DERIVATIONS AND GENERATIONS OF FINITE EXTENSIONS

BY CARL FAITH[1]

Communicated by Nathan Jacobson, May 8, 1961

Let k be a given ground field, let $\mathfrak{F}_r$ denote the class of finite (=finitely generated) field extensions of k of tr.d. (=transcendence degree) $\leqq r$, and let n be the function defined on $\mathfrak{F}=\bigcup_0^\infty \mathfrak{F}_r$ by: for any $L\in\mathfrak{F}$, $n(L)$ = the minimal number of generators of L/k. Classically it is known for suitable k that there exist purely transcendental extensions L/k having tr.d. 2, and containing impure subextensions of tr.d. 2, a fact which shows that in general n is not monotone in $\mathfrak{F}$ for all k. The main result of this note establishes that these "counterexamples to Lüroth's theorem" constitute the only barriers to the monotonicity of n (see Theorem 2 for a precise statement). In particular it is demonstrated that n is montone on $\mathfrak{F}_1$ for arbitrary k, a result which appears new even when restricted to the subclass $\mathfrak{F}_0$ of finite algebraic extensions of k.

A result of independent (and possibly more general) interest, which is proved below, and which is essential to our proof of the statements above, is that dim $\mathfrak{D}$ is montone on $\mathfrak{F}$, where for any $L\in\mathfrak{F}$, $\mathfrak{D}(L)$ is the vector space over L of k-derivations of L. The connection between n and dim $\mathfrak{D}$ is given in the lemma.

LEMMA. *Let L/k be a finite extension of tr.d. r, let $s=\dim \mathfrak{D}(L)$, and let $n=n(L)$. Then $s\leqq n\leqq s+1$; if $s>r$, then $n=s$.*[2]

PROOF. It is known (e.g. [3, Theorem 41, p. 127]) that s is the smallest natural number[3] such that there exist elements $u_1, \cdots, u_s\in L$ such that L is separably algebraic over the field $U=k(u_1, \cdots, u_s)$. Then $L=U(a)$ for some $a\in L$, so that $s\leqq n\leqq s+1$.

If $s>r$, there exists u_q in the set $S=\{u_1, \cdots, u_s\}$ such that u_q is algebraically dependent over k on the complement of u_q in S. For convenience renumber so that u_s is algebraic[4] over the field $T=k(u_1, \cdots, u_{s-1})$. A short argument shows that $L=U(a)$ for some

[1] National Science Foundation Postdoctoral Fellow in the Institute for Advanced Study, on leave from Pennsylvania State University.

[2] Expressed in the other words: If L/k is not separably generated, then $n(L)=\dim \mathfrak{D}(L)$.

[3] Strictly speaking the notation should allow for the case $s=0$. By agreement then $U=k$.

[4] In case $s=1$ set $T=k$.

$a \in L$ which is separably algebraic over T. Thus $L = T(u_s, a)$ is generated over T by two elements one of which is separable over T. Then, by a classic result in field theory (cf. [2, §43, p. 138]), $L = T(u_s')$ for suitable $u_s' \in L$. Clearly then $n = s$. Q.E.D.

If L/k is a finite extension, and L'/k a subextension, in general not every derivation of $\mathfrak{D}(L')$ can be extended to a derivation in $\mathfrak{D}(L)$. Nevertheless, the theorem below shows that dim $\mathfrak{D}$ is a monotone function.

THEOREM 1. *Let L/k be a finite field extension, and let L'/k be any subextension. Then $s = \dim \mathfrak{D}(L) \geqq s' = \dim \mathfrak{D}(L')$.*

PROOF. Let $r = \text{tr.d. } L/k$ and $r' = \text{tr.d. } L'/k$. It is easy to see that it suffices to consider only the case $r = r'$. For if $r' < r$, then there exists a field extension L'' contained in L which is purely transcendental over L' and such that tr.d. $L''/k = r$. Since L''/L' is a pure extension, every $D' \in \mathfrak{D}(L')$ is extendable to a derivation D'' in $\mathfrak{D}(L'')$. It is an easy exercise to show that if $D_1', \cdots, D_t'$ are linearly independent over L', then $D_1'', \cdots, D_t''$ are linearly independent over L'', so that $\dim \mathfrak{D}(L'') \geqq s'$. Hence it remains only to show that $s \geqq s'$ when $r = r'$. An argument similar to the one just completed shows that $s \geqq s'$ when L/L' is separable. The proof now proceeds by induction on the algebraic degree $|L : L'|$ of the extension L/L'. One can therefore assume the theorem for all extensions L'' of k which contain L' and such that $|L'' : L'| < |L : L'|$. Then clearly one can suppose that L' is a maximal proper subfield of L. Since the separable case already has been decided, assume that k has characteristic $p > 0$, and that L/L' is inseparable. Then the maximality of L' shows that $k(L^p) \subseteq L'$. By [1, p. 218] or [3, Theorem 41, p. 127], one has

$$p^s = |L : k(L^p)|, \quad \text{and} \quad p^{s'} = |L' : k(L'^p)|,$$

so that the inclusions

$$L \supset L' \supseteq k(L^p) \supseteq k(L'^p)$$

together with the inequality

$$|L : L'| \geqq |k(L^p) : k(L'^p)|$$

yield the desired inequality $p^s \geqq p^{s'}$, that is, $s \geqq s'$. Q.E.D.

COROLLARY. *Let L/k be a finite extension, and let L'/k be any subextension. Then, if either L/k or L'/k is not separably generated, then $n(L) \geqq n(L')$.*

PROOF. Let $s=\dim \mathfrak{D}(L)$, $r=\text{tr.d. } L/k$, $n=n(L)$, and let s', r', and n' be the corresponding integers for L'/k. If L'/k is not separably generated, neither is L/k, so that we can assume that L/k is not separably generated in either case, that is, that $s\geqq r+1$. Then $n=s$ by the lemma, whence $n=s\geqq s'$ by the theorem. If $n'=s'$, we are through, and if $n'\neq s'$, then $n'=s'+1=r'+1$ by the lemma again. Since $r\geqq r'$, this latter equality yields

$$n = s \geqq r + 1 \geqq r' + 1 = s' + 1 = n',$$

as desired.

The corollary is surprising in view of the troublesomeness usually associated with nonseparably generated extensions.

Before stating the last result, it is convenient to make the definition: k is an *(r)-field* in case no pure transcendental extension of k of tr.d. r contains an impure subextension of tr.d. r over k. Clearly if n is monotone in $\mathfrak{F}_r$, then k must be an (m)-field, $m=0, 1, \cdots, r$. Our next theorem establishes the converse.

THEOREM 2. *If k is an (r)-field, and if L/k is a finite extension of tr.d. r, then $n=n(L)\geqq n'=n(L')$ for any subextension L'/k of L/k.*

PROOF. Let s, r, n, and their primes be defined as in the corollary. If $s'>r'$, then $n>n'$ by the corollary. If L'/k is purely transcendental, then trivially $n\geqq n'$. Otherwise $s'=r'$ implies by the lemma that $n'=s'+1=r'+1$. Then, since k is an (r)-field, necessarily $n\geqq r+1 =r'+1=n'$, if $r=r'$. If $r>r'$, then clearly $n\geqq r\geqq r'+1=n'$. Q.E.D.

By definition, any field is a (0)-field, and, by Lüroth's theorem, any field is a (1)-field. Thus, the theorem implies the corollary:

COROLLARY. *Let k be an arbitrary field. Then n is monotone in the class $\mathfrak{F}_1$ of finite extensions of tr.d. $\leqq 1$ over k; in particular, n is monotone in the class $\mathfrak{F}_0$ of finite algebraic extensions of k.*

A consequence of Theorem 2 and the theorem of Castelnuovo-Zariski (see [4]) is the following:

COROLLARY. *Let k be an algebraically closed field of characteristic 0. Then n is monotone in the class $\mathfrak{F}_2$ of finite extensions of tr.d. $\leqq 2$ over k.*

A possible value of Theorem 2 is that in order to show that a given field is not an (r)-field, it is possible to do this by showing that n is not monotone on its finite extensions of tr.d. r, that is, one need not restrict one's attention to the pure transcendental extensions of k.

References

1. Nathan Jacobson, *Abstract derivations and Lie algebras*, Trans. Amer. Math. Soc. vol. 42 (1937) pp. 206–224.

2. B. L. van der Waerden, *Algebra* I, Vierte Auflage, Berlin-Göttingen-Heidelberg, 1955.

3. Oscar Zariski and Pierre Samuel, *Commutative algebra*, vol. I, Princeton, 1958.

4. Oscar Zariski, *On Castelnuovo's criterion of rationality* $p_a = P_2 = 0$ *of an algebraic surface*, Illinois J. Math. vol. 2 (1958) pp. 303–315.

Institute for Advanced Study