ON DERIVATIONS IN DIVISION RINGS

MORRIS WEISFELD

We are concerned with studying division rings in which Lie rings of derivations are acting. The results include the determination of dimension over the constant subring, an outer Galois theory, and miscellaneous results on inner automorphisms and powers of derivations.

Let A be a ring with an identity 1 and B be a subring of A containing 1.

1. The mappings $R_x : y \rightarrow yx$, $L_x : y \rightarrow xy$, $I_x : y \rightarrow x^{-1}yx$, $x \in A$ are called right multiplications, left multiplications and inner automorphisms respectively. For any subset N of A, $R_N = \{R_x \mid x \in N\}$, $L_N = \{L_x \mid x \in N\}$, $I_x = \{I_x \mid x \in N\}$. D is a derivation of B into A if and only if $(x + y)D = xD + yD$ and $(xy)D = xDy + xyD$ for all $x, y \in A$. The set of all such mappings is denoted by $\operatorname{Der}(B, A)$. If $B = A$, D is called a derivation in A and the set of these denoted by $\operatorname{Der}(A)$. If $D_1, \cdots, D_s \in \operatorname{Der}(A)$, we have for all $x \in A$

$$(1) \qquad R_x D_1^{k_1} \cdots D_s^{k_s} = \sum \left\{ \binom{k_1}{i_1} \cdots \binom{k_s}{s_s} D_1^{k_1 - i_1} \cdots D_s^{k_s - i_s} R_{xD_1^{i} \cdots D_s^{i_s}} \mid \right. \\ \left. 0 \leq i_j \leq k_j,\ j = 1, \cdots, s \right\} .$$

For all $D, D' \in \operatorname{Der}(A)$, $[DD'] = DD' - D'D \in \operatorname{Der}(A)$ and, if A has prime characteristic p, $D^p \in \operatorname{Der}(A)$. $\{x \mid xy - yx = 0 \text{ for all } y \in B; x \in A\}$ is called the centralizer of B in A. If c belongs to the centralizer of B in A, $DR_c \in \operatorname{Der}(B, A)$. The centralizer of A in A is called the center of A. Let C be the center of A. $\mathscr{D}$ is a Lie ring (Lie ring over C) of derivations in A if and only if $\mathscr{D} \subseteq \operatorname{Der}(A)$ and for all $D, D' \in \mathscr{D}$, $D - D' \in \mathscr{D}$, $[DD'] \in \mathscr{D}$ $(DR_c \in \mathscr{D})$. If A has prime characteristic p, $\mathscr{D}$ is restricted if, in addition, $D^p \in \mathscr{D}$.

For $x \in A$, the mapping $I'_x : y \rightarrow yx - xy$ is a derivation called an inner derivation. For $N \subseteq A$, $I'_N = \{I'_x \mid x \in N\}$. The elements of $\operatorname{Der}(A)$ not in I'_A are called outer derivations. Lie ideals are defined in the usual way for Lie rings, restricted or not, over C or not. The inner derivations in $\mathscr{D}$ form a Lie ideal in $\mathscr{D}$.

Let T be a subset of $\operatorname{Der}(B, A)$. The set of $x \in B$ such that $xD = 0$ for all $D \in T$ is a subring of B which we call the subring of T-constants and which we denote by $B(T)$. If $x \in B(T)$ and x has a multiplicative inverse x^{-1} in B, then $x^{-1} \in B(T)$. The set of derivations D in A such

Received April 15, 1959. This is a revised version of part of a dissertation submitted in candidacy for a Ph. D. degree to Yale University. The author wishes to thank Professor N. Jacobson for his advice and encouragement. An abstract was presented to the American Mathematical Society (Bull. A. M. S., Vol. 60, 1954, p. 142).

that $B \subseteq A(D)$ is a (restricted) Lie subring over C of $\mathrm{Der}(A)$ which we denote by $\mathscr{D}(B)$.

If $T_1 \subseteq T_2 \subseteq \mathrm{Der}(A)$, then $A(T_1) \supseteq A(T_2)$; and, if B_1 and B_2 are subrings of A containing 1, and $B_1 \subseteq B_2$, then $\mathscr{D}(B_1) \supseteq \mathscr{D}(B_2)$. We have the following relations:

$$(2) \qquad \mathscr{D}' \subseteq \mathscr{D}(A(\mathscr{D}'))$$

for all (restricted) Lie subrings over C of $\mathrm{Der}(A)$

$$(3) \qquad B \subseteq A(\mathscr{D}(B))$$

(for all subrings B of A containing 1. These give

$$(4) \qquad A(\mathscr{D}') = A(\mathscr{D}(A(\mathscr{D}'))$$

for all (restricted) Lie subrings over C, $\mathscr{D}'$, of $\mathrm{Der}(A)$

$$(5) \qquad \mathscr{D}(B) = \mathscr{D}(A(\mathscr{D}(B)))$$

for all subrings of A containing 1. Thus, $B = A(\mathscr{D}(B))$ if and only if $B = A(\mathscr{D})$ for some (restricted) Lie subring over C of $\mathrm{Der}(A)$, and $\mathscr{D}' = \mathscr{D}(A(\mathscr{D}'))$ if and only if $\mathscr{D}' = \mathscr{D}(B)$ for some subring B of A containing 1.

Let $\mathscr{D}$ be a (restricted) Lie subring over C of $\mathrm{Der}(A)$. Define

$$\sum(\mathscr{D}) = \{x \mid x \in A \text{ and } I'_x \in \mathscr{D}\} .$$

Regard the ring A as a (restricted) Lie algebra over C under the compositions $(x, y) \rightarrow xy - yx$ ($x \rightarrow x^p$ if A has prime characteristic p). $\Sigma(\mathscr{D})$ is then a (restricted) Lie subalgebra of A. $\Sigma(\mathscr{D})$ is invariant under $\mathscr{D}$; that is $xD \in \Sigma(\mathscr{D})$ for $x \in \Sigma(\mathscr{D})$ and $D \in \mathscr{D}$. If $\mathscr{D} = \mathscr{D}(B)$ where B is a subring of A containing 1, then $\Sigma(\mathscr{D})$ is closed with respect to ordinary multiplication and taking multiplicative inverses. This leads us to make the following definition: We say $\mathscr{D}$ is a (restricted) N-Lie subring over C or $\mathrm{Der}(A)$ if and only if $\Sigma(\mathscr{D})$ is a subring of A closed with respect to taking multiplicative inverses and invariant under $\mathscr{D}$. In this case $\Sigma(\mathscr{D})$ over C is called the associated algebra of $\mathscr{D}$. If A is a division ring, $\Sigma(\mathscr{D})$ is a division algebra over C.

Let Δ be a division ring, Φ be its center and E a division subring of Δ. The additive group of homomorphisms of $(\mathrm{E}, +)$ into $(\Delta, +)$, $\mathrm{Hom}(\mathrm{E}, + ; \Delta, +)$ is an $(R_{\mathrm{E}}, R_\Delta)$-space; that is, $\mathrm{Hom}(\mathrm{E}, + ; \Delta; +)$ is a vector space over R_{E} and a right vector space over R_Δ such that

$$(7) \qquad (R_x T)R_y = R_x(TR_y)$$

for all $x \in \mathrm{E}$, $y \in \Delta$ and $T \in \mathrm{Hom}(\mathrm{E}, + ; \Delta, +)$. $(R_{\mathrm{E}}, R_\Delta)$-subspaces are defined in the usual way. If $\mathrm{E} = \Delta$, we write $\mathrm{End}(\Delta, +)$. If S is a set of endomorphisms of Δ, End {S} is the ring of endomorphisms generated by S.

Let Γ be a division subring of Δ. $L_\Gamma(\mathrm{E}, \Delta)$ denotes the subgroup of $\mathrm{Hom}(\mathrm{E}, +; \Delta, +)$ of homomorphisms of the vector space E over Γ into the vector space Δ over Γ. If $\mathrm{E} = \Delta$, we write $L_\Gamma(\Delta)$.

Topologize $\mathrm{Hom}(\mathrm{E}, + \Delta, +)$ as follows: The sets

$$\{g \mid xg = xf; g \in \mathrm{Hom}(\mathrm{E}, +; \Delta, +)\}$$

where $x \in \mathrm{E}$ is a subbase of neighborhoods of $f \in \mathrm{Hom}(\mathrm{E}, +; \Delta, +)$. One verifies that $L_\Gamma(\Delta)$ is a closed subring containing R_Δ. That the foregoing properties characterize $L_\Gamma(\Delta)$ is a consequence of the Jacobson-Bourbaki theorem: if we associate with a closed subring B of $\mathrm{End}(\Delta, +)$ which contains R_Δ, the set Γ of $x \in \Delta$ such that L_x commutes with the elements of B, then $B = L_\Gamma(\Delta)$, and, in fact, the mapping $\Gamma \rightarrow L_\Gamma(\Delta)$ is a lattice anti-isomorphism of the set of division subrings of Δ onto the set of closed subrings of $\mathrm{End}(\Delta, +)$ containing R_Δ.

If A is a vector space and right vector space over P, $[A:P]_L$ denotes its dimension and $[A:P]_R$ its right a dimensional over p. We note the following $[\mathrm{E}:\Gamma]_L$ is finite if and only if $[L_\Gamma(\mathrm{E}, \Delta):R_\Delta]_R$ is finite and when both are finite, they are equal. If B is a subring of $\mathrm{End}(\Delta, +)$ containing R_Δ and $[B:R_\Delta]_R$ is finite, then B is a closed subring.

Again Δ is a division ring, Φ is its center, E is a division subring and M is the centralizer of E in Δ. If $T \in \mathrm{End}(\Delta, +)$, then T^* denotes the restriction of T to E. If $D_1, \cdots, D_s$ are elements of $L_\Gamma(\mathrm{E}, \Delta)$ not in the algebra generated by L_Δ and R_Δ and σ, μ are not zero, the degree of the endomorphism

$$(8) \qquad D_1^{k_1} \cdots D_s^{k_s} L_\sigma R_\mu, \quad k_j \geq 0, \quad D_j^0 = I_1, \quad j = 1, \cdots, s\,,$$

is $k_1 + \cdots + k_s$. The weight of a sum of endomorphisms of the form (8) is the largest degree for which a term with that degree appears non-trivially. If all the terms appearing non-trivially have equal degree h, we say the endomorphism is homogeneous (of weight h). Any endomorphism is a sum of homogeneous endomorphisms. Suppose $D_1, \cdots, D_s \in L_\Gamma(\Delta)$ and are derivations of E into Δ and $\sigma \in \Delta$. $D_1^{k_1} \cdots D_s^{k_s} L_\sigma$ is called an admissible endomorphism if and only if (1), restricted to E and multiplied by L_σ, holds, any term appearing in (1) is admissible, and, if Δ has prime characteristic p, $k_j < p$.

LEMMA 1. *Let $\mathfrak{M}$ be an (R_E, R_Δ)-subspace of* $\mathrm{Hom}(\mathrm{E}, +; \Delta, +)$, $\sigma_1, \cdots, \sigma_t$ *be elements of Δ, and $D_1, \cdots, D_s$ be derivations of* E *into Δ belonging $L_\Gamma(\Delta)$. Suppose no right linear combination of $L^*_{\sigma_1}, \cdots, L^*_{\sigma_t}$ with coefficients in R_M is zero, and no right linear combination of $L^*_{\sigma_{u+1}}, \cdots, L^*_{\sigma_t}$ with coefficients in R_M belongs to $\mathfrak{M}$. Suppose $D^*_1, \cdots, D^*_s$ are right* *linearly independent over R_Δ modulo $I_\Delta'^*$ and no linear combination of $D_{r+1}^*, \cdots, D_s^*$ with coefficients $R_M + L_{\sigma_1}R_M + \cdots + L_{\sigma_u}R_M$ belongs to $L_\Delta^* + \mathfrak{M}$. Then the set of non-zero admissible endomorphisms by $D_1, \cdots, D_s$ and $\sigma_1, \cdots, \sigma_t$ such that some k_j with $j > r$ is not zero or L_{σ_j} appears with $j > u$ is right linearly independent over R_Δ modulo $\mathfrak{M}$.*

Proof. Suppose we had a non-trivial linear relation. Let F be a linear relation of lowest weight q and shortest length in q. Suppose $q = 0$. Then $F = L_{\sigma_{j_1}}^* R_{\mu_1} + \cdots + L_{\sigma_{j_n}}^* R_{\mu_n} \in \mathfrak{M}$, $j_1, \cdots, j_n > u$, $\mu_i \in \Delta$, $\mu_1 = 1, n > 1$. For all $x \in \mathrm{E}$

$$R_x F - F R_x = L_{\sigma_{j_2}}^* R_{(x\mu_2 - \mu_2 x)} + \cdots + L_{\sigma_{j_n}}^* R_{(x\mu_n - \mu_n x)} .$$

This gives a shorter non-trivial relation, or $\mu_1, \cdots, \mu_n \in M$, contradicting our hypothesis. Note that for $\mu_1, \cdots, \mu_n \in M$

$$\begin{aligned} L_{\sigma_{j_1}}^* R_{\mu_1} + \cdots + L_{\sigma_{j_n}}^* R_{\mu_n} &= (R_{\mu_1} L_{\sigma_{j_1}})^* + \cdots + (R_{\mu_n} L_{\sigma_{j_n}})^* \\ &= (L_{\mu_1} L_{\sigma_{j_1}} + \cdots + L_{\mu_n} L_{\sigma_{j_n}})^* = L^*{}_{\mu_1 \sigma_{j_1} + \cdots + \mu_n \sigma_{j_n}} . \end{aligned}$$

Suppose $q \geq 1$. Write $F = F_q + F_{q-1} + \cdots + F_0$ where the F_j are homogeneous. Let s_1 be the largest element among $1, \cdots, s$ such that a term in F_q has $k_{s_1} > 0$. Make its coefficient R_μ equal to 1. Form

$$\mathfrak{M} \ni R_x F - F R_x = G_q(x) + G_{q-1}(x) + \cdots + G_0(x) .$$

This will have lower weight or shorter length in q. The coefficients of terms in $G_q(x)$ have the form $R_{x\mu - \mu x}$. If these coefficients are zero, then the μ belong to M. Since we have shorter length in q, the coefficients in $G_q(x)$ must be 0. The coefficients in $G_{q-1}(x)$ have the form $R_{xD_{n_1}R_{\rho_1} + \cdots + xD_{n_k}R_{\rho_k} + xI'_\lambda}$, where the ρ_j's belong to M. These coefficients being zero for all $x \in \mathrm{E}$ would contradict our hypothesis. If $q > 1$, a term in F_q has the factor $D_j D_{s_1}$ and so G_{q-1} has a term with factor D_{s_1} and, if x is chosen to make its coefficient non-zero, we would contradict the choice of F. Hence the only possibility left is $q = 1$. Hence F has the form

$$\begin{aligned} D_{s_1}^* L_{\rho_{j_0}} + D_{n_1}^* L_{\rho_{j_1}} R_{\mu_1} + \cdots + D_{n_k}^* L_{\sigma_{j_k}} R_{\mu_k} + D_{n_{k+1}}^* R_{\mu_{k+1}} + \cdots \\ + D_{n_m}^* R_{\mu_m} + L_{\sigma_{u+1}}^* R_{\rho_{u+1}} + \cdots + L_{\sigma_t}^* R_{\rho_t} . \end{aligned}$$

Forming $R_x F - F R_x$ would yield non-trivial relations unless all right multiplications appearing belong to R_M and $j_1, \cdots j_k \leq u$. Hence F could be written as a linear combination of $D_{r+1}^*, \cdots, D_s^*$ with coefficients in $R_M + R_M L_{\sigma_1} + \cdots + R_M L_{\sigma_u}$ plus an element of $L_\Delta^* + \mathfrak{M}$ and this contradicts our hypothesis. Hence our assertion is true.

Suppose Δ has characteristic 0 and D is an outer derivation in Δ. Then the powers D^k, $k \geq 1$ of D are right linearly independent over R_Δ

as just shown. If $\Gamma = \Delta(D)$, $[L_\Gamma(\Delta) : R_\Delta] = \infty$ and hence $[\Delta : \Gamma]_L = \infty$. Thus if Δ has an outer derivation D and $[\Delta : \Gamma]_L < \infty$ where $\Gamma = \Delta(D)$, then Δ must have prime characteristic p.

Suppose Δ has prime characteristic p and Γ is a division subring such that $\mathscr{D}' = \mathscr{D}(\Gamma)$. $\mathscr{D}'$ is a restricted N-Lie ring over Φ of derivations in Δ. Suppose $\mathscr{D}'$ is infinite dimensional over Φ. Note that $I'_{\sigma_1}, \cdots, I'_{\sigma_t}$ are right linearly independent over R_Φ if and only if $1, \sigma_1, \cdots, \sigma_t$ are linearly independent over Φ. For if $\Sigma\varphi_i\sigma_i + \varphi_0 = 0$, then $\Sigma I'_{\sigma_i}R_{\varphi_i} = I'_{\Sigma\varphi_i\sigma_i+\varphi_0} = 0$. If $\Sigma I'_{\sigma_i}R_{\varphi_i} = 0$, then $0 = \Sigma(R_{\sigma_i} - L_{\sigma_i})R_{\varphi_i} = R_{\Sigma\varphi_i\sigma_i} - \Sigma L_{\sigma_i}R_{\varphi_i}$. Applying Lemma 1 yields the result. Thus $\mathscr{D}'$ has either infinitely many outer derivations right linearly independent over Φ modulo I'_Δ or $[\Sigma(\mathscr{D}') : \Phi] = \infty$. In either case $[L_\Gamma(\Delta) : R_\Delta]_R$ will, by Lemma 1, be infinite dimensional and so will $[\Delta : \Gamma]_L$.

THEOREM 1. *Let Δ be a division ring having prime characteristic p, Φ be its center, $\mathscr{D}$ be a finite dimensional restricted N-Lie ring over Φ of derivations in Δ and $\Gamma = \Delta(\mathscr{D})$. Then if $D_1, \cdots, D_m$ is a complete set of representatives of a basis for the right vector space $\mathscr{D} - I'_{\Sigma(\mathscr{D})}$ over Φ, and $\sigma_1, \cdots, \sigma_q$ is a basis for $\Sigma(\mathscr{D})$ over Φ, then*

$$(9) \qquad \{D_1^{k_1} \cdots D_m^{k_m} L_{\sigma_j} \mid k_i = 0, 1, \cdots, p-1, \quad D_i^0 = I_1, \\ i = 1, \cdots, m, \quad j = 1, \cdots, q\}$$

is a basis for the right vector space End $\{\mathscr{D}, R_\Delta\}$ *over R_Δ. Moreover,* End $\{\mathscr{D}, R_\Delta\} = L_\Gamma(\Delta)$, $[L_\Gamma(\Delta) : R_\Delta]_R = p^m q = [\Delta : \Gamma]_L$ *and* $\mathscr{D} = \mathscr{D}(\Gamma)$.

Proof. Consider the set A of right linear combinations of elements of (9) with coefficients in R_Δ. Then clearly End $\{\mathscr{D}, R_\Delta\} \supseteq A$. Because $1 = \Sigma\sigma_j\lambda_j$, $\lambda_j \in \Phi$, $I_1 = L_{\sigma_j}R_{\lambda_j} \in A$ and, hence, $A \supseteq R_\Delta$ Since any inner derivation belonging to $\mathscr{D}$ can be written as $\Sigma(R_{\sigma_j\varphi_j} - L_{\sigma_j}R_{\varphi_j})$, where $\varphi_j \in \Phi$, $A \supseteq I'_{\Sigma(\mathscr{D})}$. Since any $D \in \mathscr{D}$ can be written as $\Sigma D_i R_{\lambda_i} + I'_\sigma$, where $\lambda_L \in \Phi$ and $\sigma \in \Sigma(\mathscr{D})$, $A \supseteq \mathscr{D}$. We have $R_x D_i = D_i R_x + R_{xD_i}$ for $x \in \Delta$, $D_i^p = \Sigma D_i R_{\lambda_i} + I'_\sigma$ with $\lambda_i \in \Phi$ and $\sigma \in \Sigma(\mathscr{D})$, $D_i D_j = D_j D_i + D$ with $D \in \mathscr{D}$, and $L_\sigma D_i = D_i L_\sigma + L_{\sigma D_i}$, for $\sigma \in \Sigma(\mathscr{D})$ and, hence, $\sigma D_i \in \Sigma(\mathscr{D})$. Also $L_\sigma L_\tau = L_{\sigma\tau} \in A$, for $\sigma, \tau \in \Sigma(\mathscr{D})$ and, hence $\sigma\tau \in \Sigma(\mathscr{D})$. Thus A is a ring and so $A =$ End $\{\mathscr{D}, R_\Delta\}$. The elements of (9) generate A and are right linearly independent by Lemma 1 and so they constitute a basis for A over R_Δ. Thus [End $\{\mathscr{D}, R_\Delta\} : R_\Delta]_R = p^m q$ and so is a closed subring of End$(\Delta, +)$ containing R_Δ. By the Jacobson-Bourbaki theorem we have End $\{\mathscr{D}, R_\Delta\} = L_\Gamma(\Delta)$ and $[\Delta : \Gamma]_L = [L_\Gamma(\Delta) : R_\Delta]_R = p^m q$. Suppose $D \in \mathscr{D}(\Gamma)$. Then $D \in L_\Gamma(\Delta)$. Hence, by Lemma 1, $D = D_1\varphi_1 + \cdots + D_m\varphi_m + I'_\tau$, $\varphi_1, \cdots, \varphi_m \in \Phi$. $I'_\tau = R_\tau - L_\tau \in \mathscr{D}(\Gamma)$ and so another application of Lemma 1 yields $\tau = \sigma_1\lambda_1 + \cdots + \sigma_q\lambda_q$, $\lambda_1, \cdots, \lambda_q \in \Phi$, so that $D \in \mathscr{D}$.

We remark that because of the symmetry in the above situation, we also have $[\Delta : \Gamma]_R = [\Delta : \Gamma]_L$.

LEMMA 2. *Let* $\mathscr{D}$ *be a* (restricted if Δ has prime characteristic p) *Lie ring over* Φ *of derivations in* Δ *and* $\Gamma = \Delta(\mathscr{D})$. *Suppose* $\mathscr{D}$ *contains all inner derivations belonging to* $\mathscr{D}(\Gamma)$. *Let* E *be a division subring of* Δ *containing* Γ *and* $[\mathrm{E} : \Gamma]_L < \infty$. *Let* M *be the centralizer of* E *in* Δ. *If* D^* *is a derivation of* E *into* Δ *and* $\Gamma \subseteq \Delta(D^*)$, *then* D^* *can be extended to a derivation in the centralizer of* M.

Proof. $D^* \in L_\Gamma(\mathrm{E}, \Delta)$; hence D^* can be extended to an element of $L_\Gamma(\Delta)$. The proof of Theorem 1 shows that $L_\Gamma(\Delta)$ is the closure of $\mathrm{End}\{\mathscr{D}, R_\Delta\}$ in $\mathrm{End}(\Delta, +)$. Since $[\mathrm{E}:\Gamma]_L < \infty$, there is an $F \in \mathrm{End}\{\mathscr{D}, R_\Delta\}$ such that $D^* = F^*$, the asterick denoting restriction to E. We have

$$D^* = F^* = \Sigma(D_i^{k_1} \cdots D_s^{k_s} L_{\sigma_j} R\mu_{k_1 \cdots k_s j})^*$$

where $D_1, \cdots, D_s, L_{\sigma_1}, \cdots, L_{\sigma_t}$ satisfy the hypotheses of Lemma 1 with $\mathfrak{M} = \{0\}$. Hence

$$D^* = D_{j_1}^* R_{\mu_1} + \cdots + D_{j_k}^* R_{\mu_k} + I_\tau'^*, \mu_1, \cdots, \mu_k \in M$$

I_τ' leaves the elements of Γ fixed so that the right hand side is a derivation in the centralizer of M and belongs to $\mathscr{D}$.

In particular, if the centralizer of Γ is Φ; that is, every non-zero derivation in $\mathscr{D}(\Gamma)$ is outer, then every derivation of E into Δ can be extended to a derivation in Δ.

Henceforth, we restrict ourselves to Δ having prime characteristic p.

LEMMA 3. *Let* $\mathscr{D}$ *be a finite-dimensional restricted N-Lie ring over* Φ *of derivations in* Δ *and* $\Gamma = \Delta(\mathscr{D})$. *If* B *is a subring of* $L_\Gamma(\Delta)$ *containing* R_Δ *and* $\mathscr{D}' = B \cap \mathscr{D}$, *then* $\mathscr{D}'$ *is a restricted N-Lie subring over* Φ *of* $\mathscr{D}$. *If* $\mathscr{D}$ *consists only of outer derivations, then* $B = \mathrm{End}\{\mathscr{D}', R_\Delta\}$.

Proof. Clearly $\mathscr{D}'$ is a finite-dimensional restricted Lie ring over Φ of derivations in Δ. Now $\Sigma(\mathscr{D}')$ is contained in $\Sigma(\mathscr{D})$ and $[\Sigma(\mathscr{D}) : \Phi] < \infty$. Hence $[\Sigma(\mathscr{D}') : \Phi] < \infty$. Since $1 \in \Phi \subseteq \Sigma(\mathscr{D}')$ and $\Sigma(\mathscr{D}')$ has no zero divisors, it is a division ring provided that it is a ring. Let $\sigma_1, \sigma_2 \in \Sigma(\mathscr{D}')$; that is, $I'_{\sigma_1}, I'_{\sigma_2} \in \mathscr{D}'$. Since B contains R_Δ and I'_{σ_1}, it contains L_{σ_1}. Since B contains R_Δ and I'_{σ_2}, it contains $I'_{\sigma_1\sigma_2} = I'_{\sigma_1} R_{\sigma_2} + L_{\sigma_1} I'_{\sigma_2}$. Hence, $I'_{\sigma_1\sigma_2} \in \mathscr{D}' = \mathscr{D} \cap B$ which implies $\sigma_1\sigma_2 \in \Sigma(\mathscr{D}')$. If $\sigma \in \mathscr{D}'$ and $D \in \mathscr{D}'$, $[I'_\sigma, D] = I'_{\sigma D} \in \mathscr{D}'$ and $\Sigma(\mathscr{D}')$ is invariant under $\mathscr{D}'$. Now let $D_1, \cdots, D_s$ be a basis for $\mathscr{D}$ over Φ such that $D_1, \cdots, D_r$ is a basis for $\mathscr{D}'$ over Φ, $r \leq s$. By Theorem 1, $B \supseteq \mathrm{End}\{\mathscr{D}, R_\Delta\}$ and we can write

$$b = \Sigma D_1^{k_1} \cdots D_s^{k_s} R_{\mu_{k_1 \cdots k_s}}$$

Since we have assumed $\Sigma(\mathscr{D}) = \Phi$. Applying Lemma 1 with $B = \mathfrak{M}$, we note that no D_j with $j > r$ can appear in this expression. Hence, $B \subseteq \operatorname{End}\{\mathscr{D}', R_\Delta\}$. Clearly, $\operatorname{End}\{\mathscr{D}', R_\Delta\} \subseteq B$ and these facts give the desired conclusion.

THEOREM 2. *Let $\mathscr{D}$ be a finite dimensional restricted Lie ring over Φ of outer derivations in Δ, $\Gamma = \Delta(\mathscr{D})$, and $\mathscr{D} = \mathscr{D}(\Gamma)$. To each restricted Lie subring over Φ, $\mathscr{D}'$, of $\mathscr{D}$ assign the division ring $\Delta(\mathscr{D}')$. To each division subring* E *of Δ containing Γ assign the restricted Lie ring $\mathscr{D}(\mathrm{E})$ over Φ of derivations in Δ. Then the correspondences $\mathscr{D}' \to \Delta(\mathscr{D}')$ and $\mathrm{E} \to \mathscr{D}(\mathrm{E})$ are inverses of each other; that is, $\mathscr{D}' = \mathscr{D}(\Delta(\mathscr{D}'))$ and $\mathrm{E} = \Delta(\mathscr{D}(\mathrm{E}))$. Moreover, $\mathscr{D}'$ is a Lie ideal over Φ of $\mathscr{D}$ if and only if $\mathrm{E} = \Delta(\mathscr{D}')$ is invariant under $\mathscr{D}$, and, in this case, the restricted Lie ring over Φ of derivations in* E *leaving the elements of Γ fixed is isomorphic to $\mathscr{D}/\mathscr{D}'$.*

Proof. Let $\mathscr{D}'$ be a restricted Lie subring over Φ of $\mathscr{D}$. $\mathscr{D}'$ satisfies the conditions of Theorem 1, for, in this case, $\Sigma(\mathscr{D}') = \Phi$, and thus $\mathscr{D}(\Delta(\mathscr{D}')) = \mathscr{D}'$. Next let E be a division subring of Δ containing Γ and $B = L_{\mathrm{E}}(\Delta)$. Then B is a subring of $L_\Gamma(\Delta)$ containing R_Δ. By Lemma 3, $B = \operatorname{End}\{\mathscr{D}', R_\Delta\}$ where $\mathscr{D}' = B \cap \mathscr{D}$. Clearly $\mathscr{D}' = \mathscr{D}(\mathrm{E})$. On the other hand, since $B = \operatorname{End}\{\mathscr{D}', R_\Delta\} = L_{\mathrm{E}}(\Delta)$, $\mathrm{E} = \Delta(\mathscr{D}')$. Thus, $\mathrm{E} = \Delta(\mathscr{D})\mathrm{E}))$.

If E is invariant under $\mathscr{D}$, then $\mathscr{D}(\mathrm{E})$ is a Lie ideal over Φ in $\mathscr{D}$. For if $D \in \mathscr{D}$ and $D' \in \mathscr{D}(\mathrm{E})$, then $x(DD' - D'D) = (xD)D' - (xD')D = 0$ for all $x \in \mathrm{E}$. Conversely, if $\mathscr{D}'$ is a Lie ideal over Φ in $\mathscr{D}$, then $\mathrm{E} = \Delta(\mathscr{D}')$ is invariant under $\mathscr{D}$. For if $D \in \mathscr{D}$, $(xD)D' = (xD')D = 0$ for all $x \in \mathrm{E}$ and $D' \in \mathscr{D}'$. Hence $xD \in \Delta(\mathscr{D}') = \mathrm{E}$ for all $x \in \mathrm{E}$. Consider the mapping $D \to D^*$ the restriction of D to D^*. This is clearly a homomorphism of $\mathscr{D}$ into the Lie ring over Φ of derivations in E leaving the elements of fixed. Using Lemma 2, one finds that the mapping is onto. Its kernel is $\mathscr{D}' = \mathscr{D}(\mathrm{E})$.

THEOREM 3. *Let $\mathscr{D}$ be a* (restricted if Δ has prime characteristic p) *Lie ring over Φ of derivations in Δ and $\Gamma = \Delta(\mathscr{D})$. Suppose $\mathscr{D}$ contains all inner derivations belonging to $\mathscr{D}(\Gamma)$. Let* E *be a division subring of Δ containing Γ and $[\mathrm{E} : \Gamma]_L < \infty$. If a^* is an isomorphism of* E *into Δ leaving the elements of Γ fixed, then a^* can be extended to an inner automorphism in Δ.*

Proof. a^* belongs to $L_\Gamma(\mathrm{E}, \Delta)$; hence a^* can be extended to $a \in L_\Gamma(\Delta)$. $L_\Gamma(\Delta)$ is the closure of $\operatorname{End}\{\mathscr{D}, R_\Delta\}$ in $\operatorname{End}\{\Delta, +)$. Since $[\mathrm{E} : \Gamma]_L < \infty$, there is an $F \in \mathrm{End}\{\mathscr{D}, R_\Delta\}$ such that $a^* = F^*$, where the asterick denotes restriction to E. We can write

$$F = \Sigma D_1^{k_1} \cdots D_s^{k_s} L_{\sigma_j} R_{\mu_{k_1 \cdots k_s j}}$$

where $D_1, \cdots, D_s, \sigma_1, \cdots, \sigma_t$, etc. are as in Lemma 1 with $\mathfrak{M} = \{0\}$. Since $R_x a^* - a^* R_{xa^*} = 0$ for all $x \in \mathrm{E}$ and $s^* = F^*$, we have

$$\Sigma (D_1^{k_1} \cdots D_s^{k_s} L_{\sigma_j} R_{x\mu_{k_1 \cdots k_s j} - \mu_{k_1 \cdots k_s j}(xa^*)})^* + \text{terms} = 0$$

By Lemma 1, we obtain from a term of highest weight

$$x\lambda - \lambda(xa^*) = 0 \text{ for all } x \in \mathrm{E} \text{ and for some } 0 \neq \lambda \in \Delta .$$

Clearly s^* can be extended to the inner automorphism determined by λ.

The following theorem is a special case of one due to Amitsur: Let Δ be a division ring, D a derivation in Δ and $\Gamma = \Delta(D)$. Let S be the set of $x \in \Delta$ such that

$$x(D^n R_{\mu_n} + D^{n-1} R_{\mu_{n-1}} + \cdots + R_{\mu_0}) = 0$$

where $\mu_n \neq 0, \mu_{n-1}, \cdots, \mu_0 \in \Delta$. Then S is a vector space over Γ of dimension $\leq n$. This result is applied in the following theorem.

THEOREM 4. *Let Δ be a division ring and D an outer derivation in Δ. Let k be the least integer greater than* 1 *such that D^k is a derivation. Then Δ has prime characteristic k. If k doesn't exist, then Δ has characteristic zero.*

Proof. By hypothesis and Leibniz's rule

$$0 = R_x D^k - D^k R_x - R_{xD^k} = \binom{k}{1} D^{k-1} R_{xD} + \cdots + \binom{k}{k-1} D R_{xD^{k-1}} .$$

Choose x so that $R_{xD} \neq 0$: If Δ has characteristic 0, $\binom{k}{1} = k \neq 0$. If k exists by Lemma 1 and the Jacobson-Bourbaki Theorem, $[\Delta : \Gamma]_L = \infty > k$, and by Amitsur's Theorem, $[\Delta : \Gamma]_L \leq k - 1 < k$. Hence, in this case, k, can't exist. If Δ has prime characteristic p, then since D^p is a derivation, $k \leq p$. Assume in this case $k < p$. Then, $\binom{k}{1} = k \neq 0$. Applying Amitsur's Theorem yields the fact that $[\Delta : \Gamma]_L \leq k - 1 < p$. By Lemma 1 and the Jacobson-Bourbaki Theorem, $[\Delta : \Gamma]_L \geq p$. This is a contradiction. Hence, if some power $k > 1$ of an outer derivation in Δ is a derivation, then Δ must have prime characteristic p and the least power of D greater than 1 which is a derivation is D^p.

Bibliography

1. F. Artin, *Galois Theory*, Notre Dame, Indiana, 1944.

2. A. A. Albert, *Structure of Algebras*, Amer. Math. Soc., New York, 1939.

3. S. Amitsur, *A generalization of a theorem on linear differential equations*, Bull. Amer. Math. Soc., **54** (1948), 937–941.

4. J. Dieudonné, *Les semi-derivations dans les extensions radicielles* C. R. Acad. Sci. Paris, **227** (1948) 1319–1320.

5. ———, *Theorie de Galois des extensions radicielles d'exposent quelconque*. C. R. Acad. Sci. Paris, **228** (1949) 148–150.

6. N. Jacobson, *Abstract derivation and Lie algebras*, Trans. Amer. Math. Soc., **42** (1937) 206–224.

7. ———, *Galois theory of purely inseparable fields of exponent one*, Amer. J. of Math., **66** (1944), 645–649.

8. ———, *Structure of Rings*, Amer. Math. Soc., New York, 1956.

Yale University