A_{\mathfrak{p}}$. A commutative ring with a unique maximal ideal is called a **local ring**.

Lemma 1.4.2 *Suppose that $B \supseteq A$ is a finite extension of commutative rings. If $\mathfrak{P}$ is a maximal ideal of B then $\mathfrak{P} \cap A$ is a maximal ideal of A. Conversely if $\mathfrak{p}$ is a maximal ideal of A then there is a prime ideal $\mathfrak{P}$ of B with $\mathfrak{P} \cap A = \mathfrak{p}$, and any such prime ideal $\mathfrak{P}$ is maximal.*

Proof If $\mathfrak{P}$ is maximal in B then $B/\mathfrak{P}$ is a field. It is integral over $A/(\mathfrak{P}\cap A)$, so if $x \in A/(\mathfrak{P}\cap A)$ then $x^{-1} \in B/\mathfrak{P}$ satisfies some monic equation over $A/(\mathfrak{P}\cap A)$, say $x^{-n}+a_{n-1}x^{-n+1}+\cdots+a_0 = 0$. But then $x^{-1} = -a_{n-1}-\cdots-a_0x^{n-1} \in A/(\mathfrak{P}\cap A)$, so $A/(\mathfrak{P}\cap A)$ is a field and $\mathfrak{P}\cap A$ is maximal. Conversely, if $\mathfrak{P}\cap A$ is maximal then $B/\mathfrak{P}$ is an integral extension of the field $A/(\mathfrak{P}\cap A)$, and is hence a field, so that $\mathfrak{P}$ is maximal.

If $\mathfrak{p}$ is a maximal ideal in A, suppose that $\mathfrak{p}B = B$. If B is generated over A by $b_1,\ldots,b_n$ then we have $b_i = \sum_j x_{ij}b_j$ with $x_{ij} \in \mathfrak{p}$. But then $\det(I-(x_{ij})) \in A$ annihilates each b_i and hence annihilates $1 \in B$, so this determinant is zero. But it is congruent to 1 modulo $\mathfrak{p}$. This contradiction shows that $\mathfrak{p}B \neq B$, so $\mathfrak{p}B$ is contained in some maximal ideal of B, which therefore intersects A in $\mathfrak{p}$. □

Lemma 1.4.3 *If an ideal I is contained in a finite union of primes $I \subseteq \mathfrak{p}_1\cup\cdots\cup\mathfrak{p}_n$ then I is contained in some $\mathfrak{p}_i$.*

Proof Suppose n is minimal, so that I is not contained in the union of any proper subset of $\{\mathfrak{p}_1,\ldots,\mathfrak{p}_n\}$, and suppose that $n > 1$. Choose $y \in I$ with $y \notin \mathfrak{p}_1\cup\cdots\cup\mathfrak{p}_{n-1}$. Then $y \in \mathfrak{p}_n$. Choose $z \in I$ with $z \notin \mathfrak{p}_n$, and $t_i \in \mathfrak{p}_i$ with $t_i \notin \mathfrak{p}_n$ for each i between 1 and $n-1$. Then $y+zt_1\ldots t_{n-1}$ is in I but is not in $\mathfrak{p}_1\cup\cdots\cup\mathfrak{p}_n$. This contradiction proves the lemma. □

Remark In the above proof, we only used the fact that $\mathfrak{p}_n$ was prime, and even this is only necessary if $n > 2$. So in fact it suffices to assume that all except possibly two of the $\mathfrak{p}_i$ are prime.

Theorem 1.4.4 *Suppose that $B \supseteq A$ is a finite extension of commutative rings.*

(i) **(Lying over)** *If $\mathfrak{p}$ is a prime ideal of A then there is a prime ideal $\mathfrak{P}$ of B with $\mathfrak{P}\cap A = \mathfrak{p}$. There are no strict inclusions between such prime ideals $\mathfrak{P}$. In this situation we say that $\mathfrak{P}$* **lies over** *$\mathfrak{p}$.*

(ii) **(Going up)** *If $\mathfrak{p}' \supset \mathfrak{p}$ are prime ideals in A and $\mathfrak{P}$ is a prime ideal in B lying over $\mathfrak{p}$ then there is a prime ideal $\mathfrak{P}'$ in B lying over $\mathfrak{p}'$ with $\mathfrak{P}' \supset \mathfrak{P}$.*

(iii) **(Transitivity)** *Suppose that A and B are integrally closed domains, and that the corresponding extension $L' \supseteq L$ of fields of fractions is* **normal** *(i.e., an irreducible polynomial over L with a root in L' splits completely in L', but is not necessarily separable). The Galois group $G = \mathrm{Gal}(L'/L)$ acts transitively on the prime ideals $\mathfrak{P}$ of B lying over the given prime ideal $\mathfrak{p}$ of A.*

(iv) **(Going down)** *Suppose that A and B are integral domains, and A is integrally closed. If $\mathfrak{p} \subset \mathfrak{p}'$ are prime ideals in A and $\mathfrak{P}'$ is a prime ideal of B lying over $\mathfrak{p}'$ then there is a prime ideal $\mathfrak{P}$ in B lying over $\mathfrak{p}$, with $\mathfrak{P} \subset \mathfrak{P}'$.*

Proof (i) We form the localization $A_{\mathfrak{p}}$ of A at $\mathfrak{p}$ and set $B_{\mathfrak{p}} = A_{\mathfrak{p}} \otimes_A B$. Then $B_{\mathfrak{p}}$ is finite over $A_{\mathfrak{p}}$. The prime ideals $\mathfrak{P}$ in B with $\mathfrak{P}\cap A = \mathfrak{p}$ correspond to the prime

ideals $\mathfrak{P}_\mathfrak{p}$ in $B_\mathfrak{p}$ with $\mathfrak{P}_\mathfrak{p} \cap A_\mathfrak{p} = \mathfrak{p}_\mathfrak{p}$. So it is enough to consider the case where $\mathfrak{p}$ is maximal, and this was dealt with in Lemma 1.4.2.

(ii) To prove this, pass down to the quotient $B/\mathfrak{P} \supseteq A/\mathfrak{p}$ and use (i).

(iii) First we treat the case where $L' \supseteq L$ is separable, so that $L = (L')^G$ and $A = B^G$ (by integral closure). Suppose that $\mathfrak{P}$ and $\mathfrak{P}'$ are prime ideals in B lying over $\mathfrak{p}$, and suppose that $\mathfrak{P}$ and $\mathfrak{P}'$ are not G-conjugate. By part (i), no conjugate of $\mathfrak{P}$ contains $\mathfrak{P}'$. So by Lemma 1.4.3, we may choose an element $x \in \mathfrak{P}'$ such that for all $g \in G$, $x \notin g(\mathfrak{P})$. Then $\prod_{g \in G} g(x)$ is an element of $B^G = A$ lying in $\mathfrak{P}'$ but not in $\mathfrak{P}$, which contradicts the hypothesis that $\mathfrak{P}' \cap A = \mathfrak{P} \cap A = \mathfrak{p}$.

Next, we treat the case where $L' \supseteq L$ is purely inseparable. In this case, the only prime ideal of B lying over $\mathfrak{p}$ is $\{x \in B \mid x^{p^n} \in \mathfrak{p} \text{ for some } n \geq 0\}$, where p is the characteristic of L. Finally, every extension is a composition of a purely inseparable and a separable extension, so the statement is proved.

(iv) Let $L' \supseteq L$ be the fields of fractions of $B \supseteq A$, and let L'' be a finite normal extension of L containing L'. Let C be the integral closure of A in L'', so that C is a finite extension of B, and choose primes Ω and Ω' in C lying over $\mathfrak{p}$ in A and $\mathfrak{P}'$ in B respectively. By (ii), we can find $\Omega'' \supset \Omega$ with Ω'' lying over $\mathfrak{p}'$. By (iii), for some $g \in \mathrm{Gal}(L''/L)$ we have $g(\Omega'') = \Omega'$. Set $\mathfrak{P} = g(\Omega) \cap A$. Then $\mathfrak{P} \subset g(\Omega'') \cap B = \Omega' \cap B = \mathfrak{P}'$ and $\mathfrak{P}$ lies over $\mathfrak{p}$. □

Corollary 1.4.5 *If $B \supseteq A$ is a finite extension of commutative rings, then the Krull dimensions of A and B are equal.* □

Corollary 1.4.6 *Suppose that G is a finite group, K is a field and V is a finite dimensional KG-module. Then the Krull dimension of $K[V]^G$ is equal to* $\dim_K(V)$.

Proof Apply the previous corollary to the extension $K[V] \supseteq K[V]^G$, and use Proposition 1.4.1. □

Remark According to Hilbert's weak Nullstellensatz (see Matsumura [59], Theorem 5.3) if K is algebraically closed then the maximal ideals in $K[V]$ are in natural one–one correspondence with the points of V, $V \cong \max K[V]$. By part (i) of the theorem, the inclusion $i : K[V]^G \to K[V]$ gives rise to a *surjective* map

$$i^* : \max K[V] \to \max K[V]^G,$$

and by part (iii) of the theorem we have

$$\max (K[V]^G) \cong V/G.$$

1.5 Noether's bound in characteristic zero

Noether [78] proved that if K is a field of characteristic zero, then $K[V]^G$ is generated by elements of degree at most $|G|$. In particular, the number of generators needed is at most

$$\binom{\dim_K(V) + |G|}{|G|}.$$

In fact, this is a special case of a relative version, which says that if H is a subgroup of G and $K[V]^H$ is generated by elements of degree at most m, then $K[V]^G$ is generated by elements of degree at most $m.|G : H|$. The proof we give is a relativization, due to B. Schmid [88], of an argument of G. W. Schwarz and R. P. Stanley.

Before we begin, we introduce the transfer. If H is a subgroup of G and V is a finite dimensional KG-module, we define

$$\mathrm{Tr}_{H,G} : K[V]^H \to K[V]^G$$

by

$$\mathrm{Tr}_{H,G}(f)(x) = \sum_{g \in G/H} g(f)(x) = \sum_{g \in G/H} f(g^{-1}(x)).$$

The notation means that the sum runs over a set of left coset representatives of H in G. Note that the composite

$$K[V]^G \hookrightarrow K[V]^H \xrightarrow{\mathrm{Tr}_{H,G}} K[V]^G$$

is equal to multiplication by $|G : H|$. In particular, if $|G : H|$ is invertible in K then the transfer is surjective, and the map

$$\pi_{G,H} = \frac{1}{|G : H|}\mathrm{Tr}_{H,G} : K[V]^H \to K[V]^G \hookrightarrow K[V]^H$$

is an idempotent projection whose image is equal to $K[V]^G$. In particular, $K[V]^H$ is a direct sum of $K[V]^G$ and the kernel of $\pi_{G,H}$. If $H = 1$, we just write π_G for $\pi_{G,1} = \frac{1}{|G|}\sum_{g \in G} g$, so that $K[V] = K[V]^G \oplus \ker(\pi_G)$.

We shall also need the following combinatorial lemma.

Lemma 1.5.1 *In characteristic zero, every monomial $u_1 \dots u_j$ is a linear combination of jth powers of sums of subsets of $u_1, \dots, u_j$.*

Proof This follows from the formula

$$j!\, u_1 \dots u_j = \sum_{I \subseteq \{1,\dots,j\}} (-1)^I \left(\sum_{i \in I} u_i\right)^j.$$

In this formula, I runs over all subsets of $\{1, \dots, j\}$. □

Theorem 1.5.2 *Suppose that V is a finite dimensional representation of a finite group G over a field K of characteristic zero. If H is a subgroup of G and $K[V]^H$ is generated by elements of degree at most m, then $K[V]^G$ is generated by elements of degree at most $m.|G:H|$.*

Proof Let A be the subalgebra of $K[V]^G$ generated by elements of degree at most md, where $d = |G:H|$, and let M be the linear subspace of $K[V]^H$ spanned by elements of degree at most $md-1$. First, we claim that $K[V]^H = AM$. Elements of degree at most $md-1$ are clearly in AM. Every element of $K[V]^H$ is a linear combination of products of elements of degree at most m, so it suffices, by the lemma, to show that for u a linear combination of elements of $K[V]^H$ of degree at most m, all the powers u^j are in AM. For $j < d$, this is clear. Now u is a root of the equation

$$\prod_{g\in G/H}(X - g(u)) = X^d + a_{d-1}X^{d-1} + \cdots + a_0$$

(the product is over a set of coset representatives of H in G) with coefficients $a_i \in A$, and so $u^d = -a_{d-1}u^{d-1} - \cdots - a_0 \in AM$. Then we have $u^{d+1} = -a_{d-1}u^d - \cdots - a_0 u \in AM$, and continuing by induction, all u^j are in AM, which completes the proof that $K[V]^H = AM$.

Finally, we apply the projection $\pi_{G,H}$ described above, to obtain

$$K[V]^G = \pi_{G,H}(K[V]^H) = \pi_{G,H}(AM) = A\pi_{G,H}(M) = A.$$

□

Corollary 1.5.3 (Noether) *Suppose that V is a finite dimensional representation of a finite group G over a field K of characteristic zero. Then $K[V]^G$ is generated by elements of degree at most $|G|$.* □

1.6 Linearly reductive algebraic groups

The third proof of finite generation that we offer also has the disadvantage of not working in the modular case, but has the advantage that it generalizes to a suitable class of linear algebraic groups. We say that a subgroup of $GL_n(K)$ is a **linear algebraic group** if it is closed in the Zariski topology, i.e., it can be written as the set of zeros of a collection of polynomials in the n^2 variables. Note that $GL_n(K)$ is the Zariski open subset of $\mathrm{Mat}_n(K) \cong K^{n^2}$ given by the non-vanishing of the determinant. By adding an extra coordinate corresponding to the inverse of the determinant, one can consider $GL_n(K)$ as a closed subgroup of K^{n^2+1}. Examples of linear algebraic groups are given by $GL_n(K)$, $SL_n(K)$, $Sp_{2n}(K)$, the unitary group $U(n)$, the group of diagonal matrices T^n, the group of upper triangular matrices with ones on the diagonal $\mathrm{Uni}(n)$, any finite group, and so on.