

THE ORDER OF INSEPARABILITY OF FIELDS

JAMES K. DEVENEY AND JOHN N. MORDESON

1. Introduction. Let L be a finitely generated field extension of a field K of characteristic $p \neq 0$. By Zorn's Lemma there exist maximal separable extensions of K in L and L is finite dimensional purely inseparable over any such field. If p^s is the smallest of the dimensions of L over such maximal separable extensions of K in L , then s is Wiel's order of inseparability of L/K [11]. Dieudonné [2] also investigated maximal separable extensions D of K in L and established that there must be at least one D such that $L \subseteq K^{p^{-\infty}}(D)$ (such fields are termed *distinguished*). Kraft [5] showed that the distinguished maximal separable subfields are precisely those over which L is of minimal degree. This concept of distinguished subfield has been the basis of a number of results on the structure of inseparable field extensions, for example see [1], [3], [5], and [6].

Let F be an intermediate field of L/K . In Section 2 it is shown that the order of inseparability of L/K ($\text{inor}(L/K)$) is greater than or equal to $\text{inor}(F/K)$. The case of equality is of particular interest, and if $\text{inor}(F/K) = \text{inor}(L/K)$ F is called a *form* of L/K . Forms are characterized by a number of linear disjointness conditions and these characterizations are used to establish the existence of a unique minimal form for L/K (such a minimal form is called *irreducible* since it has no proper forms). The remainder of Section 2 develops properties of irreducible forms. For example, Kraft [5] established that any relative p -basis for L/K contains a separating transcendence basis for a distinguished subfield and here it is shown that if L/K is irreducible then any relative p -basis with one element omitted still contains a separating transcendence basis for a distinguished subfield.

Let F/K be a form of L/K . In Section 3 relationships between the structure and invariants of L/K and those of F/K are examined. For example, F/K and L/K have the same distinguished closures [9] and the modularity of L/K [1] is always greater than or equal to the modularity of F/K .

2. Existence and properties. As noted, throughout we assume L is a finitely generated field extension of a field K of characteristic $p \neq 0$. We use the notation of Kraft [5] where: the inseparability exponent of L/K , $\text{inex}(L/K)$, is $\min\{r \mid K(L^{p^r}) \text{ is separable over } K\}$; the order of inseparability of L/K , $\text{inor}(L/K)$, is $\log_p(\min\{[L : D] \mid D \text{ is separable over } K \text{ and } L \text{ is purely inseparable over } D\})$; the inseparability of L/K , $\text{insep}(L/K)$, is $\log_p([L : K(L^p)])$ — transcendence degree of L/K .

Received January 25, 1978.

In [5], Kraft established that if F is an intermediate field of L/K , then $\text{insep}(L/K) \geq \text{insep}(F/K)$. We first establish the corresponding result for $\text{inor}(L/K)$.

LEMMA 1.1. $\text{inor}(K(L^p)/K) = \text{inor}(L/K) - \text{insep}(L/K)$.

Proof. Let s be the transcendence degree of L/K and let D be a distinguished subfield, i.e. D/K is separable and $\log_p([L : D]) = \text{inor}(L/K)$. Let n be $\text{inex}(L/K)$. Then $K(L^{p^n}) = K(D^{p^n})$ [3, Proposition 1, p. 288], and hence $\log_p([L : K(L^{p^n})]) = ns + \text{inor}(L/K)$. Since $\log_p([L : K(L^p)]) = s + \text{insep}(L/K)$, $\log_p([K(L^p) : K(L^{p^n})]) = (n - 1)s + \text{inor}(L/K) - \text{insep}(L/K)$. Thus $\text{inor}(K(L^p)/K) = \text{inor}(L/K) - \text{insep}(L/K)$.

THEOREM 1.2. *Let F be an intermediate field of L/K . Then $\text{inor}(L/K) \geq \text{inor}(F/K)$.*

Proof. We use induction on $\text{inex}(L/K)$. If $\text{inex}(L/K) = 1$, then $\text{inor}(L/K) = \text{insep}(L/K)$ and the result is that of Kraft [5, Lemma 1, p. 111]. Assume the result for $\text{inex}(L/K) = n - 1$. By Lemma 1, $\text{inor}(L/K) = \text{inor}(K(L^p)/K) + \text{insep}(L/K)$. But by Kraft, $\text{insep}(L/K) \geq \text{insep}(F/K)$ and by induction $\text{inor}(K(L^p)/K) \geq \text{inor}(K(F^p)/K)$. Thus

$$\begin{aligned} \text{inor}(L/K) &= \text{inor}(K(L^p)/K) + \text{insep}(L/K) \geq \text{inor}(K(F^p)/K) \\ &\quad + \text{insep}(F/K) = \text{inor}(F/K). \end{aligned}$$

We note that if L is separable over F , then we have equality in Theorem 1.2. For if D is a distinguished subfield of F/K , then $L = F \otimes_D S$ where S is separable over D [6, Theorem 4, p. 1178] and hence $\text{inor}(L/K) \leq \text{inor}(F/K)$. However, even if L/F is not separable, we may still have equality. Let P be a perfect field of characteristic $p \neq 0$ and let $\{x, y, z\}$ be algebraically independent over P . Let $L = P(x, u^p, ux^p + v)$, $F = P(x^p, u^p, ux^p + v)$ and $K = P(u^p, v^p)$. Then $\text{inor}(L/K) = \text{inor}(F/K) = 1$ and yet L/F is purely inseparable.

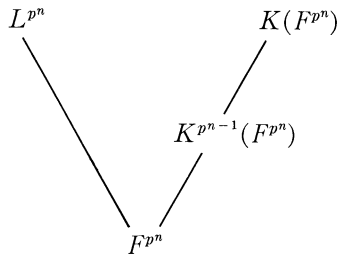
Definition. An intermediate field F of L/K is a *form* of L/K if and only if $\text{inor}(L/K) = \text{inor}(F/K)$. F is an *irreducible form* if and only if F is a form and there are no proper subfields of F/K which are forms of L/K .

Clearly L is a form of L/K and as noted above any intermediate field F over which L is separable is a form of L/K . We shall establish the existence of a unique irreducible form for any finitely generated extension.

THEOREM 1.3. *Let F be an intermediate field of L/K and let $n = \text{inex}(L/K)$. Then the following conditions are equivalent.*

- (1) F/K is a form of L/K .
- (2) L^{p^n} and $K(F^{p^n})$ are linearly disjoint over F^{p^n} .
- (3) $\text{insep}(K(F^{p^i})/K) = \text{insep}(K(L^{p^i}))$, $0 \leq i \leq n - 1$.
- (4) $K(F^{p^i})$ is a form of $K(L^{p^i})$, $0 \leq i \leq n - 1$.

Proof. (1) if and only if (2). We use induction on $\text{inex}(L/K)$. The case $\text{inex}(L/K) = 1$ is [5, Lemma 1, p. 111]. Let $\text{inex}(L/K) = n$. From Lemma 1.1 $\text{inor}(L/K) = \text{inor}(K(L^p)/K) + \text{insep}(L/K)$. From [5, Lemma 1, p. 111], $\text{insep}(L/K) = \text{insep}(F/K)$ if and only if L^p and $K(F^p)$ are linearly disjoint over F^p i.e. if and only if L^{p^n} and $K^{p^{n-1}}(F^{p^n})$ are linearly disjoint over F^{p^n} , and by induction $\text{inor}(K(L^p)/K) = \text{inor}(K(F^p)/K)$ if and only if $K^{p^{n-1}}(L^{p^n})$ and $K(F^{p^n})$ are linearly disjoint over $K^{p^{n-1}}(F^{p^n})$. But using the standard lemma on linear disjointness [4, Lemma, p. 162] on the diagram



L^{p^n} and $K(F^{p^n})$ are linearly disjoint over F^{p^n} if and only if L^{p^n} and $K^{p^{n-1}}(F^{p^n})$ are linearly disjoint over F^{p^n} and $K^{p^{n-1}}(L^{p^n})$ and $K(F^{p^n})$ are linearly disjoint over $K^{p^{n-1}}(F^{p^n})$.

(2) implies (3). If L^{p^n} and $K(F^{p^n})$ are linearly disjoint over F^{p^n} , then since $K(F^{p^n}) \supseteq K^{p^{n-i}}(F^{p^n}) \supseteq F^{p^n}$, $0 \leq i \leq n - 1$, $K^{p^{n-i}}(L^{p^n})$ and $K(F^{p^n})$ are linearly disjoint over $K^{p^{n-i}}(F^{p^n})$ and taking p^{n-i-1} th roots, we have $K^p(L^{p^{i+1}})$ and $K^{p^{-n+i+1}}(F^{p^{i+1}})$ (all we need is $K(F^{p^{i+1}})$) are linearly disjoint over $K^p(F^{p^{i+1}})$. Thus by [5, Lemma 1, p. 111], $\text{insep}(K(F^{p^i})/K) = \text{insep}(K(L^{p^i})/K)$.

(3) implies (4). The proof follows by descending induction on i and the fact that $\text{inor}(K(L^{p^i})) = \text{insep}(K(L^{p^i})) + \text{inor}(K(L^{p^{i+1}}))$ as in Lemma 1.1.

(4) implies (1) is immediate.

THEOREM 1.4. *Any finitely generated extension L/K has a unique irreducible form.*

Proof. Let $\{L_\alpha\}_{\alpha \in A}$ be the set of all forms of L/K and let $n = \text{inex}(L/K)$. It suffices to show $\bigcap_\alpha L_\alpha$ is a form of L/K . By Theorem 1.3, L^{p^n} and each $K(L_\alpha^{p^n})$ are linearly disjoint and hence L^{p^n} and $\bigcap_\alpha K(L_\alpha^{p^n})$ are linearly disjoint over their intersection [10, Theorem 1.1, p. 39]. Since

$$(\bigcap_\alpha K(L_\alpha^{p^n})) \cap L^{p^n} = \bigcap_\alpha ((K(L_\alpha^{p^n}) \cap L^{p^n}) = \bigcap_\alpha L_\alpha^{p^n},$$

we have that L^{p^n} and $\bigcap_\alpha K(L_\alpha^{p^n})$ are linearly disjoint over $\bigcap_\alpha L_\alpha^{p^n}$. But

$$\bigcap_\alpha K(L_\alpha^{p^n}) \supseteq K(\bigcap_\alpha L_\alpha^{p^n}) = K((\bigcap_\alpha L_\alpha)^{p^n}) \supseteq \bigcap_\alpha L_\alpha^{p^n},$$

and hence L^{p^n} and $K((\bigcap_\alpha L_\alpha)^{p^n})$ are linearly disjoint over $(\bigcap_\alpha L_\alpha)^{p^n}$. By Theorem 1.3, $\bigcap_\alpha L_\alpha$ is a form of L/K .

Before studying properties of irreducible extensions we review the following:

L is *reliable* over K if and only if $L = K(B)$ for every relative p -basis B of L over K . L is *modular* over K if and only if L^{p^i} and K are linearly disjoint over their intersection for all i . The modularity of L/K , $\text{mod}(L/K)$, is the $\max\{r | L/K(L^{p^r}) \text{ is modular}\}$ if it exists and is ∞ otherwise. There exist unique minimal intermediate fields C^* and Q^* of L/K such that L/C^* is separable and L/Q^* is modular. C^*/K is reliable and C^*/Q^* is purely inseparable modular [1, Theorems 1.1 and 1.4].

THEOREM 1.5. *Assume L/K is irreducible with $n = \text{inex}(L/K)$ and let Q^* be the unique minimal intermediate field over which L is modular. Then*

- (1) L is reliable over K .
- (2) Let B be any relative p -basis of L/K and let $|B| = t$. Then any subset of B with $t - 1$ elements contains a separating transcendence basis for a distinguished subfield.
- (3) $Q^* \supseteq K(L^{p^n})$ and hence $\text{mod}(L/K) \leq n$ unless L/K is algebraic and modular of exponent n over its maximal separable intermediate field.

Proof. (1). If S is an intermediate field of L/K and L is separable over S , then as noted earlier S is a form of L/K and hence $S = L$. Thus L/K is reliable [7, Theorem 1, p. 523].

(2). Let $\{b_1, \dots, b_i\}$ be a relative p -basis for L/K . Consider $L_1 = K(L^p)(b_1, \dots, \hat{b}_i, \dots, b_i)$. Since L/K is irreducible, $\text{inor}(L_1/K) < \text{inor}(L/K)$. $\{b_1, \dots, b_i^p, \dots, b_i\}$ certainly contains a relative p -basis for L_1/K and hence a separating transcendence basis for a distinguished subfield D_1 of L_1/K [5, Lemma 2, p. 113]. Since L/K is irreducible, a degree argument shows D_1 is a distinguished subfield of L/K . Thus if we show b_i^p cannot be part of a separating transcendence basis for D_1/K , one must be composed by the elements of $\{b_1, \dots, \hat{b}_i, \dots, b_i\}$. If $b_i^p \notin D_1$ it is not part of a separating transcendence basis, hence assume $b_i^p \in D_1$. Then $L = D_1(b_i) \otimes_{D_1} L_1$. If b_i^p were p -independent in D_1/K , $D_1(b_i)$ would be separable over K and hence $\text{inor}(L/K) = \text{inor}(L_1/K)$, a contradiction.

(3). Since L/K is reliable, L/Q^* has bounded exponent [1, Theorem 1.4] and hence has a subbasis $\{b_1, \dots, b_s\}$. If each $b_i^{p^n}$ is in Q^* , then $K(L^{p^n}) \subset Q^*$ as desired. If one is not, say $b_1^{p^n}$, then the exponent of L over $L_1 = Q^*(b_1^{p^{n+1}}, b_2, \dots, b_s)$ is $n + 1$ and $L = L_1(b_1)$. Then $[L : L_1(b_1^p)] = p$ and as in part (2) $L_1(b_1^p)$ contains a distinguished subfield D_1 for L/K . Thus $K(L^{p^n}) = K(D_1^{p^n})$ [3, Proposition 1, p. 288] $\subseteq K(L_1^{p^n}(b_1^{p^{n+1}})) \subseteq L_1$. This contradicts the fact that the exponent of L over L_1 is $n + 1$. Thus $\text{mod}(L/K) \leq n$ unless $K(L^{p^n}) = K(L^{p^{n+1}})$ in which case $K(L^{p^n})$ is separable algebraic over K .

COROLLARY 1.6. *L/K is irreducible if and only if L/K is reliable and every subfield L_1 where $[L : L_1] = p$ contains a distinguished subfield of L/K .*

Proof. Assume L/K is irreducible and $[L : L_1] = p$. Since L/K is reliable, L/L_1 is reliable and hence purely inseparable. Thus $\text{inor}(L_1/K) = \text{inor}(L/K) - 1$ and any distinguished subfield for L_1/K will be one for L/K . Conversely

let L_1 be any proper intermediate field. Since L/L_1 is reliable, there exists $L_2 \supseteq L_1$ such that L/L_2 is purely inseparable of degree p . Thus L_2 contains a distinguished subfield for L/K and $\text{inor}(L/K) = \text{inor}(L_2/K) + 1$. By Lemma 1.1, $\text{inor}(L_2/K) \geq \text{inor}(L_1/K)$.

3. Relationships. We now investigate the relationship between L/K and forms for L/K . The distinguished closure of L/K is the unique minimal purely inseparable extension J^* of K such that $L(J^*)/J^*$ is separable [9, Theorem 3, p. 608].

LEMMA 2.1. *Suppose L_1/K is a form of L/K . If M/K is a finite degree purely inseparable field extension, then $L_1(M)$ is a form of $L(M)/K$.*

Proof. Let D_1 and D be distinguished intermediate fields of L_1/K and L/K respectively. Then D_1 and D are distinguished for $L_1(M)/K$ and $L(M)/K$ respectively. Since $L_1 \subseteq L$, $[L(M) : L] \leq [L_1(M) : L_1]$. Thus $[L(M) : L] \times [L : D] \leq [L_1(M) : L_1][L_1 : D_1]$, i.e. $[L(M) : D] \leq [L_1(M) : D_1]$. But by Lemma 1.1, $[L(M) : D] \geq [L_1(M) : D_1]$.

THEOREM 2.2. *Let L_1 be a form of L/K . Then*

- (1) L_1/K and L/K have the same distinguished closures.
- (2) If D is any distinguished subfield for L/K , then $L = D(L_1)$.

Proof. (1) Let J_1^* and J^* be the distinguished closures, and let D_1 and D be distinguished subfields of L_1/K and L/K respectively. By Lemma 2.1, $[L(J_1^*) : D] = [L_1(J_1^*) : D_1]$. Also $[D(J_1^*) : D] = [J_1^* : K] = [D_1(J_1^*) : D_1]$. Since $D_1(J_1^*) = L_1(J_1^*)$, $[L(J_1^*) : D] = [D(J_1^*) : D]$ so $L(J_1^*) = D(J_1^*)$. Hence $L \subseteq D(J_1^*)$ and $J^* \subseteq J_1^*$ by [9, Theorem 3, p. 608]. Since $L(J^*)$ is separable over J^* , $L_1(J^*)$ is separable over J^* , and hence $J_1^* \subseteq J^*$.

(2) $L^{p^n} \supseteq L_1^{p^n}(D^{p^n}) \supseteq L_1^{p^n}$. Since L_1 is a form of L/K , L^{p^n} and $K(L_1^{p^n})$ are linearly disjoint over $L_1^{p^n}$ by Theorem 1.2. By the lemma on linear disjointness [4, Lemma, p. 162], L^{p^n} and $K(L_1^{p^n}D^{p^n})$ are linearly disjoint over $L_1^{p^n}(D^{p^n})$. But since D is distinguished, $L^{p^n} \subseteq K(L_1^{p^n}D^{p^n})$ and hence $L^{p^n} = L_1^{p^n}(D^{p^n})$, i.e. $L = L_1(D)$.

Let J denote the maximal purely inseparable extension of K in L . Then L/K is said to *split* when $L = J \otimes_K D$ where D is separable over K .

COROLLARY 2.3. *The following conditions are equivalent,*

- (1) L/K splits.
- (2) J/K is a form of L/K .
- (3) L_1/K splits for all forms L_1 of L/K .
- (4) L_1/K splits for some form of L/K .

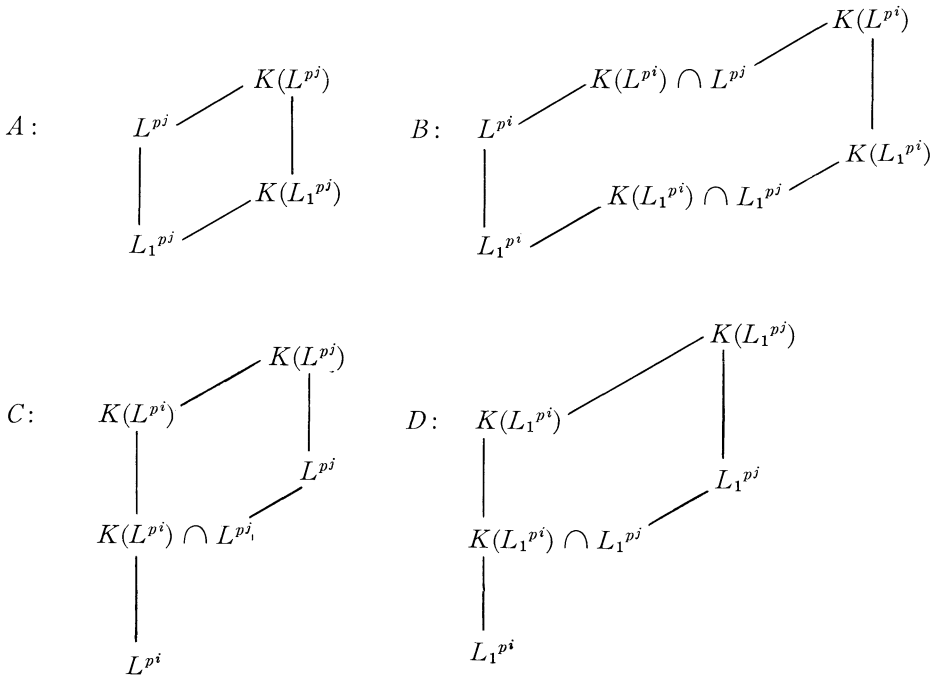
Proof. If L/K splits, $\text{inor}(L/K) = \log_p [J : K]$. Hence J is a form of L/K . If J is a form of L/K , then since J is finite dimensional purely inseparable over K , J is the unique minimal form of L/K , and hence any form L_1 must contain

J. Since J is also a form of L_1/K , $L_1 = D_1J = D_1 \otimes_K J$ where D_1 is a distinguished subfield of L_1/K (Theorem 2.2 (2)). Thus L_1/K splits. Assume L_1/K splits for some form. Then $L_1 = (K^{p^{-\infty}} \cap L_1) \otimes_K D_1$. Thus $K^{p^{-\infty}} \cap L_1$ is the distinguished closure of L_1 , whence of L by Theorem 2.2 (1), and hence L/K splits.

For the case where L/K is algebraic, the forms can easily be determined by degree arguments. L_1/K is a form if and only if L/L_1 is separable and hence L/K is irreducible if and only if L/K is reliable. Recall that the modularity of L/K , $m(L/K)$, is $\max\{r \mid L \text{ is modular over } K(L^{p^r})\}$ if it exists and is ∞ otherwise.

THEOREM 2.4. *Let L_1/K be a form of L/K . Then $m(L/K) \geq m(L_1/K)$.*

Proof. Let $n = \text{inex}(L/K)$. Assume $L_1/K(L_1^{p^i})$ is modular. Consider the following diagrams where $j \leq i$,



In diagram *A*, L^{p^j} and $K(L_1^{p^j})$ are linearly disjoint over $L_1^{p^j}$ by Theorem 1.3 if $j \leq n$ and by separability if $j > n$. Similarly for *B*. Since we are assuming L_1 is modular over $K(L_1^{p^i})$ we have the linear disjointness of *D* and we need to establish the linear disjointness of *C*. Let X be a linear basis of $K(L_1^{p^i})$ over $K(L_1^{p^i}) \cap L_1^{p^j}$. Then X is a basis of $K(L_1^{p^j})$ over $L_1^{p^j}$ by *D*. Hence by *A*, X is a basis of $K(L^{p^j})$ over L^{p^j} . By *B*, we see that X spans $K(L^{p^i})$ over $K(L^{p^i}) \cap L^{p^j}$. Hence for *C*, a spanning set for $K(L^{p^i})$ over $K(L^{p^i}) \cap L^{p^j}$ is

independent over L^{p^j} , and hence must actually be a basis for $K(L^{p^i})$ over $K(L^{p^i}) \cap L^{p^j}$. Thus $K(L^{p^i})$ and L^{p^j} are linearly disjoint and L is modular over $K(L^{p^i})$ and hence $m(L/K) \geq m(L_1/K)$.

We note that there can be strict inequality. Let $K = P(u^p, v^p)$, $L_1 = K(x^p, ux^p + v)$ and $L = K(x, ux^p + v)$ where P is a perfect field and $\{u, x, v\}$ is algebraically independent over P . Then it is straightforward that $m(L/K) = 2$ and $m(L_1/K) = 1$. However, in one case we do have equality.

THEOREM 2.5. *Suppose L_1 is a form of L/K . Then $m(L/K) = \infty$ if and only if $m(L_1/K) = \infty$.*

Proof. From the previous result, if $m(L_1/K) = \infty$ certainly $m(L/K) = \infty$. Suppose $m(L/K) = \infty$, and let C^* be the unique minimal intermediate field such that L/C^* is separable, and C^*/K is reliable [1, Theorem 1.2]. Let Q^* be the unique minimal intermediate field such that L/Q^* is modular and let L^* be the irreducible form of L/K . By [1, Theorem 2.4] Q^*/K is separable algebraic and C^*/Q^* is purely inseparable modular [1, Theorem 1.4]. Since L/C^* is separable, C^* is a form of L/K and hence $C^* \supseteq L^*$. But using Theorem 1.3 we see that L^*/K is also a form of C^*/K , and since C^*/K is reliable algebraic it is irreducible and hence $C^* = L^*$. Since C^*/Q^* is purely inseparable modular and Q^*/K is separable algebraic, $K(C^{*p^i}) = Q^*(C^{*p^i})$ and hence $C^*/K(C^{*p^i})$ is modular for all i , i.e. $m(C^*/K) = m(L^*/K) = \infty$. But now $L_1 \supseteq L^*$ and hence $m(L_1/K) \geq m(L^*/K)$.

COROLLARY 2.6. *Suppose $m(L/K) = \infty$. Then the unique irreducible form of L/K is the unique minimal intermediate field over which L is separable.*

Recall that if C^* is the unique minimal intermediate field of L/K over which L is separable then C^*/K is a form of L/K . Thus the unique minimal form L^*/K of L/K must be contained in C^* and hence be a form of C^*/K . We now present an example to show even if L/K is reliable, L/L^* may be transcendental. Let $K = P(x, y)$, $L_1 = K(w_1, w_1x^{p-1} + y^{p-1})$ and $L = L_1(w_2, w_2x^{p-1} + w_1^{p-1}y^{p-1})$ where P is a perfect field and $\{x, y, w_1, w_2\}$ is algebraically independent over P . Then L/K is reliable [6, Lemma, p. 43], $D_1 = K(w_1)$ and $D = K(w_2x^{p-1} + w_1^{p-1}y^{p-1}, w_2)$ are distinguished subfields of L_1/K and L/K respectively. Since $[L : D] = [L : D_1] = p$, L_1/K is a form of L/K and yet L/L_1 is of transcendence degree one.

REFERENCES

1. J. Deveney and J. Mordeson, *Subfields and invariants of inseparable field extensions*, Can. J. Math. 29 (1977), 1304–1311.
2. J. Dieudonné, *Sur les extensions transcendentes*, Summa Brasil. Math. 2 (1947), 1–20.
3. N. Heerema, *p*th powers of distinguished subfields, Proc. Amer. Math. Soc. 55 (1976), 287–292.
4. N. Jacobson, *Lectures in abstract algebra*. Vol. III: Theory of fields and Galois theory (Van Nostrand, Princeton, N.J., 1964).
5. H. Kraft, *Inseparable Körperweiterungen*, Comment. Math. Helv. 45 (1970), 110–118.

6. H. Kreimer and N. Heerema, *Modularity vs. separability for field extensions*, Can. J. Math. *27* (1975), 1176–1182.
7. J. Mordeson and B. Vinograde, *Relatively separated transcendental field extensions*, Archiv der Mathematik *24* (1973), 521–526.
8. ——— *Inseparable embeddings of separable transcendental extensions*, Archiv der Mathematik *27* (1976), 42–47.
9. J. Mordeson, *Splitting of field extensions*, Archiv der Mathematik *26* (1975), 606–610.
10. W. Waterhouse, *The structure of inseparable field extensions*, Trans. Amer. Math. Soc. *211* (1975), 39–56.
11. A. Weil, *Foundations of algebraic geometry*, Amer. Math. Soc. Colloq. Publ., vol. *29*, Amer. Soc. (Providence, R.I., 1946).

*Virginia Commonwealth University,
Richmond, Virginia;
Creighton University,
Omaha, Nebraska*