Let $K$ be a field of characteristic $p \neq 0$ and $\text{Der} K$ denote the set of all derivations of $K$ into itself, i.e., of additive maps $\phi$ of $K$ into itself such that $\phi(xy) = \phi(x)y + x\phi(y)$ for all $x$ and $y$ in $K$. Then $\text{Der} K$ is (1) a vector space over $K$, (2) closed under the formation of $p$th powers, i.e., $\phi$ in $\text{Der} K$ implies $\phi^p$ is in $\text{Der} K$, and (3) a Lie subring of the ring of additive endomorphisms of $K$, i.e., $\phi, \psi$ in $\text{Der} K$ imply $\phi\psi - \psi\phi$ is in $\text{Der} K$. 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 $\text{Der} K$, 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 $\text{Der}_k K$ 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 $\dim_K (\text{Der}_k K) = m$. Conversely, Jacobson demonstrated that given a restricted subring $D$ of $\text{Der} K$ 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 $\phi$ in $D$, then in fact $D = \text{Der}_k K$, whence if $\dim_K D = m$, then $[K:k] = p^m$. If $\phi$ is in $\text{Der}_k K$ then we say that $\phi$ 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 $\text{Der} K$. In fact, if we define a restricted subspace of $\text{Der} K$ to be a subset which is a vector space over $K$ and which is closed under the formation of $p$th powers, then one may assert: If $D$ is a finite-dimensional restricted subspace of $\text{Der} K$, and if $k$ is the field consisting of all $x$ in $K$ such that $\phi(x) = 0$ for all $\phi$ in $D$, then $D = \text{Der}_k K$. It follows a posteriori that $D$ must be a Lie subring of $\text{Der} K$. 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 $\text{Der} K$ denote the set of derivations of $K$ into itself. Given $\phi$ in $\text{Der} K$, the set of $x$ in $K$ such that $\phi(x) = 0$ forms a subfield $K_\phi$ of $K$ called the constant field of $\phi$; if $x$ is in $K_\phi$ 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

\footnote{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 \( \phi \) in \( \text{Der} K \). Therefore, if \( a \) is in \( K \) but not in \( K_\phi \), then \([K_\phi(a): K_\phi] = p\).

Suppose given \( \phi \) in \( \text{Der} K \) 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 \( \psi \) of \( \phi \) having \( a \) as a proper vector with proper value unity. Note that \( K_\phi = K_\psi \). Suppose now that for some \( \phi \) in \( \text{Der} K \) and \( a, b \) in \( K \), we have \( \phi(a) = \lambda a, \phi(b) = \mu b \) with \( \lambda, \mu \) in \( K_\phi \). Then \( \phi(a^{-1}) = -\lambda a \) and \( \phi(ab) = (\lambda + \mu)ab \). It follows that if \( \phi(a') = \lambda a' \) and also \( \phi(a'') = \lambda a'' \), \( \lambda \) in \( K_\phi \), then \( \phi(a'/a'') = 0 \), i.e., \( a'/a'' \) lies in \( K_\phi \). Therefore, if \( \lambda \) is in \( K_\phi \), 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 \( K_\phi \).

**Lemma 1.** Suppose given \( \phi \) in \( \text{Der} K \) 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 \( f_i(t), i = 0, 1, \ldots, p-1 \) 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 \( F_p \) of \( p \) elements, are linearly independent over this field, since indeed, if \( \sum \gamma_i f_i(t) = 0, \gamma_i \) in \( F_p \), 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 \( F_p \), is a linear combination over \( F_p \) of the polynomials \( f_i(t) \). In particular, we have \( \sum \alpha_i f_i(t) = 1 \) for suitable integers \( \alpha_i \) (mod \( p \)).

Now suppose that \( b \) is in \( K_\phi \), 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 \( (\phi-i)(b_i) = 0 \), \( i = 0, 1, \ldots, p-1 \). But \( (\phi-i)(a_i) = 0 \), whence \( b_i/a_i \) is in \( K_\phi \), and therefore \( b_i \) is in \( K_\phi(a) \) for \( i = 0, 1, \ldots, p-1 \). 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 \( x_1, \ldots, x_n \) of elements of \( K \) is said to be \( p \)-independent over \( k \) if the \( p^\alpha \) monomials \( x_1^{p^\alpha_1} \cdots x_n^{p^\alpha_n}, 0 \leq i_\alpha < p \) 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 \([K:kK^p] = p^n \) and is finite, then the dimension (i.e., cardinality) of a
A \textit{p}-basis of $K$ over $k$ is $m$, and conversely, and a necessary and sufficient condition that $x_1, \ldots, x_m$ be a $p$-basis over $k$ is that there exist $\phi_1, \ldots, \phi_m$ in $\text{Der}_k K$ such that denoting by $\delta_{ij}$ the Kronecker delta ($\delta_{ij} = 0$ if $i \neq j$, $\delta_{ii} = 1$), one has $\phi_i(x_j) = \delta_{ij}$. These $\phi_i$ then constitute a basis over $K$ for $\text{Der}_k K$. A detailed discussion of $p$-bases can be found in Zariski-Samuel, Vol. I \cite[p. 129]{ZS}, or Jacobson \cite[p. 180]{J}. Given $\phi$ in $\text{Der}_K$, let $D_{\phi}$ denote the smallest restricted subspace of $\text{Der}_K$ containing $\phi$. Since for any $\psi$ in $\text{Der}_K$ and $a$ in $K$, $(a\psi)^p$ can easily be shown to be of the form $b\psi + a\psi'$ for certain $b$ and $c$ in $K$, $D_{\phi}$ 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 $K$, $m = 0, 1, \ldots$. We shall not, however, need this remark.

\textbf{Lemma 2.} If $\phi$ is in $\text{Der}_K$ and $x_1, \ldots, x_n$ are $p$-independent over $K_{\phi}$, then there exist $\phi_1, \ldots, \phi_n$ in $D_{\phi}$ such that $\phi_i(x_j) = \delta_{ij}$. (These $\phi_i$ are then, in particular, linearly independent over $K$.)

\textbf{Proof.} It is clearly sufficient to show that there exists a $\psi$ in $D_{\phi}$ 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 $a_0\phi$, $a$ in $K$, such that $a_0\phi(x_2) = x_2$. Setting $\phi' = (a\phi)^p - (a\phi)$, we have $\phi'$ in $D_{\phi}$, 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, we can construct $\phi''$ in $D_{\phi}$ with $K_{\phi''} = K_{\phi'}(x_3) = K_{\phi}(x_2, x_3)$. Continuing, we obtain an element $\psi$ in $D_{\phi}$ with $K_{\psi} = K_{\phi}(x_2, \ldots, x_n)$. 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

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

\textbf{Proof.} Since $K^p \subset K_{\phi}$, if $[K:K_{\phi}]$ is infinite, then the dimension of a $p$-basis of $K$ over $K_{\phi}$ is infinite, and there exist, by the lemma, for every positive $n$, at least $n$ elements of $D_{\phi}$ 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 $x_1, \ldots, x_n$ is a $p$-basis of $K$ over $K_{\phi}$, then the $\phi_1, \ldots, \phi_n$ of the lemma are a basis over $K$ for the Lie ring of derivations of $K$ over $K_{\phi}$. Since $D_{\phi}$ 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 $\phi$ in $\text{Der}_k K$ such that $K_{\phi} = k$. Indeed, if $(x_i)$ is a $p$-basis for $K$ over $k$, then a derivation $\phi$ of $K$ over $k$ is completely
determined by its values at the $x_i$. Choosing $\phi(x_i) = \lambda_i x_i$, $\lambda_i$ in $k$, we have for any monomial $M$ of the form $x_{i_1}^{j_1} \cdots x_{i_n}^{j_n}$, $0 \leq j_q < p$, $\phi(M) = (\lambda_1 j_1 + \cdots + \lambda_n j_n) M$, and it is sufficient to choose the $\lambda_i$ 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 $\lambda_i$ 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 $\lambda_i$ are linearly independent over $k^p$, hence a fortiori over the prime field.

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

**Lemma 3.** Given $\phi, \psi$ in $\text{Der } K$, let $x_1, \ldots, x_m$ be elements of $K$ which are $p$-independent over $K_0$, and $y$ be an element of $K_0$ with $\psi(y) \neq 0$. Then there exists an element $\theta$ in $D_{\phi, \psi}$ such that $x_1, \ldots, x_m, y$ are $p$-independent over $K_0$. Further, $[K : K_0 \cap K_\psi]$ is finite if and only if $\dim_K D_{\phi, \psi}$ is finite, and in the latter case there exists a $\theta$ in $D_{\phi, \psi}$ such that $K_\theta = K_0 \cap K_\psi$ and $D_\theta = D_{\phi, \psi}$.

**Proof.** By Lemma 2, there exist $\phi_1, \ldots, \phi_n$ in $D_\phi$ such that $\phi_i(x_i) = \delta_{ij}$. Since $y$ is in $K_\phi$, we have further that $\phi_i(y) = 0$. It follows that subtracting from $\psi$ a suitable linear combination over $K$ of the $\phi_i$, and multiplying the result by a suitable element of $K$, we can obtain a $\psi'$ in $D_{\phi, \psi}$ with $\psi'(x_i) = 0$, $j = 1, \ldots, n$, and $\psi'(y) = 1$. Now set $x_i^p = \lambda_i$, $y^p = \mu$, and set $\theta = \sum \lambda_i x_i + \mu y \psi'$. Then, as in the final remark of the preceding section, $\theta$ 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 $K_0$.

As for the rest (observe that if at least one is infinite), and as both $[K : K_\theta] \leq [K : K_0 \cap K_\psi]$ and $\dim_K D_\theta \leq \dim_K D_{\phi, \psi}$ for all such $\theta$, it follows that both $\dim_K D_{\phi, \psi}$ and $[K : K_0 \cap K_\psi]$ are infinite. In the contrary case, there exists a $\theta$ in $D_{\phi, \psi}$ for which $\dim_K D_\theta$ is finite and maximal. Then for this $\theta$ we must have $K_\theta = K_0 \cap K_\psi$, for were this not the case then there would exist a $y$ in $K_\theta$ which was not in $K_0 \cap K_\psi$, whence either $\phi(y) \neq 0$ or $\psi(y) \neq 0$. Assuming, without loss of generality, the latter, and letting $x_1, \ldots, x_n$ be the $p$-basis of $K$ over $K_0$, the first part of the lemma would construct a new $\theta$ with $[K : K_\theta]$ even larger, a contradiction. Therefore indeed $K_\theta = K_0 \cap K_\psi$, 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 $\theta$ in $D$ such that $K_{\theta} = k$, whence $D_{\theta} = \text{Der}_k K$.

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 $\text{Der} K$, 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 $D = \text{Der}_k K$. Moreover, $D$ is then a Lie subring of $\text{Der} K$, there is an element $\theta$ in $D$ such that $k = K_{\theta}$, and for any such $\theta$ 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 $\text{Der} K$ with constant field $k$, and if $[K:k]$ is known a priori to be finite, then $D = \text{Der}_k K$. 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**

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 \( \{\lambda_n\} \) of complex numbers, the problem of determining those intervals \( I \) on which the exponentials \( e^{\lambda_n x} \) 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 \( \{\lambda_n\} \). With the function space taken to be \( L^p(I) \) for \( 1 \leq p < \infty \), or \( C(I) \), the continuous functions on \( I \), the general character of the results has been that there exist sparse real sequences (\( \lim r^{-1} = 0 \), 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 \( \lambda_n \) is close enough to \( k \), the length of \( I \) cannot exceed \( 2\pi \) [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 \( \{\lambda_n\} \) [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 \( \{\lambda_n\} \) 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,