COMMUTATIVE RESTRICTED LIE ALGEBRAS[1]

N. JACOBSON

A Lie algebra of characteristic $p \neq 0$ is called *restricted* if in addition to the usual compositions one has defined a unary operation $a \to a^{[p]}$ such that

$$(\alpha a)^{[p]} = \alpha^p a^{[p]}, \qquad \alpha \text{ in the base field},$$

$$[a, b^{[p]}] = [\cdots [ab] \cdots b], \qquad (p\ b\text{'s})$$

$$(a + b)^{[p]} = a^{[p]} + b^{[p]} + \sum_1^{p-1} s_i(a, b),$$

where $is_i(a, b)$ is the coefficient of λ^{i-1} in

$$[\cdots [[a, \lambda a + b]\lambda a + b] \cdots \lambda a + b],[2] \qquad (p - 1\ (\lambda a + b)\text{'s}).$$

Examples of such algebras are subspaces of associative algebras of characteristic $p \neq 0$ which are closed under the Lie multiplication $[ab] = ab - ba$ and under pth powers. Then one may take $a^{[p]} = a^p$. It is known that every restricted Lie algebra is isomorphic to one of this type. For this reason we may simplify our notation in the sequel and write a^p for $a^{[p]}$. We call the mapping $a \to a^p$ the *p-operator* in $\mathfrak{L}$.

We shall call a restricted Lie algebra $\mathfrak{L}$ *commutative* if $[ab] \equiv 0$ in $\mathfrak{L}$. These algebras play an important role in the theory of simple restricted Lie algebras since in all known examples every such algebra contains a commutative (restricted) Cartan subalgebra. Moreover, Zassenhaus has shown recently that if $\mathfrak{L}$ is a Lie algebra of characteristic $p \neq 0$ which has a representation with nondegenerate trace form, then the Cartan subalgebras of $\mathfrak{L}$ are all commutative. The present author has extended Zassenhaus' result to show that if $\mathfrak{L}$ is restricted and has nondegenerate trace form in a (restricted) representation, then the Cartan subalgebras are also semi-simple in the sense defined below. These results and some of those contained herein will be used in a forthcoming paper by G. Seligman on the classification of simple restricted Lie algebras which admit nondegenerate trace forms.

1. In defining subalgebras, ideals for a restricted Lie algebra, one requires closure with respect to the p-operator as well as the usual closures relative to the other compositions. Similarly, homomor-

Received by the editors July 21, 1954.

[1] The results of this paper were presented at the Summer Conference on Lie Groups and Lie Algebras (1953) sponsored by the American Mathematical Society under a grant from the National Science Foundation.

[2] See [3] for the definition and results stated without proof in this paragraph.

phisms are required to commute with the p-operator. If $\mathfrak{L}$ is commutative, the conditions on the p-operator reduce to

$$(a + b)^p = a^p + b^p, \qquad (\alpha a)^p = \alpha^p a^p.$$

Thus the p-operator is a semi-linear transformation relative to the isomorphism $\alpha \to \alpha^p$ in the base field Φ. Since $\mathfrak{L}$ is commutative every subalgebra is an ideal and these are just the subspaces invariant under the p-operator. In fact, it is clear that the study of $\mathfrak{L}$ is equivalent to that of the given semi-linear transformation.

From now on we suppose $\mathfrak{L}$ finite dimensional and Φ perfect. The latter condition implies that $\alpha \to \alpha^p$ is an automorphism.

An element $a \in \mathfrak{L}$ is *nilpotent* if $a^{p^k} (= (a^{p^{k-1}})^p) = 0$ for some $k \geqq 0$ and a commutative $\mathfrak{L}$ will be called *semi-simple* if it has no nilpotent elements $\neq 0$. It is clear that $\mathfrak{L}$ is semi-simple if and only if the p-operator is an onto mapping in $\mathfrak{L}$. Fitting's lemma gives a decomposition of $\mathfrak{L} = \mathfrak{L}_0 \oplus \mathfrak{L}_1$ where every element of $\mathfrak{L}_0$ is nilpotent and $\mathfrak{L}_1$ is semi-simple.

Consider now, more generally, any semi-linear transformation T in a finite dimensional vector space $\mathfrak{L}$ and denote the associated automorphism in Φ by σ. To study the decomposition of $\mathfrak{L}$ relative to T one introduces the polynomial ring $\Phi[t, \sigma]$ of formal polynomials in t with coefficients in Φ such that $\alpha t = t\alpha^\sigma$, $\alpha \in \Phi$. $\mathfrak{L}$ can be regarded as a $\Phi[t, \sigma]$-module.[3] The theory of these modules shows that we can decompose $\mathfrak{L}$ as a direct sum of cyclic subspaces $[x_1] \oplus [x_2] \oplus \cdots \oplus [x_r]$. Here $[x_i]$ is the space spanned by the vectors x_i, x_iT, x_iT^2, $\cdots$. If a_i denotes the polynomial of least degree n_i and leading coefficient 1 such that $x_i a_i = 0$ then $(x_i, x_iT, \cdots, x_iT^{n_i-1})$ is a basis for $[x_i]$. It is known that we can choose the x_i so that a_i is a total divisor of a_{i+1} in the sense that there exists a two-sided ideal $a_i^* \Phi[t, \sigma]$ so that

$$a_i \Phi[t, \sigma] \supseteq a_i^* \Phi[t, \sigma] \supseteq a_{i+1} \Phi[t, \sigma].$$

If $\mathfrak{L}$ is a restricted Lie algebra, then we shall call $\mathfrak{L}$ *cyclic* if it has a basis of the form $(a, a^p, a^{p^2}, \cdots, a^{p^{n-1}})$. The polynomial $\mu(t)$ of least degree (leading coefficient 1) such that $a\mu(t) = 0$ is called the order of the generator a. If $\mu(t) = t^n - t^{n-1}\alpha_1 - t^{n-2}\alpha_2 - \cdots - \alpha_n$ then we have the relation

$$a^{p^n} = \alpha_1 a^{p^{n-1}} + \alpha_2 a^{p^{n-2}} + \cdots + \alpha_n a. \tag{1}$$

The result indicated is that any commutative restricted Lie algebra

[3] [2, p. 29]. The arithmetic of the polynomial domain $\Phi[t, \sigma]$ where σ is the automorphism $\alpha \to \alpha^p$ has been considered by Ore in [4].

is a direct sum of cyclic ones and the orders can be chosen as indicated.

We now distinguish two cases: σ of finite order and σ of infinite order. For the p-operator these correspond, respectively, to Φ finite and Φ infinite. The theory for the first case is quite well worked out. Moreover, for the applications to Lie algebras the case of an algebraically closed field is most important. Hence we shall assume in the remainder of this section that σ is of infinite order. In this case it is known that the only polynomials a^* such that $a^*\Phi[t, \sigma]$ is two-sided are the Φ-multiples of the powers t^k.[4] It follows that if T is non-singular then $r=1$ in the decomposition into cyclic subspaces. For the p-operator this gives

THEOREM 1. *Every semi-simple commutative restricted Lie algebra is cyclic.*

If $\mathfrak{L}$ is cyclic with generator a whose order is $\mu(t)=t^n-t^{n-1}\alpha_1-\cdots-\alpha_n$, then $(a, a^p, \cdots, a^{p^{n-1}})$ is a basis and $a^{p^n}=\alpha_1 a^{p^{n-1}}+\alpha_2 a^{p^{n-2}}+\cdots+\alpha_n a$. It follows that the p-operator is an onto mapping if and only if $\alpha_n \neq 0$. Hence this is the condition on $\mu(t)$ that $\mathfrak{L}$ be semi-simple.

2. We shall now derive a condition that $\mu(t)$ in $\Phi[t, \sigma]$ be divisible on the left by $t-\alpha$. For this purpose we set $N_0(\alpha)=1$, $N_k(\alpha)=\alpha\alpha^\sigma\alpha^{\sigma^2}\cdots\alpha^{\sigma^{k-1}}$. Then we have the following

LEMMA. *$t-\alpha$ is a left factor of $\mu(t)=\sum_0^n t^k\mu_k$ if and only if*

$$\sum_0^n N_k(\alpha)\mu_k = 0.$$

PROOF. We have the identity

$$(t-\alpha)(t^{k-1}+t^{k-2}\alpha^{\sigma k-1}+t^{k-3}\alpha^{\sigma k-2}\alpha^{\sigma^{k-1}}+\cdots+\alpha^\sigma\cdots\alpha^{\sigma^k}) = t^k - N_k(\alpha).$$

Right multiplication by μ_k and summation on k gives

$$\mu(t) - \sum N_k(\alpha)\mu_k = (t-\alpha)Q(t).$$

The result is now clear.

We suppose now that Φ is algebraically closed of characteristic p and σ is the automorphism $\alpha\to\alpha^p$. Then $N_k(\alpha)=\alpha^{1+p+\cdots+p^{k-1}}=\alpha^{(p^k-1)/(p-1)}$ and the condition that $t-\alpha$ is a left factor of $\mu(t)$ is that α is a root of $\tilde{\mu}(\lambda)=\sum\lambda^{(p^k-1)/(p-1)}\mu_k$.[5] Thus the only irreducible poly-

[4] [2, p. 38 and pp. 49–53].

[5] This result is due to Ore [4].

nomials in $\Phi[t, \sigma]$ of positive degree are the linear ones. A restricted Lie algebra is called simple if and only if it has no proper ideals $\neq 0$. For commutative algebras this means that $\mathfrak{L}$ has no proper subspaces $\neq 0$ invariant under the p-operator. Our results show that this is the case if and only if $\mathfrak{L}$ is cyclic and the order of the generator is irreducible in $\Phi[t, \sigma]$. We can now prove

THEOREM 2. *If Φ is algebraically closed, then the simple restricted commutative Lie algebras over Φ are all one dimensional. There are just two nonisomorphic types of such algebras.*

PROOF. If $\mathfrak{L}$ is simple commutative and Φ is algebraically closed, then the foregoing argument shows that $\mathfrak{L}$ is generated by an element a such that $a^p = \alpha a$. This implies the first statement. If $\alpha = 0$, $\mathfrak{L}$ is nilpotent. Otherwise, we replace a by $h = \alpha^{-1/(p-1)}a$ and obtain $h^p = h$. The second statement is now clear.

We can now prove our main result.

THEOREM 3. *If $\mathfrak{L}$ is a semi-simple commutative restricted Lie algebra over an algebraically closed field, then $\mathfrak{L}$ has a basis $(h_1, h_2, \cdots, h_n)$ such that $h_i^p = h_i$, $i = 1, 2, \cdots, n$.*

PROOF. In view of Theorem 2 the result to be proved is that $\mathfrak{L}$ is a direct sum of simple non-nilpotent subalgebras. Now it is known that a cyclic space $[x]$ relative to a semi-linear transformation is a direct sum of irreducible subspaces if and only if the order a is a least common right multiple of irreducible polynomials in $\Phi[t, \sigma]$.[6] The result we require is therefore the following. Let Φ be algebraically closed of characteristic p and let σ be the automorphism $\alpha \to \alpha^p$ in Φ. Then every polynomial $\mu(t) = \sum_0^n t^k \mu_k$ with $\mu_0 \neq 0$ is a least common right multiple of linear polynomials in $\Phi[t, \sigma]$. As before let $\tilde{\mu}(\lambda) = \sum \lambda^{(p^k-1)/(p-1)} \mu_k$ and let $\tilde{\mu}(\lambda)'$ be the derivative of $\tilde{\mu}(\lambda)$. Then

$$\tilde{\mu}(\lambda)'\lambda = \tilde{\mu}(\lambda) - \mu_0.$$

Hence $(\tilde{\mu}(\lambda), \tilde{\mu}(\lambda)') = 1$ and $\tilde{\mu}(\lambda)$ has $(p^n-1)/(p-1)$ distinct roots α_i $(\neq 0)$. It follows that $\mu(t)$ has exactly $(p^n-1)/(p-1)$ linear left factors $t - \alpha_i$. Since $\mu(t)$ is a product of linear factors we can write $\mu(t) = \nu(t)(t-\alpha)$. Since $\nu(t)$ is of lower degree than $\mu(t)$ the result just obtained shows that $\mu(t)$ has a left factor $t-\beta$ which is not a left factor of $\nu(t)$. Hence $\mu(t)$ is a least common right multiple of $t-\beta$ and $\nu(t)$. Since we may assume that $\nu(t)$ is a least common multiple of linear factors the result follows also for $\mu(t)$.

[6] [2, p. 34].

3. If T is a semi-linear transformation the set $\mathcal{E}$ of linear transformations commuting with T is a ring. In fact if Φ_0 is the subfield of Φ of fixed elements under σ, then $\mathcal{E} \supseteq \Phi_0$ and $\mathcal{E}$ can be regarded as an algebra over Φ_0. In particular we see that if $\mathfrak{L}$ is a commutative restricted Lie algebra, then the endomorphisms of $\mathfrak{L}$ form a ring $\mathcal{E}$ under the natural composition of addition and multiplication. Also, in this case Φ_0 is the set of elements of Φ satisfying $\alpha^p = \alpha$ so that Φ_0 is the prime field and $\mathcal{E}$ is an algebra over the prime field. In general, if we consider the vector space $\mathfrak{L}$ as a $\Phi[t, \sigma]$-module in the usual way, then $\mathcal{E}$ is the algebra of $\Phi[t, \sigma]$-endomorphisms of $\mathfrak{L}$. We shall show that $\mathcal{E}$ is always finite-dimensional over Φ_0. To do this we require a result on certain types of equations involving the automorphism σ.

We note first that if Φ is regarded as a one-dimensional vector space over itself, then σ is a semi-linear transformation. This is clear since for $\xi, \alpha \in \Phi$, $(\xi\alpha)^\sigma = \xi^\sigma \alpha^\sigma$. If $\mu(t) = \sum t^i \mu_i \in \Phi[t, \sigma]$ then we denote by $\mu(\sigma)$ the mapping $\xi \to \sum \xi^{\sigma^i} \mu_i$ in Φ. The correspondence $\mu(t) \to \mu(\sigma)$ is a homomorphism. It has been shown by Amitsur [1] that the maximum number of linearly independent solutions over Φ_0 of the equation $\xi\mu(\sigma) = 0$ is at most the degree of $\mu(t)$. We shall require the following

LEMMA. *The space of solutions* $(\xi_1, \xi_2, \cdots, \xi_n)$ *of a system of equations* $\sum_{i=1}^n \xi_i p_{ij}(\sigma) = 0$, $j = 1, 2, \cdots, r$, *is finite-dimensional over* Φ_0.

PROOF. We may replace the ξ_i by $\eta_i = \sum \xi_i u_{ik}(\sigma)$ where $(u_{ik}(t))$ is a unit in the matrix ring $\Phi[t, \sigma]_n$. Also we may replace the given equations by an equivalent system consisting of suitable linear combinations. This replaces the given system by an equivalent one of the form $\sum \eta_i \hat{p}_{ij}(\sigma) = 0$ where the matrix $(\hat{p}) = (u)(p)(v)$, (u) and (v) units. The invariant factor theorem shows that (u) and (v) can be chosen so that $(\hat{p})$ is diagonal. Thus the given system is equivalent to a system of the form $\eta_1 a_1(\sigma) = 0, \cdots, \eta_r a_r(\sigma) = 0$. It follows now from Amitsur's result that the solutions spaces are finite dimensional over Φ_0.

We can now prove

THEOREM 4. *Let* T *be a semi-linear transformation in a finite dimensional vector space* $\mathfrak{L}$ *over* Φ *and let* Φ_0 *be the subfield of fixed elements of the automorphism* σ *of* T. *Then the algebra* $\mathcal{E}$ *of linear transformations in* $\mathfrak{L}$ *commuting with* T *is finite dimensional over* Φ_0.

PROOF. Let $(e_1, e_2, \cdots, e_n)$ be a basis for $\mathfrak{L}$ over Φ and write $e_i T = \sum t_{ij} e_j$ and $e_i A = \sum \alpha_{ij} e_j$ for $A \in \mathcal{E}$. The condition $AT = TA$ is equivalent to $(\alpha_{ij}^\sigma)(t_{ij}) = (t_{ij})(\alpha_{ij})$. Thus the coordinates α_{ij} satisfy a

system of equations of the type considered in the lemma. Hence $\mathcal{E}$ is finite dimensional over Φ_0.

COROLLARY. *If $\mathfrak{L}$ is a commutative restricted Lie algebra over a perfect field Φ, then the ring of endomorphisms $\mathcal{E}$ of $\mathfrak{L}$ over Φ is a finite ring.*[7]

PROOF. Since $\mathcal{E}$ is finite dimensional over Φ_0 and Φ_0 is a finite field, this is clear.

It is easy to determine the ring $\mathcal{E}$ for a semi-simple $\mathfrak{L}$ over an algebraically closed field. Here we have a basis $(h_1, h_2, \cdots, h_n)$ such that $h_i^p = h_i$. If $h_iA = \sum \alpha_{ij} h_j$, the condition that $A \in \mathcal{E}$ gives $\alpha_{ij}^p = \alpha_{ij}$ (cf. the proof of Theorem 4). Hence the α_{ij} are in the prime field Φ_0. It follows that $\mathcal{E}$ is isomorphic to the matrix algebra Φ_{0n}. It is clear also that the group of automorphisms of $\mathfrak{L}$ is isomorphic to the group of nonsingular matrices over Φ_0.

BIBLIOGRAPHY

1. A. S. Amitsur, *A generalization of a theorem on linear differential equations*, Bull. Amer. Math. Soc. vol. 54 (1948) pp. 937–942.

2. N. Jacobson, *Theory of rings*, New York, 1943.

3. ———, *Restricted Lie algebras of characteristic p*, Trans. Amer. Math. Soc. vol. 50 (1941) pp. 15–25.

4. O. Ore, *On a special class of polynomials*, Trans. Amer. Math. Soc. vol. 35 (1933) pp. 559–584.

YALE UNIVERSITY

[7] A special case of this has been proved by Ore [4, p. 580].