Can. J. Math., Vol. XXIX, No. 6, 1977, pp. 1304–1311

SUBFIELDS AND INVARIANTS OF INSEPARABLE FIELD EXTENSIONS

JAMES K. DEVENEY AND JOHN N. MORDESON

Introduction. Let L/K be a field extension of characteristic $p \neq 0$. The existence of intermediate fields over which L is regular, separable, or modular is important in recent Galois theories. For instance, see [**1**; **2**; **3**; **4**; **7**; **8**; **9** and **14**]. In Section 1 we prove the existence of unique minimal intermediate fields H^*, C^*, Q^* of L/K such that L/H^* is regular, L/C^* is separable and L/Q^* is modular. If R^* denotes the field of constants of all infinite higher derivations on L over K, then $R^* = \bigcap C^*(L^{p^n}) = \bigcap H^*(L^{p^n})$.

Dieudonné introduced and applied the concept of a distinguished subfield of a field extension with finite inseparability exponent. In Section 2 we introduce two numerical invariants on L/K which we connect with known measures of inseparability in order to determine properties of L/K via distinguished subfields. For instance, if L/K has finite inseparability exponent, we give a necessary and sufficient condition for L to be modular over every distinguished subfield. In certain cases, the same invariant can be related to the structure of Q^*/K. Distinguished subfields are characterized in terms of the other numerical invariant.

Unless specified otherwise, L/K always denotes an arbitrary field extension of characteristic $p \neq 0$. The *inseparability exponent* of L/K is the

$$\min \{n | K(L^{p^n})/K \text{ is separable}\}$$

if this exists, and is ∞ otherwise. We say L/K *splits*, and write $L = F \otimes_K J$, when L is the field composite over K of two intermediate fields F and J where F/K is separable and J/K is purely inseparable. L is *modular* over K if and only if L^{p^n} and K are linearly disjoint for all n. L is *reliable* over K if $L = K(M)$ for every relative p-basis M of L/K. We often use the fact that if L/K is reliable, then L/L' is reliable for every intermediate field L' [**16**, Proposition 1.15, p. 9].

1. Unique minimal intermediate fields.

THEOREM (1.1). *There exist unique minimal intermediate fields H^*, C^*, and Q^* of L/K such that L/H^* is regular, L/C^* is separable, and L/Q^* is modular. These intermediate fields satisfy the properties $H^* \supseteq C^* \supseteq Q^*$, $H^* = \bar{C}^* = \bar{Q}^*$ (the algebraic closure of Q^* in L), C^*/Q^* is purely inseparable modular, and $H^* = S \otimes_{Q^*} C^*$ where S is the maximal separable intermediate field of H^*/Q^*.*

Proof. Let $H = \{H_\alpha | H_\alpha$ is an intermediate field of L/K such that L/H_α is

Received January 12, 1977.

regular. Since $L \in H$, $H \neq \emptyset$. Now L^p and H_α are linearly disjoint over $H_\alpha{}^p$. By [**21**, Theorem 1.1, p. 39], L^p and $\bigcap_\alpha H_\alpha$ are linearly disjoint over $L^p \cap (\bigcap_\alpha H_\alpha) = \bigcap_\alpha (L^p \cap H_\alpha) = \bigcap_\alpha H_\alpha{}^p = (\bigcap_\alpha H_\alpha)^p$. Set $H^* = \bigcap_\alpha H_\alpha$. Then L/H^* is separable. Any element of L which is algebraic over H^* is also algebraic over every H_α, and hence is in every H_α. Thus H^* is the unique minimal intermediate field over which L is regular. The existence of C^* follows in a similar manner. The existence of Q^* is nearly immediate from [**21**, Theorem 1.1, p. 39]. Clearly $H^* \supseteq C^* \supseteq Q^*$. Since $\bar{C}^*/C^*$ is algebraic, $L/\bar{C}^*$ is separable. Since also $\bar{C}^*$ is algebraically closed in L, $L/\bar{C}^*$ is regular. Hence $\bar{C}^* \supseteq H^*$. Since $\bar{C}^*/C^*$ is separable algebraic, $\bar{C}^*/H^*$ is separable algebraic. Thus $\bar{C}^* = H^*$. Since L/Q^* is modular, $L/(Q^{*p^{-\infty}} \cap L)$ is separable and $(Q^{*p^{-\infty}} \cap L)/Q^*$ is modular by [**13**, Theorem 1, p. 1177]. Since $L/(Q^{*p^{-\infty}} \cap L)$ is separable, $Q^{*p^{-\infty}} \cap L \supseteq C^*$ by the minimality of C^*. Since L/C^* is separable and $(Q^{*p^{-\infty}} \cap L)/C^*$ is purely inseparable, $Q^{*p^{-\infty}} \cap L = C^*$. Clearly $H^* = \bar{Q}^*$ and $H^* = S \otimes_{Q*} C^*$. This completes the proof.

Clearly $K^{p^{-\infty}} \cap L \subseteq C^*$. If either L/K is modular or L/K splits, then $C^* = K^{p^{-\infty}} \cap L$. In fact, if L/K is modular, then $\bar{K}$, the algebraic closure of K in L, is modular over K since $K = Q^*$ and hence $\bar{K} = H^*$. If L/K is relatively separated ($L/K(M)$ is separable algebraic for every relative p-basis M), then L/C^* and L/H^* have finite separating transcendence bases by [**17**, Corollary, p. 418] and [**17**, Theorem 1, p. 418]. Hence if L/K is relatively separated and modular, then L/K splits by [**10**, Proposition 1, p. 2].

If L/K (or C^*/K) has finite inseparability exponent e and $K(L^{p^e})/K$ (or $K(C^{*p^e})/K$) has a finite separating transcendence basis, then C^*/K is relatively separated by [**17**, Theorem 2, p. 419]. If L/K (or C^*/K) is finitely generated, then C^*/K is relatively separated.

THEOREM (1.2). *If C^*/K is relatively separated, then C^*/K has the following properties*:

1. *C^* is a maximal intermediate field of L/K which is reliable over K.*
2. *C^* is the only intermediate field of L/K such that L/C^* is separable and C^*/K is reliable.*

Proof. 1. Since C^*/K is relatively separated and has no proper coseparable intermediate fields, C^*/K is reliable [**18**, Theorem 1, p. 523]. Let F be any intermediate field of L/C^*. Then C^* is a coseparable intermediate field of F/K. Thus if F/K is reliable, $F = C^*$. Hence C^* is a maximal intermediate field of L/K such that C^*/K is reliable.

2. Let R be an intermediate field of L/K such that L/R is separable and R/K is reliable. Then $R \supseteq C^*$ by the minimality of C^*, whence $R^* = C^*$ by (1).

Example (1.3). C^* is not necessarily unique with respect to being a maximal intermediate field of L/K which is reliable over K: Let $L = P(x, y, z)$ and $K = P(x^p, y^p)$ where P is a perfect field of characteristic $p \neq 0$ and x, y, z are algebraically independent indeterminates over P. Set $R = K(z, zx + y)$.

Then R/K is reliable by [**18**, Example 1, p. 522]. Now $[L : R] = p$ and L/K is not reliable since $L/K(x, y)$ is separable. Thus R is a maximal intermediate field of L/K which is reliable over K. Now $C^* = K(x, y)$ since $L/K(x, y)$ is separable and $K(x, y)/K$ is reliable.

The following result generalizes the structure theorem of Heerema and Tucker [**10**, Corollary 7, p. 4] given for finitely generated extensions.

THEOREM (1.4). *Suppose C^*/K is reliable. Then L/Q^* has finite inseparability exponent, C^*/Q^* is purely inseparable modular with bounded exponent, and $L = F \otimes_S (S \otimes_{Q^*} C^*)$ where S is the maximal separable intermediate field of H^*/Q^* and F is an intermediate field of L/S which is regular over S and separable over Q^*.*

Proof. By (1.1), C^*/Q^* is purely inseparable modular. Since C^*/K is reliable, C^*/Q^* is reliable and [**17**, Proposition 1.23, p. 16] shows C^*/Q^* is of bounded exponent. By (1.1), $H^* = S \otimes_{Q^*} C^*$, and thus H^* is of bounded exponent over S. Since L/H^* is separable, $L = F \otimes_S H^*$ by [**13**, Theorem 4, p. 1178]. Thus $L = F \otimes_S (S \otimes_{Q^*} C^*)$.

It is well known that the field of constants R^* of all infinite higher derivations on L/K is such that L/R^* is regular [**9**, Theorem 2.3, p. 264]. Hence $R^* \supseteq H^*$. We now determine R^* by using H^* and C^*.

THEOREM (1.5). [**2**, Theorem 1, p. 50] *The following conditions are equivalent on L/K.*

1. *L/K is separable and $\bigcap_{i=1}^{\infty} K(L^{p^i}) = K$.*
2. *K is a field of constants of a set of infinite higher derivations on L.*

THEOREM (1.6). *Let R^* be the field of constants of all infinite higher derivations on L/K. Then*

$$R^* = \bigcap_{i=1}^{\infty} H^*(L^{p^i}) = \bigcap_{i=1}^{\infty} C^*(L^{p^i}).$$

Furthermore, R^* is the unique maximal relatively perfect field extension of C^* in L.

Proof. We first show that L is separable over $\bigcap_{i=1}^{\infty} C^*(L^{p^i})$. Since L/C^* is separable, L/C^* is modular. Thus $L/\bigcap_{i=1}^{\infty} C^*(L^{p^i})$ is modular. Hence it suffices to show that $L^p \cap \bigcap_{i=1}^{\infty} C^*(L^{p^i}) = (\bigcap_{i=1}^{\infty} C^*(L^{p^i}))^p$. Since L/C^* is separable, $C^* \cap L^p = C^{*p}$. Since $C^*(L^{p^i})$ and $C^*(L^{p^i}) \cap L^p$ are intermediate fields of L^p/C^{*p} and since C^* and L^p are linearly disjoint over C^{*p}, we have that C^* and $C^*(L^{p^i})$ are linearly disjoint over C^{*p} and that C^* and $C^*(L^{p^i}) \cap L^p$ are linearly disjoint over C^{*p}. Now $C^*(C^{*p}(L^{p^i})) = C^*(L^{p^i})$ and since $C^{*p}(L^{p^i}) \subseteq C^*(L^{p^i}) \cap L^p \subseteq C^*(L^{p^i})$, it follows that $C^*(C^*(L^{p^i}) \cap L^p) = C^*(L^{p^i})$. Thus $C^{*p}(L^{p^i}) = L^p \cap C^*(L^{p^i})$. Hence

$$L^p \cap \bigcap_{i=1}^{\infty} C^*(L^{p^i}) = \bigcap_{i=1}^{\infty} (L^p \cap C^*(L^{p^i})) = \bigcap_{i=1}^{\infty} C^{*p}(L^{p^i}) = \left(\bigcap_{i=1}^{\infty} C^*(L^{p^i})\right)^p.$$

https://doi.org/10.4153/CJM-1977-131-4 Published online by Cambridge University Press

Therefore $L/\bigcap_{i=1}^{\infty} C(L^{p^i})$ is separable. It is straightforward that

$$\bigcap_{i=1}^{\infty} ((\bigcap_{i=1}^{\infty} C^*(L^{p^i}))(L^{p^i})) = \bigcap_{i=1}^{\infty} C^*(L^{p^i}).$$

Thus by (1.5), $\bigcap_{i=1}^{\infty} C^*(L^{p^i})$ is the field of constants of a set of infinite higher derivations and $R^* \subseteq \bigcap_{i=1}^{\infty} C^*(L^{p^i})$. Since $R^* \supseteq C^*$, $R^* = \bigcap_{i=1}^{\infty} R^*(L^{p^i}) \supseteq \bigcap_{i=1}^{\infty} C^*(L^{p^i})$ and we have $R^* = \bigcap_{i=1}^{\infty} C^*(L^{p^i})$. Since H^*/C^* is separable algebraic, $R^* = \bigcap_{i=1}^{\infty} H^*(L^{p^i})$. Since R^* is contained in $C^*(L^p)$, no element of R^* which is relatively p-independent over C^* can be relatively p-independent in L/C^*. Since L/R^* is also separable, R^* must have the empty set as a relative p-basis over C^*, i e., R^*/C^* is relatively perfect. Since any relatively perfect field extension of C^* must be contained in $\bigcap_{i=1}^{\infty} C^*(L^{p^i})$, R^* is the unique largest such field extension of C^*.

COROLLARY (1.7). *Suppose L/K is relatively separated. Then $R^* = H^*$.*

Proof. Since L/K is relatively separated, L/C^* has a finite separating transcendence basis as noted in the comments preceeding (1.2). Thus $\bigcap_{i=1}^{\infty} C^*(L^{p^i}) = \bar{C}^* = H^*$ by [**18**, Theorem 2, p. 524].

2. Distinguished subfields. In 1947 Dieudonne introduced the concept of distinguished subfields of L/K. An intermediate field F is *distinguished* if and only if F is separable over K and $L \subseteq F(K^{p^{-\infty}})$. If L/K is of finite inseparability exponent, then there always exists distinguished subfields, but an example is given in [**5**] of an extension which does not have a distinguished subfield. If L/K is finitely generated then L has the same degree over each distinguished subfield and this degree is Weil's order of inseparability. The results in [**12**] for the finitely generated case can be extended to field extensions L/K of finite inseparability exponent to show that L has the same cannonical invariants [**16**, Definition 1.30, p. 27] over each distinguished subfield. However, the structure of L over different distinguished subfields can vary.

Example (2.1). L is modular over one distinguished subfield, but is not modular over every distinguished subfield: let $K = P(w, x, y)$ and $L = K(z, zw^{p^{-2}}, zw^{p^{-2}}x^{p^{-1}} + y^{p^{-1}})$ where P is a perfect field of characteristic $p \neq 0$ and w, x, y, z are algebraically independent indeterminants over P. Then L/K has inseparability exponent 2. $K(z)$ and $K(zw^{p^{-2}}x^{p^{-1}} + y^{p^{-1}})$ are distinguished intermediate fields of L/K. $L/K(z)$ is not modular since $z^{p^2}w, x, y$ are p-independent in $K(z)$ ([**16**, Example 1.59, p. 55]). However $L/K(zw^{p^{-2}}x^{p^{-1}} + y^{p^{-1}})$ is modular with modular basis $\{z, zw^{p^{-2}}\}$.

We introduce a numerical invariant on L/K, namely $m(L/K) = \max \{r | L/K(L^{p^r}) \text{ is modular}\}$ if the maximum exists and $m(L/K) = \infty$ otherwise. If $L/K(L^{p^n})$ is modular then $L/K(L^{p^r})$ is also modular for $r \leqq n$. We use the invariant to study properties of L over its distinguished subfields and in particular apply it to the fields C^* and H^* introduced earlier.

https://doi.org/10.4153/CJM-1977-131-4 Published online by Cambridge University Press

THEOREM (2.2). *Suppose L/K has finite inseparability exponent e. Then $m(L/K) \geqq e$ if and only if L/F is modular for every distinguished intermediate field F.*

Proof. Suppose $m(L/K) \geqq e$ and let F be a distinguished subfield. Since F/K is separable, F is an equiexponential modular extension of $K(F^{p^e})$ of exponent e. Since $L \subseteq F(K^{p^{-e}})$, $K(L^{p^e}) = K(F^{p^e})$. Since $L/K(L^{p^e})$ is also modular of exponent e, it follows that F is pure in $L/K(L^{p^e})$. Thus L/F is modular [**21**, Definition and Note, p. 41].

Conversely, suppose L/F is modular for every such F. Then $L/\bigcap_F F$ is modular [**21**, Proposition 1.2, p. 40]. Hence it suffices to show $\bigcap_F F = K(L^{p^e})$. Clearly $K(L^{p^e}) \subseteq \bigcap_F F$. Let $c \in L - K(L^{p^e})$ and let $F = K(L^{p^e})\ (Y)$ be a distinguished intermediate field of L/K where Y is relatively p-independent in L/K and Y^{p^e} is a relative p-basis of $K(L^{p^e})/K$. Since $F/K(L^{p^e})$ is modular, it follows that $\bigcap_{y \in Y} K(L^{p^e})\ (Y - \{y\}) = K(L^{p^e})$. Hence there exists $y \in Y$ such that $c \notin K(L^{p^e})\ (Y - y)$. Since L/F has exponent e, there exists $x \in L$ such that x has exponent e over $K(L^{p^e})\ (Y)$. Y is an equi-exponential modular basis of exponent $e + 1$ of $F/K(L^{p^{e+1}})$. Thus y has exponent $e + 1$ over $K(L^{p^{e+1}})$ $(Y - \{y\})$. Now both x and $x + y$ have exponent e over $K(L^{p^e})\ (Y)$ and either x or $x + y$ has exponent $e + 1$ over $K(L^{p^{e+1}})\ (Y - \{y\})$. That is, there exists $z \in L$ such that z has exponent e over $K(L^{p^e})\ (Y)$ and exponent $e + 1$ over $K(L^{p^{e+1}})\ (Y - \{y\})$. Since clearly z has exponent e over $K(L^{p^{e+1}})\ (Y - \{y\})$, $K(L^{p^e})(Y) \cap K(L^{p^e})(Y - \{y\}, z) = K(L^{p^e})(Y - \{y\})$. Hence $c \notin K(L^{p^e})(Y) \cap K(L^{p^e})\ (Y - \{y\}, z)$. We now show that $K(L^{p^e})\ (Y - \{y\}, z)$ is a distinguished intermediate field so that for any $c \in L - K(L^{p^e})$, there exists two distinguished intermediate fields for which c is not in their intersection whence not in the intersection of all distinguished intermediate fields. Thus $K(L^{p^e}) = \bigcap_F F$. Now $z \notin K(L^p)\ (Y - \{y\})$ else $z^{p^{e-1}} \in K(L^{p^e})\ (Y - \{y\})$. Thus $(Y - \{y\}) \cup \{z\}$ is relatively p-independent in L/K. Also $z^{p^e} \notin K(L^{p^{e+1}})$ $(Y^{p^e} - \{y^{p^e}\})$ else $z^{p^e} \in K(L^{p^{e+1}})\ (Y - \{y\})$. Thus $(Y^{p^e} - \{y^{p^e}\}) \cup z^{p^e}$ is a relative p-basis of $K(L^{p^e})/K$. Hence $K(L^{p^e})\ (Y - \{y\}, z)$ is a distinguished intermediate field of L/K.

As an application of (2.2) we consider the following. Every extension of a field K of characteristic $p \neq 0$ is separable if and only if $[K : K^p] = 1$. In [**13**] it is shown that every extension of K is modular if and only if $[K : K^p] \leqq p$.

COROLLARY (2.3). *The following are equivalent for a field K of characteristic $p \neq 0$.*

1) $[K : K^p] \leqq p^2$.

2) $m(L/K) \geqq e$ *for every extension L of inseparability exponent e.*

Proof. Assume 1). It suffices to consider the case where $[K : K^p] = p^2$. Let L be any extension of K of exponent e and let D be a distinguished subfield of L/K. Let $\{x, y\}$ be a p-basis for K. Then $D(x^{p^{-e}}, y^{p^{-e}}) \supseteq L \supseteq D$. Since

$D(x^{p^{-e}}, y^{p^{-e}})$ is modular over D, [**16**, Proposition 2.5, p. 76] shows L is modular over D. By (2.2) L is modular over $K(L^{p^e})$ and hence $m(L/K) \geqq e$.

Conversely, assume 2). Suppose $[K : K^p] > p^2$, and we find a contradiction. Let $\{w, x, y\}$ be part of a p-basis for K. Then $L = K(z, zw^{p^{-2}}, zw^{p^{-2}}x^{p^{-1}} + y^{p^{-1}})$, as in Example (2.1), is of exponent 2 and yet $L/K(L^{p^2})$ is not modular.

If $m(L/K) \geqq e$, then $Q^* \subseteq K(L^{p^e})$ so Q^*/K is separable. In fact, $m(L/K) \geqq e$ if and only if $Q^* \subseteq K(L^{p^e})$ since when $Q^* \subseteq K(L^{p^e})$, $Q^*(L^{p^e}) = K(L^{p^e})$ and $L/Q^*(L^{p^e})$ is modular.

We now direct our attention to the structure of Q^*/K.

If L/K has finite inseparability exponent e and $K(L^{p^e})/K$ has a finite separating transcendence basis (whence if L/K is finitely generated), then $\bigcap_{i=1}^{\infty} K(L^{p^i})$ is the separable algebraic closure of K in L ([**18**, Theorem 2, p. 524]).

THEOREM (2.4). *Suppose $\bigcap_{i=1}^{\infty} K(L^{p^i})$ is the separable algebraic closure of K in L. Then $m(L/K) = \infty$ if and only if Q^*/K is separable algebraic. If $m(L/K) = \infty$, then $H^* = C^*$ if and only if $Q^* = \bigcap_{i=1}^{\infty} K(L^{p^i})$.*

Proof. Suppose $m(L/K) = \infty$. Then $L/\bigcap_{i=1}^{\infty} K(L^{p^i})$ is modular. By the minimality of Q^*, $\bigcap_{i=1}^{\infty} K(L^{p^i}) \supseteq Q^*$. Hence Q^*/K is separable algebraic. Conversely, suppose Q^*/K is separable algebraic. Then $\bigcap_{i=1}^{\infty} K(L^{p^i}) \supseteq Q^*$ whence $\bigcap_{i=1}^{\infty} K(L^{p^i}) = \bigcap_{i=1}^{\infty} Q^*(L^{p^i})$. Since L/Q^* is modular, $L/\bigcap_{i=1}^{\infty} Q^*(L^{p^i})$ whence $L/\bigcap_{i=1}^{\infty} K(L^{p^i})$ is modular. Thus $m(L/K) = \infty$. It follows easily from (1.1) that $m(L/K) = \infty$ implies that the equivalence of $H^* = C^*$ and $Q^* = \bigcap_{i=1}^{\infty} K(L^{p^i})$.

COROLLARY (2.5). *Suppose L/K is reliable. Then $\bigcap_{i=1}^{\infty} K(L^{p^i})$ is the separable algebraic closure of K in L and $m(L/K) = \infty$ if and only if L/K is algebraic and is of bounded exponent and modular over its maximal separable intermediate field.*

Proof. Since L/K has no proper coseparable intermediate fields, $L = C^*$ and C^*/K is reliable. Thus L/Q^* is purely inseparable modular with bounded exponent by (1.4). Hence if Q^*/K is separable algberaic, then $\bigcap_{i=1}^{\infty} K(L^{p^i})$ is the separable algebraic closure in L by the comments preceding (2.4). The conclusion is now immediate from (2.4).

THEOREM (2.6). *Suppose L/K is algebraic and let S denote the maximal separable intermediate field of L/K. Then L/S is modular if and only if Q^* is the maximal separable intermediate field of C^*/K. If L/S is modular, then Q^* is the unique minimal intermediate field over which L splits.*

Proof. Suppose L/S is modular. Then $Q^* \subseteq S$ by the minimality of Q^*. Hence Q^*/K is separable algebraic. By (1.1), C^*/Q^* is purely inseparable. Conversely, suppose Q^* is the maximal separable intermediate field of C^*/K. Then $Q^* \subseteq S$ and so S/Q^* is separable algebraic. Since C^*/Q^* is purely in-

https://doi.org/10.4153/CJM-1977-131-4 Published online by Cambridge University Press

separable and L/C^* is separable algebraic, $L = S \otimes_{Q*} C^*$. Hence L/S is modular since C^*/Q^* is modular. Now suppose L/S is modular and L/Q splits where Q is an intermediate field of L/K. Say $L = S' \otimes_Q C$ where S' and C are intermediate fields of L/Q such that S'/Q is separable algebraic and C/Q is purely inseparable. If Q/K is not separable, then there exists Q', $Q \supset Q' \supseteq K$ where Q/Q' is purely inseparable and Q'/K is separable algebraic. Thus C/Q' is purely inseparab'e and L/C is separable algebraic and hence L splits over Q' say $L = S'' \otimes_{Q'} C$. If suffices to show $Q' \supseteq Q^*$. As Q'/K is separable, $S'' \subseteq S$. Now L/S'' is purely inseparable, so $S'' = S$. Now L/C is separable, so $C^* \subseteq C$. Since L/S is modular, $Q^* = S \cap C^* \subseteq S \cap C = Q'$ whence $Q \supseteq Q^*$

Definition (2.7). Let F be an intermediate field of L/K. The *purity index* of F in L/K is defined to be the largest nonnegative integer r such that F and $K(L^{p^i})$ are linearly disjoint over $K(F^{p^i})$ for $i = 0, 1, \ldots, r$ if such an r exists, otherwise ∞ is the purity index.

It is possible that F and $K(L^{p^i})$ are linearly disjoint over $K(F^{p^i})$ for some integer i and yet F and $K(L^{p^{i-1}})$ are not linearly disjoint over $K(F^{p^{i-1}})$. We note that if L/K is separable, then L is separable over an intermediate field F if and only if the purity index of F in L/K is positive.

If L/K is purely inseparable modular, then every basic intermediate field [**21**] has purity index ∞. For L/K arbitrary, we characterize distinguished intermediate fields in terms of purity index.

LEMMA (2.8). *Let F be an intermediate field of L/K. If there exists a field extension H/K such that $F \otimes_K H$ is a field and $L \subseteq F \otimes_K H$, then purity index $(F) = \infty$.*

Proof. We have $K(F^{p^i}) \subseteq K(L^{p^i}) \subseteq K(F^{p^i}) \otimes_K K(H^{p^i})$ and F and $K(F^{p^i}) \otimes_K K(H^{p^i})$ are linearly disjoint over $K(F^{p^i})$, $i = 0, 1, \ldots$. Thus F and $K(L^{p^i})$ are linearly disjoint over $K(F^{p^i})$, $i = 0, 1, \ldots$, that is, purity index $(F) = \infty$.

THEOREM (2.9). *Let F be an intermediate field of L/K such that L/F is purely inseparable and F/K is separable. Then F is distinguished if and only if purity index $(F) = \infty$.*

Proof. Suppose F is distinguished. Then $L \subseteq F \otimes_K K^{p^{-\infty}}$ so by (2.8) purity index $(F) = \infty$. Conversely, suppose purity index $(F) = \infty$. Let $x \in K^{p^{-\infty}}(L)$. Then $x \in F^{p^{-\infty}}(L) = F^{p^{-\infty}}$. Thus $x \in F^{p^{-i}}$ and $x \in K^{p^{-j}}(L)$ for some i and j. Let $r = \max\{i, j\}$. Then $x \in F^{p^{-r}} \cap K^{p^{-r}}(L)$. Since F, $K(L^{p^r})$ are linearly disjoint over $K(F^{p^r})$, $F^{p^{-r}}$ and $K^{p^{-r}}(L)$ are linearly disjoint over $K^{p^{-r}}(F)$. Thus $x \in F^{p^{-r}} \cap K^{p^{-r}}(L) = K^{p^{-r}}(F)$. Hence $x \in K^{p^{-\infty}}(F)$. Therefore $K^{p^{-\infty}}(L) \subseteq K^{p^{-\infty}}(F)$ so $L \subseteq K^{p^{-\infty}}(F)$. Since F/K is separable $K^{p^{-\infty}}(F) = F \otimes_K K^{p^{-\infty}}$ so F is a distinguished subfield.

References

1. S. Chase, *On inseparable Galois theory*, Bull. Amer. Math. Soc. *77* (1971), 413–417,
2. R. Davis, *Higher derivations and field extensions*, Trans. Amer. Math. Soc. *180* (1973), 47–52.
3. J. Deveney, *Fields of constants of infinite higher derivations*, Proc. Amer. Math. Soc. *41* (1973), 394–398.
4. ——— *An intermediate theory for a purely inseparable Galois theory*, Trans. Amer. Math. Soc. *198* (1974), 287–295.
5. ——— *A counterexample concerning inseparable field extensions*, Proc. Amer. Math. Soc. *55* (1976), 33–34.
6. J. Dieudonne, *Sur les extensions transcendantes separables*, Summa Brasil Math. *2* (1947), 1–20.
7. M. Gerstenhaber and A. Zaromp, *On the Galois theory of purely inseparable field extensions*, Bull. Amer. Math. Soc. *76* (1970), 1011–1014.
8. N. Heerema, *A galois theory for inseparable field extensions*, Trans. Amer. Math. Soc. *154* (1971), 193–200.
9. N. Heerema and J. Deveney, *Galois theory for fields K/k finitely generated*, Trans. Amer. Math. Soc. *189* (1974), 263–274.
10. N. Heerema and D. Tucker, *Modular field extensions*, Proc. Amer. Math. Soc. *53* (1975), 1–6.
11. L. Kime, *Purely inseparable, modular extensions of unbounded exponent*, Trans. Amer. Math. Soc. *176* (1973), 335–349.
12. H. Kraft, *Inseparable Korpererweiterungen*, Comment. Math. Helv. *45* (1970), 110–118.
13. H. Kreimer and N. Heerema, *Modularity* vs. *separability for field extensions*, Can. J. Math. *27* (1975), 1176–1182.
14. J. Mordeson, *On a Galois theory for inseparable field extensions*, Trans. Amer. Math. Soc. (1975), 337–347.
15. ——— *Splitting of field extensions*, Archiv der Mathematik *26* (1975), 606–610.
16. J. Mordeson and B. Vinograde, *Structure of arbitrary purely inseparable extension fields*, Lecture Notes in Math., Vol. 173 (Springer-Verlag, New York, 1970).
17. ——— *Separating p-basis and transcendental extension fields*, Proc. Amer. Math. Soc. *31*, (1972), 417–422.
18. ——— *Relatively separated transcendental field extensions*, Archiv der Mathematik *24* (1973), 521–526.
19. ——— *Inseparable embeddings of separable transcendental extensions*, Archiv der Mathematik *27* (1976), 42–47.
20. G. Pickert, *Inseparable Korpererweiterungen*, Math. Zeit. *52* (1949), 81–135.
21. W. Waterhouse, *The structure of inseparable field extensions*, Trans. Amer. Math. Soc. *211* (1975), 39–56.

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