ON THE ALGEBRAIC HULL OF A LIE ALGEBRA

G. HOCHSCHILD

Let $F$ be a field of characteristic 0, and let $V$ be a finite dimensional vector space over $F$. Let $E$ denote the algebra of all endomorphisms of $V$, and let $L$ be any Lie subalgebra of $E$. Among the algebraic Lie algebras contained in $E$ and containing $L$, there is one that is contained in all of them, and this is called the algebraic hull of $L$ in $E$. Here, an algebraic Lie algebra is defined as the Lie algebra of an algebraic group. It is an easy consequence of the definitions that if $A$ and $B$ are algebraic groups of automorphisms of $V$ such that $A \subseteq B$ then the Lie algebra of $A$ is contained in the Lie algebra of $B$. Hence the existence of the algebraic hull of $L$ is an immediate consequence of the following basic result: let $G$ be the intersection of all algebraic groups of automorphisms of $V$ whose Lie algebras contain $L$. Then the Lie algebra of $G$ contains $L$.

This theorem reduces at once to the case where $L$ is one dimensional. For any $x \in E$, let $G_x$ be the intersection of all algebraic groups of automorphisms of $V$ whose Lie algebras contain $x$. Then we have $G_x \subseteq G$, whenever $x \in L$, and it suffices to show that the Lie algebra of $G_x$ contains $x$. This is part of [1, Theorem 10, p. 165], but it is not clear from the proof given in [1] that, although this result is not as obvious as it might seem at first sight, it can be proved quite directly without invoking any special knowledge of algebraic groups. The proof we give here is based on the simple idea of recovering $G_x$ from its generic point $\exp(tx)$.

We use an auxiliary variable $t$ over $F$ and introduce the ring $F\{t\}$ of the integral power series in $t$ with coefficients in $F$. Let $E^*$ denote the dual space of $E$, and let $P$ be the algebra of all polynomial functions on $E$. The elements of $E^*$ are canonically extended to become $F\{t\}$-linear maps of $E \otimes F\{t\}$ into $F\{t\}$, and the elements of $P$ are extended accordingly to become $F\{t\}$-valued functions on $E \otimes F\{t\}$. With $x \in E$, we interpret the formal power series $\exp(tx)$ as the element of $E \otimes F\{t\}$ that is determined by the conditions

$$p(\exp(tx)) = \sum_{n=0}^{\infty} \frac{p(x^n)}{n!} t^n,$$

for every $p \in E^*$.

Now we consider the $F$-algebra homomorphism $p \mapsto p(\exp(tx))$ of

Received by the editors June 2, 1959.
$P$ into $F\{t\}$. The elements $e \in E$ operate as algebra endomorphisms on $P$ by left and right translation, as follows: for $p \in P$, we define the left translate $e \cdot p \in P$ and the right translate $p \cdot e \in P$ by

$$(e \cdot p)(z) = p(ze), \quad \text{and} \quad (p \cdot e)(z) = p(ez),$$

for all $z \in E$. We shall denote by $D_x$ the derivation of $P$ that annihilates $F$ and coincides with the left translation $p \rightarrow x \cdot p$ on $E^*$. Clearly, $D_x$ commutes with every right translation. Let $\delta$ denote the derivation with respect to $t$ on $F\{t\}$. It follows easily from the definitions that

(1) $D_x(p)(\exp(tx)) = \delta(p(\exp(tx))), \quad \text{for every } p \in P.$

Let $Q$ be the kernel of our homomorphism $p \rightarrow p(\exp(tx))$, and let $G$ be the set of all automorphisms of $V$ that are zeros of $Q$. We shall show that $G$ coincides with the group $H$ of all automorphisms $e$ of $V$ for which $Q \cdot e = Q$.

If $I$ denotes the identity automorphism of $V$ then, for every $p \in P$, $p(I)$ is the constant term of $p(\exp(tx))$, and we have

(2) $p(\exp(tx)) = \sum_{n=0}^{\infty} \frac{1}{n!} D^n_x(p)(I)t^n.$

From this we see easily that $H \subset G$. Now let $e \in G$ and $p \in Q$. By (1), we have $D^n_x(p) \in Q$, for all $n \geq 0$. Hence

$$D^n_x(p \cdot e)(I) = (D^n_x(p) \cdot e)(I) = D^n_x(p)(e) = 0, \quad \text{for all } n \geq 0.$$ 

By (2), this implies that $p \cdot e \in Q$. Thus $Q \cdot e \subset Q$. If $Q_n$ denotes the subspace of $Q$ consisting of the elements of degree $\leq n$, it follows that $Q_n \cdot e \subset Q_n$. Since $Q_n$ is finite dimensional and $e$ is an automorphism, we conclude that $Q_n \cdot e = Q_n$. Hence $Q \cdot e = Q$, so that $e \in H$. Thus $G \subset H$, and therefore $G = H$.

Now let $T$ be any algebraic group of automorphisms of $V$ whose Lie algebra contains $x$. Let $A$ be the ideal of all polynomial functions vanishing on $T$. Our assumption means that $D_x(A) \subset A$. Hence, for all $p \in A$ and all $n \geq 0$, $D^n_x(p)(I) = 0$. By (2), this implies that $p \in Q$. Thus we have $A \subset Q$, whence $G \subset T$. We conclude that $G \subset G_x$.

If $F$ is algebraically closed it follows at once from the Hilbert Nullstellensatz that $Q$ is the ideal of all polynomial functions vanishing on $G$. Since $D_x(Q) \subset Q$, this implies that $x$ belongs to the Lie algebra of $G$, and hence that $G = G_x$. In the general case, the application of the Hilbert Nullstellensatz must be replaced with a specialization argument resting on the fact, to be proved, that $P/Q$
is contained in a purely transcendental extension field of $F$.

If $K$ is any field containing $F$, and $A$ is any vector space or algebra over $F$, we abbreviate the tensor product $A \otimes_F K$ by $A^K$, and we identify $A$ with its canonical image in $A^K$. As usual, we identify $E^K$ with the algebra of all endomorphisms of the $K$-space $V^K$. Finally, the algebra of the polynomial functions on $E^K$ may be identified with $P^K$.

Let $K$ be a finite Galois extension of $F$ containing all the characteristic roots of the given endomorphism $x$. The Galois group $S$ of $K$ over $F$ operates in the natural fashion on $P^K$ and on $K \{t\} = F \{t\} \otimes_F K$. The homomorphism $p \mapsto p(\exp(tx))$ of $P^K$ into $K \{t\}$ is evidently an $S$-homomorphism and induces an isomorphism of the $F$-algebra $P/Q$ onto the $F$-algebra consisting of the $S$-fixed elements of the image of $P^K$ in $K \{t\}$.

We can decompose $V^K$ into the direct sum of $x$-stable subspaces $V_i$ such that each $V_i$ is annihilated by a power of $x - c_i I$, where $c_i \in K$. If $x_i$ is the endomorphism induced by $x$ on $V_i$, it is clear that the image of $P^K$ by the homomorphism $p \mapsto p(\exp(tx))$ is generated as a $K$-algebra by the constants and the power series $p_i(\exp(tx))$, where, for each $i$, $p_i$ ranges over the linear functions on the algebra of endomorphisms of $V_i$. If we write $x_i = c_i I + u_i$, with $u_i^p = 0$, we find that

$$p_i(\exp(tx_i)) = \exp(tc_i) \sum_{k=0}^{d_i-1} \frac{p_i(u_i^k)}{k!} t^k.$$

Hence we see that the image of $P^K$ is contained in the ring $K[t, \exp(tc_1), \cdots, \exp(tc_p)]$, where $c_1, \cdots, c_p$ are the characteristic roots of $x$.

Let $a_1, \cdots, a_q$ be a free basis for the additive group generated by the elements $c_1, \cdots, c_p$ of $K$. Then the set $(t, \exp(ta_1), \cdots, \exp(ta_q))$ is algebraically free over $K$ (cf. [1, Lemma 2, p. 151]), and the image of $P^K$ is contained in the field $K(t, \exp(ta_1), \cdots, \exp(ta_q))$. Since the automorphisms belonging to $S$ permute the $c_i$ among themselves, it follows that they permute among themselves also the monomials, with negative exponents allowed, in the elements $t, \exp(ta_1), \cdots, \exp(ta_q)$. In particular, the field $K(t, \exp(ta_1), \cdots, \exp(ta_q))$ is stable under the action of $S$ on the field of quotients of $K \{t\}$, and $P/Q$ is isomorphic as an $F$-algebra with an $F$-subalgebra of the field of the $S$-fixed elements of $K(t, \exp(ta_1), \cdots, \exp(ta_q))$. Hence, in order to conclude that $P/Q$ is contained in a purely transcendental extension of $F$, it suffices to prove the following lemma.
Lemma. Let $K$ be a field, and let $L = K(u_1, \ldots, u_r)$, where $(u_1, \ldots, u_r)$ is algebraically free over $K$. Let $M$ denote the multiplicative group generated by the $u_i$. Let $S$ be a finite group of automorphisms of $L$, and assume that both $K$ and $M$ are $S$-stable. Assume also that the restriction map of $S$ into the automorphism group of $K$ is a monomorphism. Let $F$ denote the field of the $S$-fixed elements of $K$. Then the field of the $S$-fixed elements of $L$ is contained in a purely transcendental extension of $F$.

Proof. Let $v = (v_{ij})$ ($i = 1, \ldots, r; j = 1, \ldots, n = [K:F]$) be a set of independent variables over $K$, and let $k_1, \ldots, k_n$ be a basis for $K$ over $F$. Let $\phi$ be the homomorphism of $M$ into the multiplicative group of the nonzero elements of $K(v)$ such that

$$\phi(u_i) = \sum_{j=1}^{n} v_{ij} k_j.$$ 

Let $S$ operate on $K(v)$ coefficientwise, and define the homomorphism $\psi$ on $M$ by $\psi = \prod_{s \in S} s \circ \phi \circ s^{-1}$. Then $\psi \circ s = s \circ \psi$, for every $s \in S$. We have

$$s(\phi(u_i)) = \sum_{j=1}^{n} v_{ij} s(k_j).$$

Since the $K$-linear combinations of the elements of $S$ constitute the algebra of all $F$-endomorphisms of $K$, it is clear that, for each fixed $i$, the elements $v_{ij}$ ($j = 1, \ldots, n$) can be expressed as $K$-linear combinations of the elements $s(\phi(u_i))$ ($s \in S$). It follows that the $s(\phi(u_i))$ ($i = 1, \ldots, r; s \in S$) are algebraically independent over $K$. Let $N_s$ be the multiplicative group generated by the $s(\phi(u_i))$, with $i = 1, \ldots, r$, and let $N$ be the multiplicative group generated by all the $s(\phi(u_i))$. Then $N$ is the direct product of the $N_s$. If $s_1$ is the identity element of $S$ then $\phi$ is clearly an isomorphism of $M$ onto $N_{s_1}$. Hence $s \circ \phi \circ s^{-1}$ is an isomorphism of $M$ onto $N_s$, and $\psi$ is a monomorphism of $M$ into $N$.

Since the elements of $N$ are $K$-linearly independent, $\psi$ extends to a $K$-algebra monomorphism $K[M] \rightarrow K[N]$, which further extends to a field monomorphism $K(u_1, \ldots, u_r) \rightarrow K(v)$ that leaves the elements of $K$ fixed and commutes with the automorphisms from $S$. Hence the field of the $S$-fixed elements of $K(u_1, \ldots, u_r)$ is mapped monomorphically into the field of the $S$-fixed elements of $K(v)$, i.e., into $F(v)$. This completes the proof of the lemma.

Returning to our main theme, we may now conclude from the lemma that $P/Q \subset F(z_1, \ldots, z_n)$, where $(z_1, \ldots, z_n)$ is algebraically
free over $F$. Now let $Q_1$ denote the ideal of all polynomial functions vanishing on $G$. Evidently, $Q \subset Q_1$. Suppose that $Q \neq Q_1$, and choose $b \in Q_1$ such that $b \not\in Q$. Let $d$ be the determinant function on $E$. For every $p \in P$, let $p'$ denote its canonical image in $P/Q$. Then $b'd' \neq 0$. Write $b'd' = f(z_1, \ldots, z_n)/g(z_1, \ldots, z_n)$, where $f$ and $g$ are polynomials. Let $p_1, \ldots, p_m$ be a basis for $E^*$, and write

$$p'_i = f_i(z_1, \ldots, z_n)/g_i(z_1, \ldots, z_n),$$

where $f_i$ and $g_i$ are polynomials. We can find elements $s_1, \ldots, s_n$ in $F$ such that $f g_1 \cdots g_m$ does not vanish at $(s_1, \ldots, s_n)$. Let $e$ be the element of $E$ for which $p_i(e) = f_i(s_1, \ldots, s_n)/g_i(s_1, \ldots, s_n)$. Then we have $(b'd')(e) = f(s_1, \ldots, s_n)/g(s_1, \ldots, s_n) \neq 0$. This means that $e$ is an automorphism of $V$ and not a zero of $Q_1$. On the other hand, $e$ is a zero of $Q$, so that $e \in G$. This is a contradiction, and we conclude that $Q_1 = Q$.

As we have already seen above, it follows that $x$ belongs to the Lie algebra of $G$, and that $G = G_x$. Evidently, $\exp(tx)$ is a generic point of $G_x$.

Reference


University of California, Berkeley