§2. Galois Theory

conclusion of the Bergman-Roseblade Theorem can be rewritten—every element in P has a unique representation $\Sigma f(b)b$ where $b \in B$ and $f(b) \in P \cap k[D]$. Thus $k[A]$ is the group ring $(k[D])[B]$ for a finitely generated free abelian group B.

Roseblade proves that the fixed ring $(k[A])^G$ lies in $k[D]$ ([10], Lemma 10). This will also be a consequence of the first lemma in the next section. In any event, it has a remarkable consequence.

THEOREM 1. *Assume that G is an arbitrary group acting multiplicatively on $k[A]$. Then $k[A]^G$ is finitely generated.*

Proof. As we have remarked, $(k[A])^G = (k[D])^G$. But G acts like a finite group of automorphisms on the affine algebra $k[D]$. Noether's Theorem ([11]), states that, in this case, the algebra of invariants is a finitely generated algebra. □

This is an unexpected surprise. In contrast to the situation for linear actions, Hilbert's 14th problem holds for multiplicative actions without any restriction on the group!

The theme of the paper has emerged. A theory of invariants for multiplicative actions is ultimately a theory for finite groups.

§ 2. GALOIS THEORY

We begin this section by establishing an analogue to the "finiteness" phenomenon of the previous section, for a multiplicative action of G on $k(A)$. Notation is taken from § 1.

LEMMA 2. *Suppose that G acts multiplicatively on $k(A)$. Then $k(A)^G \subset k(D)$.*

Proof. The crucial fact is that $k(D)[B]$ is a unique factorization domain. If ${}^g f = f$ for $f \in k(A)$ then we can write $f = \alpha/\beta$ where α and β in $k(D)[B]$ have no common factors. The invariance of f becomes

$$({}^g\alpha)\beta = ({}^g\beta)\alpha \quad \text{for all} \quad g \in G .$$

Hence $\alpha \mid {}^g\alpha$ and ${}^g\alpha \mid \alpha$; we have $({}^g\alpha)\alpha^{-1}$ a unit in $k(D)[B]$. A similar result holds for β.

$${}^g\alpha = u(g)\alpha \quad \text{and} \quad {}^g\beta = w(g)\beta$$

for $u(g), w(g) \in k(D)^* \cdot B$.

It is easy to check that $u: G \to k(\underline{D})^* \cdot B$ is a crossed homomorphism. Define a "crossed" action of G on the set $k(\underline{D})^* \cdot B$ by $g \circ x = u(g)^{-1}({}^g x)$. This extends additively to an action of G on $k(\underline{D})[B]$. The defining equation for u now says $g \circ \alpha = \alpha$. Consequently, when we write out α as a non-redundant sum of elements in $k(\underline{D})^* \cdot B$,

$$\alpha = \sum_{j=1}^{N} r_j b_j \quad (b_j \text{ distinct})$$

G permutes these terms (under the crossed action). There is a subgroup H of finite index in G which fixes each term.

As we observed in the previous section, $C_G(D)$ is a subgroup of finite index in G which centralizes $k(\underline{D})$ under the ordinary action. Thus

$${}^g b_i = u(g) b_i \quad \text{for all} \quad g \in C_H(D) \quad \text{and} \quad i = 1, \ldots, N .$$

It follows that ${}^g(b_i b_j^{-1}) = b_i b_j^{-1}$ for all $g \in C_H(D)$. Since $|\, G : C_H(D) \,| < \infty$, we find that $b_i b_j^{-1} \in D$. Thus $\alpha = r_1 b_1$.

A parallel result holds for β. We conclude that $f = \xi b$ where $\xi \in k(\underline{D})^*$ and $b \in B$. Now ${}^g(\xi b) = \xi b$ for all $g \in C_H(D)$. Therefore ${}^g b = b$ for all such g, whence $b \in D \cap B = 1$. We have $f = \xi$, as desired. □

The argument we have just completed proves a bit more. We shall record the exact statement now and return to discuss it at the end of the section.

LEMMA 2′. *Suppose that G acts multiplicatively on $k(\underline{A})$. If U denotes the group of units for $k(\underline{D})[B]$ then the sequence*

$$1 \to H^1(G, U) \to H^1(G, k(\underline{A})^*)$$

is exact. □

THEOREM 3. *$k(\underline{A})^G$ is the field of fractions of $k[\underline{A}]^G$.*

Proof. According to Lemma 2, it suffices to check that $k(\underline{D})^G$ lies in the field of fractions of $k[\underline{D}]^G$. The improvement lies in the fact that G acts like a finite group of automorphisms on $k(\underline{D})$. For finite group actions, the theorem is always true ([11], Lemma 2.5.12). (Briefly, every $\alpha \in k[\underline{A}]$ divides its norm $N(\alpha) = \prod_{g \in G} ({}^g\alpha)$, so every element in $k(\underline{A})$ can be written as a fraction with an invariant denominator. If such a fraction is invariant, then its numerator must be invariant as well.) □

THEOREM 4. $\text{tr. deg.}\,(k(\underline{A}) \mid k(\underline{A})^G) = \text{rank}\, A/D$.

Proof. Once again, Lemma 2 tells us that $k(\underline{A})^G = k(\underline{D})^G$. Elementary Galois Theory tells us that $k(\underline{D})$ is a finite field extension of $k(\underline{D})^G$. Hence the transcendancy degrees of $k(\underline{A}) \mid k(\underline{A})^G$ and $k(\underline{A}) \mid k(\underline{D})$ are the same.

On the other hand, the Bergman-Roseblade Theorem implies that $k(\underline{A})$ is the field of fractions of $k(\underline{D})[B]$. Since B is a free abelian group, $k(\underline{A})$ is the rational function field in rank B variables over the base field $k(\underline{D})$. Thus

$$\text{tr. deg.}\,(k(\underline{A}) \mid k(\underline{D})) = \text{rank}\, B = \text{rank}\, A/D\,. \qquad \square$$

As promised, we complete this portion of the paper with some remarks about Lemma 2′. In one sense, it measures an obstruction to the truth of Hilbert's Theorem 90 for multiplicative actions. Of course there is an intimate connection between invariant theory and crossed homomorphisms. Suppose that Λ is any k-algebra and G acts as a group of k-algebra automorphisms of Λ. If $\lambda \in \text{Hom}(G, k^*)$ then a semi-invariant with weight λ is a nonzero element f in Λ such that ${}^g f = \lambda(g) f$ for all $g \in G$. The vanishing of $H^1(G, k(\underline{A})^*)$ is a statement about the triviality of semi-invariants. To be more precise, we add a condition which separates k and $\underline{A}$.

PROPOSITION 5. *Assume that* $k^* \cap \underline{A} = 1$. *Then*

$$1 \to \text{Hom}(G/C_G(D), k^*) \to \text{Hom}(G, k^*) \to H^1(G, k(\underline{A})^*)$$

is exact.

Proof. Let $M = \ker(\text{Hom}(G, k^*) \to H^1(G, k(\underline{A})^*))$. The problem is to prove that $M = \{\lambda \in \text{Hom}(G, k^*) \mid \lambda(C_G(D)) = 1\}$.

First suppose that $\lambda \in M$. Then there is a nonzero $f \in k(\underline{A})$ such that ${}^g f = \lambda(g) f$ for all $g \in G$. By Lemma 2′, we can write $f = \xi b$ for some $\xi \in k(\underline{D})^*$ and $b \in B$. If $g \in C_G(D)$ then ${}^g b = \lambda(g) b$ which, in turn, implies that $\lambda(g) = ({}^g b) b^{-1} \in k^* \cap \underline{A}$. We conclude that λ vanishes on $C_G(D)$.

For the opposite inclusion, assume that $\lambda(C_G(D)) = 1$. Then $\lambda \in \text{Hom}(\mathscr{G}, k^*)$ where $\mathscr{G} = G/C_G(D)$ is a finite group of automorphisms of $k(\underline{D})$. Hilbert's Theorem 90 now applies: $H^1(\mathscr{G}, k(\underline{D})^*) = 1$. Certainly the image of $\text{Hom}(\mathscr{G}, k^*)$ in $H^1(\mathscr{G}, k(\underline{D})^*)$ is trivial. In other words, there is an $\eta \in k(\underline{D})^*$ such that ${}^t\eta = \lambda(t)\eta$ for $t \in \mathscr{G}$. Clearly ${}^g\eta = \lambda(g)\eta$ for $g \in G$. Thus λ vanishes in $H^1(G, k(\underline{A})^*)$. $\square$

A similar application of Lemma 2′ will yield the analogue of Theorem 3 for semi-invariants: if $k^* \cap \underline{A} = 1$ then

$$k(\underline{A})^G_\lambda = (k[\underline{A}]^G)^{-1}(k[\underline{A}]^G_\lambda).$$

Recall that $G/C_G(D)$ is a finite group. Hence $\mathrm{Hom}(G/C_G(D), k^*)$ is finite. Consequently, when $\mathrm{Hom}(G, k^*)$ is infinite the proposition implies that $H^1(G, k(\underline{A})^*) \neq 1$. It is quite plausible (under the assumption $k^* \cap \underline{A} = 1$) that $H^1(G, k(\underline{A})^*)$ vanishes if and only if G is finite.

The extra bothersome assumption is vacuous in the case of group algebras. One can read off the following observation from Lemma 2′.

PROPOSITION 6. *Assume that* $D = 1$. *Then*

$$1 \to \mathrm{Hom}(G, k^*) \times H^1(G, A) \to H^1(G, k(A)^*) \quad \textit{is exact}. \qquad \square$$

I have been unable to determine if the injection given by the proposition always splits. Here is one situation where it does.

PROPOSITION 7. *Suppose that* A *can be fully ordered so that* G *acts as a group of order automorphisms of* A. *Then the natural map*

$$H^1(G, k^* \cdot A) \to H^1(G, k(A)^*)$$

splits.

Proof. Let $V: k[A]\backslash\{0\} \to k^* \cdot A$ be the function which sends an element to its "lowest term" with respect to the ordering. The usual degree argument which shows that a polynomial ring is a domain, establishes that V is multiplicative. Since elements of G act monotonically, V is a map of (multiplicative) G-modules. It is not difficult to check that V extends to a multiplicative G-map from $k(A)^*$ to $k^* \cdot A$.

Obviously $k^* \cdot A \to k(A)^* \xrightarrow{V} k^* \cdot A$ provides the necessary splitting. $\square$

The hypothesis of Proposition 7 is very restrictive, even for an infinite cyclic group G. We leave the following long exercise to the reader. A matrix in $GL(n, \mathbf{Z})$ is order preserving for some ordering on $\mathbf{Z}^n$ and only if each rational irreducible factor of its characteristic polynomial has a positive real root.

§ 3. THE SHEPHARD-TODD-CHEVALLEY THEOREM

Recall that a matrix in $GL(n, \mathbf{C})$ is a pseudo-reflection if it has finite order and 1 is an eigenvalue of multiplicity $n - 1$. The remaining eigenvalue for a pseudo-reflection must be a root of unity; when it is -1 we call