Invariants of finite group schemes

Serge Skryabin

Chebotarev Research Institute, Kazan, Russia

Let $k$ be an algebraically closed field, $G$ a finite group scheme over $k$ operating on a scheme $X$ over $k$. Under assumption that $X$ can be covered by $G$-invariant affine open subsets the classical results in [3] and [14] describe the quotient $X/G$. In case of a free action $X$ is known to be a principal homogeneous $G$-space over $X/G$. Furthermore, the category of $G$-linearized quasi-coherent sheaves of $\mathcal{O}_X$-modules is equivalent then to the category of quasi-coherent sheaves of $\mathcal{O}_{X/G}$-modules.

In this paper we attempt to describe the situation when generic stabilizers of points on $X$ are nontrivial. To avoid technical complications we assume that $X$ is an algebraic variety, although the results can be extended to reduced schemes. The stabilizer $G_x$ of a rational point $x \in X$ is a subgroup scheme of $G$, and we define its index $(G : G_x)$ by analogy with the ordinary finite groups. A point $x$ is regular with respect to the action of $G$ if the index $(G : G_x)$ attains the maximal possible value $q(X)$. Theorem 2.1 shows that the set $X_{G-reg}$ of all regular points is an open $G$-invariant subset of $X$, the restriction to which of the canonical morphism $\pi : X \to X/G$ is finite flat of degree $q(X)$. For every $x \in X_{G-reg}$ the fibre $\pi^{-1}(x)$ is $G$-equivariantly isomorphic with the quotient $G_x \backslash G$ and there is a bijective correspondence between the $G$-invariant closed subschemes of $X_{G-reg}$ and the closed subschemes of $\pi(X_{G-reg})$. We prove also that the field of rational functions $k(X)$ has degree $q(X)$ over the subfield of $G$-invariants $k(X)^G$. The arguments used in [3] and [14] are essential ingredients in our approach too. At the same time, what we prove is not quite a generalization of the classical results as we need more restrictions on $X$.

If $X_{G-reg} = X$ then the equivalence between categories of sheaves mentioned at the beginning extends to our settings in only as much as we restrict to $G$-linearized quasi-coherent sheaves generated locally by $G$-invariant sections (Proposition 3.2). Suppose that $\mathcal{F}$ is an arbitrary $G$-linearized coherent sheaf of $\mathcal{O}_X$-modules. In Theorem 3.3 we describe an open $G$-invariant subset $U \subset X$ such that the sheaf of $\mathcal{O}_{X/G}$-modules $(\pi_*\mathcal{F})^G$ is locally free of rank $s$ over the open subset $\pi(U) \subset X/G$, where $s$ is equal to the minimum dimension of the subspaces of $G_x$-invariant elements $\mathcal{F}(x)^G$, in the finite dimensional $G_x$-modules $\mathcal{F}(x) = \mathcal{F}_x \otimes_{\mathcal{O}_x} k(x)$, $x \in U$ (here $\mathcal{F}_x$ denotes the stalk of $\mathcal{F}$ at $x$ and $k(x)$ the residue field of the local ring $\mathcal{O}_x$). In particular, $(\mathcal{F} \otimes_{\mathcal{O}_x} k(x))^G$ has dimension $s$ over $k(X)^G$. We use this result to describe the $G$-socle of the $G$-module $\mathcal{F} \otimes_{\mathcal{O}_x} k(X)$ in Corollary 3.4. Given a point $x \in X_{G-reg}$ such that $\mathcal{F}_x$ is a free $\mathcal{O}_x$-module, we show in Theorem 3.6 that $\mathcal{F}(x)$ is an injective $G_x$-module if and only if there exists a $G$-invariant affine open neighbourhood $U$ of $x$ such that $\mathcal{F}|_U$ is projective in the category of $G$-linearized sheaves of quasi-coherent $\mathcal{O}_U$-modules. Moreover, $\mathcal{F}(U)$ and $\mathcal{F} \otimes_{\mathcal{O}_x} k(X)$ are injective $G$-modules in this case. To simplify the statements of results we actually consider only affine varieties $X$ and speak about modules over the function algebra $k[X] = \mathcal{O}_X(X)$ rather than quasi-coherent sheaves. A $G$-linearization on a $k[X]$-module is just a $G$-module structure subject to a certain compatibility requirement.

Let us call a group scheme linearly reductive if all its representations are completely reducible. Theorem 4.2 says that a point $x \in X$ has a linearly reductive stabilizer $G_x$ if and only if $x$ is contained in a $G$-invariant affine open subset $U \subset X$.
such that $k[U]$ is an injective $G$-module. This turns out to be quite a general fact. Unlike results in previous sections $X$ can be here any scheme over $k$. When $X$ is a variety, the set of points with linearly reductive stabilizers is nonempty if and only if $k(X)$ is an injective $G$-module. Moreover, the structure of $k(X)$ as a $G$-module is completely determined in this case.

If $\text{char } k = 0$, any finite group scheme over $k$ is constant. Then for all $x$ in a nonempty open subset of $X$ the stabilizer $G_x$ coincides with the largest subgroup of $G$ acting trivially on the whole $X$. This is the reason why our results present an interest mainly for fields of characteristic $p > 0$. In particular, if $G = \mathfrak{S}(\mathfrak{g})$ is the group scheme of height one corresponding to a finite dimensional $p$-Lie algebra $\mathfrak{g}$ then the actions of $G$ on $X$ correspond to actions of $\mathfrak{g}$ by derivations of the structure sheaf $\mathcal{O}_X$. Probably A. Milner was the first who observed that the degree of $k(X)$ over the subfield of $\mathfrak{g}$-invariants $k(X)^g$ can be expressed in terms of Lie algebra stabilizers of points on $X$. He considered the special case of the adjoint representation of $\mathfrak{g}$ on its symmetric algebra $S(\mathfrak{g})$ and used the fact just mentioned to derive a lower bound for the maximum dimension of irreducible $\mathfrak{g}$-modules [12].

In fact we are able to generalize Theorem 2.1 to the actions of not necessarily finite dimensional $p$-Lie algebras (Theorem 5.2). Moreover, if $X$ is a smooth affine variety and $f_1, \ldots, f_n$ are $G$-invariant regular functions on $X$, taken in a suitable number, then $k[X]^g$ is generated by $f_1, \ldots, f_n$ over the subalgebra $k[X]^{(p)}$ of $p$-th powers in $k[X]$ provided that the differentials $d_x f_1, \ldots, d_x f_n$ are linearly independent at all points $x$ in an open subset of $X$ whose complement has codimension at least 2 (Theorem 5.4). In this case $k[X]^g$ is free over $k[X]^{(p)}$ and is a locally complete intersection ring. A similar result is valid for invariants of Frobenius kernels of reduced algebraic groups. This generalizes the work of Friedlander and Parshall [6], and Donkin [5] who considered, respectively, the adjoint and the conjugating actions of a semisimple algebraic group. We discuss yet another example of the adjoint action of the Jacobson-Witt algebra $W_n$. Other applications to invariants of Lie algebras of Cartan type will be a subject of separate papers.

I would like to thank the referee for making comments and correction in attributing the formula for the $p$-th powers of derivations in section 5.

1. Preliminaries.

Let $k$ be an algebraically closed field. It is the ground field for our considerations, so that the functors $\otimes$, $\text{Hom}$ etc. are assumed to be taken over $k$ unless the base ring is indicated explicitly. Let $G$ be a finite group scheme over $k$ and $k[G]$ the associated finite dimensional Hopf algebra. We will be considering a group action $\mu : X \times G \to X$ of $G$ on a scheme $X$ over $k$ from the right. By [3] a scheme can be regarded as a functor on the category of commutative $k$-algebras. For each commutative algebra $K$ the group $G(K)$ operates on $X(K)$, and this action is natural in $K$. If $X$ is affine with algebra $k[X]$ then the quotient $X/G$ is defined to be $\text{Spec } k[X]^G$ where $k[X]^G \subset k[X]$ is the subalgebra of $G$-invariants. More generally, if $X$ can be covered by $G$-invariant affine open subsets $U$, then $X/G$ is obtained by patching together the affine quotients $U/G$. We list below the properties of the canonical morphism $\pi : X \to X/G$ assuming $X$ to be of finite type (see [3], Ch. III, §2, 6.1 and [14], Ch. III, §12):

1. $\pi$ is finite and surjective,
2. the set-theoretic fibers of $\pi$ coincide with the orbits of the group $G(k)$,
3. $X/G$ has the quotient topology with respect to $\pi$; in particular, $\pi$ is open,

2
(4) if $U \subset X$ is a $G$-invariant open subscheme, then $U/G \cong \pi(U)$ and $U = \pi^{-1}(\pi(U))$.

According to [3], Ch. III, §2, 2.3 the action is said to be free if $G(K)$ operates freely on $X(K)$ for each commutative algebra $K$. In case of a free action $\pi$ is finite flat of degree $|G| = \dim k[G]$ (which means that $k[U]$ are free of rank $|G|$ over $k[U]$ for a suitable covering of $X$ by $G$-invariant affine open subsets) and the canonical morphism $\nu = (\pi_1, \mu) : X \times G \to X \times_{X/G} X$, where $\pi_1 : X \times G \to X$ denotes the projection, is an isomorphism.

If $G' \subset G$ is a subgroup scheme, we let $G' \backslash G$ denote the quotient with respect to the action of $G'$ on $G$ by left translations. Then $G' \backslash G$ is a finite scheme with the algebra $k[G' \backslash G] \cong k[G]^G$, the invariants with respect to the left regular representation of $G'$ on $k[G]$. Define the index of $G'$ in $G$ to be $(G : G') = \dim k[G' \backslash G]$. The algebra $k[G]$ is a free module of rank $|G|$ over $k[G' \backslash G]$. Hence $|G| = (G : G') \cdot |G'|$. The index can be interpreted in terms of dual Hopf algebras. By [16] or [15] $k[G]^*$ is free both as a left and a right module over its subalgebra $k[G']^*$. Clearly, the ranks of these modules are equal to $(G : G')$.

If $x \in X(k)$ then its stabilizer $G_x \subset G$ is a subgroup scheme such that $G_x(K) = \{g \in G(K) \mid x_K g = x_K\}$ for each commutative algebra $K$, where $x_K$ denotes the image of $x$ in $X(K)$. Let $i_x : \text{Spec} k \to X$ be the morphism corresponding to $x$ and

$$\mu_x : G \cong \text{Spec} k \times G \xrightarrow{i_x \times \text{id}_G} X \times G \xrightarrow{\mu} X.$$ 

the orbit morphism. Then $G_x$ coincides with the fiber of $\mu_x$ above $x$ and $\mu_x$ factors through a morphism $\rho : G_x \backslash G \to X$. By [3], Ch. III, §3, 5.2 $\rho$ is an immersion. In fact $\rho$ is a closed immersion because $G' \backslash G$ has only rational points. Since the case of finite group schemes is especially easy, below we sketch a proof of an equivalent assertion for the reader’s convenience:

**Proposition 1.1.** Suppose that $A \subset k[G]$ is a subalgebra, stable under the right regular representation of $G$, and $m_A = m \cap A$ where $m$ is the augmentation ideal of $k[G]$. Then $A = k[G' \backslash G]$ where $G'$ is the stabilizer of $m_A$ in $G$.

**Proof.** Put $B = k[G' \backslash G], R = k[G]$. The group scheme $G$ operates from the right on $X = \text{Spec} A$ and the inclusion $A \subset R$ corresponds to a $G$-equivariant morphism $G \to X$. The latter is the orbit morphism $\mu_x$ of the point $x \in X(k)$ corresponding to $m_A$. Since $G' = G_x$, the orbit morphism factors through $G' \backslash G$, which means that $A \subset B$. Let $K = R/\text{Im} A$, and let $g \in G(K)$ be the point corresponding to the canonical homomorphism $R \to K$. Since the composite homomorphism $A \to R \to K$ factors through $A/\text{Im} A$, we have $x_K g = \mu_x(g) = x_K$, which yields $g \in G'(K)$. It follows that the composite $B \to R \to K$ factors through $B/\text{Im} B$ where $m_B = m \cap B$. In other words, $m_B = \text{Im} A \cap B$. However, $\text{Im} A \cap B = \text{Im} B A$ because $R$ is free over $B$. Hence $B = k + m_B = A + B m_A$. Since $R$ is finite over $A$, the map $G(k) \to X(k)$ determined by $\mu_x$ is surjective. This means that $G(k)$ transitively permutes the maximal ideals of $A$. Then $B = A + B n$ for all maximal ideals $n$ of $A$. An application of Nakayama’s lemma yields $B = A$. □

Suppose now that $A$ is any unital associative algebra on which $G$ operates by automorphisms. This means that $A$ has a $G$-module structure and for each commutative algebra $K$ the group $G(K)$ operates on $A \otimes K$ via automorphisms. We call $A$ a $G$-algebra in this case. By an $(A, G)$-module we mean a right $A$-module $M$ equipped with an additional $G$-module structure such that the $A$-module structure
map \( M \otimes A \to M \) is \( G \)-equivariant. Denote by \( \mathcal{M}_A \) the category of \((A, G)\)-modules. The morphisms in \( \mathcal{M}_A \) are maps which are simultaneously \( A \)-module and \( G \)-module homomorphisms.

This definition is meaningful for an arbitrary group scheme. When \( G \) is finite, the category of \( G \)-modules is equivalent to the category of left \( k[G]^* \)-modules (see [9], Part I, Ch. 8), and \( \mathcal{M}_A \) is equivalent to the category of left modules over the smash product algebra \( A^{op} \# k[G]^* \) where \( A^{op} \) is the algebra \( A \) with the opposite multiplication. When \( A \) is commutative, \( A^{op} = A \). We refer the reader to [19] or [13] concerning the precise definition of smash products. Here we just point out that \( A \neq k[G]^* \) contains \( A \) and \( k[G]^* \) as subalgebras and the multiplication map \( A \otimes k[G]^* \to A \# k[G]^* \) is bijective. One of our tools is the following theorem whose interpretations can be found in [2], [10], [20]:

Imprimitivity Theorem. Suppose that \( A = k[G\setminus G] \), and let \( m_A \) be the augmentation ideal of \( A \). Then the functor \( M \mapsto M/Mm_A \) is an equivalence between \( \mathcal{M}_A \) and the category of \( G' \)-modules. If \( M \in \mathcal{M}_A \), then there is an isomorphism of \( G \)-modules \( M \cong \text{ind}^G_{G'} M/Mm_A \).

Given a \( G' \)-module \( V \), the induced \( G \)-module is \( \text{ind}^G_{G'} V = (V \otimes k[G])^{G'} \). To be precise, we compute the \( G' \)-invariants with respect to the tensor product of the \( G' \)-module structure on \( V \) and the left regular \( G' \)-module structure on \( k[G] \), and we use the right regular \( G' \)-module structure on \( k[G] \) to get one on \( \text{ind}^G_{G'} V \). This differs from the conventions adopted in [9]. In terms of the dual algebras

\[
\text{ind}^G_{G'} V \cong \text{Hom}_{k[G]}(k[G]^*, V).
\]

It follows that \( \dim \text{ind}^G_{G'} V = (G : G') \cdot \dim V \). We mention also that the injective \( G \)-modules are projective, and vice versa, because finite dimensional Hopf algebras are Frobenius (see [19]). Waterhouse proved that every finite group scheme is geometrically reductive [22].

Below we prove two lemmas. Suppose that \( A \) is a commutative integral domain and \( K \) its field of fractions. For a prime ideal \( \mathfrak{p} \) of \( A \) denote \( k(\mathfrak{p}) = A_\mathfrak{p}/A_\mathfrak{p}\mathfrak{p} \).

**Lemma 1.2.** Let \( F \) be a finitely generated projective \( A \)-module, \( F' \) its submodule. Denote by \( I(\mathfrak{p}) \) the image of the canonical map \( F' \otimes_A k(\mathfrak{p}) \to F \otimes_A k(\mathfrak{p}) \) and put \( q = \dim_K F' \otimes_A K \). Then:

1. \( q = \max_{\mathfrak{p} \in \text{Spec } A} \dim_{k(\mathfrak{p})} I(\mathfrak{p}) \).
2. The subset \( U = \{ \mathfrak{p} \in \text{Spec } A \mid \dim_{k(\mathfrak{p})} I(\mathfrak{p}) = q \} \) is Zariski open and coincides with the subset \( U' = \{ \mathfrak{p} \in \text{Spec } A \mid F'_\mathfrak{p} \text{ is a direct summand of } F_\mathfrak{p} \} \).
3. If \( U = \text{Spec } A \) then \( F' \) is projective of rank \( q \) and is a direct summand of \( F \).

**Proof.** We identify all localizations of \( F \), as well as localizations of \( F' \), with their images in \( F \otimes_A K \). Let \( \mathfrak{p} \in \text{Spec } A \). Suppose that \( u_1, \ldots, u_r \in F'_\mathfrak{p} \) are elements whose images in \( F_\mathfrak{p}/pF_\mathfrak{p} \cong F \otimes_A k(\mathfrak{p}) \) are linearly independent over \( k(\mathfrak{p}) \). Then \( S = A_\mathfrak{p}u_1 + \ldots + A_\mathfrak{p}u_r \) is a direct summand of the free \( A_\mathfrak{p} \)-module \( F_\mathfrak{p} \) (see [1], Ch. II, §3, Cor. 1 to Prop. 5). In particular, \( S \) is free over \( A_\mathfrak{p} \) with a basis \( u_1, \ldots, u_r \). We get \( r = \dim_K S \otimes_A K \leq q \). It follows \( \dim_{k(\mathfrak{p})} I(\mathfrak{p}) \leq q \) by definition of \( q \) the equality holds here for \( \mathfrak{p} = (0) \).

Suppose that \( \mathfrak{p} \in U \). Then we can take \( q \) elements \( u_1, \ldots, u_q \) above, so that \( r = q \). By modularity law \( S \) is a direct summand of \( F'_\mathfrak{p} \). So \( F'_\mathfrak{p} = S \oplus C \) where \( C \subset F_\mathfrak{p} \) is an \( A_\mathfrak{p} \)-submodule. Tensoring with \( K \) and comparing dimensions over \( K \),
we deduce that \( C \otimes_A K = 0 \). However, \( F_p \) is torsion-free since \( A_p \) is a domain. It follows \( C = 0 \), i.e., \( F'_p = S \). Thus \( p \in U' \).

Conversely, suppose that \( p \in U' \). Then \( F'_p \) is free of rank \( q \) over \( A_p \) and the map \( F' \otimes_A k(p) \to F \otimes_A k(p) \) is injective. It follows \( \dim_k I(p) = q \). There exists an \( A_p \)-module epimorphism \( \varphi : F_p \to F'_p \) which is identity on \( F'_p \). Since \( F \) is finitely generated, \( \varphi(F) \subset F'_s \) for a suitable \( s \in A \setminus p \). Then \( \varphi(F_s) = F'_s \), and so \( F'_s \) is a direct summand of \( F_s \). This shows that \( U' \) is open in \( \text{Spec} \, A \). Finally, (3) is obtained by an application of [1], Ch. II, §5, Th. 1 and §3, Cor. 1 to Prop. 12.

**Lemma 1.3.** Let \( F \) be a finitely generated projective \( A \)-module, \( F' \) and \( F'' \) its direct summands. Denote by \( I'(p) \), \( I''(p) \) the images, respectively, of \( F' \otimes_A k(p) \), \( F'' \otimes_A k(p) \) in \( F \otimes_A k(p) \), and put \( s = \min_{p \in \text{Spec} \, A} \dim_k I'(p) / I''(p) \). Then:

1. The subset \( U = \{ p \in \text{Spec} \, A \mid \dim_k I'(p) / I''(p) = s \} \) is open in Spec \( A \) and consists precisely of those \( p \) for which \( F_p' + F_p'' \) is a direct summand of \( F_p \).

2. For all \( p \in U \) the canonical map \( (F' \cap F'') \otimes_A k(p) \to F \otimes_A k(p) \) is an isomorphism onto \( I'(p) / I''(p) \).

3. If \( U = \text{Spec} \, A \) then the \( A \)-module \( F' \cap F'' \) is projective of rank \( s \) and is a direct summand of \( F \).

**Proof.** Since \( F', F'' \) are direct summands of \( F \), the dimensions of vector spaces \( I'(p) \), \( I''(p) \) do not depend on \( p \). Then \( U \) is the set of those \( p \in \text{Spec} \, A \) for which \( I'(p) + I''(p) \) has maximal possible dimension. Apply now Lemma 1.2 taking \( F' + F'' \) instead of \( F' \) in it. We get assertion (1) of Lemma 1.3. If \( p \in U \) then \( F_p' + F_p'' \) is a free \( A_p \)-module. Since \( F_p' \) is a direct summand of \( F_p' + F_p'' \), the \( A_p \)-module \[ F_p' / (F_p' \cap F_p'') \cong (F_p' + F_p'') / F_p'' \] (\( * \)) is free too. Then \( F_p' \cap F_p'' \) is a direct summand of \( F_p' \), hence also a direct summand of \( F_p \). In particular, \( (F' \cap F'')_p \cong F'_p \cap F''_p \) is free over \( A_p \) and the map in (2) is injective. Denoting by \( I(p) \) the image of that map and tensoring \((*)\) with \( k(p) \), we obtain an isomorphism \( I'(p) / I(p) \cong (I'(p) + I''(p)) / I''(p) \). It follows \( I(p) = I'(p) \cap I''(p) \). The last assertion is a special case of Lemma 1.2(3).

2. The set of \( G \)-regular points and the properties of the quotient.

Let \( G \) be a finite group scheme operating from the right on an irreducible algebraic variety \( X \). Suppose that \( X \) can be covered by \( G \)-invariant affine open subsets, so that \( X / G \) exists (as is well known it suffices to require that the \( G(k) \)-orbit of each closed point of \( X \) is contained in an affine open subset). We will be considering only closed points of \( X \), so that \( x \in X \) means \( x \in X(k) \). If \( U \subset X \) is an open subset, stable under all automorphisms of \( X \) determined by the elements of \( G(k) \), then the composite morphism \( U \times G \to X \times G \to X \) factors through \( U \), i.e., \( U \) is \( G \)-invariant. In particular, if \( U \subset X \) is any open subset, \( \cap_{p \in G(k)} Ug \) is a \( G \)-invariant open subset contained in \( U \). It follows that the field of rational functions \( k(X) \) is a direct limit of the \( G \)-algebras \( k[U] \) where \( U \) runs through the \( G \)-invariant affine open subvarieties of \( X \). Hence \( G \) operates on \( k(X) \) by automorphisms. Put

\[ q(X) = \max_{x \in X} (G : G_x), \]

\[ X_{G-\text{reg}} = \{ x \in X \mid (G : G_x) = q(X) \}. \]
THEOREM 2.1.  $X_{G\text{-reg}}$ is a $G$-invariant open subset of $X$. Furthermore:

1. $\pi|_{X_{G\text{-reg}}}: X_{G\text{-reg}} \rightarrow \pi(X_{G\text{-reg}})$ is a finite flat morphism of degree $q(X)$.
2. For every $x \in X_{G\text{-reg}}$ the fibre of $\pi$ above $\pi(x)$ is $G$-equivariantly isomorphic with $G_x \setminus G$.
3. The $G$-invariant closed subschemes $Z$ of $X_{G\text{-reg}}$ are in a bijective correspondence with the closed subschemes $W$ of $\pi(X_{G\text{-reg}})$. If $Z$ and $W$ correspond to each other, then $W \cong Z/G$ and $Z \cong W \times_{X/G} X$.
4. One has $(Y \times_{X/G} X)/G \cong Y$ for any scheme $Y$ on which $G$ operates trivially and a morphism $Y \rightarrow \pi(X_{G\text{-reg}})$.
5. $[k(X) : k(X)^G] = q(X)$.

We first reformulate the assertions of the theorem in the affine case.

Proposition 2.2. Suppose that $X \cong \text{Spec} A$ and $X_{G\text{-reg}} = X$. Then:

1. $A$ is a projective $A^G$-module of rank $q(X)$.
2. If $m$ is a maximal ideal of $A$ and $n = m \cap A^G$ then $nA$ is a maximal $G$-invariant ideal of $A$ and the algebra $A/nA$ is $G$-equivariantly isomorphic with $k[G_m \setminus G]$ where $G_m$ is the stabilizer of $m$ in $G$.
3. The assignment $I \mapsto I^G$ establishes a bijection between the $G$-invariant ideals of $A$ and the ideals of $A^G$. The inverse correspondence is given by $J \mapsto JA$. The canonical maps $A^G \rightarrow (A/I)^G$ are surjective.
4. If $B$ is an $A^G$-algebra on which $G$ operates trivially then $(B \otimes_{A^G} A)^G \cong B$.

Proof. Given any covering of $X$ by $G$-invariant open subvarieties, it suffices to prove the theorem for the induced action of $G$ on each of these subvarieties. In particular, we may assume $X$ to be affine. Let $A = k[X]$, $R = k[G]$, and let $\mu^*: A \rightarrow A \otimes R$, $i_x^*: A \rightarrow k$, $\mu_z^*: A \rightarrow R$ be the comorphisms of $\mu, i_x, \mu_z$, respectively. Denote by $m_x$ the maximal ideal of $A$ consisting of functions vanishing at $x$.

Consider $F = A \otimes R$ as an $A$-module by means of the algebra homomorphism $\mu_1^*: A \rightarrow A \otimes R$, $a \mapsto a \otimes 1$. Clearly $F$ is free of finite rank over $A$. Put

$$F' = (A \otimes 1) \cdot \mu^*(A) \subset F.$$ 

Then $F'$ is an $A$-submodule of $F$ generated by $\mu^*(A)$. Denote by $I(x)$ the image of the canonical map $F'/m_x F' \rightarrow F/m_x F$. We have $F/m_x F \cong A/m_x \otimes R \cong R$ and $I(x) = \mu^*_x(A)$ since $\mu^*_x = (i_x^* \otimes \text{id}_R) \circ \mu^*$. Now $\mu^*_x$ is a $G$-equivariant algebra homomorphism. Since $G_x$ coincides with the stabilizer of $m_x$ in $G$, Proposition 1.1 ensures $\mu^*_x(A) = k[G_x \setminus G]$. Hence $\dim I(x) = (G : G_x)$. It follows that $X_{G\text{-reg}}$ coincides with the set $U$ of those points $x \in X$ for which $\dim I(x)$ attains its maximal value $q = q(X)$. We can now apply Lemma 1.2. By (2) of the lemma $U$ is open. Each $g \in G(k)$ determines an inner automorphism of $G$ which induces an isomorphism $G_x \cong G_z$. Hence $(G : G_{xz}) = (G : G_z)$. It follows that $U$ is $G$-invariant.

Let $y \in U$ and let $O \subset X$ be the $G(k)$-orbit of $y$. Then $\dim I(z) = q$ for all $z \in O$. Since $O$ is finite, we can find $a_1, \ldots, a_q \in A$ such that $\mu^*_x(a_1), \ldots, \mu^*_x(a_q)$ are a basis of $I(z)$ for each $z \in O$. Furthermore, we may assume $a_1 = 1$ since $\mu^*_x(1) = 1$ for all $x$. Applying Lemma 1.2 to the $A$-submodule of $F$ generated by $\mu^*(a_1), \ldots, \mu^*(a_q)$, we see that the set $U_1$ of those $x \in X$ for which $\mu^*_x(a_1), \ldots, \mu^*_x(a_q)$ are linearly
independent is open in \( X \). Clearly \( U_1 \subset U \). Since \( \pi \) is a finite morphism, the set \( W = \pi(X \setminus U_1) \) is closed in \( X/G \). Since \( \pi^{-1}(\pi(y)) = O \subset U_1 \), we have \( \pi(y) \notin W \). Let \( V \) be an open affine neighbourhood of \( \pi(y) \) in \( X/G \). Then \( \pi^{-1}(V) \) is an open affine \( G \)-invariant neighbourhood of \( y \) in \( X \) and \( \pi^{-1}(V) \subset U_1 \).

To prove the remainder of the theorem we can again use the local character of the assertions and pass to the actions of \( G \) on the invariant open subsets of the form \( \pi^{-1}(V) \) constructed above. We may thus assume that \( U_1 = X \).

By Lemma 1.2 \( F' \) is a direct summand of the \( A \)-module \( F \) and for each maximal ideal \( m \) of \( A \) the localization \( F'_m \) is free of rank \( q \) over \( A_m \). If \( \varphi : A^q \rightarrow F' \) is the \( A \)-module homomorphism sending the standard generators of \( A^q \) to \( \mu^*(a_1), \ldots, \mu^*(a_q) \) then the localizations of \( \varphi \) at maximal ideals of \( A \) are all isomorphisms. Hence \( \varphi \) is itself an isomorphism, i.e., \( F' \) is a free \( A \)-module with a basis \( \mu^*(a_1), \ldots, \mu^*(a_q) \).

Hence for each \( a \in A \) there are \( b_1, \ldots, b_q \in A \) such that

\[
\mu^*(a) = \sum (b_i \otimes 1) \cdot \mu^*(a_i). \tag{\ast}
\]

Let \( \varepsilon : R \rightarrow k \) be the counit and \( m^* : R \rightarrow R \otimes R \) the comultiplication maps. Applying \( \text{id}_A \otimes \varepsilon \) to both sides of (\ast), we get \( \mu^*(a) = \sum b_i a_i \) since \( \text{id}_A \otimes \varepsilon \circ \mu^* = \text{id}_A \).

Applying \( \mu^* \otimes \text{id}_R \) and \( \text{id}_A \otimes m^* \) to both sides of (\ast), and taking into account the identity \( (\mu^* \otimes \text{id}_R) \circ \mu^* = (\text{id}_A \otimes m^*) \circ \mu^* \), we get

\[
\sum (\mu^*(b_i) \otimes 1) \cdot (\mu^* \otimes \text{id}_R) \mu^*(a_i) = \sum (b_i \otimes 1 \otimes 1) \cdot (\mu^* \otimes \text{id}_R) \mu^*(a_i) \tag{\ast\ast}
\]
in \( A \otimes R \). If \( \gamma : A \rightarrow A' \) is a homomorphism of commutative algebras then \( A' \otimes_A F' \) is a free \( A' \)-module with basis elements \( 1 \otimes \mu^*(a_i), i = 1, \ldots, q \). Since the canonical map \( A' \otimes_A F' \rightarrow A' \otimes_A F \cong A' \otimes R \) is injective, the elements

\[
(\gamma \otimes \text{id}_R) \mu^*(a_i) \in A' \otimes R, \quad i = 1, \ldots, q,
\]

are linearly independent over \( A' \). Taking \( A' = A \otimes R \) and \( \gamma = \mu^* \), we deduce from (\ast\ast) that \( \mu^*(b_i) = b_i \otimes 1 \), that is, \( b_i \in A^G \) for all \( i \). Hence \( A = A^G a_1 + \cdots + A^G a_q \).

If now \( \sum c_i a_i = 0 \) for some \( c_1, \ldots, c_q \in A^G \) then \( \sum (c_i \otimes 1) \mu^*(a_i) = \mu^*(\sum c_i a_i) = 0 \), whence \( c_i = 0 \) for all \( i \). Thus \( A \) is free of rank \( q \) over \( A^G \).

Suppose that \( N \) is an \( A^G \)-module and \( M = N \otimes_{A^G} A \) is given a \( G \)-module structure by means of the comodule structure map

\[
\text{id}_N \otimes \mu^* : N \otimes_{A^G} A \rightarrow N \otimes_{A^G} (A \otimes R) \cong (N \otimes_{A^G} A) \otimes R.
\]

We claim that the assignment \( n \mapsto n \otimes 1 \) yields an isomorphism \( N \cong M^G \). This amounts to showing that the exactness of the sequence of \( A^G \)-modules

\[
0 \rightarrow A^G \rightarrow A \xrightarrow{\mu^* - p_i^*} A \otimes R
\]
is preserved under tensoring with \( N \) over \( A^G \). Now \( A = A^G \oplus (A^G a_2 + \cdots + A^G a_q) \) as we assume \( a_1 = 1 \). Next, \( (\mu^* - p_i^*)(A) \) is an \( A^G \)-submodule of \( F \) generated by the elements \( \mu^*(a_i) - a_i \otimes 1 \), \( i = 2, \ldots, q \). Note that these elements together with \( \mu^*(a_1) = 1 \otimes 1 \) give a basis for \( F' \) over \( A' \). Then the \( A \)-submodule generated by \( \mu^*(a_i) - a_i \otimes 1 \), \( i = 2, \ldots, q \), is a direct summand of \( F' \), hence also of \( F \). We have seen that \( A^G \) is a direct summand of \( A \), hence also \( (\mu^* - p_i^*)(A) \) is a direct summand of \( F \) as \( A^G \)-modules. Our claim follows.
Assertion (4) of the theorem is local on \( Y \), hence it suffices to consider an affine scheme \( Y \cong \text{Spec} \ B \). This is then a special case of what we have just proved. Next, taking \( N = J \) where \( J \) is an ideal of \( A^G \), we get \( JA \cap A^G = J \) since \( J \otimes_A^R A \cong JA \) by projectivity of \( A \) over \( A^G \). Taking \( N = A^G/J \), we deduce that the canonical map \( A^G \to (A/IA)^G \) is surjective. Suppose that \( I \) is a \( G \)-invariant ideal of \( A \). Then \( \mu^*(I) \subseteq I \cap R = IF \). Since on the other hand \( \mu^*(A) \subseteq F' \) and \( F' \) is a direct summand of \( F \), we get \( \mu^*(I) \subseteq F' \cap IF = IF' \). Given \( a \in I \), we can write therefore the expression \( (\ast) \) with \( b_i \in I \). As we have seen, this implies \( a = \sum b_i a_i \) and \( b_i \in A^G \). Thus \( I = I^G A \), which completes the proof of (3). If \( n \) is a maximal ideal of \( A^G \) then \( nA \) is a maximal \( G \)-invariant ideal of \( A \) by (3). If now \( n = m \cap A^G \) then \( \mu^*(nA) = (n \otimes 1) \cdot \mu^*(A) \subseteq m \otimes R \), whence \( \mu^*(nA) = 0 \). It follows that \( \ker \mu^* = nA \), and \( A/nA \cong A^G \) via \( \mu^* \). This proves (2). Assertion (5) follows from (1) since \( k(X)^G \) is the field of fractions of the ring \( A^G \). \( \square \)

**Corollary 2.3.** If \( x \) is a smooth point of \( X_{G\text{-reg}} \) then \( \pi(x) \) is a smooth point of \( X/G \).

**Proof.** The local ring \( O_{x,X} \) is a flat extension of \( O_{\pi(x),X/G} \). Since \( O_{x,X} \) is a regular local ring, so is \( O_{\pi(x),X/G} \) too by [11], (21.D). \( \square \)

**Remark.** Theorem 2.1 can be generalized to the case when \( k \) is any field and \( X \) is a reduced scheme over \( k \). In general the stabilizer \( G_x \) is a subgroup scheme of \( G \otimes k(x) \) where \( k(x) \) is the residue field of a point \( x \in X \), and one can define \( X_{G\text{-reg}} \) to be the set of all points where the function \( x \mapsto (G \otimes k(x) : G_x) \) is locally constant. It can also be proved that the morphism \( \nu : X_{G\text{-reg}} \times G \to X_{G\text{-reg}} \times_{\pi(X_{G\text{-reg}})} X_{G\text{-reg}} \) is finite flat. The assumption that \( X \) is reduced is needed to ensure that \( F' \) is a direct summand of \( F \) in the proof of theorem 2.1. Simple examples show what can happen without this assumption. Suppose, for instance, that \( X = \text{Spec} \ A \) where \( A = k[x] \), \( x^3 = 0 \), and \( G \) is the cyclic order 2 group with a generator \( \sigma \) which acts on \( A \) as the automorphism sending \( x \) to \(-x \). Here \( A^G = k + kx^2 \) (provided \( \text{char} \, k \neq 2 \)). Clearly \( A \) is not free over \( A^G \). At the same time \( X \) contains a single point, so that \( X_{G\text{-reg}} = X \).

### 3. \( G \)-linearized modules.

We keep our assumptions on \( G \) and \( X \) from section 2. Moreover, we assume here that \( X \) is affine. Let \( R = k[G] \), \( A = k[X] \) and \( K = k(X) \). Recall that \( \mathcal{M}_A \) denotes the category of \((A,G)\)-modules. Denote by \( \mu^A : M \to M \otimes R \) the map that gives \( M \in \mathcal{M}_A \) the \( R \)-comodule structure corresponding to the \( G \)-module structure. In particular, \( A \) is an \( R \)-comodule via the map \( \mu^A : A \to A \otimes R \) which is the comorphism of \( \mu \). We may view \( M \otimes R \) as a module over \( A \otimes R \) in a natural way. The compatibility of \( A \)- and \( G \)-module structures on \( M \) can be expressed in terms of the identity \( \mu^A(ma) = \mu^M(m) \cdot \mu^A(a) \) where \( m \in M \) and \( a \in A \). We note also that \((S^{-1}M)^G \cong S^{-1}M^G \) for every multiplicatively closed subset \( S \subset A^G \).

**Lemma 3.1.** Suppose that \( X = X_{G\text{-reg}} \) and \( M \in \mathcal{M}_A \). Then

\[ M^G A = \{ m \in M \mid \mu^M(m) \in (M \otimes 1) \cdot \mu^A(A) \} \]

\[ = \{ m \in M \mid m \otimes 1 \in \mu^M(M) \cdot (A \otimes 1) \}. \]

**Proof.** Let \( F = A \otimes R \) and \( F' = (A \otimes 1) \cdot \mu^A(A) \) as in the proof of Theorem 2.1. For every \( A \)-module \( N \) we consider \( F_N = N \otimes R \) as an \( F \)-module in a natural
way and as an $A$-module by means of the homomorphism $p_1^*: A \to F$. Then $F_N \cong N \otimes_A F$. Put $F_N' = (N \otimes 1) \cdot \mu^*(A) \subset F_N$. Since $F'$ is a direct summand of $F$, the canonical map $N \otimes_A F' \to N \otimes_A F$ is a split monomorphism of $A$-modules. Clearly its image coincides with $F_N'$. Hence $F_N' \cong N \otimes_A F'$.

Suppose that $m \in M$ and $\mu^M(m) \in F_N'$. To prove that $m \in M^G A$ it suffices to show that for every $x \in X$ there exists $f \in A^G$ such that $f(x) \neq 0$ and $mf \in M^G A$. Passing to suitable localizations $A_f$ and $M_f$, we may thus assume as in the proof of Theorem 2.1 that $F'$ is a free $A$-module with basis elements $\mu^*(a_1), \ldots, \mu^*(a_q)$. Then $\mu^M(m) = \sum (m_i \otimes 1) \cdot \mu^*(a_i)$ for some $m_1, \ldots, m_q \in M$. Let $\varepsilon$ and $m^*$ be the counit and the comultiplication in $R$. Applying $id_M \otimes \varepsilon$ to both sides of the equality, we get $m = \sum m_i a_i$. Applying $\mu^M \otimes id_R$ and $id_M \otimes m^*$, we get

$$\sum (\mu^M(m_i) \otimes 1) \cdot (\mu^* \otimes id_R)\mu^*(a_i) = \sum (m_i \otimes 1 \otimes 1) \cdot (\mu^* \otimes id_R)\mu^*(a_i)$$

in $M \otimes R \otimes R$. If $n_1, \ldots, n_q$ are elements of an $A$-module $N$ with the property that $\sum (n_i \otimes 1) \cdot \mu^*(a_i) = 0$ in $F_N$ then $\sum n_i \otimes \mu^*(a_i) = 0$ in $N \otimes_A F'$ by the discussion at the beginning of the proof, whence $n_i = 0$ for all $i$. Now take $N = M \otimes R$ with the $A$-module structure given by means of the algebra homomorphism $\mu^*: A \to A \otimes R$.

Then $A \otimes R$ operates in $N \otimes R \cong M \otimes R \otimes R$ by means of the algebra homomorphism $\mu^* \otimes id_R$, and it follows from the displayed equation above that $\mu^M(m_i) = m_i \otimes 1$, i.e., $m_i \in M^G A$. Hence $m \in M^G A$.

Suppose now that $m \in M$ and $m \otimes 1 = \mu^M(m_i) \cdot (b_1 \otimes 1)$ for some elements $m_1, \ldots, m_q \in M$ and $b_1, \ldots, b_r \in A$. If $\beta: R \to B$ is the algebra homomorphism corresponding to a point $g \in G(B)$ where $B$ is a commutative algebra then, applying $id_M \otimes \beta$ to both sides of the equality, we get $g \cdot m \otimes 1 = \sum g(m_i \otimes 1 \cdot (b_1 \otimes 1))$ in $M \otimes B$ (regarded as a module over $A \otimes B$). Replacing here $g$ with $g^{-1}$ and applying $g$ to both sides of the equality obtained, we get $g \cdot m \otimes 1 = \sum (m_i \otimes 1 \cdot (b_1 \otimes 1))$. If now $B = R$ and $g \in G(R)$ is the point corresponding to the identity homomorphism $R \to R$, this can be rewritten as $\mu^M(m) = \sum (m_i \otimes 1) \cdot \mu^*(b_1)$. Thus we have come to the case already considered.

**Proposition 3.2.** Suppose that $X = X_{\text{G-reg}}$ and denote by $M'_{A}$ the full subcategory of $\mathcal{M}_{A}$ consisting of $(A, G)$-modules $M$ such that $M = M^G A$. Then:

1. $M'_{A}$ is closed under taking submodules and factor modules.
2. The functor $M \mapsto M^G$ is an equivalence between $M'_{A}$ and the category of $A^G$-modules. The inverse functor is $N \mapsto N \otimes_{A^G} A$.
3. If $M \in M'_{A}$ is projective of rank $r$ as an $A$-module then $M^G$ is projective of rank $r$ as an $A^G$-module.

**Proof.** (1) We use the same notations as in the preceding lemma. Clearly, $F_N/F_N' \cong N \otimes_A F/F'$ for every $A$-module $N$. Let $N$ be an $(A, G)$-submodule of $M \in M'_{A}$. Since $F' \otimes F'$ is a projective $A$-module, the canonical map $N \otimes_A F/F' \to M \otimes_A F/F'$ is injective. It follows from the commutative diagram

$$0 \to F_N' \to F_N \to N \otimes_A F/F' \to 0$$

that $F_N' = F_N \cap F_M'$. Now $\mu^M(N) \subset F_N$ and $\mu^M(M) \subset F_M'$, whence $\mu^M(N) \subset F_N'$. Hence $N \in M'_{A}$ by Lemma 3.1. The assertion about factor modules is obvious.
(2) If $N$ is an $A^G$-module and $M = N \otimes_A A$ then $N \cong M^G$ as we have seen in the proof of Theorem 2.1. Conversely, suppose that $M \in \mathcal{M}_G^1$ and $M_1 = M^G \otimes_A A$. The canonical map $\varphi : M \to M$ is a morphism in $\mathcal{M}_A$. It is surjective by the definition of $\mathcal{M}_A$. Now $\ker \varphi \in \mathcal{M}_A$ by (1), hence $\ker \varphi$ is generated over $A$ by $G$-invariant elements. But we have proved already that $M^G = M^G \otimes 1$. Since $\varphi$ is injective on $M^G$, we get $\ker \varphi = 0$, i.e., $\varphi$ is an isomorphism.

(3) follows from [1], Ch. I, §3, Prop. 12 and Ch. II, §5, Prop. 4. □

Suppose that $M \in \mathcal{M}_A$ is finitely generated over $A$. Put

$$\text{rk} M = \dim_K \text{M} \otimes_A K \quad \text{and} \quad M(x) = M/\text{m}_x \quad \text{for} \quad x \in X$$

where $\text{m}_x$ is the maximal ideal of $A$ corresponding to $x$. Then $\dim M(x) \geq \text{rk} M$ for all $x \in X$. By [1], Ch. 2, §3, Prop. 7 and §5, Corollary to Prop. 2, the set

$$X_M = \{x \in X \mid \dim M(x) = \text{rk} M\}$$

is open in $X$ and consists precisely of those $x$ for which $M_{\text{m}_x}$ is a free $A_{\text{m}_x}$-module. If $\text{m}_x$ is stable under $G$ then $\mu^G(M_{\text{m}_x}) = \mu^G(M) \cdot \mu^G(\text{m}_x) \subset M_{\text{m}_x} \otimes R$ since $\mu^G(\text{m}_x) \subset \text{m}_x \otimes R$. In general, applying this observation to the action of $G_x$, we see that $M_{\text{m}_x}$ is stable under $G_x$, and so $G_x$ operates in $M(x)$. Put

$$s(M) = \min_{x \in X_{G\text{-reg}}} \dim M(x)^{G_x},$$

$$X_{M,\text{reg}} = \{x \in X_{G\text{-reg}} \mid \dim M(x) = \text{rk} M \quad \text{and} \quad \dim M(x)^{G_x} = s(M)\}.$$

We call $X_{M,\text{reg}}$ the set of $M$-regular points in $X$.

**Theorem 3.3.** (1) $X_{M,\text{reg}}$ is a $G$-invariant open subset of $X$.

(2) For all $x \in X_{M,\text{reg}}$ the canonical map $M \to M(x)$ induces a surjection $M^G \twoheadrightarrow M(x)^{G_x}$.

(3) If $X_{M,\text{reg}} = X$ then the map $M^G \otimes_A A \to M$ given by $m \otimes a \mapsto ma$ is a split monomorphism of $A$-modules and $M^G$ is projective of rank $s(M)$ over $A^G$.

(4) $\dim_K (M \otimes_A K)^G = s(M)$.

**Proof.** If $x \in X$ and $g \in G(k)$ then $g$ induces a linear isomorphism $M(x) \to M(xg)$ compatible with the actions of stabilizers. Hence $M(x)^{G_x} \cong M(xg)^{G_{xg}}$. It follows that $X_M$ and $X_{M,\text{reg}}$ are stable under the action of $G(k)$. Then $X_M$ is a $G$-invariant open subset, and so is $X_{G\text{-reg}} \cap X_M$ too. Localizing if necessary, we may assume that $X = X_{G\text{-reg}}$ and $M_{\text{m}_x}$ is free over $A_{\text{m}_x}$ for all $x$. Then $M$ is a projective $A$-module.

We are going to apply Lemma 1.3 in which we take $F = M \otimes R$ with the $A$-module structure obtained again via $p_1^* : A \to A \otimes R$. Take $F'' = M \otimes 1$, which is clearly a direct summand of $F$. Put $F' = \mu^M(M) \cdot (A \otimes 1)$, and let $I'(x)$, $I''(x)$ be the images, respectively, of $F'/F'^{\text{m}_x}$ and $F''/F''^{\text{m}_x}$ in $F/F^{\text{m}_x} \cong M(x) \otimes A$. We have $I''(x) \cong M(x) \otimes 1$. If $\mu^M_x$ denotes the composite

$$M \xrightarrow{\mu^M} M \otimes A \xrightarrow{\text{id} \otimes \text{id}_R} M(x) \otimes R,$$

then $I'(x) = \mu^M_x(M)$. Consider two $G$-module structures on $M \otimes R$: the first one is the tensor product of the given $G$-module structure on $M$ and the left regular $G$-module structure on $R$; the second one is the tensor product of the trivial $G$-module structure on $M$ and the left regular $G$-module structure on $R$. Therefore, we can choose $M \otimes R$ so that $\text{rk} M \otimes R = \dim_K M \otimes A$. It is surjective over $M \otimes A$. \[\square\]
structure on $M$ and the right regular $G$-module structure on $R$. The map $\mu^M$ is $G$-equivariant with respect to the second structure and is a bijection of $M$ onto the subspace $(M \otimes R)^G$ of $G$-invariant elements with respect to the first structure (see [9], Part I, 3.7, (5) and (6); however, we interchanged the left and right regular $G$-module structures). These two structures on $M \otimes R$ induce a $G_x$-module and a $G$-module structures on $M(x) \otimes R$. We get

$$\mu^M_x(M) \subset (M(x) \otimes R)^{G_x} = \text{ind}^{G_x}_{G} M(x).$$

Since $\mu^M_x$ is $G$-equivariant, $\mu^M_x(M)$ is a $G$-submodule of the induced module. Furthermore, $\mu^M_x(ma) = \mu^M_x(m) \cdot \mu^M_x(a)$ for $m \in M$, $a \in A$, whence $\mu^M_x(M)$ is stable under the action of $\mu^*_x(A) \subset R$. By Proposition 1.1 $\mu^*_x(A) = k[G_x \setminus G]$. The canonical $G_x$-equivariant map $\varphi : \text{ind}^{G_x}_{G} M(x) \to M(x)$ is the restriction of the map $1 \otimes \varepsilon : M(x) \otimes R \to M(x)$. Hence the composite $\varphi \circ \mu^M_x$ coincides with the canonical projection $M \to M(x)$, it is therefore surjective. It follows that the inclusion $\iota : \mu^M_x(M) \hookrightarrow \text{ind}^{G_x}_{G} M(x)$ corresponds under the equivalence of the Imprimitivity Theorem to a surjective map of $G_x$-modules. Then $\iota$ must itself be surjective, i.e., $\mu^M_x(M) = \text{ind}^{G_x}_{G} M(x)$. In particular,

$$\dim I'(x) = \dim \text{ind}^{G_x}_{G} M(x) = (G : G_x) \cdot \dim M(x) = q(X) \text{rk}(M),$$

which does not depend on $x$. By Lemma 1.2 $F'$ is a direct summand of $F$. Thus the hypotheses of Lemma 1.3 are fulfilled. By our previous description $I'(x) \cap I''(x) = (M(x) \otimes 1)^{G_x} \cong M(x)^{G_x}$. Hence $s = s(M)$ and $X_{M, \text{reg}}$ is the set of rational points of the open subset $U \subset \text{Spec } A$ defined in Lemma 1.3. Thus $X_{M, \text{reg}}$ is open in $X$. It is $G$-invariant by observation at the beginning of the proof. Therefore we may localize further and assume $X = X_{M, \text{reg}}$. By Lemma 3.1 $F' \cap F'' = M^G A \otimes 1$. Then (2) of Lemma 1.3 implies (2) of the theorem. Lemma 1.3 ensures that the $A$-module $M^G A$ is projective of rank $s(M)$ and is a direct summand of the $A$-module $M$. By Proposition 3.2 $M^G$ is a projective $A^G$-module of rank $s(M)$ and $M^G \otimes_A A$ is mapped isomorphically onto $M^G A$. This proves (3). Assertion (4) is immediate since $(M \otimes_A K)^G \cong M^G \otimes_A K^G$.

Let $M, N \in \mathcal{M}_A$ and $P = \text{Hom}_A(N, M)$. For every finite dimensional commutative algebra $B$ we have

$$P \otimes B \cong \text{Hom}_A \otimes B(N \otimes B, M \otimes B).$$

If $g \in G(B)$ and $\xi \in P \otimes B$ then we put $g_P(\xi) = g_M \circ \xi \circ g_N^{-1}$ where $g_M$ and $g_N$ are the operators on $M \otimes B$ and $N \otimes B$, respectively, corresponding to $g$. In this way we obtain a group action of $G(B)$ on $P \otimes B$ which is natural in $B$. If $B$ is infinite dimensional then each point $g \in G(B)$ still belongs to $G(B')$ where $B' \subset B$ is a finite dimensional subalgebra. Indeed, we can take $B'$ to be the image of the algebra homomorphism $R \to B$ corresponding to $g$. Extend the action of $g$ in $P \otimes B'$ by $B$-linearity to the action in $P \otimes B$. If $g, h \in G(B)$ are two points then there exists a finite dimensional subalgebra $B'$ such that $G(B')$ contains both of them. It follows that $(gh)_P = g_P h_P$. Thus $P$ is equipped with a $G$-module structure, which is clearly compatible with the $A$-module structure, i.e., $P \in \mathcal{M}_A$.

Let $V$ be a $G$-module. Then $V \otimes A$, considered with the natural $A$-module structure and the tensor product $G$-module structure, is an object of $\mathcal{M}_A$. Hence so is $\text{Hom}(V, M) \cong \text{Hom}_A(V \otimes A, M)$ too.
Suppose that \( M, N \in \mathcal{M}_A \) are finitely generated over \( A \) and \( V \) a finite dimensional \( G \)-module. Put
\[
s(N, M) = \min_{x \in X_{G,\text{reg}} \cap X_N \cap X_M} \dim \text{Hom}_G(N(x), M(x)),
\]
\[
s(V, M) = \min_{x \in X_{G,\text{reg}} \cap X_M} \dim \text{Hom}_G(V, M(x)).
\]

**Corollary 3.4.**
1. \( \dim_{K^G} \text{Hom}_{(K,G)}(N \otimes_A K, M \otimes_A K) = s(N, M) \).
2. \( \dim_{K^G} \text{Hom}_G(V, M \otimes_A K) = s(V, M) \).
3. \( \dim_{K^G} \text{soc}_G(M \otimes_A K) = \sum s(V, M) \dim V \), the sum over isomorphism classes of irreducible \( G \)-modules \( V \).

**Proof.**
1. Let \( P = \text{Hom}_A(N, M) \). Then \( P \otimes_A K \cong \text{Hom}_K(N \otimes_A K, M \otimes_A K) \) and \( P(x) \cong \text{Hom}(N(x), M(x)) \) for all \( x \in X_N \). Since \( X_M \cap X_N \subset X_P \), we get \( s(P) = s(N, M) \). Apply Theorem 3.3(4) to the \((A, G)\)-module \( P \), noting that
\[
\text{Hom}_{(K,G)}(N \otimes_A K, M \otimes_A K) \cong (P \otimes_A K)^G.
\]

Assertion (2) is a special case of (1) with \( N = V \otimes A \). Next, the \( G \)-socle \( \text{soc}_G(M \otimes_A K) \) is a direct sum of isotypic components \( I^V \) corresponding to irreducible \( G \)-modules \( V \). Since \( \text{End}_G(V) \cong k \), we have \( I^V \cong \text{Hom}_G(V, M \otimes_A K) \otimes V \), and (3) follows from (2). \( \square \)

We continue to assume that \( M \in \mathcal{M}_A \) is finitely generated over \( A \).

**Lemma 3.5.** If \( x \in X_{G,\text{reg}} \cap X_M \) and \( n = m_x \cap A^G \) then \( M/Mn \cong \text{ind}_x^G M(x) \) as \( G \)-modules. The restriction of the canonical map \( M/Mn \rightarrow M(x) \) yields a linear isomorphism \( (M/Mn)^G \cong M(x)^{G_x} \).

**Proof.** Since \( X_{G,\text{reg}} \cap X_M \) is a \( G \)-invariant open subset, there exists \( f \in A^G \setminus n \) such that \( A_f \) is free of rank \( q(X) \) over \( A^G_f \) and \( M_f \) is free over \( A_f \). Then \( M_f \) is free of rank \( q(X) \) \( \text{rk}(M) \) over \( A^G_f \), and so \( M/Mn \cong M_f/M_f n \) has dimension \( q(X) \) \( \text{rk}(M) \). In the proof of Theorem 3.3 we constructed a surjective \( G \)-module homomorphism \( \mu_x^M : M \rightarrow \text{ind}_x^G M(x) \). Since \( \mu^M(Mn) = \mu^M(M) \cdot (n \otimes 1) \subset M(m_x \otimes R) \), we see that \( Mn \subset \ker \mu_x^M \). Comparing dimensions, we conclude that \( Mn = \ker \mu_x^M \). The final assertion is a special case of the Frobenius reciprocity. \( \square \)

Put \( X_{M,\text{inj}} = \{ x \in X_{G,\text{reg}} \cap X_M \mid M(x) \) is an injective \( G_x \)-module \}. \( \square \)

**Theorem 3.6.**
1. \( X_{M,\text{inj}} \) is open in \( X \) and consists precisely of those points \( x \in X_{G,\text{reg}} \cap X_M \) for which there exists \( f \in A^G \) such that \( f(x) \neq 0 \) and \( M_f \) is a projective \((A_f, G)\)-module.
2. \( X_{M,\text{inj}} \) is nonempty if and only if \( M \otimes_A K \) is a projective \((K, G)\)-module.
3. The induced \( G \)-modules \( \text{ind}_x^G M(x) \) corresponding to points \( x \in X_{M,\text{inj}} \) are all isomorphic to each other.
4. For every \( x \in X_{M,\text{inj}} \) there exist \( f \in A^G \) and a \( G \)-submodule \( V \subset M \) such that \( f(x) \neq 0 \), \( V \cong \text{ind}_x^G M(x) \) and the linear map \( V \otimes A^G_f \rightarrow M_f \) given by the rule \( m \otimes a \rightarrow ma \) is bijective. In particular, \( M_f \) is an injective \( G \)-module.
5. If \( X_{M,\text{inj}} \) is nonempty then \( M \otimes_A K \cong V \otimes K^G \) as \((K^G, G)\)-modules. In particular, \( M \otimes_A K \) is an injective \( G \)-module.
Proof. Let \( x \in X_{M, \text{inj}} \). The \( G \)-module \( V_x = \text{ind}_G^{G_x} M(x) \) is injective by [9], Part I, 3.9, hence it is also projective. Then, in view of Lemma 3.5, there exists a \( G \)-submodule \( V \subset M \) such that \( M = V \oplus M n \) where \( n = m_x \cap A^G \). Clearly \( V \cong V_x \). Define a homomorphism of \( A^G \)-modules \( \varphi : V \otimes A^G \to M \) by the formula \( \varphi(m \otimes a) = ma \) for \( m \in V, \ a \in A^G \). Since \( x \in X_{G, \text{reg}} \cap X_M \), the algebra \( A_n \) is free over \( A_n^G \) and \( M_n \) is free over \( A_n \). Then \( M_n \) is free over \( A_n^G \), and it follows that \( \varphi \) induces an isomorphism \( V \otimes A_n^G \to M_n \). There exists \( f \in A^G \setminus n \) such that

\[
\varphi_f : V \otimes A^G_n \to M_f
\]

is an isomorphism (see [1], Ch. 3, §5, Prop. 2). As a \( G \)-module, \( M_f \) is a direct sum of a family of copies of the \( G \)-module \( V \), and so it is injective. This proves (4), and (5) is an immediate consequence.

If \( n' \) is a maximal ideal of \( A^G \) such that \( f \notin n' \) then \( A_f^G = k \oplus A^G_f n' \), whence \( M_f = V \oplus M_f n' \), and \( M/Mn' \cong M_f/M_fn' \cong V \) as \( G \)-modules. Again by Lemma 3.5 \( \text{ind}_G^{G_x} M(y) \cong V \) for all \( y \in X_{G, \text{reg}} \cap X_M \) such that \( f(y) \neq 0 \). If \( x' \in X_{M, \text{inj}} \) is another point then, similarly, \( \text{ind}_G^{G_x} M(y) \cong V_{x'} \) for all \( y \) in a nonempty open subset of \( X \). Since \( X \) is irreducible, we conclude \( V_x \cong V_{x'} \), whence (3).

Suppose that \( N \in \mathcal{M}_A \) is free of finite rank over \( A \) and \( \varphi : N \to M \) is an epimorphisms in \( \mathcal{M}_A \). Let \( \varphi_x : N(x) \to M(x) \) be the epimorphism of \( G_x \)-modules obtained from \( \varphi \) by reduction modulo \( m_x \). Since \( M(x) \) is projective, there exists a \( G_x \)-module homomorphism \( \psi_x : M(x) \to N(x) \) such that \( \varphi_x \circ \psi_x = \text{id}_{M(x)} \). Put \( P = \text{Hom}_A(M, N) \). Then \( X_M \subset X_P \) and for \( x \in X_M \) there is an isomorphism of \( G_x \)-modules \( P(x) \cong \text{Hom}(M(x), N(x)) \cong M(x)^* \otimes N(x) \). Since \( k[G_x]^* \) is a Frobenius algebra, the \( G_x \)-module \( M(x)^* \) is injective. By [9], Part I, 3.10 \( P(x) \) is also injective. As we know already, there exists a \( G \)-submodule \( W \subset P \) such that \( P = W \oplus Pn \). By Lemma 3.5 the restriction of the canonical map \( W \to P/Pn \to P(x) \) yields a linear isomorphism \( W^G \cong P(x)^{G_x} \). Let \( \psi \in W^G \subset P^G \) be the element corresponding to \( \psi_x \in P(x)^G \). We may regard \( \psi \) as a morphism \( M \to N \) in \( \mathcal{M}_A \) whose reduction modulo \( m_x \) is \( \psi_x \). Then \( \gamma = \varphi \circ \psi \) is an \( \mathcal{M}_A \)-endomorphism of \( M \) whose reduction modulo \( m_x \) is the identity transformation of \( M(x) \). Let \( U \) be the set of those \( y \in X_M \) for which the reduction of \( \gamma \) modulo \( m_y \) is invertible. By [1], Ch. 2, §3, Corollary to Prop. 6 and §5, Prop. 2 \( U \) is open and consists precisely of those \( y \in X_M \) for which \( \gamma_{m_y} : M_{m_y} \to M_{m_y} \) is bijective. Since \( \gamma \) is \( G(k) \)-equivariant, \( U \) is \( G \)-invariant. As \( U = \pi^{-1}(U) \) and \( \pi(U) \) is an open neighbourhood of \( \pi(x) \) in \( X/G \), there exists \( f \in A^G \) such that \( x \in X_f \subset U \) where \( X_f = \{ y \in X \mid f(y) \neq 0 \} \). Then \( \gamma_f : M_f \to M_f \) is bijective, and therefore \( N_f = \ker \varphi_f \oplus \text{im} \varphi_f \). In other words, \( \varphi_f : N_f \to M_f \) is a split epimorphism in \( \mathcal{M}_{A_f} \). Since \( M \) is finitely generated over \( A \), it is an epimorphic image of a finitely generated free \( A \# k[G]^* \)-module. We can take the latter to be our \( N \). We see that \( M_f \) is a direct summand of a free \( A_f \# k[G]^* \)-module for a suitable \( f \).

Conversely, suppose that \( x \) is any point in \( X_{G, \text{reg}} \cap X_M \cap X_f \) such that \( M_f \) is a projective \( A_f \# k[G]^* \)-module. If \( n = m_x \cap A^G \) then \( M/Mn \cong M_f/M_fn \) is a projective \( (A/An) \# k[G]^* \)-module. By Theorem 2.1(2) \( A/An \cong k[G_x]^G \). The \( G_x \)-module \( M(x) \) corresponds to \( M/Mn \) under the category equivalence of the Imprimitivity Theorem. It is therefore projective, hence injective. We get (1).

Suppose that \( M \otimes_A K \) is projective in \( \mathcal{M}_K \). We want to show that \( M_f \) is projective in \( \mathcal{M}_{A_f} \) for a suitable \( 0 \neq f \in A^G \) and then apply (1). Since \( X_M \) is open and \( G \)-invariant, we may assume that \( X_M = X \) passing at the very beginning to a suitable localization of \( A \). Then \( M \) is projective as an \( A \)-module. Let \( \varphi : N \to M \) be an epimorphism in \( \mathcal{M}_A \) with \( N \) a free \( A \# k[G]^* \)-module. It extends to an epimorphism \( \varphi_K : N \otimes_A K \to M \otimes_A K \) in \( \mathcal{M}_K \). By our assumptions the latter
admits a splitting $\psi : M \otimes_A K \to N \otimes_A K$ in $\mathcal{M}_K$. Since $N$ is free over $A$, the localizations $N_f$ are identified with their images in $N \otimes_A K$, and the same is valid for $M$. Since $M$ is finitely generated over $A$, hence also over $A^G$, we have $\psi(M) \subset N_f$ for a suitable $f$. Then $\psi(M_f) = N_f$, which means that $\varphi_f : N_f \to M_f$ is a split epimorphism in $\mathcal{M}_{A_f}$. That completes the proof of (2). □

4. Actions with linearly reductive stabilizers.

We weaken our assumptions for this section considerably. In the next proposition $G$ is any affine group scheme over $k$, not necessarily finite, and $A$ is any $G$-algebra, not necessarily commutative. What we prove is a special case of results due to Doi [4] obtained in the context of coactions of Hopf algebras.

**Proposition 4.1.** The following properties of a $G$-algebra $A$ are equivalent:

1. All objects $M \in \mathcal{M}_A$ are injective $G$-modules.
2. There exist an injective $G$-module $Q$ and a homomorphism of $G$-modules $\psi : Q \to A$ such that $1 \in \psi(Q^G)$.
3. There exists a $G$-module homomorphism $\varphi : k[G] \to A$ (where $k[G]$ is given the left regular $G$-module structure) such that $\varphi(1) = 1$.
4. There are linear maps $\Phi_M : M \to M^G$, defined for each $M \in \mathcal{M}_A$, which are natural in $M$ and satisfy $\Phi_M(m) = m$ for all $m \in M^G$.
5. The functor $M \to M^G$ is exact on $\mathcal{M}_A$.
6. $A$ is a projective $(A,G)$-module.

If $A$ is commutative they are equivalent to another property:

7. Every object $M \in \mathcal{M}_A$ which is finitely generated and projective as an $A$-module is projective in $\mathcal{M}_A$.

**Proof.**

1. $\Rightarrow$ (2). By (1) $A$ is an injective $G$-module. So we can take $Q = A$ and $\psi = \text{id}_A$.

2. $\Rightarrow$ (3). Let $q \in Q^G$ be an element such that $\psi(q) = 1$. By injectivity of $Q$ the $G$-module homomorphism $k \to Q$ sending 1 to $q$ extends to a homomorphism $k[G] \to Q$. Composing the latter with $\psi$, we get $\varphi$.

3. $\Rightarrow$ (4). Define $\Phi_M$ as the composite map

$$M \xrightarrow{\mu^M} M \otimes k[G] \xrightarrow{\text{id}_M \otimes \varphi} M \otimes A \longrightarrow M$$

where the last map is afforded by the $A$-module structure on $M$. Recall that $\mu^M(M) = (M \otimes k[G])^G$. Since the two final maps in the decomposition of $\Phi_M$ are $G$-equivariant, we get $\Phi_M(M) \subset M^G$. If $m \in M^G$ then $\mu^M(m) = m \otimes 1$, whence $\Phi_M(m) = m$. That the maps $\Phi_M$ are natural in $M$ is clear.

4. $\Rightarrow$ (5). The fixed point functor is clearly left exact. Suppose that $\xi : M \to N$ is an epimorphism in $\mathcal{M}_A$. Given $n \in N^G$, take $m \in M$ such that $\xi(m) = n$. Then $\Phi_M(m) \in M^G$ and $\xi(\Phi_M(m)) = \Phi_N(\xi(m)) = n$. Thus $\xi$ induces a surjection $M^G \to N^G$.

5. $\Rightarrow$ (1). We may view $\text{Hom}(V,M) \cong V^* \otimes M$ for each finite dimensional $G$-module $V$ as an $(A,G)$-module taking the tensor product of $G$-module structures and letting $A$ operate on the second tensorand. If $W \subset V$ is a $G$-submodule then we have an epimorphism $\text{Hom}(V,M) \to \text{Hom}(W,M)$ in $\mathcal{M}_A$. Applying the fixed point functor, we deduce the surjectivity of the canonical map $\text{Hom}_G(V,M) \to$
Hom\(_G(W,M)\). Since all \(G\)-modules are locally finite dimensional, this gives the injectivity of \(M\).

(5) \(\Leftrightarrow\) (6). Every morphism \(A \to M\) in \(\mathcal{M}_A\) is given by the rule \(a \mapsto ma\) where \(m \in M^G\). Hence \(\text{Hom}_{(A,G)}(A,M) \cong M^G\). Note that the projectivity of \(A\) in \(\mathcal{M}_A\) means that the functor \(M \mapsto \text{Hom}_{(A,G)}(A,M)\) is exact.

(5) \(\Rightarrow\) (7). If \(M, N\) are \(A\)-modules, \(P = \text{Hom}_A(M,N)\) and \(B\) a commutative algebra then the canonical map \(P \otimes B \to \text{Hom}_{A \otimes B}(M \otimes B, N \otimes B)\) is bijective when \(M\) is free of finite rank, hence also when \(M\) is finitely presented. If \(M, N \in \mathcal{M}_A\) and \(M\) is finitely presented as an \(A\)-module then \(G(B)\) operates in \(P \otimes B\), naturally in \(B\). This gives \(P\) a \(G\)-module structure. Assuming \(A\) to be commutative, we have \(P \in \mathcal{M}_A\). If, moreover, \(M\) is projective as an \(A\)-module then every epimorphism \(N \to N'\) in \(\mathcal{M}_A\) induces an epimorphism \(\text{Hom}_A(M,N) \to \text{Hom}_A(M,N')\). Applying the fixed point functor, we deduce the surjectivity of the map \(\text{Hom}_{(A,G)}(M,N) \to \text{Hom}_{(A,G)}(M,N')\).

(7) \(\Rightarrow\) (6) is obvious. \(\square\)

Let \(X\) be an arbitrary scheme over \(k\), and \(G\) a finite group scheme operating on \(X\) from the right. We still need the assumption that \(X\) can be covered by \(G\)-invariant affine open subschemes. We say that the stabilizer \(G_x\) of a point \(x \in X(k)\) is linearly reductive if all \(G_x\)-modules are completely reducible. This is equivalent to the semisimplicity of the Hopf algebra \(k[G_x]^*\). By [3], Ch. IV, \(\S\)3, 3.6 \(G_x\) is linearly reductive if and only if its identity component \(G_x^0\) is diagonalizable and the index \((G_x : G_x^0)\) is prime to \(p = \text{char} k\) when \(p > 0\). Put

\[X_{\text{lin.reduced}} = \{x \in X(k) \mid G_x\text{ is linearly reductive}\}.

**Theorem 4.2.** The set \(X_{\text{lin.reduced}}\) consists precisely of those \(x \in X(k)\) which are contained in a \(G\)-invariant affine open subscheme \(U \subset X\) such that \(k[U]\) is an injective \(G\)-module. In particular, \(X_{\text{lin.reduced}}\) is the set of rational points of an open \(G\)-invariant subscheme of \(X\). If, moreover, \(X\) is an algebraic variety, then:

1. The condition \(X_{\text{lin.reduced}} \neq \emptyset\) is equivalent to each of the two below:
   a. \(k(X)\) is an injective \(G\)-module.
   b. The smash product algebra \(k(X) \# k[G]^*\) is semisimple.

2. For every \(x \in X_{G,\text{reg}} \cap X_{\text{lin.reduced}}\) there exist a \(G\)-invariant affine open neighbourhood \(U\) of \(x\) and a \(G\)-submodule \(V \subset k[U]\) such that \(V \cong \text{ind}_{G_x}^G k\) and the map \(V \otimes k[U]^G \to k[U]\) given by the multiplication in \(k[U]\) is bijective.

3. If \(X_{\text{lin.reduced}}\) is nonempty then there exists a \(G\)-submodule \(V \subset k[X]\) such that \(V \cong \text{ind}_{G_x}^G k\) for all \(x \in X_{G,\text{reg}} \cap X_{\text{lin.reduced}}\), and the map \(V \otimes k(X)^G \to k(X)\) given by the multiplication in \(k(X)\) is bijective.

**Proof.** We may assume that \(X\) is affine. Put \(A = k[X]\). Given \(x \in X(k)\), the orbit morphism \(\mu_x : G \to X\) determines a \(G\)-equivariant homomorphism of algebras \(\mu_x^* : A \to k[G]\) whose image is \(k[G_x \setminus G]\) by Proposition 1.1. If \(x \in X_{\text{lin.reduced}}\) then all \(G_x\)-modules are injective. Hence \(k[G_x \setminus G] = \text{ind}_{G_x}^G k\) is an injective \(G\)-module by [9], Part I, 3.9. As it is also projective, there is a \(G\)-submodule \(V \subset A\) mapped isomorphically onto \(k[G_x \setminus G]\) under \(\mu_x^*\). Take \(f \in V\) such that \(\mu_x^*(f) = 1\). Then \(f \in A^G\), and the map \(V \to A_f\), \(v \mapsto vf^{-1}\), is a \(G\)-module homomorphism under which \(f \mapsto 1\). Since \(V\) is an injective \(G\)-module, so is \(A_f\) too by implication (2) \(\Rightarrow\) (1) of Proposition 4.1. Furthermore, \(f(x) = 1\) since \(\ker \mu_x^* \subset m_x\). Thus \(\text{Spec} A_f\) is the required open neighbourhood of \(x\).
Conversely, suppose that $x \in U(k)$ where $U \subset X$ is a $G$-invariant affine open subscheme such that $k[U]$ is an injective $G$-module. As $\mu_x$ factors through $U$, it induces a $G$-equivariant algebra homomorphism $k[U] \to k[G_x \backslash G]$. Hence we may view $k[G_x \backslash G]$ as a $(k[U], G)$-module. By Proposition 4.1 $k[G_x \backslash G]$ is an injective $G$-module. It is then a direct summand of $k[G]$. By [9], Part I, 4.12 $k[G_x \backslash G]$ is also an injective $G_x$-module. Now $k$ is a direct summand of $k[G_x \backslash G]$ as a $G_x$-module. Hence $k$ is an injective $G_x$-module. Then all $G_x$-modules are injective, which implies that all $G_x$-modules are completely reducible.

Suppose that $X$ is an algebraic variety and $K = k(X)$. Apply Theorem 3.6 to the $(A, G)$-module $A$. Noting that $X_{\text{in.red.}}$ is precisely the set of points $x$ for which $A/m_x \cong k$ is an injective $G_x$-module, we get assertions (2) and (3) of Theorem 4.2. Furthermore, $X_{\text{in.red.}}$ is nonempty if and only if $K$ is a projective $(K, G)$-module. By Proposition 4.1 this is equivalent to $K$ being an injective $G$-module. This is equivalent also to the condition that every $M \in \mathcal{M}_K$ of finite dimension over $K$ is projective in $\mathcal{M}_K$. This means, in particular, that all ideals of the algebra $K \# k[G]^*$ are projective, which is equivalent to condition (b).

5. Invariants of restricted Lie algebras.

Suppose that $\text{char } k = p > 0$. Let $X$ be an affine algebraic variety, and $\mathfrak{g}$ a $p$-Lie algebra over $k$. Put $A = k[X]$ and $K = k(X)$. Define an action of $\mathfrak{g}$ on $X$ to be a homomorphism of $p$-Lie algebras $\rho : \mathfrak{g} \to \text{Der } A$ into the derivation algebra of $A$. Define $\mathfrak{g}_x \subset \mathfrak{g}$ to be the stabilizer of the maximal ideal $m_x$ of $A$ corresponding to a point $x \in X$. Since $\rho(\mathfrak{g})(m_x^2) \subset m_x$, we have a linear map $\mathfrak{g} \to T_x X = (m_x/m_x^2)^*$ whose kernel is precisely $\mathfrak{g}_x$. Hence $\text{codim}_\mathfrak{g} \mathfrak{g}_x \leq \dim T_x X$. Since the dimensions of tangent spaces are bounded, it is meaningful to define

$$c_\mathfrak{g}(X) = \max_{x \in X} \text{codim}_\mathfrak{g} \mathfrak{g}_x,$$

$$X_{\mathfrak{g}-\text{reg}} = \{ x \in X \mid \text{codim}_\mathfrak{g} \mathfrak{g}_x = c_\mathfrak{g}(X) \}.$$

If $\dim \mathfrak{g} < \infty$, there is a finite group scheme of height one $G = \mathfrak{G}(\mathfrak{g})$ associated with $\mathfrak{g}$ (see [3], Ch. II, §7, 3.9). One has $k[G] \cong u(\mathfrak{g})^*$ where $u(\mathfrak{g})$ is the restricted universal enveloping algebra of $\mathfrak{g}$. The action of $\mathfrak{g}$ on $X$ corresponds to a group action of $G$ according to [3], Ch. II, §7, 3.10. Furthermore, $G_x \cong \mathfrak{G}(\mathfrak{g}_x)$, so that $k[G_x \backslash G] \cong \text{Hom}_{u(\mathfrak{g}_x)}(u(\mathfrak{g}), k)$ and $(G : G_x) = p^{\text{codim}_\mathfrak{g} \mathfrak{g}_x}$ for all $x \in X$. It follows then that $X_{\mathfrak{g}-\text{reg}} = X_{G-\text{reg}}$. However, we want to extend Theorem 2.1 to the case of infinite dimensional $\mathfrak{g}$.

The Lie algebra $\text{Der } A$ has a natural $A$-module structure. Given $f \in A$ and $D, D' \in \text{Der } A$, we have

$$[fD, D'] = f[D, D'] - D'(f)D,$$

$$(fD)^p = f^pD^p + (fD)^{p-1}(f)D.$$

The first formula is easily checked straightforwardly. The second one is proved by Hochschild [8], Lemma 1. It follows that the $A$-submodule $L = A \cdot \rho(\mathfrak{g})$ is also a $p$-Lie subalgebra of $\text{Der } A$. Define a linear map

$$d : A \to L^*_A = \text{Hom}_A(L, A)$$

by the rule $(df)(D) = D(f)$ for $f \in A, D \in L$. 

16
**Lemma 5.1.** (1) \( c_\varphi(X) = c_L(X) \) and \( X_{\varphi,\text{reg}} = X_{L,\text{reg}} \).

(2) \( X_{L,\text{reg}} \) is open in \( X \) and consists precisely of those \( x \in X \) for which \( L_{mx} \) is a free \( A_{mx} \)-module and \( L^*_A = dA + mxL^*_A \).

(3) If \( X_{L,\text{reg}} = X \) then \( L \) is projective of rank \( c_L(X) \) over \( A \) and \( L^*_A = A \cdot dA \).

**Proof.** If \( L_x \) is the stabilizer of \( m_x \) in \( L \) then \( m_xL \subseteq L_x \), whence \( L = \rho(g) + L_x \). It follows that \( L/L_x \cong g/g_x \), and (1) is immediate.

Take a finite system of generators \( a_1, \ldots, a_n \) of the algebra \( A \) and define a homomorphism of \( A \)-modules \( \varphi : L \to F \), where \( F = A^n \), by the rule \( \varphi(D) = (Da_1, \ldots, Da_n) \) for \( D \in L \). Since each derivation of \( A \) is determined by its values on generators, we have \( \ker \varphi = 0 \). Hence \( L \cong F' \). Denote by \( I(x) \) the image of the map \( L/m_xL \cong F'/m_xF' \to F/m_xF \) induced by \( \varphi \). If \( D \in L \) then \( D \in L_x \) if and only if \( D(A) \subseteq mx \) (as \( A = k + mx \)), if and only if \( Da_i \in mx \) for all \( i \). It follows that \( I(x) \cong L/L_x \). Applying Lemma 1.2, we see that \( X_{L,\text{reg}} \) is open and coincides with the set of points \( x \in X \) for which \( F'_{mx} \) is a direct summand of the \( A_{mx} \)-module \( F_{mx} \), i.e., \( \varphi_{mx} : L_{mx} \to F_{mx} \) is a split monomorphism of \( A_{mx} \)-modules. Assuming that the \( A_{mx} \)-module \( L_{mx} \) is free, \( \varphi_{mx} \) splits if and only if the localization at \( m_x \) of the dual homomorphism \( \varphi^* : \text{Hom}_A(F, A) \to \text{Hom}_A(L, A) \) is surjective. By Nakayama's lemma this is equivalent to the equality \( L^*_A = N + mxL^*_A \) where \( N \) is the image of \( \varphi^* \). Clearly, \( N \) is the \( A \)-submodule of \( L^*_A \) generated by \( da_1, \ldots, da_n \). Since \( d(ab) = a \cdot db + b \cdot da \) for \( a, b \in A \), we have \( N = A \cdot dA \). Then \( N + mxL^*_A = dA + mxL^*_A \) since \( A = k + mx \). We get (2).

If \( x \in X_{L,\text{reg}} \) then the map \( F/m_xF \to F/m_xF \) is injective. Hence \( L_x = mxL \) and dim \( L/m_xL = c_L(X) \). Now (3) follows from (2) by globalization. \( \square \)

**Theorem 5.2.** The subset \( X_{\varphi,\text{reg}} \) is open in \( X \). Furthermore:

(1) If \( X_{\varphi,\text{reg}} = X \) then \( A \) is a projective \( A^g \)-module of rank \( p^{\varphi}(X) \).

(2) If \( x \in X_{\varphi,\text{reg}} \) and \( n = m_x \cap A^g \) then \( nA \) is a maximal \( g \)-invariant ideal of \( A \) and the algebra \( A/nA \) is \( g \)-equivariantly isomorphic with \( \text{Hom}_{u(g)}(u(g), k) \).

(3) If \( X_{\varphi,\text{reg}} = X \) then the assignment \( I \to I^g \) establishes a bijection between the \( g \)-invariant ideals of \( A \) and the ideals of \( A^g \). The canonical maps \( A^g \to (A/I)^g \) are surjective.

(4) If \( X_{\varphi,\text{reg}} = X \) then \( (B \otimes_{A^g} A)^g \cong B \) for every \( A^g \)-algebra \( B \) on which \( g \) operates trivially.

(5) \( [k(X) : k(X)^g] = p^{\varphi}(X) \).

**Proof.** As is immediate from the definition of \( L \), the \( L \)-invariants coincide with the \( g \)-invariants, and an ideal of \( A \) is stable under \( L \) if and only if it is stable under \( g \). Since \( g_x = \rho^{-1}(L_x) \), the algebra map \( \text{Hom}_{u(L_x)}(u(L), k) \to \text{Hom}_{u(g_x)}(u(g), k) \) induced by \( \rho \) is an isomorphism. It follows that all assertions of the theorem for the \( p \)-Lie algebra \( g \) are equivalent to corresponding assertions for the \( p \)-Lie algebra \( L \).

Put \( c = c(g)(X) = c_L(X) \).

Given \( x \in X_{L,\text{reg}} \), we have \( \dim L^*_A/m_xL^*_A = c \). Take \( a_1, \ldots, a_c \in A \) such that \( da_1, \ldots, da_c \) are a basis for a complement of \( m_xL^*_A \) in \( L^*_A \). Since the \( A_{mx} \)-module \( L_{mx} \) and its dual are free, passing to a suitable affine open neighbourhood of \( x \), we may assume that \( L \) is a free \( A \)-module and \( da_1, \ldots, da_c \) are a basis for \( L^*_A \) over \( A \). Let \( D_1, \ldots, D_c \) be the dual basis for \( L \) over \( A \). This means that \( D_i(a_l) = da_l(D_i) = \delta_{il} \) for all \( i, l \). As \( L \) is a Lie subalgebra, we have \( [D_i, D_j] = \sum_{l=1}^c g_{ijl} D_l \) for certain \( g_{ijl} \in A \). Applying the derivations on both sides of the equality to \( a_1 \), we deduce \( g_{111} = 0 \). Since \( L \) is closed under \( p \)-th powers, we have \( D^p_i = \sum_{l=1}^c h_{il} D_l \) for certain \( h_{il} \in A \).
We deduce similarly that \( h_{il} = 0 \). Thus the linear span \( a = \langle D_1, \ldots, D_r \rangle \subset L \) is an abelian Lie subalgebra with zero \( p \)-map. Since \( L = Aa \), the assertions of the theorem for \( L \) are equivalent to those for \( a \). Since \( \dim a < \infty \) they are equivalent also to the assertions of Theorem 2.1 for the corresponding action of the finite group scheme \( \mathfrak{G}(a) \) (in fact this action is free). □

**Corollary 5.3.** Suppose that \( h \subset g \) is a \( p \)-Lie subalgebra such that \( g = h + g_x \) for at least one \( x \in X_{p \text{-reg}} \). Then \( A^g = A^h \).

**Proof.** Obviously \( h_x = g_x \cap h \). By the hypotheses \( h_x / h_x \cong g_x / g_x \) for some point \( x \in X_{p \text{-reg}} \). Then \( c_h(X) \geq \text{codim}_p h_x = c_g(X) \). It follows that \([K : K^h] \geq [K : K^g] \).

On the other hand, \( K^g \subset K^h \), whence \( K^g = K^h \). We conclude that \( A^g = A \cap K^g = A \cap K^h = A^h \). □

For every \( r \geq 1 \) put \( A^{(p^r)} = \{ f^{(p^r)} : f \in A \} \). The notations \( K^{(p^r)} \), \( m_2^{(p^r)} \) will have a similar meaning. For \( f \in A \) let \( dx f : T_x X \to k \) denote the differential of \( f \) at \( x \).

**Theorem 5.4.** Suppose that \( X \) is a smooth affine variety and \( f_1, \ldots, f_n \in A^g \) where \( n = \dim X - c_g(X) \). Denote by \( U \) the open set of those \( x \in X \) for which \( dx f_1, \ldots, dx f_n \) are linearly independent. If \( U \neq \emptyset \) then \( K^h = K^{(p)}(f_1, \ldots, f_n) \). In particular, \( \text{dim}_X X \setminus U \geq 2 \) then:

1. \( A^g = A^{(p)}[f_1, \ldots, f_n] \) and \( A^g \) is free of rank \( p^n \) over \( A^{(p)} \).
2. \( A^g \) is a locally complete intersection.
3. If \( \pi : X \to X/\mathfrak{g} = \text{Spec} A^g \) is the canonical morphism then \( \pi(U) \) is the set of all smooth rational points of \( X/\mathfrak{g} \).

**Proof.** Put \( B = A^{(p)}[f_1, \ldots, f_n] \), \( Y = \text{Spec} B \), \( X^{(p)} = \text{Spec} A^{(p)} \). The scheme \( X^{(p)} \) is obtained from \( X \) by base change \( \tilde{f} : k \to k \) where \( \tilde{f} \) is the Frobenius automorphism of \( k \). Since smoothness is preserved under base change, \( X^{(p)} \) is smooth. Denote by \( \psi : Y \to X^{(p)} \) and \( \varphi : X \to Y \) the morphisms corresponding to the inclusions \( A^{(p)} \subset B \subset A \). Both \( \varphi \) and \( \psi \) are homeomorphisms. In particular, \( X \), \( Y \) and \( X^{(p)} \) have the same dimension. Put \( d = \dim X \).

For each commutative algebra \( R \) denote by \( \Omega_R \) the \( R \)-module of Kähler differentials of \( R \) over \( k \). By [11], (27.B), \( \dim_k \Omega_K = \deg \text{tr} K/k = d \) since \( K \) is separably generated over \( k \). Furthermore, if \( u_1, \ldots, u_d \in K \) are any elements such that \( du_1, \ldots, du_d \) are a basis for \( \Omega_K \) over \( K \) then the elements \( u_1^{m_1} \cdots u_d^{m_d} \) with \( 0 \leq m_i < p \) constitute a basis for \( K \) over \( K^{(p)} \). In particular, \([K : K^{(p)}] = p^d \).

We have \( \Omega_K \cong \Omega_A \otimes_A K \) where \( \Omega_A \) is a projective \( A \)-module since \( X \) is smooth (see [11], (29.B), Lemma 1). Assume that \( U \neq \emptyset \). If \( x \in U \) then \( df_1, \ldots, df_n \) are linearly independent modulo \( m_x \Omega_A \), hence constitute a basis for the direct summand of the free \( A_{m_x} \)-module \( (\Omega_A)_{m_x} \). In particular, \( df_1, \ldots, df_n \) are linearly independent over \( A_x \), hence also over \( K \). It follows that \([L : K^{(p)}] = p^n \) where \( L = K^{(p)}(f_1, \ldots, f_n) \) is the field of fractions of \( B \). Since \( L \subset K^g \) and \([K : L] = p^{d-n} = p^{\text{codim} X} = [K : K^g] \), we deduce \( L = K^g \).

By the above \( B \) is free over its subalgebra \( A^{(p)} \) with basis elements \( f_1^{m_1} \cdots f_n^{m_n} \) where \( 0 \leq m_i < p \). Then \( B \cong A^{(p)}[t_1, \ldots, t_n]/I \) where \( t_1, \ldots, t_n \) are indeterminates and \( I \) is the ideal of the polynomial algebra generated by \( n \) elements \( t_i^p - t_i^p \). This means that \( Y \) is isomorphic with the scheme-theoretic fibre \( F = \tau^{-1}(0) \) of the morphism \( \tau : X^{(p)} \times \mathbb{A}^n \to \mathbb{A}^n \) where \( \mathbb{A}^n \) is the affine space of dimension \( n \) and the components of \( \tau \) are the functions \( f_i^p - t_i^p \), \( i = 1, \ldots, n \). Note that \( F \) is a complete intersection in the smooth variety \( X^{(p)} \times \mathbb{A}^n \) since \( F \) has codimension \( n \). It follows that \( B \) is a locally complete intersection ring. In particular, \( B \) is Cohen-Macaulay.
The tangent space $T_z F$ at a point $z \in F$ coincides with the kernel of the linear map $d_z \tau : T_z(X^{(p)} \times \mathbb{A}^n) \to T_0 \mathbb{A}^n$ induced by $\tau$ in tangent spaces. Let $z = (x^{(p)}, a)$ where $x^{(p)} = (\psi \circ \varphi)(x) \in X^{(p)}$ for some $x \in X$ and $a \in \mathbb{A}^n$. It is easy to differentiate $\tau$: for $(u, v) \in T_{x^{(p)}} X^{(p)} \oplus T_0 \mathbb{A}^n \cong T_Z(X^{(p)} \times \mathbb{A}^n)$ the vector $(d_z \tau)(u, v) \in T_0 \mathbb{A}^n \cong k^n$ has components $(d_{x^{(p)}} f^p_i)(u)$, $i = 1, \ldots, n$. Note that $T_{x^{(p)}} X^{(p)} \cong T_Z X \otimes_k k$ and the maps $d_{x^{(p)}} f^p_i : T_Z X \otimes_k k \to k$ are just $d_x f_i \otimes \text{id}_k$ in this realization. The variety $F$ is smooth at $z$ if and only if $d_z \tau$ is surjective, if and only if $d_{x^{(p)}} f^p_1, \ldots, d_{x^{(p)}} f^p_n$ are linearly independent, if and only if $d_x f_1, \ldots, d_x f_n$ are linearly independent. In other words, the smoothness of $Y$ at $\varphi(x)$ is equivalent to the inclusion $x \in U$. The codimension of the closed subset $Y \cap \varphi(U)$ in $Y$ is equal to that of $X \cap U \subset X$. Suppose that it is at least 2. Then $Y$ is smooth in codimension 1. By Serre’s normality criterion $B$ is integrally closed (see [11], (17.I)). Then $A^0 = B$ since both algebras have the same field of fractions. □

Suppose that $\mathfrak{g} = \text{Lie} \mathcal{G}$ where $\mathcal{G}$ is a reduced algebraic group operating on $X$ from the right. Then there is the induced action of $\mathfrak{g}$ on $X$. For $x \in X$ denote by $\mathcal{G}_x$ the scheme-theoretic stabilizer of $x$ in $\mathcal{G}$. Let $X_{\text{reg}} \subset X$ be the open subset consisting of points $x$ for which the orbit $x \mathcal{G}$ has a maximal possible dimension. Theorem 5.5. Suppose that $X$ is a smooth affine variety and $f_1, \ldots, f_n \in A^G$ where $n = \dim X - c_{\mathfrak{g}}(X)$. Suppose also that the open set $U$ introduced in theorem 5.4 is nonempty. Then $X_{\mathfrak{g}_{\text{reg}}} = \{ x \in X_{\text{reg}} \mid \mathcal{G}_x \text{ is reduced} \}$. If $G$ denotes the $r$-th Frobenius kernel of $\mathcal{G}$ for some $r \geq 1$ then $K^G = K^{(r)}(f_1, \ldots, f_n)$. If, moreover, codim $X \cap U \geq 2$ then:

1. $A^G = A^{(r)}[f_1, \ldots, f_n]$ and $A^G$ is free of rank $r^n$ over $A^{(r)}$.

2. $A^G$ is a locally complete intersection.

3. $\pi(U)$ is the set of all smooth rational points of $X/G$ where $\pi : X \to X/G$ is the canonical morphism.

Proof. Consider the morphism $\varphi : X \to \mathbb{A}^n$ with components $f_1, \ldots, f_n$. Let $x \in U$. The differential $d_x \varphi : T_x X \to k^n$ is then surjective. By [3], Ch. I, §4, 4.15 $\varphi$ is smooth, hence also flat at $x$. Then $\dim_x F_x = \dim X - \dim \mathbb{A}^n = d - n$ by [3], Ch. I, §3, 6.3, where $F_x = \varphi^{-1}(\varphi(x))$ and $d = \dim X$. Since $F_x$ is a $\mathcal{G}$-invariant closed subscheme of $X$, we have $x \mathcal{G} \subset F_x$, and so $\dim x \mathcal{G} \leq d - n = c_{\mathfrak{g}}(X)$.

Since $U$ is open in $X$, we get $\dim x \mathcal{G} \leq c_{\mathfrak{g}}(X)$, hence also $\dim \mathcal{G}_x \geq \dim \mathcal{G} - c_{\mathfrak{g}}(X)$ for all $x \in X$. As $\mathcal{G} = \text{dim} \mathfrak{g}$, we can rewrite the last inequality in the form

$$c_{\mathfrak{g}}(X) - \text{codim}_{\mathfrak{g}} \mathcal{G}_x \geq \dim \mathcal{G}_x - \dim \mathcal{G}.$$  \hfill (*)

The subset $X_{\mathfrak{g}_{\text{reg}}}$ consists of those $x$ for which $\dim x \mathcal{G} = c_{\mathfrak{g}}(X)$, which is equivalent to an equality in (*). By [3], Ch. III, §2, 2.6 Lie$\mathcal{G}_x = \mathcal{G}_x$. Furthermore, $\dim \mathcal{G}_x \geq \dim \mathcal{G}_x$ and the equality holds here precisely when $\mathcal{G}_x$ is smooth (which is equivalent to $\mathcal{G}_x$ being reduced for an algebraically closed field) by [3], Ch. II, §5, 2.1. As is easy to see, we have equalities everywhere above if and only if the left hand side of (* is zero, i.e., $x \in X_{\mathfrak{g}_{\text{reg}}}$. This proves the first assertion of the theorem.

We have $[G] = p^{\dim \mathfrak{g}}$ (see [9], Part I, 9.6, (2)). Next, $G_x = G \cap \mathcal{G}_x$ for all $x \in X$. By [9], Part I, 9.4, (2) $G_x$ coincides with the $r$-th Frobenius kernel of $\mathcal{G}_x$. If $x \in X_{\mathfrak{g}_{\text{reg}}}$ then $G_x$ is reduced, whence $[G_x] = p^{\dim \mathcal{G}_x}$, and $[G : G_x] = [G] / [G_x] = p^{\text{codim}_{\mathfrak{g}} \mathcal{G}_x}$. Since both $X_{G_{\text{reg}}}$ and $X_{\mathfrak{g}_{\text{reg}}}$ are open and nonempty, they have a common point, which shows that $q(X) = p^{\text{reg}(X)}$ in the notations of Theorem 2.1. We deduce that $[K : K^G] = p^{\text{reg}(X)}$. 19
Let $L_i = K^{(p^i)}(f_1, \ldots, f_n)$ for each $i \geq 1$. If $i > 1$ then $K^{(p^i)}(f_1, \ldots, f_n) \subset L_i \subset L_i$. As we have seen in Theorem 5.4 the elements $f_1^{m_1} \cdot \cdots \cdot f_n^{m_n}$ with $0 \leq m_i < p$ are linearly independent over $K^{(p)}$. It follows that $[L_i : L_i^{(p^i)}] = p^n$. Hence

$$[L_i : K^{(p^i)}] = p^n[L_i^{(p^i)} : K^{(p^i)}] = p^n[L_i^{(p^i)} : K^{(p^i-1)}].$$

We have also $[K : K^{(p^i)}] = [K : K^{(p)}] \cdot [K^{(p)} : K^{(p^i)}] = p^{d_1}K : K^{(p^i-1)}]$. Proceeding by induction on $i$ we deduce that $[L_i : K^{(p^i)}] = p^{d_1}$ and $[K : K^{(p^i)}] = p^{d_1}$. Taking $i = r$, we get $[K : L_r] = p^{d_1}$. Since $L_r \subset K^{G}$, it follows $L_r = K^{G}$. The remainder of the theorem is proved in the same way as Theorem 5.4 with obvious changes.

Two classical cases of Theorem 5.5 are those when $G$ is a semisimple algebraic group operating either on $g$ via the adjoint representation or on itself by conjugations. Let $n$ denote the rank of $G$. Under assumption that $p$ does not divide the order of the Weyl group of $G$ it was shown by Veldkamp [21] that $k[g]^G$ is generated by $n$ algebraically independent polynomials $J_1, \ldots, J_n$ and $g_{reg}$ consists precisely of those $x \in g$ for which $d_x J_1, \ldots, d_x J_n$ are linearly independent. The complement of $g_{reg}$ has pure codimension 3 in $g$. The stabilizer $g_x$ is just the centralizer of $x$ in $g$.

As $\dim g_x = n$ for all $x \in g_{reg}$, we have $c_1(g) = \dim g - n$.

Suppose that $G$ is simply connected. Then the algebra of regular functions on $G$, constant on the conjugacy classes, is generated by the characters $\chi_1, \ldots, \chi_n$ of fundamental irreducible representations of $G$. As shown by Steinberg [18], $G_{reg}$ consists precisely of those $x \in G$ for which $d_x \chi_1, \ldots, d_x \chi_n$ are linearly independent. The complement of $G_{reg}$ in $G$ again has codimension 3. If $x \in G$ then $\mathfrak{g}_x = \ker d_x \mu_x$ where $\mu_x : G \rightarrow G$ is the morphism defined by the rule $y \mapsto y^{-1} xy$. It follows that $\mathfrak{g}_x = \{v \in g \mid (Ad x)v = v\}$. If $T \subset G$ is a maximal torus then there exists $t \in T$ such that $a(t) \neq 1$ for all roots $a$. Then $\mathfrak{g}_t = \text{Lie } T$, and so $c_1(G) = \dim G - n$. No restrictions on $p$ are needed in this case. The invariants of $g$ and Frobenius kernels were described by Friedlander and Parshall [6], and Donkin [5].

We give yet another example showing that Theorem 5.4 has a wider range of applications. Let $g = W_n$ be the Jacobson-Witt algebra. Recall that $g = \text{Der } B_n$ where $B_n = k[x_1, \ldots, x_n]$, $x_i^p = 0$, is the truncated polynomial algebra. If $G = \text{Aut } B_n$ then $\text{Lie } G$ is the subalgebra of codimension $n$ in $g$ consisting of derivations that leave stable the maximal ideal $\mathfrak{n}$ of $B_n$. For $D \in g$ denote by $\chi_D(t)$ the characteristic polynomial of $D$ as a linear transformation of $B_n$. As is proved by Premet in [17], $\chi_D(t) = t^n + \sum_{i=0}^{n-1} \psi_i(D)t^i$ where $\psi_i$ are algebraically independent polynomial functions generating the algebra $k[g]^G$. There exists an open subset of $g$ consisting of elements $D$ such that $\dim g_D = n$ and $g = \text{Lie } G \oplus g_D$ where $g_D$ is the centralizer of $D$ in $g$ ([17], Lemma 1). Hence $c_1(g) = d - n$ where $d = \dim g$, and $\psi_0, \ldots, \psi_{n-1}$ are $g$-invariant according to Corollary 5.3. Let $\varphi : g \rightarrow \mathbb{A}^n$ be the morphism with components $\psi_0, \ldots, \psi_{n-1}$ and $U$ the subset of those $D \in g$ for which $d_D \psi_0, \ldots, d_D \psi_{n-1}$ are linearly independent. Premet proved that each fibre $F_D = \varphi^{-1}(\varphi(D))$ is irreducible of dimension $d - n$ and $F_D \cap U$ is nonempty ([17], Lemmas 12 and 13).

Put $U_1 = \{D \in g \mid \psi_0(D) \neq 0\}$. If $D \in U_1$, then $D$ is a linear combination of $D^p, \ldots, D^{p^n}$ as $D^n + \sum_{i=1}^{n-1} \psi_i(D)D^p = 0$. Hence $D$ is semisimple, and we can find its eigenvectors $y_1, \ldots, y_n \in B_n$ such that $B_n = \langle y_1, \ldots, y_n \rangle \oplus (k + n^2)$. Then the monomials $y_1^{m_1} \cdots y_n^{m_n}$ with $0 \leq m_i < p$ constitute a basis for $B_n$. Let $\lambda_1$ be the eigenvalue of $y_i$. Since the rank of $D$ as a linear transformation is equal to $p^n - 1,$
the equality $\sum m_i \lambda_i = 0$ can hold only for $m_1 = \ldots = m_n = 0$. This implies that $D$ generates a torus of dimension $n$ in $g$. If $D' \in g_D$ then

$$n^{-1} \sum_{i=0}^{n-1} (d_D \psi_i)(D') D^p = -\psi_0(D) D',$$

which is a special case of [17], Lemma 7, (i). Taking $D' = D^p$ where $0 \leq j < n$, we see that $(d_D \psi_i)(D') \neq 0$ only for $i = j$. Hence $U_1 \subset U$. Suppose that $Z$ is an irreducible component of the closed subset $g \setminus U_1$ having codimension 1 in $g$ (in fact it can be shown that $\psi_0$ is irreducible). Note that $\varphi(Z) \neq k^n$ as $\psi_0(Z) = \{0\}$. By the theorem on dimensions of fibres we have $\dim Z \cap F_D \geq \dim Z - \dim \varphi(Z) \geq d - n$ for all $D \in Z$. It follows that $Z$ is a union of fibres of $\varphi$. In particular, $Z \cap U \neq \emptyset$. We deduce that $\text{codim}_g g \setminus U \geq 2$. Thus we meet the hypotheses of Theorem 5.4:

**Corollary 5.6.** If $A$ denotes the algebra of polynomial functions on $W_n$ then $A^{W_n} = A^{(p)}[\psi_0, \ldots, \psi_{n-1}]$. Moreover, $A^{W_n}$ is free of rank $p^n$ over $A^{(p)}$ and is a locally complete intersection.

In conclusion we make comments concerning the results of section 4. Assume that $\dim g < \infty$. According to [7] the algebra $u(g_x)$ is semisimple if and only if $g_x$ is a torus. Thus Theorem 4.2 says that $g_x$ is toral if and only if $x$ lies in an affine open subset $U \subset X$ such that $k[U]$ is an injective $u(g)$-module. Such points $x$ exist if and only if $k(X)$ is an injective $u(g)$-module. A. Premet pointed out to me that the openness of the set of points with a toral $g_x$ can be proved by geometric arguments.

**References**

1. N. Bourbaki, Commutative Algebra, Springer, Berlin, 1989.
2. E. Cline, B. Parshall and L. Scott, A Mackey imprimitivity theory for algebraic groups, Math. Z. **182** (1983) 447–471.
3. M. Demazure and P. Gabriel, Groupes Algébriques I, Masson, Paris, 1970.
4. Y. Doi, Algebras with total integrals, Comm. Algebra **13** (1985) 2137–2159.
5. S. Donkin, Infinitesimal invariants of algebraic groups, J. London Math. Soc. **45** (1992) 481–490.
6. E.M. Friedlander and B.J. Parshall, Rational actions associated to the adjoint representation, Ann. Sci. École Norm. Sup. **20** (1987) 215–226.
7. G.P. Hochschild, Representations of restricted Lie algebras of characteristic $p$, Proc. Amer. Math. Soc. **5** (1954) 603–605.
8. G.P. Hochschild, Simple algebras with purely inseparable splitting fields of exponent 1, Trans. Amer. Math. Soc. **79** (1955) 477–489.
9. J. Jantzen, Representations of algebraic groups, Academic Press, 1987.
10. M. Koppinen and T. Neuvonen, An imprimitivity theorem for Hopf algebras, Math. Scand. **41** (1977) 193–198.
11. H. Matsumura, Commutative Algebra, Second Edition, Benjamin, 1980.
12. A.A. Mil'ner, Irreducible representations of modular Lie algebras, Izv. Akad. Nauk SSSR Ser. Mat. **39** (1975) 1240–1259 [In Russian]. Translation in Math. USSR Izv. **9** (1975) 1169–1187.
13. S. Montgomery, Hopf algebras and Their Actions on Rings, CBMS Regional Conference Series in Mathematics, Vol. 82, American Mathematical Society, 1993.
14. D. Mumford, Abelian Varieties, Oxford University Press, Oxford, 1970.
15. W.D. Nichols and M.B. Zoeller, A Hopf algebra freeness theorem, Amer. J. Math. \textbf{111} (1989) 381–385.
16. U. Oberst and H.-J. Schneider, Über Untergruppen endlicher algebraischer Gruppen, Manuscripta Math. \textbf{8} (1973) 217–241.
17. A.A. Premet, The theorem on restriction of invariants and nilpotent elements in $W_n$, Mat. Sbornik \textbf{182} (1991) 746–773 [In Russian]. Translation in Math. USSR Sbornik \textbf{73} (1992) 135–159.
18. R. Steinberg, Regular elements of semisimple algebraic groups, IHES Publ. Math. \textbf{25} (1965) 49–80.
19. M.E. Sweedler, Hopf Algebras, Benjamin, New York, 1969.
20. M. Takeuchi, Relative Hopf modules—equivalences and freeness criteria, J. Algebra \textbf{60} (1979) 452–471.
21. F.D. Veldkamp, The center of the universal enveloping algebra of a Lie algebra in characteristic $p$, Ann. Sci. École Norm. Sup. \textbf{5} (1972) 217–240.
22. W.C. Waterhouse, Geometrically reductive affine group schemes, Arch. Math. \textbf{62} (1994) 306–307.