PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 81, Number 3, March 1981

CALCULATING INVARIANTS OF INSEPARABLE FIELD EXTENSIONS

JAMES K. DEVENEY AND JOHN N. MORDESON

ABSTRACT. Let L be a finitely generated nonalgebraic extensions of a field K of characteristic $p \neq 0$ and let M be a finite purely inseparable extension of L. This paper is concerned with calculating inseparability-related numerical invariants of M/K from those of L/K.

I. Introduction. Let L be a finitely generated field extension of a field K of characteristic $p \neq 0$. If D is a maximal separable extension of K in L, then L is purely inseparable finite dimensional over D. If p^s is the smallest of the dimensions of L over such maximal separable extensions, then s is Weil's order of inseparability of L/K (denoted $\operatorname{inor}(L/K)$) [7]. If $[L : D]$ is minimal, then $L \subseteq K^{p^{-\infty}}(D)$ and D is called distinguished for L/K [3], [6]. There are two other important invariants of L/K which were introduced in [6], the inseparability exponent of L/K, $\operatorname{inex}(L/K) = \min\{r \mid K(L^{p^r}) \text{ is separable over } K\}$ and the inseparability of L/K, $\operatorname{insep}(L/K) = \log_p[L : K(L^p)] -$ transcendence degree of L/K. These are related, for example $\operatorname{inex}(L/K) = \min\{r \mid K(L^{p^r}) = K(D^{p^r}) \text{ for a distinguished } D\} = \min\{r \mid L \subseteq K^{p^{-r}}(D) \text{ for a distinguished } D\}$ [5, Proposition 1, p. 288].

This paper is concerned with the following question. Given D, a finitely generated separable extension of K, and $L = D(c_1, c_2, \ldots, c_m)$, where each c_i is purely inseparable over D, how can one calculate $\operatorname{inor}(L/K)$, $\operatorname{inex}(L/K)$ and $\operatorname{insep}(L/K)$? There are two main tools which will be used. First are the fields $K(L^{(r)}) = \{x \in L \mid x^{p^j} \in K(L^{p^{r+j}}) \text{ for some } j > 0\}$ which were studied in [5]. $L = K(L^{(0)}) \supseteq K(L^{(1)}) \supseteq K(L^{(2)}) \supseteq \cdots$ and $K(L^{(\infty)})$ will denote $\bigcap_r K(L^{(r)})$. Recall that $K(L^{(\infty)})$ is the algebraic closure of K in L [5, Theorem 5, p. 289]. Also note that $\bigcap_r K(L^{p^r}) \equiv K(L^{\infty})$ is the separable algebraic closure of K in L [4, Theorem 7.2, p. 273]. The second main tool is the concept of a form. An intermediate field F of L/K is a form of L/K if and only if $\operatorname{inor}(L/K) = \operatorname{inor}(F/K)$. Forms were first studied in [2]. Every finitely generated L/K has a unique minimal form L', $L \supseteq L' \supseteq K$. The results established here can be used to determine properties of $L \supseteq L' \supseteq K$ and to construct examples with proper forms.

We introduce some notation which will be used to state the main results. $L = D(c_1, c_2, \ldots, c_m)$ where D is finitely generated separable over K and each c_i is purely inseparable over D. We define $L_i = D(c_1, c_2, \ldots, c_i)$; $L_0 = D$; $p^{e_i} = [L_i : L_{i-1}]$; $n_i = \operatorname{inex}(L_i/K)$; $c_i^{p^{e_i}} \in L_{i-1}$, and $r_i = \max\{t \mid c_i^{p^{e_i}} \in K(L_{i-1}^{(t)})\}$ if the

Received by the editors February 10, 1980; presented to the Society, April 18, 1980.
1980 *Mathematics Subject Classification*. Primary 12F15.
Key words and phrases. Order of inseparability, distinguished subfield.

0002-9939/81/0000-0106/$02.00

maximum exists and is ∞ otherwise; $j_i = \min\{\mu | c_i^{p^{e_i+\mu}} \in K(L_{i-1}^{p^{r_i+\mu}})\}$ if $r_i < \infty$ and $j_i = \min\{\mu | c_i^{p^{e_i+\mu}} \in K(L^\infty)\}$ if $r_i = \infty$. (We note that if $r_i = \infty$, then c_i is algebraic over K and since $K(L^\infty)$ is the separable algebraic closure of K in L, $e_i + j_i$ is the least pth power of c_i which is separable over K.) The main results on the stated problem are

$$\operatorname{inor}(L/K) = \sum_{i=1}^{m} \min\{e_i, r_i\};$$

$$\operatorname{inex}(L/K) = \max\{q_1 + j_1, \ldots, q_m + j_m\}, \qquad q_i = \min\{e_i, r_i\};$$

$$\operatorname{insep}(L/K) = d$$

where d is the number of c_i such that $c_i^{p^{e_i}} \in K(L_{i-1}^p)$.

II. The first result is essentially contained in **[2]**, but is presented here for clarity. It gives an exponent-independent characterization of a form of L/K.

PROPOSITION 0. *Let L be a finitely generated extension of K and let L_1 be an intermediate field. Then L_1 is a form of L/K if and only if L^{p^r} and $K(L_1^{p^r})$ are linearly disjoint over $L_1^{p^r}$ for all r.*

PROOF. Let n be the exponent of L over K. If we have linear disjointness for all r, then we certainly have it for $r = n$, so L_1 is a form of L/K [**2**, Theorem 1.3, p. 656]. Assume we have disjointness for n. If $r < n$, then since $K(L_1^{p^n}) \supset K^{p^{n-r}}(L_1^{p^n}) \supset L_1^{p^n}$, L^{p^n} and $K^{p^{n-r}}(L_1^{p^n})$ are linearly disjoint over $L_1^{p^n}$. Taking p^{n-r}th roots of these fields gives the desired linear disjointness. If $r > n$, by induction it suffices to prove the case $r = n + 1$. Taking pth roots, we need L^{p^n} and $K^{p^{-1}}(L_1^{p^n})$ linearly disjoint over $L_1^{p^n}$. But since $K^{p^{-1}}(L_1^{p^n}) \supset K(L_1^{p^n}) \supset L_1^{p^n}$, by the standard lemma on linear disjointness we only need show $K(L^{p^n})$ and $K^{p^{-1}}(L_1^{p^n})$ are linearly disjoint over $K(L_1^{p^n})$. But this follows since $K(L^{p^n})$ and $K^{p^{-1}}$ are linearly disjoint over K, as $K(L^{p^n})$ is separable over K.

LEMMA 1. *Let F be a finitely generated extension of K and let $x \in F \setminus F^p$.*
(1) *If $x \in K(F^p)$, then* $\operatorname{inor}(F(x^{p^{-1}})/K) = \operatorname{inor}(F/K) + 1$.
(2) *If $x \in K(F^{(1)})$, then* $\operatorname{inor}(F(x^{p^{-1}})/K) = \operatorname{inor}(F/K) + 1$.
(3) *If $x \in F \setminus K(F^{(1)})$, then* $\operatorname{inor}(F(x^{p^{-1}})/K) = \operatorname{inor}(F/K)$.

PROOF. Since $K(F^p) \subseteq K(F^{(1)})$, (1) follows once we prove (2). Since $x \in K(F^{(1)})$, $x^{p^r} \in K(F^{p^{r+1}})$ for some r. If the conclusion of (2) were false, then F/K would be a form of $F(x^{p^{-1}})/K$. Thus by Proposition 0, $(F(x^{p^{-1}}))^{p^{r+1}}$ and $K(F^{p^{r+1}})$ are linearly disjoint over $F^{p^{r+1}}$, and in particular have $F^{p^{r+1}}$ as their intersection. But then $x^{p^r} \in F^{p^{r+1}}$ and hence $x \in F^p$, a contradiction. Thus we have (2). For (3), $F^{p^s}(x^{p^{s-1}})$ and $K(F^{p^s})$ must be linearly disjoint over F^{p^s} since $[F^{p^s}(x^{p^{s-1}}): F^{p^s}] = p$ and $x^{p^{s-1}} \notin K(F^{p^s})$. Thus F/K is a form of $F(x^{p^{-1}})/K$.

THEOREM 2. *Let F be a finitely generated extension of K and let $x \in F \setminus F^p$. Assume $r = \max\{t | x \in K(F^{(t)})\}$ if it exists and $r = \infty$ otherwise. Then* $\operatorname{inor}(F(x^{p^{-e}})) = \operatorname{inor}(F/K) + \min\{e, r\}$, $e > 0$.

PROOF. The proof is by induction on e. If $e = 1$, the result is Lemma 1. Consider the chain of fields $F(x^{p^{-e}}) \supseteq F(x^{p^{-e+1}}) \supseteq F$. Since $[F(x^{p^{-e+1}}): F] = p^{e-1}$, $\operatorname{inor}(F(x^{p^{-e+1}})/K) = \min\{e - 1, r\}$ by induction. Thus the result will be established once we show $\operatorname{inor}(F(x^{p^{-e}})/K) = \operatorname{inor}(F(x^{p^{e+1}})/K) + 1$ if and only if $e \leqslant r$. Suppose $\operatorname{inor}(F(x^{p^{-e}})/K) = \operatorname{inor}(F(x^{p^{-e+1}})/K) + 1$. Then $x^{p^{-e+1}} \in K((F(x^{p^{-e+1}}))^{(1)})$ by Lemma 1. Thus $(x^{p^{-e+1}})^{p^s} \in K((F(x^{p^{-e+1}}))^{p^{s+1}})$ for some s, and in fact for s as large as we wish. Hence take $s \geqslant e - 1$. Then $x^{p^j} \in K(F^{p^{e+j}})(x^{p^{j+1}})$ where $j = -e + 1 + s$. Thus x^{p^j} is separable over $K(F^{p^{e+j}})$. Hence $x^{p^j} \in K(F^{p^{e+j}})$ and so $e \leqslant r$. Conversely, suppose $e \leqslant r < \infty$. Then $x^{p^j} \in K(F^{p^{e+j}})$ for some j and j can be taken as large as we wish. Thus for $j = -e + 1 + s$ where $s \geqslant e - 1$, $(x^{p^{-e+1}})^{p^s} \in K((F(x^{p^{-e+1}}))^{p^{s+1}})$. Hence $x^{p^{-e+1}} \in K((F(x^{p^{-e+1}}))^{(1)})$ and so $\operatorname{inor}(F(x^{p^{-e}})/K) = \operatorname{inor}(F(x^{p^{-e+1}})/K) + 1$ by Lemma 1. Suppose $e \leqslant r = \infty$. However, if $r = \infty$, then x and hence $x^{p^{-e+1}}$ is algebraic over K. Thus $x^{p^{-e+1}} \in K((F(x^{p^{-e+1}}))^{(\infty)})$ and $\operatorname{inor}(F(x^{p^{-e}})/K) = \operatorname{inor}(F(X^{p^{-e+1}})/K) + 1$ by Lemma 1.

COROLLARY 3. *In the notation of the introduction*, $\operatorname{inor}(L/K) = \sum_{i=1}^{m} \min\{e_i, r_i\}$.

PROOF. This follows from m applications of Theorem 2 to the chain of fields $D = L_0 \subset L_1 \subset \cdots \subset L_m = L$ and the fact that $\operatorname{inor}(D/K) = 0$.

LEMMA 4. *Let F be a finitely generated extension of K and let $x \in F \setminus F^p$. Let $r = \max\{t \mid x \in K(F^{(t)})\}$ if it exists and $r = \infty$ otherwise. If $e > r$, then*

$$\operatorname{inex}(F(x^{p^{-e}})/K) = \operatorname{inex}(F(x^{p^{-r}})/K).$$

PROOF. By Theorem 2, $\operatorname{inor}(F(x^{p^{-e}})/K) = \operatorname{inor}(F(x^{p^{-r}})/K) = \operatorname{inor}(F/K) + r$. Thus $F(x^{p^{-r}})$ is a form of $F(x^{p^{-e}})$ and hence they both have the same inseparability exponent [**2**, Theorem 1.3, p. 656].

THEOREM 5. *Let F be a finitely generated extension of K and let $x \in F \setminus F^p$. Let $r = \max\{t \mid x \in K(F^{(t)})\}$ if it exists and $r = \infty$ otherwise. Let j be the least nonnegative integer such that $x^{p^j} \in K(F^{p^{r+j}})$. Then*

$$\operatorname{inex}(F(x^{p^{-e}})/K) = \max(\operatorname{inex}(F/K), \min(e, r) + j).$$

PROOF. In view of Lemma 4, we may assume $e \leqslant r$. Let D be a distinguished subfield of F/K and let $t = \operatorname{inex}(F/K)$. Then $F \subseteq K^{p^{-t}}(D)$ [**5**, Proposition 1, p. 288]. By Theorem 2, $\operatorname{inor}(F(x^{p^{-e}})/K) = \operatorname{inor}(F/K) + e$, so D is also distinguished for $F(x^{p^{-e}})/K$. Now $x^{p^j} \in K(F^{p^{r+j}})$. So $x^{p^{-e}} \in K^{p^{-e-j}}(F^{p^{r-e}}) \subseteq K^{p^{-e-j}}(F) \subseteq K^{p^{-\max\{t,e+j\}}}(D)$. Thus $F(x^{p^{-e}}) \subseteq K^{p^{-\max\{t,e+j\}}}(D)$ and $\operatorname{inex}(F(x^{p^{-e}})/K) \leqslant \max\{\operatorname{inex}(F/K), e + j\}$. Now assume $F(x^{p^{-e}}) \subseteq K^{p^{-s}}(D)$. Then clearly $s \geqslant \operatorname{inex}(F/K)$. Suppose $s < e + j \leqslant r + j$. Then $x^{p^{-e}} \in K^{p^{-s}}(D)$. Thus $(x^{p^{-e}})^{p^{e+j}} = x^{p^j} \in K^p(D^{p^{e+j}})$ and $x^{p^j} \in K(F^{p^{r+j}})$. But since $x^{p^j} \in D$ and $K(F^{p^{r+j}})$ and $D \cap K(F^{p^{r+j}}) = K(D^{p^{r+j}})$ [**1**, Theorem 2.9, p. 1310], $x^{p^j} \in K^p(D^{p^{e+j}}) \cap K(D^{p^{r+j}}) = K^p(D^{p^{r+j}})$ since D is separable over K. Thus $x^{p^{j-1}} \in K(D^{p^{r+j-1}}) \subseteq K(F^{p^{r+j-1}})$. If $j > 0$, this contradicts the definition of j and if $j = 0$, this contradicts the degree of $x^{p^{-e}}$ over F. Thus $s < e + j$ is impossible.

COROLLARY 6. *In the notation of the introduction,*

$$\operatorname{inex}(L/K) = \max\{q_1 + j_1, q_2 + j_2, \ldots, q_m + j_m\},$$
$$q_i = \min\{e_i, r_i\}.$$

THEOREM 7. *Let F be a finitely generated extension of a field K and let $x \in F \setminus F^p$, $e > 0$.*

(1) *If* $x \notin K(F^p)$, $\operatorname{insep}(F(x^{p^{-e}})/K) = \operatorname{insep}(F/K)$.

(2) *If* $x \in K(F^p)$, $\operatorname{insep}(F(x^{p^{-e}})/K) = \operatorname{insep}(F/K) + 1$.

PROOF. (1) x is p-independent in F/K. Let $\{x\} \cup C$ be a relative p-basis of F/K. Then $\{x^{p^{-e}}\} \cup C$ is a relative p-basis of $F(x^{p^{-e}})/K$.

(2) Since $x \in K(F^p)$, $K((F(x^{p^{-e}}))^p)$ and F are linearly disjoint over $K(F^p)$. Thus if C is a relative p-basis of F/K, C is also relatively p-independent in $F(x^{p^{-e}})/K$. Suppose for some $c \in C$, $c \in K(F^p)(x^{p^{-e}}, C \setminus \{c\})$. Then by the exchange property, $x^{p^{-e}} \in K(F^p)(x^{p^{-e+1}}, C)$. This contradicts the fact that the exponent of $x^{p^{-e}}$ over F is e. Thus $C \cup \{x^{p^{-e}}\}$ is a relative p-basis of $F(x^{p^{-e}})/K$.

COROLLARY 8. *In the notation of the introduction,* $\operatorname{insep}(L/K) = d$ *where d is the number of c_i such that $c_i^{p^{e_i}} \in K(L_{i-1}^p)$.*

It is clear that, in the notation of the introduction where $L = D(c_1, \ldots, c_m)$, D being separable over K is merely a matter of convenience. For example, if D/K is inseparable, then Corollary 3 would simply be $\operatorname{inor}(L/K) = \operatorname{inor}(D/K) + \sum_{i=1}^m \min\{e_i, r_i\}$. Thus, if D is inseparable over K, D/K is a form of L/K if and only if each $r_i = 0$. This shows how to construct extension with proper forms. Similarly, by a degree argument, every distinguished subfield of D/K is one of L/K if and only if $e_i \leqslant r_i$ for all i.

REFERENCES

1. J. Deveney and J. Mordeson, *Subfields and invariants of inseparable field extensions*, Canad. J. Math. **29** (1977), 1304–1311.

2. ______, *The order of inseparability of fields*, Canad. J. Math. **31** (1979), 655–662.

3. J. Dieudonné, *Sur les extensions transcendantes separables*, Summa Brasil. Math. **2** (1947), 1–20.

4. N. Heerema and J. Deveney, *Galois theory for fields K/k finitely generated*, Trans. Amer. Math. Soc. **189** (1974), 263–274.

5. N. Heerema, *pth powers of distinguished subfields*, Proc. Amer. Math. Soc. **55** (1976), 287–292.

6. H. Kraft, *Inseparable Korpererweiterungen*, Comment. Math. Helv. **45** (1970), 110–118.

7. A. Weil, *Foundations of algebraic geometry*, Amer. Math. Soc. Colloq. Publ., vol. 29, Amer. Math. Soc., Providence, R. I., 1946.

DEPARTMENT OF MATHEMATICAL SCIENCES, VIRGINIA COMMONWEALTH UNIVERSITY, RICHMOND, VIRGINIA 23284

DEPARTMENT OF MATHEMATICS, CREIGHTON UNIVERSITY, OMAHA, NEBRASKA 68134 (Current address of J. N. Mordeson)

Current address (J. K. Deveney): Department of Mathematics, Louisiana State University, Baton Rouge, Louisiana 70803