ON THE GALOIS THEORY OF INSEPARABLE EXTENSIONS

BY MURRAY GERSTENHABER[1]

Communicated by N. Jacobson, March 9, 1964

Let K be a field of characteristic $p \neq 0$ and Der K denote the set of all derivations of K into itself, i.e., of additive maps ϕ of K into itself such that $\phi(xy)=\phi(x)y+x\phi(y)$ for all x and y in K. Then Der K is (1) a vector space over K, (2) closed under the formation of pth powers, i.e., ϕ in Der K implies ϕ^p is in Der K, and (3) a Lie subring of the ring of additive endomorphisms of K, i.e., ϕ, ψ in Der K imply $\phi\psi-\psi\phi$ is in Der K. A theorem of Jacobson [6] gives a relationship between the subfields k of K with $K^p \subset k$ and $[K:k] < \infty$, and "restricted" Lie subrings of Der K, which are finite-dimensional vector spaces over K, i.e., the subsets D satisfying (1), (2), and (3) with $\dim_K D < \infty$. Indeed, given such a k, then the set $\mathrm{Der}_k K$ of those derivations of K into itself which vanish on k is clearly a restricted Lie subring of finite dimension over K, and if $[K:k]=p^m$, then one has $\dim_K(\mathrm{Der}_k K)=m$. Conversely, Jacobson demonstrated that given a restricted subring D of Der K which is a finite-dimensional vector space over K, and denoting by k the constant field of D, i.e., the set of all x in K such that $\phi(x)=0$ for all ϕ in D, then in fact $D=\mathrm{Der}_k K$, whence if $\dim_K D=m$, then $[K:k]=p^m$. If ϕ is in $\mathrm{Der}_k K$ then we say that ϕ is a derivation "over k."

It is remarkable that from the hypotheses of Jacobson's theorem *one may delete the assumption that D be a Lie subring* of Der K. In fact, if we define a *restricted subspace* of Der K to be a subset which is a vector space over K and which is closed under the formation of pth powers, then one may assert: *If D is a finite-dimensional restricted subspace of* Der K, *and if k is the field consisting of all x in K such that $\phi(x)=0$ for all ϕ in D, then $D=$* $\mathrm{Der}_k K$. It follows a posteriori that D must be a Lie subring of Der K. The purpose of the present note is to give a simple proof of this strengthened result. For connections with other work, see the "concluding remarks."

1. **Derivations of a field.** Let K be a field of characteristic $p \neq 0$ and Der K denote the set of derivations of K into itself. Given ϕ in Der K, the set of x in K such that $\phi(x)=0$ forms a subfield K_ϕ of K called the constant field of ϕ; if x is in K_ϕ then $\phi(xy)=x\phi(y)$ for all y in K, and conversely. We note that since $\phi(x^p)=0$ for all x in K, we

[1] The author wishes to acknowledge the support of the National Science Foundation under contract G-24412.

have $K^p \subset K_\phi$ for every ϕ in Der K. Therefore, if a is in K but not in K_ϕ, then $[K_\phi(a):K_\phi]=p$.

Suppose given ϕ in Der K and a in K such that $\phi(a)\neq 0$. Then setting $\psi=a\phi(a)^{-1}\phi$, we have $\psi(a)=a$. Therefore, $\phi(a)\neq 0$ implies that there is a multiple ψ of ϕ having a as a proper vector with proper value unity. Note that $K_\phi=K_\psi$. Suppose now that for some ϕ in Der K and a, b in K, we have $\phi(a)=\lambda a$, $\phi(b)=\mu b$ with λ, μ in K_0. Then $\phi(a^{-1})=-\lambda a$ and $\phi(ab)=(\lambda+\mu)ab$. It follows that if $\phi(a')=\lambda a'$ and also $\phi(a'')=\lambda a''$, λ in K_ϕ, then $\phi(a'/a'')=0$, i.e., a'/a'' lies in K_ϕ. Therefore, if λ is in K_ϕ, then the set of those a in K such that $\phi(a)=\lambda a$ is either reduced to the zero element or is a one-dimensional vector space over K_ϕ.

LEMMA 1. *Suppose given ϕ in* Der K *and $a\neq 0$ in K such that $\phi(a)=a$. Set $\psi=\phi^p-\phi$. Then $K_\psi=K_\phi(a)$.*

PROOF. Since $\phi(a)=a$ implies $\phi^p(a)=a$, it follows that $\psi(a)=0$, whence $K_\psi\supset K_\phi(a)$. It remains to prove the reverse inclusion.

Note first that since the characteristic is p, we have $\phi^p-\phi=\phi(\phi-1)(\phi-2)\cdots(\phi-p+1)$. Set now $f(t)=t^p-t=t(t-1)\cdots(t-p+1)$, and define polynomials $f_i(t)$, $i=0, 1, \cdots, p-1$ of degree $p-1$ in t by $f_i(t)=f(t)\cdot(t-i)^{-1}$. We have then $f_i(j)=0$ if $i\neq j$, but $f_i(i)\neq 0$. Therefore, the polynomials $f_i(t)$, which have coefficients in the Galois field $\boldsymbol{F}_p$ of p elements, are linearly independent over that field, since indeed, if $\sum\gamma_i f_i(t)=0$, γ_i in $\boldsymbol{F}_p$, then substituting j for t, one finds $\gamma_j=0$. It follows that every polynomial $g(t)$ of degree $p-1$ or less, with coefficients in $\boldsymbol{F}_p$, is a linear combination over $\boldsymbol{F}_p$ of the polynomials $f_i(t)$. In particular, we have $\sum\alpha_i f_i(t)=1$ for suitable integers α_i (mod p).

Now suppose that b is in K_ψ, i.e., that $(\phi^p-\phi)(b)=\phi(\phi-1)\cdots(\phi-p+1)(b)=0$. It follows that $(\phi-i)f_i(\phi)(b)=0$, or setting $f_i(\phi)(b)=b_i$, we have $(\phi-i)(b_i)=0$, $i=0, 1, \cdots, p-1$. But $(\phi-i)(a^i)=0$, whence b_i/a^i is in K_ϕ, and therefore b_i is in $K_\phi(a)$ for $i=0, 1, \cdots, p-1$. However, $\sum\alpha_i f_i(\phi)=1$, whence $\sum\alpha_i b_i=b$, and b being thus a linear combination with integer coefficients of elements of $K_\phi(a)$, we have shown that b lies in the same field. Therefore indeed $K_\psi\subset K_\phi(a)$, ending the proof.

We recall that if K is an inseparable extension of a field k, then a finite set $x_1, \cdots, x_n$ of elements of K is said to be *p-independent* over k if the p^n monomials $x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$, $0\leqq i_q<p$ are linearly independent over kK^p. An infinite set is independent if every finite subset is, and a maximal p-independent set is a *p-basis* of K over k. If $[K:kK^p]=p^m$ and is finite, then the dimension (i.e., cardinality) of a

p-basis of K over k is m, and conversely, and a necessary and sufficient condition that $x_1, \cdots, x_m$ be a p-basis over k is that there exist $\phi_1, \cdots, \phi_m$ in $\operatorname{Der}_k K$ such that denoting by δ_{ij} the Kronecker delta ($\delta_{ij}=0$ if $i\neq j$, $\delta_{ii}=1$), one has $\phi_i(x_j)=\delta_{ij}$. These ϕ_i then constitute a basis over K for $\operatorname{Der}_k K$. A detailed discussion of p-bases can be found in Zariski-Samuel, Vol. I [8, p. 129], or Jacobson [7, p. 180].

Given ϕ in $\operatorname{Der} K$, let D_ϕ denote the smallest restricted subspace of $\operatorname{Der} K$ containing ϕ. Since for any ψ in $\operatorname{Der} K$ and a in K, $(a\psi)^p$ can easily be shown to be of the form $b\psi^p+c\psi$ for certain b and c in K, D_ϕ is just the set of all derivations of the form $a_0\phi+a_1\phi^p+\cdots+a_m\phi^{p^m}$, a_i in K, $m=0, 1, \cdots$. We shall not, however, need this remark.

Lemma 2. *If ϕ is in* Der K *and $x_1, \cdots, x_m$ are p-independent over K_ϕ, then there exist $\phi_1, \cdots, \phi_n$ in D_ϕ such that $\phi_i(x_j)=\delta_{ij}$. (These ϕ_i are then, in particular, linearly independent over K.)*

Proof. It is clearly sufficient to show that there exists a ψ in D_ϕ such that $\psi(x_1)\neq 0$ but $\psi(x_2)=\cdots=\psi(x_n)=0$. Since $\phi(x_2)\neq 0$, there exists a multiple $a\phi$, a in K, such that $a\phi(x_2)=x_2$. Setting $\phi'=(a\phi)^p-(a\phi)$, we have ϕ' in D_ϕ, and by Lemma 1, $K_{\phi'}=K_\phi(x_2)$. Since the latter field does not contain x_3, we have $\phi'(x_3)\neq 0$, and proceeding as before, can construct ϕ'' in D_ϕ with $K_{\phi''}=K_{\phi'}(x_3)=K_\phi(x_2, x_3)$. Continuing, we obtain an element ψ in D_ϕ with $K_\psi=K_\phi(x_2, \cdots, x_n)$. Since x_1 is not in the latter field, we have $\psi(x_1)\neq 0$ but $\psi(x_2)=\cdots=\psi(x_n)=0$, as required. This ends the proof.

The foregoing has the following

Corollary. *$[K:K_\phi]$ is finite if and only if* $\dim_K D_\phi$ *is finite, and in that case D_ϕ is the set of all derivations of K vanishing on K_ϕ. In particular, D_ϕ is then a Lie subring of* Der K.

Proof. Since $K^p\subset K_\phi$, if $[K:K_\phi]$ is infinite, then the dimension of a p-basis of K over K_ϕ is infinite, and there exist, by the lemma, for every positive n, at least n elements of D_ϕ which are linearly independent over K. Therefore $\dim_K D_\phi$ in this case is infinite. On the other hand, if $[K:K_\phi]=p^n$ and is finite, and if $x_1, \cdots, x_n$ is a p-basis of K over K_ϕ, then the $\phi_1, \cdots, \phi_n$ of the lemma are a basis over K for the Lie ring of derivations of K over K_ϕ. Since D_ϕ is contained in the latter ring and also contains a basis over K for it, it coincides with it. This ends the proof.

Finally, one may remark that if k is a subfield of K such that $K^p\subset k$, then there is a ϕ in $\operatorname{Der}_k K$ such that $K_\phi=k$. Indeed, if (x_i) is a p-basis for K over k, then a derivation ϕ of K over k is completely determined by its values at the x_i. Choosing $\phi(x_i)=\lambda_i x_i$, λ_i in k, we have for any monomial M of the form $x_{i_1}^{j_1}\cdots x_{i_n}^{j_n}$, $0\leqq j_q<p$, $\phi(M)=(\lambda_1 j_1+\cdots+\lambda_n j_n)M$, and it is sufficient to choose the λ_i in such a way that no expression of the form $\lambda_1 j_1+\cdots+\lambda_n j_n$ vanishes except if all the j_q are zero, i.e., such that the λ_i are linearly independent over the prime field. To this end it is sufficient to take $\lambda_i=(x_i)^p$, for the x_i being linearly independent over k, it follows that the λ_i are linearly independent over k^p, hence a fortiori over the prime field.

2. **The main theorem.** Given ϕ and ψ in Der K, we shall denote by $D_{\phi,\psi}$ the smallest restricted subspace of Der K containing both ϕ and ψ.

LEMMA 3. *Given ϕ, ψ in* Der K, *let $x_1,\cdots,x_m$ be elements of K which are p-independent over K_ϕ, and y be an element of K_ϕ with $\psi(y)\neq 0$. Then there exists an element θ in $D_{\phi,\psi}$ such that $x_1,\cdots,x_m$, y are p-independent over K_θ. Further, $[K:K_\phi\cap K_\psi]$ is finite if and only if* $\dim_K D_{\phi,\psi}$ *is finite, and in the latter case there exists a θ in $D_{\phi,\psi}$ such that $K_\theta=K_\phi\cap K_\psi$ and $D_\theta=D_{\phi,\psi}$.*

PROOF. By Lemma 2, there exist $\phi_1,\cdots,\phi_n$ in D_ϕ such that $\phi_i(x_j)=\delta_{ij}$. Since y is in K_ϕ, we have further that $\phi_i(y)=0$. It follows that subtracting from ψ a suitable linear combination over K of the ϕ_i, and multiplying the result by a suitable element of K, we can obtain a ψ' in $D_{\phi,\psi}$ with $\psi'(x_j)=0$, $j=1,\cdots,n$, and $\psi'(y)=1$. Now set $x_i^p=\lambda_i$, $y^p=\mu$, and set $\theta=\sum\lambda_i x_i\phi_i+\mu y\psi'$. Then, as in the final remark of the preceding section, θ can not vanish on any monomial M in the x_i and y with non-negative exponents less than p except $M=1$. The x_i and y are therefore p-independent, as asserted, over K_θ.

As for the rest (observe that if at least one is infinite), and as both $[K:K_\theta]\leqq[K:K_\phi\cap K_\psi]$ and $\dim_K D_\theta\leqq\dim_K D_{\phi,\psi}$ for all such θ, it follows that both $\dim_K D_{\phi,\psi}$ and $[K:K_\phi\cap K_\psi]$ are infinite. In the contrary case, there exists a θ in $D_{\phi,\psi}$ for which $\dim_K D_\theta$ is finite and maximal. Then for this θ we must have $K_\theta=K_\phi\cap K_\psi$, for were this not the case then there would exist a y in K_θ which was not in $K_\phi\cap K_\psi$, whence either $\phi(y)\neq 0$ or $\psi(y)\neq 0$. Assuming, without loss of generality, the latter, and letting $x_1,\cdots,x_n$ be the p-basis of K over K_θ, the first part of the lemma would construct a new θ with $[K:K_\theta]$ even larger, a contradiction. Therefore indeed $K_\theta=K_\phi\cap K_\psi$, whence by Lemma 2 we have also $D_\theta=D_{\phi,\psi}$. This ends the proof.

The foregoing has the following immediate

COROLLARY. *Let D be a finite-dimensional restricted subspace of*

Der K, *and* k *be its constant field. Then there exists a* θ *in* D *such that* $K_\theta = k$, *whence* $D_\theta = \mathrm{Der}_k\, K$.

This in turn immediately implies the final result.

THEOREM. *Let* K *be a field of characteristic* $p \neq 0$, D *be a restricted subspace of* Der K, *and* k *be the constant field of* D. *Then* $[K:k]$ *is finite if and only if* $\dim_K D$ *is finite, and in the latter case* $D = \mathrm{Der}_k\, K$. *Moreover,* D *is then a Lie subring of* Der K, *there is an element* θ *in* D *such that* $k = K_\theta$, *and for any such* θ *we have* $D = D_\theta$.

3. **Concluding remarks.** The analogy between Jacobson's theorem and the fundamental theorem of the Galois theory has led to highly successful attempts, mainly by Hochschild [2], and more recently by Hoechsmann [3], to use restricted Lie algebras in the study of simple algebras with purely inseparable splitting fields. Many basic ideas are traceable to Jacobson [4], [5]. The central role of Jacobson's theorem is evident in [2], where another proof is given. The usefulness of having a restricted space of derivations generated by a single element can be seen in [3].

A weaker form of the present main theorem has been obtained independently by Jacobson, who proved that if D is a restricted subspace of Der K with constant field k, and if $[K:k]$ is known a priori to be finite, then $D = \mathrm{Der}_k\, K$. The proposition is given as Exercise 4, p. 190 of [7], in which it is required to show that D is closed under commutation, Jacobson's original theorem then being applicable.

The starting point of the present investigation, and one of the intimations that the hypothesis of Lie closure was inessential, came from the deformation theory for rings and algebras initiated by the author [1]. The present note is, in fact, a fragment split from a paper in preparation in which the concepts of separability and degree of inseparability are defined for arbitrary algebras, and a form of Galois theory given in which the notion of deformation is central. The reason for publishing this fragment separately is that while assuming very little and using only elementary techniques, it rapidly both proves and strengthens a fundamental theorem.

REFERENCES

1. M. Gerstenhaber, *On the deformation of rings and algebras*, Ann. of Math. (2) **79** (1964), 59–104.

2. G. Hochschild, *Simple algebras with purely inseparable splitting fields of exponent one*, Trans. Amer. Math. Soc. **79** (1955), 477–489.

3. K. Hoechsmann, *Simple algebras and derivations*, Trans. Amer. Math. Soc. **108** (1963), 1–12.

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

5. ———, *p-Algebras of exponent p*, Bull. Amer. Math. Soc. **43** (1937), 667–670.

6. ———, *Galois theory of purely inseparable fields of exponent one*, Amer. J. Math. **46** (1944), 645–648.

7. ———, *Lectures in abstract algebra*, Vol. III, Van Nostrand, Princeton, N. J., 1964.

8. O. Zariski and P. Samuel, *Commutative algebra*, Van Nostrand, Princeton, N. J., 1958.

UNIVERSITY OF PENNSYLVANIA

A SPARSE REGULAR SEQUENCE OF EXPONENTIALS CLOSED ON LARGE SETS

BY H. J. LANDAU

Communicated by P. D. Lax, March 30, 1964

Introduction. For a given sequence $\{\lambda_k\}$ of complex numbers, the problem of determining those intervals I on which the exponentials $\{e^{i\lambda_k x}\}$ are complete in various function spaces has been extensively studied [3]. Since the problem is invariant under a translation of I, only the lengths of I are involved, and attention has focused on the relation between these lengths and the density of the sequence $\{\lambda_k\}$. With the function space taken to be $L^p(I)$ for $1 \leqq p < \infty$, or $C(I)$, the continuous functions on I, the general character of the results has been that there exist sparse real sequences ($\lim r^{-1}$ (the number of $|\lambda_k| < r) = 0$, for example) for which I can be arbitrarily long [2], but all such sequences are nonuniformly distributed; when a sequence is sufficiently regular, in the sense that λ_k is close enough to k, the length of I cannot exceed 2π [4, p. 210]. Most recently, in a complete solution which accounts for all these phenomena, Beurling and Malliavin have proved that the supremum of the lengths of I is proportional to an appropriately defined density of $\{\lambda_k\}$ [1].

The purpose of this note is to show that the situation is quite different when the single interval I is replaced by a union of intervals. Specifically, we will construct a real symmetric (or positive) sequence $\{\lambda_k\}$ arbitrarily close to the integers, for which the corresponding exponentials are complete in $C(S)$, where S is any finite union of the intervals $|x - 2n\pi| < \pi - \delta$, with integer n and $\delta > 0$, and so has arbitrarily large measure. Thus, for sets S more general than intervals,