ALGEBRAIC LIE ALGEBRAS[1]

BY GEORGE B. SELIGMAN

It is my objective in this address to survey results analogous to the third theorem of Lie (and its converse) for linear algebraic groups and their Lie algebras. In particular, I wish to report some slight progress on the problem of deciding from its structure whether a given Lie p-algebra ("restricted Lie algebra") over an arbitrary field F of prime characteristic p is realizable as the Lie algebra of a linear algebraic group defined over F. It is to be hoped that the criteria here presented for the commutative case will find extensions, at least to the solvable or nilpotent case.

1. **Matrix groups and their Lie algebras.** In this section I assume the base field F to be *algebraically closed*. I believe that the gains in explicitness afforded by this assumption are sufficient to offset the demands of comprehensiveness, which are well satisfied in [8]. As a *linear algebraic group* over F, I take here the most primitive notion, namely that of a subgroup G of a full matrix group $GL(n, F)$ such that G is the intersection with $GL(n, F)$ of the family of zeros in F^{n^2} of a set of polynomials. The group G is connected if G is irreducible as an algebraic subset of $GL(n, F)$. Denoting by $F[X]$ the polynomial ring in the n^2 variables X_{ij} corresponding to the matrix entries and by $\mathfrak{a}$ the ideal in $F[X]$ vanishing on G, the algebra $A(G)$ of everywhere-defined rational functions on G is generated over F by the restrictions to G of the X_{ij} and the reciprocal of the determinant function [1], [36], and thus may be identified with $B/\mathfrak{a}B$, where $B = F[X_{ij}, \det(X)^{-1}]$, (X) denoting the indeterminate matrix (X_{ij}). Thus G is an affine algebraic set over F, with affine algebra $A(G)$, and the rings of rational functions defined at points (or at irreducible algebraic subsets) of G are localizations of $A(G)$.

A tangent vector at a point of G (defined by analogy with [7]) is thus determined by its effect on $A(G)$, and a right-invariant tangent vector field T on G is determined by the effect on $A(G)$ of the tangent vector which T assigns at the identity. Now the tangent space at the identity I can be realized as follows: Let (α) be an arbitrary n by n matrix, and consider the unique F-derivation $D_{(\alpha)}$ of $F[X]$ sending X_{ij} into $\sum_k \alpha_{ik} X_{kj}$, the (i, j)-entry in (α) (X). Suppose that (α) is such that $D_{(\alpha)}$ maps the ideal $\mathfrak{a}$ into itself. Then $D_{(\alpha)}$ induces a derivation,

also written $D_{(\alpha)}$, of $A(G)$ into itself, commuting with right transla-
tions by elements of G; moreover, every tangent vector at I is ob-
tained by applying one such $D_{(\alpha)}$, then evaluating the resulting func-
tion at I [8], [32]. By this means, one identifies the Lie algebra of all
such matrices (α) (with $[(\alpha), (\beta)] = (\alpha)(\beta) - (\beta)(\alpha)$) and the Lie alge-
bra (under the Poisson bracket) of all right-invariant tangent vector
fields on G. If the characteristic of F is a prime p, then the pth power
$(\alpha)^p$ is in this Lie algebra whenever (α) is, and the resulting derivation
is the pth iterate of $D_{(\alpha)}$. The Lie algebra of matrices so defined is *the
Lie algebra of* G, denoted here by $\mathfrak{L}(G)$.

In this setting, the question of algebraicity is: *Given a Lie algebra* $\mathfrak{L}$
of n by n matrices over F, when is $\mathfrak{L} = \mathfrak{L}(G)$ *for some algebraic subgroup
G of $GL(n, F)$?* For the case of characteristic zero, a complete answer
to this question has been given by Chevalley [8] (see also [18]). One
defines *replicas* of a matrix (α) as those matrices (β) whose "infinitesi-
mal tensor invariants" include those of (α); then $\mathfrak{L}$ is algebraic if and
only if for each $(\alpha) \in \mathfrak{L}$ all replicas of (α) are in $\mathfrak{L}$, and in this case
$\mathfrak{L} = \mathfrak{L}(G)$ for a unique connected algebraic subgroup G of $GL(n, F)$.
More concretely, if (α) is taken in Jordan form, the replicas of (α) are
all linear combinations of the matrices obtained as follows: (1) By re-
placing the diagonal of (α) by zeros—the result here is the "nilpotent
part" of (α); (2) By considering the diagonal matrix $\operatorname{diag}\{\alpha_{11}, \cdots, \alpha_{nn}\}$
having the same diagonal as (α)—the "semisimple part" of (α)—and
forming all diagonal matrices $\operatorname{diag}\{\beta_{11}, \cdots, \beta_{nn}\}$ such that if m_i are
rational integers with $\sum m_i\alpha_{ii} = 0$, one has $\sum m_i\beta_{ii} = 0$.

Since I want to emphasize the problem of recognition of a Lie
algebra as algebraic in terms of structural characteristics, a few re-
marks seem in order as to some properties which assure that a Lie
algebra $\mathfrak{L}$ of matrices (over a field of characteristic zero) is algebraic.
For instance, if $\mathfrak{L}$ is the derived algebra of some Lie algebra, $\mathfrak{L}$ is alge-
braic; in particular, if $\mathfrak{L} = [\mathfrak{L}\mathfrak{L}]$ (thus whenever $\mathfrak{L}$ is semisimple), $\mathfrak{L}$ is
algebraic. In this line, we also know that $\mathfrak{L}$ is algebraic if and only if
its (solvable) radical is algebraic. From the above remarks on replicas
it is clear that any Lie algebra $\mathfrak{N}$ consisting of nilpotent matrices is
algebraic; in fact, $\mathfrak{N} = \mathfrak{L}(G)$ where the elements of G may be realized
uniquely as the products of $d = \dim \mathfrak{N}$ matrix factors (in specified
order) $\exp(\lambda_i u_i)$, u_i running over a basis for $\mathfrak{N}$ and λ_i over the field F.
Thus the underlying variety of G is an affine space. Other subalgebras
$\mathfrak{L}$ of matrices which are algebraic include stabilizers of subspaces,
centralizers of sets of matrices, derivation-algebras, and other ex-
amples to be found along with these in [8], which is the reference for
all the above.

In case F is of prime characteristic p, one still has the notion of replica; when (α) is taken in Jordan form, the replicas of its nilpotent part N consist of all p-polynomials $\sum \beta_i N^{p^i}$, and form a vector space of dimension k where $N^{p^k} = 0$, $N^{p^{k-1}} \neq 0$ [13], [40]. The replicas of its semisimple part are just as in characteristic zero [6]. Moreover, both the semisimple and nilpotent parts of (α) are p-polynomials in (α), and combinations of their replicas exhaust the replicas of (α) [6], [8], [14], [33]. Thus the replicas of (α) are just the p-polynomials in (α), and the condition that $\mathfrak{L}$ contain with (α) all its replicas amounts to requiring that $\mathfrak{L}$ *be closed under the operation of taking pth powers*.

Now if $\mathfrak{L}$ is a simple Lie algebra of matrices, and if $\mathfrak{L} = \mathfrak{L}(G)$ for a connected algebraic subgroup of $GL(n, F)$, then it follows, from the fact that the Lie algebra of a normal subgroup is an ideal in $\mathfrak{L}$, that G has no nontrivial connected normal algebraic subgroups, therefore is a member of a list which has been determined by Chevalley [11]. The Lie algebras of the groups in this list may be separately determined, or one may use more unified methods, as in [20], for their determination. It turns out that the only simple Lie algebras among them are of the form $\mathfrak{L}_Z \otimes F$, where $\mathfrak{L}_Z$ is a Chevalley lattice [10] in a simple Lie algebra $\mathfrak{L}_C$ over the complex field, and not even all of these are simple [16], [30], [38]. On the other hand, there are many simple Lie algebras over F, not of this form, which may be realized as Lie algebras of matrices closed under pth powers. Simplest examples are the Lie algebra of p by p matrices of trace zero, modulo scalar matrices ($p > 2$) and the Lie algebra of derivations of the group ring over F of an elementary abelian p-group (of order greater than p if $p = 2$ or 3). (For a list apparently complete to date, see [34, Chapter V].) Thus the replica criterion gives a necessary, but not sufficient, condition for algebraicity.

Structural conditions sufficient for algebraicity of a Lie algebra are present under some circumstances, usually when the Lie algebra $\mathfrak{L}$ is presented as a subalgebra of the Lie algebra $\mathfrak{M}$ of some (connected) algebraic subgroup G of $GL(n, F)$. Some of the more interesting, and quite typical, of these conditions are the following: (Although this is often superfluous, the ground field is assumed algebraically closed and of characteristic $\neq 2, 3$.)

(A) If G is an algebraic torus (i.e., a connected algebraic group of diagonal matrices), then every p-subalgebra of $\mathfrak{L}(G)$ is algebraic, and is the Lie algebra of a subtorus (not unique) of G [14].

(B) If $x \in \mathfrak{L}(G)$ is semisimple, then the centralizer of x in $\mathfrak{L}(G)$ is algebraic, and is the Lie algebra of the centralizer of x in G [2].

(C) The maximal ideal in $\mathfrak{L}(G)$ consisting of nilpotent matrices is

algebraic, and is the Lie algebra of the unipotent radical (maximal normal subgroup of unipotent elements) of G [20].

(D) Each Cartan subalgebra of $\mathfrak{L}(G)$ is algebraic, since it is the centralizer of a semisimple regular element (see (B)), and the correspondence between (connected) centralizers in G of regular semisimple elements of $\mathfrak{L}(G)$ and Cartan subalgebras of $\mathfrak{L}(G)$ is one-one [20]. (These subgroups need not be "Cartan subgroups" [9], [11].)

(E) Each maximal toral subalgebra (i.e., commutative subalgebra of semisimple elements) of $\mathfrak{L}(G)$ is algebraic, and is the Lie algebra of a maximal torus of G. If G is *reductive* (has trivial unipotent radical—see (C)), the resulting correspondence between maximal tori of G and maximal toral subalgebras of $\mathfrak{L}(G)$ is one-one [20].

(F) Each maximal solvable subalgebra containing a maximal toral subalgebra of $\mathfrak{L}(G)$ is algebraic, and is the Lie algebra of a maximal solvable subgroup of G [41]. The resulting correspondence between Borel subgroups (maximal solvable connected subgroups) of G and maximal solvable subalgebras of $\mathfrak{L}(G)$ containing a maximal toral subalgebra is one-one [20].

Most of the results cited above are also to be found in [17] (see especially Exposés XII–XIV).

One striking case where one can assert algebraicity of a Lie p-algebra $\mathfrak{L}$ of matrices is that where $\mathfrak{L}$ is generated by a single matrix (α), that is, where $\mathfrak{L} = \langle(\alpha)\rangle$ consists of all p-polynomials in (α)—or, what is the same, of all replicas of (α). For by decomposing (α) into semisimple and nilpotent parts we see by (A) above that the p-algebra generated by the semisimple part is algebraic. Dieudonné has also shown, with the aid of his "hyperexponential" group laws, that the p-algebra generated by the nilpotent part is algebraic, and is the Lie algebra of a commutative unipotent group commuting elementwise with a torus whose Lie algebra is generated by the semisimple part. Thus $\mathfrak{L}$ is the Lie algebra of a commutative algebraic group. The hyperexponential group involved is isomorphic to an additive Witt group, and has thereby an underlying variety which is an affine space [14], [15]. The choice of $G \subseteq GL(n, F)$ with $\mathfrak{L} = \mathfrak{L}(G)$ is by no means unique. Moreover, it is now clear that the condition that $\langle(\alpha)\rangle$ be algebraic for every (α) in the p-algebra $\mathfrak{L}$ brings us no closer than before to the algebraicity of $\mathfrak{L}$, whereas a corresponding condition in characteristic zero is sufficient.

2. **The problem for abstract Lie algebras.** When one examines the theorems of Lie in their original form, one observes that the analogy which served as the basis for §1 is not the most accurate one. Namely,

the classical results produced a (local) Lie group whose Lie algebra has the same structural constants as a given Lie algebra—in other words, which is isomorphic to the given Lie algebra. Thus we should perhaps reformulate our question as follows: *Given an abstract Lie algebra $\mathfrak{L}$, when is there a linear algebraic group G such that $\mathfrak{L}$ and $\mathfrak{L}(G)$ are isomorphic?*

As in §1, we begin with characteristic zero. The question is whether $\mathfrak{L}$ has a faithful representation to which the considerations of §1 apply. It is not hard to see that there are still exceptions to algebraicity; for if $\mathfrak{L}$ is algebraic in our sense, then there is an *adjoint* group, which is an algebraic group of automorphisms of $\mathfrak{L}$ having as Lie algebra the Lie algebra ad $\mathfrak{L}$ of inner derivations of $\mathfrak{L}$ [8]. However, it is not true in general that ad $\mathfrak{L}$ is closed under taking replicas. For example, consider the solvable Lie algebra $\mathfrak{L}$ with basis $e_1, \cdots, e_5$ and $[e_1e_3] = e_3$, $[e_2e_3] = -e_3$, $[e_1e_4] = e_3 + e_4$, $[e_2e_4] = -e_4$, $[e_1e_5] = e_5$, $[e_2e_5] = -e_3 - e_5$, all other products being either determined by anticommutativity or equal to zero. Then if $y \in \mathfrak{L}$ is to be such that ad y is the semisimple part of ad e_1, we must have $[ye_i] = 0$, $i = 1, 2$ and $[ye_j] = e_j$, $j = 3, 4, 5$; one verifies at once that $\mathfrak{L}$ contains no such y, hence that $\mathfrak{L}$ is not algebraic in our extended sense. This Lie algebra $\mathfrak{L}$ may be realized as all matrices of the form

$$\begin{pmatrix} \alpha & \alpha & \gamma & \delta \\ 0 & \alpha & 0 & \epsilon \\ 0 & 0 & \beta & \beta \\ 0 & 0 & 0 & \beta \end{pmatrix}$$

If we let $\mathfrak{M}$ be the subalgebra for which $\alpha = \beta$, we obtain a nilpotent Lie algebra of matrices which evidently does not contain the semisimple part of the matrix with $\alpha = \beta = 1$, $\gamma = \delta = \epsilon = 0$. Thus there is no algebraic subgroup G of $GL(4, F)$ with $\mathfrak{M} = \mathfrak{L}(G)$. On the other hand, one knows by Harish-Chandra's proof of Ado's theorem (cf. [23, Chapter VI]; also [19], for a somewhat stronger result) that $\mathfrak{M}$ has a faithful representation by nilpotent matrices so that $\mathfrak{M}$ is algebraic in the sense of this section by a result cited in §1. More generally, any Lie algebra whose (solvable) radical is nilpotent is algebraic.

Let us now turn to the case of prime characteristic p. Here it is clear that the only Lie algebras that have a chance to be algebraic are those in which a p-power operation can be introduced which agrees with the pth power for matrices in some faithful representation. Since an abstract setting for Lie algebras with a p-power operation has been given by Jacobson ([21], [23, Chapter V]), it seems

appropriate to formulate our problem in this setting, that of "restricted Lie algebras," or "Lie p-algebras." Thus the problem reads: *Given a Lie p-algebra $\mathfrak{L}$, when is there a linear algebraic group G such that $\mathfrak{L}$ is isomorphic, as Lie p-algebra, to $\mathfrak{L}(G)$?*

To get a hint of the richness of this problem, consider the case where $\mathfrak{L}$ is of dimension one, with basis x. As ordinary Lie algebra, $\mathfrak{L}$ is the Lie algebra of any one-dimensional group G; however, if we take into account the p-power, we have $x^p = \lambda x$ for some $\lambda \in F$. With F algebraically closed, $\mathfrak{L}$ is the Lie algebra of an additive group G_a resp. of a multiplicative group G_m according as λ is or is not zero. If we consider general fields F, then $\mathfrak{L}$ is the Lie p-algebra of a linear algebraic group *over* F if and only if $\lambda = \mu^{(p-1)/2}$ for some $\mu \in F$. (These considerations will be developed in what follows.)

3. **Lie algebras of affine groups.** It seems most efficient to present the notion of linear algebraic group over a general field F and of its Lie algebra in a context which is really that of affine schemes over F. For motivation, let us reconsider some notions of §1, where F is assumed algebraically closed, G is an algebraic subgroup of $GL(n, F)$ and $A(G)$ is the F-algebra of rational functions defined everywhere on G. In this setting, one has a product group $G \times G$, which may be regarded in a rather evident way as an algebraic subgroup of $GL(2n, F)$ consisting of diagonal blocks from G, and one may identify $A(G \times G)$ with $A(G) \otimes_F A(G)$ [8]. Corresponding to the map $((\alpha), (\beta))$ $\rightarrow (\alpha)(\beta)$ of $G \times G$ into G, we have a homomorphism of F-algebras with unit $\Delta: A(G) \rightarrow A(G) \otimes A(G)$ defined by $(f\Delta)((\alpha), (\beta)) = f((\alpha)(\beta))$ for $f \in A(G)$, $((\alpha), (\beta)) \in G \times G$. Associativity of G is reflected in co-associativity of $\Delta: \Delta(\Delta \otimes 1) = \Delta(1 \otimes \Delta)$, as maps of $A(G)$ into $A(G)$ $\otimes A(G) \otimes A(G)$. Likewise the mapping sending an element of G to its inverse yields an automorphism η of $A(G)$: $(f\eta)((\alpha)) = f((\alpha)^{-1})$, and corresponding to the identity I of G we have a homomorphism ϵ of F-algebras from $A(G)$ onto $F \subseteq A(G)$ sending f onto $f\epsilon = f(I)$. The group properties of G are faithfully reflected in the commutativity of various diagrams involving these maps, as displayed in [5] or [26]. Conversely, one can recover G (up to isomorphism) from $A(G)$ by taking the affine algebraic set of all F-homomorphisms of $A(G)$ into F and introducing product, inverse and identity by means of Δ, η, ϵ, respectively.

Consider therefore a commutative F-algebra A with unit, finitely generated over the (now arbitrary) field F, together with homomorphisms of F-algebras $\Delta: A \rightarrow A \otimes_F A$; $\eta: A \rightarrow A$; $\epsilon: A \rightarrow F \subseteq A$, making commutative the list of diagrams indicated above. Such an object will be called an *affine group over F*.

To define its Lie algebra, let us again consider the model of §1. There the elements of $\mathfrak{L}(G)$ correspond to derivations D of $A(G)$ as F-algebra, commuting with right translations by elements of G, or to F-derivations of $A = A(G)$ making the following diagram commutative:

$$
\begin{array}{ccc}
A & \xrightarrow{\Delta} & A \otimes A \\
D \downarrow & & \downarrow D \otimes 1 \\
A & \xrightarrow{\Delta} & A \otimes A
\end{array}
$$

(*)

Exactly such derivations of A, now defined abstractly as in the preceding paragraph, constitute a Lie algebra $\mathfrak{L}(A)$ over F (with $[DE] = DE - ED$), closed under pth iterates if F has prime characteristic p. We call $\mathfrak{L}(A)$ *the Lie algebra of the affine group A*. Considering only Lie p-algebras, the original question now becomes: *Given a Lie p-algebra $\mathfrak{L}$ over F, when is there an affine group A over F such that $\mathfrak{L}$ and $\mathfrak{L}(A)$ are isomorphic Lie p-algebras?*

In view of earlier remarks, it may seem at first rather surprising that the answer to this last question is: ALWAYS. The ideas for the construction of A given below seem to have originated independently with Manin [25] and Cartier [5]. Namely, let $\mathfrak{U}$ be the Jacobson "u-algebra" ([23, Chapter V]) of $\mathfrak{L}$, an associative algebra with unit over F of dimension p^n, $n = \dim \mathfrak{L}$. Denote by Δ^* the product in $\mathfrak{U}$; thus $\Delta^*: \mathfrak{U} \otimes {}_F \mathfrak{U} \to \mathfrak{U}$ is F-linear, as is ϵ^*, the isomorphism of F onto $F1 \subseteq \mathfrak{U}$. There is also an antiautomorphism η^* of $\mathfrak{U}$ of period two, sending elements of $\mathfrak{L}(\subseteq \mathfrak{U})$ into their negatives; a homomorphism $\pi^*: \mathfrak{U} \to \mathfrak{U} \otimes \mathfrak{U}$, sending each $x \in \mathfrak{L}$ onto $x \otimes 1 + 1 \otimes x$; and a homomorphism $\mu^*: \mathfrak{U} \to F1 \subseteq \mathfrak{U}$, sending each $x \in \mathfrak{L}$ to zero. Now let $A = \mathfrak{U}^*$, the dual space of $\mathfrak{U}$ over F, and denote the duals of the starred mappings above by removing stars. Then μ and π define on A a structure of p^n-dimensional F-algebra with unit, which is easily seen to be associative and commutative. The maps Δ, η, ϵ in turn give A the structure of affine group over F.

Now let $D \in \mathfrak{L}(A)$, and let $D^*: \mathfrak{U} \to \mathfrak{U}$ be the dual of D. From dualizing the diagram (*), we see that D^* commutes with all right multiplications in $\mathfrak{U}$, hence is left multiplication by some $u \in \mathfrak{U}$. Then dualizing the relation $\pi D = (D \otimes 1 + 1 \otimes D)\pi$, which expresses the fact that D is a derivation, shows that $u\pi^* = u \otimes 1 + 1 \otimes u$ (i.e., that u is a *primitive* element of $\mathfrak{U}$). But the elements u of $\mathfrak{U}$ satisfying this last condition are exactly those of $\mathfrak{L}$ [23, Chapter V], [28]. Now it is an easy matter to verify the isomorphism of $\mathfrak{L}(A)$ with $\mathfrak{L}$.

The reason for the disparity with earlier remarks lies in the generality admitted for A; namely, the kernel of ϵ above constitutes a nilpotent ideal of codimension one. From this it is clear that the only F-homomorphism of A into a field extension of F is the map ϵ, analogous to the identity of the group G when $A = A(G)$. (In the language of schemes, the only "geometric point" over F of Spec A is ϵ.) To return to the geometric case, we require that A be (the affine ring of a variety) *defined over F* in the sense of Weil, that is, that A be an integral domain whose field of quotients is a regular extension of F, or that $A \otimes_F K$ be an integral domain for every field extension K of F. We *impose this condition on A in further considerations.*

A few comments before passing on are in order. The affine group A of the construction above is a special case of an *infinitesimal formal group*, and a characterization of a class of infinitesimal formal groups corresponding exactly to the Lie p-algebras (not necessarily finite-dimensional) over F, in a manner extending that discussed here, has been given by Cartier [5] (see also [17, Exposés VII A, B]). Such groups actually arise in the context of linear algebraic groups, when one wishes to have something which plays the part of the kernel of a purely inseparable isogeny (cf. [37]).

4. Lie algebras of commutative affine groups.
The only cases where something like a systematic study of our question has been made are that of the *simple* Lie p-algebras, where the classification of Chevalley [11] in the algebraically closed case and that of Tits [39] in general give considerable information, and that of commutative Lie p-algebras. In the latter case, one is dealing simply with a vector space $\mathfrak{L}$ over F, of characteristic $p > 0$, and with a given p-semilinear mapping $x \to x^p$ of $\mathfrak{L}$ into $\mathfrak{L}$. It is this case which occupies the remainder of my talk, and indeed the formally more restricted question as to whether $\mathfrak{L}$ can occur as the Lie algebra of a *commutative* affine group defined over F.

Let $\mathfrak{L}^{p^k}$ denote the subspace of $\mathfrak{L}$ generated by the image of $\mathfrak{L}$ under the kth iterate of the mapping $x \to x^p$. Then these subspaces evidently form a descending chain, so stabilize at some point in a subalgebra $\mathfrak{T}$ with $\mathfrak{T}^p = \mathfrak{T}$, and with every element of $\mathfrak{N} = \mathfrak{L}/\mathfrak{T}$ being nilpotent with respect to the (induced) p-power operation. One says that $\mathfrak{T}$ is *toral* and $\mathfrak{N}$ is *nil*, and has the exact sequence $0 \to \mathfrak{T} \to \mathfrak{L} \to \mathfrak{N} \to 0$. If the field F is *perfect*, $\mathfrak{L}^p$ is actually the image of $\mathfrak{L}$ under $x \to x^p$, and Fitting's lemma applies to split the exact sequence, giving $\mathfrak{L} = \mathfrak{T} \oplus \mathfrak{N}$ [4, Exercise §1, #23]. Otherwise the sequence need not split. Although some Lie p-algebras of nonsplit type do occur as Lie algebras of

algebraic groups (for instance, the multiplicative group of a purely inseparable extension of F has such a Lie algebra), the only definite piece of information we have is that $\mathfrak{T}$ must be algebraic if $\mathfrak{L}$ is to be the Lie algebra of a commutative affine group defined over F. It seems unlikely that this necessary condition is sufficient. The answer seems to be unknown (for $p > 2$) even in the simplest case: Let $\mathfrak{L}$ have basis x, y, with $x^p = x$, $y^p = \alpha x$, where $\alpha \in F$ is not a pth power. (In case $p = 2$, this is the Lie algebra of the multiplicative group of $F(\alpha^{1/p})$.) I now further limit consideration to the cases where the sequence *does* split, and indeed to toral and nil algebras. From the theory of algebraic groups, it suffices to ask when a toral algebra $\mathfrak{T}$ over F is the Lie algebra of an algebraic torus defined over F and when a nil commutative Lie algebra over F is the Lie algebra of a commutative unipotent group defined over F. The former question will be dealt with in §5. Thus let $\mathfrak{N}$ be nil, commutative, over the field F of prime characteristic p.

If F is *perfect*, one has a well-developed theory of a single semilinear transformation which applies here to show that $\mathfrak{N}$ is a direct sum of cyclic subalgebras $\langle x \rangle$ (i.e., linear combinations of $x, x^p, x^{p^2}, \cdots$; see [22]). Now the construction of Dieudonné cited in §1 shows that $\langle x \rangle$ is the Lie algebra of a Witt group over F, so that $\mathfrak{N}$ is the Lie algebra of a direct sum of Witt groups, and is therefore algebraic in the sense demanded here. When F is *not* perfect, the theory of a p-semilinear transformation is inadequate; one can, however, obtain a quite explicit form for a nilpotent p-semilinear transformation, wherein certain parameters reflect the failure of the space to be a direct sum of cyclic subspaces. Namely, one readily produces a direct sum $\mathfrak{U}_1$ of cyclic subspaces, each of dimension k, containing $\mathfrak{N}^{p^{k-1}} \neq 0$, where $\mathfrak{N}^{p^k} = 0$. Then one enlarges $\mathfrak{U}_1$ by a subspace $\mathfrak{U}_2^1$ of $\mathfrak{N}^{p^{k-2}}$ supplementary to $\mathfrak{N}^{p^{k-2}} \cap \mathfrak{U}_1$, and constructs a subspace $\mathfrak{U}_2$, containing $\mathfrak{U}_2^1$, supplementary to $\mathfrak{U}_1$, and such that $\mathfrak{U}_2 + \mathfrak{N}^{p^{k-1}}$ is, modulo $\mathfrak{N}^{p^{k-1}}$, a direct sum of cyclic subspaces of dimension $k - 1$. The elements of $\mathfrak{U}_2^{p^{k-1}}$ are certain linear combinations of our canonical basis for $\mathfrak{U}_1^{p^{k-1}}$; they may be adjusted to be zero if F is perfect, but not in general. One repeats the process to express $\mathfrak{N}$ as a direct sum of subspaces $\mathfrak{U}_1 \oplus \mathfrak{U}_2 \oplus \cdots \oplus \mathfrak{U}_k$, where $\mathfrak{N}^{p^{k-j}}$ is contained in $\mathfrak{U}_1 \oplus \cdots \oplus \mathfrak{U}_j$, $\mathfrak{U}_j + \mathfrak{N}^{p^{k-j+1}}$ is a direct sum of cyclic subspaces of dimension $k - j + 1$, modulo $\mathfrak{N}^{p^{k-j+1}}$, and where $\mathfrak{U}_j^{p^{k-j+1}}$ is expressible in terms of a previously canonically chosen basis for those $\mathfrak{U}_i$, $i < j$. These last expressions introduce the indicated parameters, and $\mathfrak{N}$ is a direct sum of cyclic algebras exactly when the parameters can be made zero, as is the case with perfect fields.

Having an explicit comparison of $\mathfrak{N}$ with a direct sum of cyclic algebras, we can now reexamine the definition of (a direct sum of) Witt groups (see [42] or [24], Chapter III), with a view to introducing additional parameters which complicate the situation just enough to compensate for the parameters in our canonical form for $\mathfrak{N}$. It turns out that the desired complication can be achieved [35], retaining the property that the underlying variety of the resulting commutative unipotent group U is an affine space over F, with $\mathfrak{L}(\mathrm{U}) = \mathfrak{N}$, and with $\mathrm{U}^{p^j}/\mathrm{U}^{p^{j+1}}$ a vector group having as Lie algebra $\mathfrak{N}^{p^j}/\mathfrak{N}^{p^{j+1}}$ for each j. When all the parameters are zero, the construction yields a direct sum of Witt groups. The conclusion is the following theorem:

THEOREM I. *Let $\mathfrak{N}$ be a finite-dimensional commutative Lie p-algebra over F, with nilpotent p-power operation of exponent k. Then there is a commutative unipotent algebraic group U defined over F, of exponent p^k, with underlying variety an affine space over F, and such that $\mathfrak{L}(U)$ is isomorphic to $\mathfrak{N}$.*

As an illustration of the above, let $\mathfrak{N}$ have basis e_1, e_2, e_3 with $e_2^p = e_1$, $e_3^p = \alpha e_1$, $e_1^p = 0$, $\alpha \notin F^p$. The resulting group U may be regarded as affine 3-space over F, with operation (written additively)

$$(\xi_1, \xi_2, \xi_3) + (\eta_1, \eta_2, \eta_3) = (\zeta_1, \zeta_2, \zeta_3),$$

where

$$\zeta_2 = \xi_2 + \eta_2, \quad \zeta_3 = \xi_3 + \eta_3,$$

$$\zeta_1 = \xi_1 + \eta_1 - \sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!} (\xi_2^i \eta_2^{p-i} + \alpha \xi_3^i \eta_3^{p-i}).$$

The tangent vectors at the origin along the respective axes satisfy the same relations as do e_1, e_2, e_3.

A tempting conjecture, which I have only been able to prove in some special cases, is that Theorem I remains valid when the two occurrences of the word "commutative" are deleted.

5. Lie algebras of algebraic tori.

By an *algebraic torus* over F we shall understand an affine algebraic group over F (i.e., an algebra A defined over F as in §3) such that upon suitable extension of the base field, say to K, there is an isomorphism of A_K (respecting all operations, including ϵ, η, Δ) with $K[Z^n]$, the group algebra of a free (multiplicative) abelian group of rank n. The operations ϵ, η, Δ for $K[Z^n]$ are determined by: $x\epsilon = 1$; $x\eta = x^{-1}$; $x\Delta = x \otimes x$, for all $x \in Z^n$. This latter group will be called a *split torus* over K of dimension n, and K will be called a *splitting field* for A. It is known (cf. [3, p. 61]) that

every algebraic torus A over F has a splitting field K such that K/F is a finite Galois extension, and that a subfield K of a given separable closure S of F is a splitting field for A if and only if every K-automorphism σ of S, when acting on A_S in such a way as to be σ-semilinear and to fix A, also fixes all elements of $Z^n \subseteq A_S$. (The map Δ enables the elements of Z^n to be distinguished as those $x \in A_S$ such that $x\Delta = x \otimes x$—the *characters* of A.) By taking K to be the fixed field of the subgroup $\mathfrak{G}$ fixing Z^n in the Galois group $\mathfrak{G}(S/F)$, we obtain a unique minimal splitting field for A, with K/F a finite Galois extension.

When $A = F[Z^n]$ is a split torus over F, with $x_1, \cdots, x_n$ free generators for Z^n, the tangent space at the identity has as basis the partial derivatives, evaluated at $x_1 = \cdots = x_n = 1$, with respect to the x_i, and each of these tangent vectors extends uniquely to an element D_i of $\mathfrak{L}(A)$, the Lie algebra. One has $x_i D_j = \delta_{ij} x_j$, and the D_i form a basis for $\mathfrak{L}(A)$ over F, with $D_i^p = D_i$ for all i when the characteristic is a prime p. Here $\mathfrak{L}(A)$ is isomorphic to a direct sum $F \oplus \cdots \oplus F$ of n commutative Lie p-algebras isomorphic to F with its own p-power operation. A Lie p-algebra having this structure is clearly toral, and will be called the (n-dimensional) *split toral algebra*.

Now every toral algebra $\mathfrak{T}$ over a field F is split by a finite Galois extension K of F, and K is minimal when chosen as a (minimal) splitting field for the family of minimal p-polynomials satisfied by a basis for $\mathfrak{T}$ [33]. It follows that every homomorphism ϕ, of Lie p-algebras over F, mapping $\mathfrak{T}$ into an algebraic closure of F containing K actually maps $\mathfrak{T}$ into K. Such homomorphisms form an additive group, the group of *characters* of $\mathfrak{T}$. By inspection of their extensions to $\mathfrak{T}_K$, one sees that the characters of $\mathfrak{T}$ are an elementary p-group of order p^n, where $n = \dim \mathfrak{T}$.

Suppose now that $\mathfrak{T} = \mathfrak{L}(A)$, where A is an algebraic torus over F. Let K/F be a finite Galois extension with group $\mathfrak{G}$, splitting A. Then $\mathfrak{T}_K = \mathfrak{L}(A_K)$ is a split toral algebra over K, from which it follows that $\mathfrak{T}$ is a toral algebra over F with K as a splitting field. Thus the characters of $\mathfrak{T}$ have their values in K, and so are acted on in an obvious way by the automorphisms in $\mathfrak{G}$. From the action of $\mathfrak{G}$ on A_K, one sees that for $x \in A_K$, $\sigma \in \mathfrak{G}$, $(x^\sigma)\Delta = (x\Delta)(\sigma \otimes \sigma)$, so that σ maps into itself the set of those $x \in A_K$ with $x\Delta = x \otimes x$; this is just the character group of A, identified with Z^n in our presentation of A_K. Thus $\mathfrak{G}$ acts on *this* character group.

Starting with a character x of A, we may form its differential dx, which turns out to be a character of $\mathfrak{T}$. With the action of $\mathfrak{G}$ as above, the mapping $x \to dx$ is actually a $\mathfrak{G}$-homomorphism of Z^n onto the

character group of $\mathfrak{T}$. One can see all this without having to discuss differentials, as follows: Let $x_1, \cdots, x_n$ be free generators for the character group of A, and let $D_1, \cdots, D_n$ be the associated basis for $\mathfrak{T}_K$ as defined above. Then the monomials $x_1^{\nu_1} \cdots x_n^{\nu_n}$ ($\nu_i \in \mathbf{Z}$) form a basis for A_K, identified with $\mathbf{Z}^n$; moreover, the displayed element is a common eigenvector for all the D_i, corresponding to the eigenvalue ν_i of D_i. Now one sees at once that the mapping sending $x_1^{\nu_1} \cdots x_n^{\nu_n}$ to that character of T_K whose value at D_i is ν_i is a homomorphism of $\mathbf{Z}^n$ onto the character group of $\mathfrak{T}_K$ (which is also that of $\mathfrak{T}$), with kernel consisting of those monomials with all ν_i divisible by p. From the manner of action of $\mathfrak{G}$ on both groups it is seen that this mapping is a $\mathfrak{G}$-homomorphism.

Taking K to be the minimal splitting field for A, we see that a splitting field for $\mathfrak{T}$ is obtained as a fixed field L of that subgroup $\mathfrak{H}$ of $\mathfrak{G}$ which acts trivially on the characters of $\mathfrak{T}$, and that L is the minimal splitting field for $\mathfrak{T}$. But $\mathfrak{H}$ is just the kernel of the homomorphism of $\mathfrak{G}$, now regarded as a group of automorphisms of $\mathbf{Z}^n$, onto the group of automorphisms of $\mathbf{Z}^n/p\mathbf{Z}^n$ induced by $\mathfrak{G}$. That is, $\mathfrak{H}$ is the subgroup of $\mathfrak{G}$, a finite group of integral matrices, consisting of those elements of $\mathfrak{G}$ which are congruent to the identity modulo p. In these circumstances, it is well known that $\mathfrak{H}$ must be trivial unless $p = 2$, in which case there is a basis for $\mathbf{Z}^n$ relative to which $\mathfrak{H}$ consists of diagonal matrices with ± 1 on the diagonal [29]. That is, *K is also a minimal splitting field for $\mathfrak{T}$ unless $p = 2$. In particular, if A is a torus over F, of prime characteristic $\neq 2$, then $\mathfrak{X}(A)$ is split if and only if A is split.*

The characteristic two is really exceptional in the above. For example, the group of elements of norm one in an Artin-Schreier extension of F (with $p = 2$) may be described in our formalism as follows: Let $\alpha \in F$ be such that $X^2 + X + \alpha$ is irreducible in $F[X]$; let $A = F[x, y]$, subject to the relation $x^2 + xy + \alpha y^2 = 1$. Let ϵ send x to 1, y to 0; let Δ send x to $x \otimes x + \alpha y \otimes y$, y to $x \otimes y + y \otimes x + y \otimes y$; let η send x to $x + y$, y to y. Then one verifies easily that A defines an affine group over F. Let $K = F(\mu)$, where $\mu^2 + \mu + \alpha = 0$, and let $X = x + \mu y \in A_K$. Then $X^{-1} = x + y + \mu y = X\eta \in A_K$, $X\Delta = X \otimes X$, and $A_K = K[X, X^{-1}]$, X being transcendental over K. Thus K is a splitting field for the algebraic torus A over F, and the generating automorphism σ of the Galois group $\mathfrak{G}(K/F)$ sends μ into $\mu + 1$; hence interchanges X and X^{-1}. It follows that no character other than the trivial one is fixed by σ, so that K is a minimal splitting field for A. In particular, A is not a split torus. However, the derivation of $F[X, Y]$ sending X to X, Y to 1, i.e., the operator $X\partial/\partial X + \partial/\partial Y$, yields a

nonzero derivation D of A over F which is seen to be in $\mathfrak{L}(A)$ and to satisfy $D^2 = D$. Thus D is a basis for $\mathfrak{L}(A)$, a split toral algebra even though the torus A is not split.

The following theorem characterizes the Lie algebras of algebraic tori:

THEOREM II. *Let $\mathfrak{L}$ be a Lie p-algebra of dimension n over the field F of prime characteristic p. Then $\mathfrak{L}$ is the Lie algebra of an algebraic torus over F if and only if the following hold:*

  (1) *$\mathfrak{L}$ is toral;*

  (2) *There is a finite Galois extension K/F which splits $\mathfrak{L}$, an action of the Galois group $\mathfrak{G} = \mathfrak{G}(K/F)$ on Z^n, and a $\mathfrak{G}$-homomorphism of Z^n onto the character group of $\mathfrak{L}$.*

We have already seen the necessity of the conditions. Conversely, the assumed action of $\mathfrak{G}$ on Z^n combines with the action of $\mathfrak{G}$ on K to give a representation of $\mathfrak{G}$ by semilinear F-automorphisms of $K[Z^n]$, commuting (in the appropriate senses) with the operators Δ, η, ϵ for the K-split torus $K[Z^n]$. It follows that the fixed set A of this action constitutes an F-form of $K[Z^n]$, i.e., an n-dimensional torus over F split by K (cf. [31]). The character group of A is Z^n, so one has a $\mathfrak{G}$-isomorphism of Z^n/pZ^n onto the character group of $\mathfrak{L}(A)$. Thus $\mathfrak{L}$ and $\mathfrak{L}(A)$ are toral, split by K, and have $\mathfrak{G}$-isomorphic character groups. Now $\mathfrak{L}_K$ may be viewed dually as the set of homomorphisms of its character group into K, forming a K-vector space closed under p-powers. From the $\mathfrak{G}$-isomorphism of the character groups, one obtains a $\mathfrak{G}$-isomorphism of $\mathfrak{L}_K$ and $\mathfrak{L}(A)_K$; hence an isomorphism (over F) of $\mathfrak{L}$ and $\mathfrak{L}(A)$.

In particular, a one-dimensional Lie p-algebra $\mathfrak{L}$ over F with basis x, $x^p = \lambda x \neq 0$, satisfies (1) and will satisfy (2) only if $\mathfrak{L}$ is split by a quadratic extension K of F (the action of $\mathfrak{G}$ on Z can only be $\pm I$). Then there is $\mu \in K$, $(\mu x)^p = \mu x$, or $\mu^{p-1}\lambda = 1$, so that λ is a $(p-1)$th power in K. If λ is a $(p-1)$th power in F, then $\mathfrak{L}$ is split and we are done. If not, but if $\lambda = \nu^{p-1}$, $\nu \in K$, then $p > 2$ and inspection of the minimum polynomial for ν over F shows that $\nu^2 \in F$, $\lambda \in F^{(p-1)/2}$. In particular, if F is finite $\lambda = \pm 1$. This case $\lambda \notin F^{p-1}$, $\lambda = \mu^{(p-1)/2}$, $\mu \in F$, is actually algebraic and may be realized as the Lie algebra of the multiplicative group of elements of norm one of $F\sqrt{\mu}$), a group for which the algebra A may be given analogously to the example of an Artin-Schreier extension above.

Combining our theorems, we see that *a commutative Lie p-algebra over F which splits into a toral and a nil algebra* (a condition which is always satisfied if F is perfect) *is the Lie algebra of a commutative*

affine algebraic group over F *if and only if its toral part satisfies the condition* (2) *of Theorem* II.

One may also ask which commutative Lie p-algebras over F can occur as Lie algebras of general commutative group-varieties over F, in particular of abelian varieties. Here one already sees in dimension one that the class of algebraic Lie algebras is larger than the above. The question awaits further study.

BIBLIOGRAPHY

1. A. Borel, *Groupes linéaires algébriques*, Ann. of Math. **64** (1956), 20–82.

2. A. Borel and T. A. Springer, *Rationality properties of linear algebraic groups*, Proc. Sympos. Pure Math., Vol. 9, Amer. Math. Soc., Providence, R. I., 1966, pp. 26–32.

3. A. Borel and J. Tits, *Groupes réductifs*, Inst. Hautes. Études Scientifiques Publ. Math. 27 (1965), 55–150.

4. N. Bourbaki, "Algèbres de Lie" in *Groupes et algèbres de Lie*, Hermann, Paris, 1960, Chapter I.

5. P. Cartier, *Groupes algébriques et groupes formels*, Colloq. Théorie des gpes. Algs., Brussels, 1962, pp. 87–111.

6. C. Chevalley, *A new kind of relationship between matrices*, Amer. J. Math. **65** (1943), 521–531.

7. ———, *Theory of Lie groups*. I, Princeton Univ. Press, Princeton, N. J., 1946.

8. ———, "Groupes algébriques" in *Théorie des groupes de Lie*, Hermann, Paris, 1951, Vol. II.

9. ———, "Théorèmes généraux sur les algèbres de Lie" in *Théorie des groupes de Lie*, Hermann, Paris, 1951, Vol. III.

10. ———, *Sur certains groupes simples*, Tôhoku Math. J. 7 (1956), 14–66.

11. C. Chevalley et al., *Classification des groupes de Lie algébriques*, Vols. 1, 2, Séminaire C. Chevalley, Paris, 1958.

12. C. Chevalley and H. F. Tuan, *On algebriac Lie algebras*, Proc. Nat. Acad. Sci. USA **31** (1945), 195–196.

13. I. S. Cohen, *Note on a note of H. F. Tuan*, Bull. Amer. Math. Soc. 52 (1946), 175–177.

14. J. Dieudonné, *Sur les groupes de Lie algébriques sur un corps de caractéristique* $p > 0$, Rend. Circ. Mat. Palermo 1(1952), 380–402.

15. ———, *Witt groups and hyperexponential groups*, Mathematika 2(1955), 21–31.

16. ———, *Les algèbres de Lie simples associées aux groupes simples algébriques sur un corps de caractéristique* $p > 0$, Rend. Circ. Mat. Palermo 6(1957), 198–204.

17. A. Grothendieck et al., *Schémas en groupes*, Report of Inst. Hautes Études Scientifiques Séminaire de Géométrie algébrique, Paris, 1963/64.

18. G. Hochschild, *On the algebraic hull of a Lie algebra*, Proc. Amer. Math. Soc. 11(1960), 195–199.

19. ———, *An addition to Ado's theorem*. Proc. Amer. Math. Soc. 17(1966), 531–533.

20. J. E. Humphreys, *Algebraic groups and modular Lie algebras*, Mem. Amer. Math. Soc. No. 71(1967).

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

22. ———, *Commutative restricted Lie algebras*, Proc. Amer. Math. Soc. 6(1955), 476–481.

23. ———, *Lie algebras*, Interscience, New York, 1962.

24. ———, "Theory of fields and Galois theory" in *Lectures in abstract algebra*, Vol. III, Van Nostrand, Princeton, N. J., 1964.

25. Ju. I. Manin, *A remark on Lie p-algebras*, Sibirsk. Mat. Ž. 3(1962), 479–480. (Russian)

26. ———, *The theory of commutative formal groups over fields of finite characteristic*, Uspehi Mat. Nauk 18(1963), 3–90 = Russian Math. Surveys 18(1963), 1–80.

27. L. Maurer, *Zur Theorie der continuierlichen, homogenen und linearen Gruppen*, Sitzungsber. Bayr. Akad. Math.-Phys. Cl. 24(1894), 297–341.

28. J. W. Milnor and J. C. Moore, *On the structure of Hopf algebras*, Ann. of Math. 81(1965), 211–264.

29. H. Minkowski, *Gesammelte Abhandlungen*, Bd. 1, Abh. V and VI, Teubner, Leipzig, 1911.

30. T. Ono, *Sur les groupes de Chevalley*, J. Math. Soc. Japan 10(1958), 307–313.

31. ———, *Arithmetic of algebraic tori*, Ann. of Math. 74(1961), 101–139.

32. G. B. Seligman, *Algebraic groups*, Yale Lecture notes, 1964.

33. ———, *Some results on Lie p-algebras*, Bull. Amer. Math. Soc. 73(1967), 528–530.

34. ———, *Modular Lie algebras*, Springer, Berlin, 1967.

35. ———, *On some commutative unipotent groups*, Invent. Math. 5(1968), 129–137.

36. J.-P. Serre, *Faisceaux algébriques cohérents*, Ann. of Math. 61(1955), 197–278.

37. ———, *Quelques propriétés des variétés abéliennes en caractéristique p*, Amer. J. Math. 80 (1958), 715–739.

38. R. Steinberg, *Automorphisms of classical Lie algebras*, Pacific J. Math. 11 (1961), 1119–1129.

39. J. Tits, *Classification of algebraic semisimple groups*, Proc. Sympos. Pure Math., Vol. 9, Amer. Math. Soc., Providence, R. I., 1966, pp. 33–62.

40. H. F. Tuan, *A note on the replicas of nilpotent matrices*, Bull. Amer. Math. Soc. 51 (1945), 305–312.

41. D. J. Winter, *Solvable and nilpotent subalgebras of Lie algebras*, Bull. Amer. Math. Soc. 74 (1968), 754–758.

42. E. Witt, *Zyklische Koerper und Algebren der Charakteristik p vom Grad p^n*, J. für Math. (Crelle) 176 (1937), 126–140.

YALE UNIVERSITY