Canad. Math. Bull. Vol. 29 (2), 1986

UNIQUENESS OF SUBFIELDS

BY

JAMES K. DEVENEY and JOHN N. MORDESON

ABSTRACT. Let L be a finitely generated field extension of a field K. The order of inseparability of L/K is the minimum of $\{n|[L:S] = p^n$ where S is a separable extension of $K\}$. If L^1 is a subfield of L/K, then its order of inseparability is less than or equal to that of L/K. This paper examines the question of when there are unique minimal subfields L_{n-j}^* of order of inseparability $n - j$, $0 \leq j \leq n$.

Let L be a finitely generated field extension of a field K of characteristic $p \neq 0$. The order of inseparability of L/K, inor(L/K), is defined to be the minimum of $\{n|[L:S] = p^n$ where S is a maximal separable extension of $K\}$. By Zorn's Lemma, maximal separable extensions of K in L exist and L is necessarily purely inseparable over any such field. If S is maximal separable, then $[L:S]$ is called the codegree of S. If L/K is algebraic, then the set of codegrees of maximal separable subfields consists of a single integer since there is a unique maximal separable subfield. If L/K is not algebraic then the set of codegrees may be infinite. Recent works [3], [4] and [6] have examined when this set is bounded or consists of a single integer. The main application of this paper is to provide an affirmative answer to a conjecture in [3] and thus characterize when the set of codegrees consists of a single integer. Some information is also obtained concerning when the set is bounded.

Let the order of inseparability of L/K be n. This paper examines the questions of when (a) There are unique minimal subfields L_{n-j}^* of order of inseparability $n - j$, $0 \leq j \leq n$; (b) There are unique maximal subfields L'_{n-j} of order of inseparability $n - j$, $0 \leq j \leq n$; (c) There are unique subfields L_{n-j} of order of inseparability $n - j$, $0 \leq j \leq n$. If L/K is algebraic, (a) and (b) are equivalent. However, if L is not algebraic over K, (b) implies (a) but they no longer need be equivalent.

The main technical tool is the concept of a form [1]. If L_1 is a subfield of L/K, then inor$(L/K) \geq$ inor(L/K_1) and we have equality if and only if L^{p^r} and $K(L_1^{p^r})$ are linearly disjoint over $L_1^{p^r}$ for all r (in this case L_1 is called a form of L/K). Every L/K has a unique minimal form L^* which is the intersection of all forms of L/K. A field extension with no proper forms is called irreducible and we note that L need not be algebraic over its irreducible form [1]. The inseparability of L/K is defined by insep$(L/K) = \log_p[L:K(L^p)]$ − transendence degree of L/K, that is, insep(L/K) is the number of extra elements is a relative p-basis of L/K.

Received by the editors August 28, 1984 and in revised form, March 8, 1985.

AMS(MOS) Subject Classification: 12F15.

https://doi.org/10.4153/CMB-1986-031-5 Published online by Cambridge University Press

THEOREM 1. *Suppose* insep$(L/K) = 1$ *and* inor$(L/K) = n$. *Then L/K has unique minimal subfields L^*_{n-j} of order of inseparability $n - j$ for $j = 0, 1, \ldots, n$. The subfield L^*_{n-j} is the unique irreducible form of $K(L^{*p}_{n-j+1})/K$ for $j = 1, \ldots n$.*

PROOF. The irreducible form L^*_n of L/K [1, Theorem 1.4, p. 657] is the unique minimal subfield of inor n. Let L_{n-1} be any minimal subfield of L/K such that inor $(L_{n-1}/K) = n - 1$. Suppose inor$(L_{n-1}(L^{*p})/K) = n$. Then $L^*_n \subseteq L_{n-1}(L^{*p}_n)$ and hence $L_{n-1}(L^*_n) = L_{n-1}(L^{*p}_n)$. Thus $L_{n-1}(L^*_n) = L_{n-1}(L^{*p^i}_n)$ for all i, so $L_{n-1}(L^*_n) = \cap \{L_{n-1}(L^{*p^i}_n)|1 \leq i < \infty\} \subseteq \cap \{L_{n-1}(L^p)^i|1 \leq i < \infty\} = (L_{n-1})_s$, the separable algebraic closure of L_{n-1} in L [7, Theorem 7.2, p. 273]. This forces inor$(L_{n-1}/K) = n$ [1, p. 656], a contradiction. Thus inor$(L_{n-1}(L^{*p}_n)/K) = n - 1$. Since L_{n-1} and $K(L^{*p}_n)$ are both subfields of $L^*_{n-1}(L^p_n)$ and all have order of inseparability $n - 1$ over K, $L_{n-1} \cap K(L^{*p}_n)$ must have order of inseparability $n - 1$ over K. By the minimality of L_{n-1}, $L_{n-1} \subseteq K(L^{*p}_n)$. Thus L_{n-1} is the unique irreducible form of $K(L^{*p}_n)/K$. Thus the theorem is true for $j = 0, 1$ and we now induct on j. Assume the result is true for $j = r$. Now L^*_{n-r} is irreducible and insep$(L^*_{n-r}/K) = 1$. Thus by the last case, L^*_{n-r} has a unique minimal subfield $\bar{L}_{n-r-1}$ of order of inseparability $n - r - 1$ and $\bar{L}_{n-r-1}$ is the unique irreducible form of $K(L^{*p}_{n-r})/K$. Assume there is another subfield L_{n-r-1}, minimal in L/K or order of inseparability $n - r - 1$. Since L_{n-r-1} is minimal, $L_{n-r-1} \cap \bar{L}_{n-r-1}$ has order of inseparability less than $n - r - 1$. Thus $L_{n-r-1}(\bar{L}_{n-r-1})$ has order of inseparability of least $n - r$, and hence contains $L_{n-r-1}(L^*_{n-r})$. Thus $L_{n-r-1}(L^*_{n-r}) \supseteq L_{n-r-1}(\bar{L}_{n-r-1}) = L_{n-r-1}L(^{*p}_{n-r})$. Thus $L_{n-r-1}(L^{*p}_{n-r}) = L_{n-r-1}(L^*_{n-r})$ and as in the previous case inor$(L_{n-r-1}) = n - r$, a contradiction. Thus there is no other.

THEOREM 2. *If L/K is inseparable with order of inseparability $n > 0$ and L/K has unique minimal subfields L^*_{n-j} of order of inseparability $n - j$, $0 \leq j \leq n$, then insep $(L/K) = 1$.*

PROOF. Suppose insep$(L/K) > 1$. Let D be a distinguished subfield of L/K. Let b_1 and b_2 be relatively p-independent in L/D. Then there exist non-negative integers e_1 and e_2 such that $D(b_1^{p^{e_1}}) \neq D(b_2^{p^{e_2}})$ and $D(b_1^{p^{e_1+1}}) = D(b_2^{p^{e_2+1}})$. Since $D(b_1^{p^{e_1+1}}) = D(b_2^{p^{e_2+1}})$, inor $(D(b_1^{p^{e_1}})/K) =$ inor $(D(b_2^{p^{e_2}})/K)$, say j, and $j >$ inor $(D(b_1^{p^{e_1+1}})/K)$. Now $D(b_1^{p^{e_1}})/K$ and $D(b_2^{p^{e_2}})/K$ have minimal subfields with respect to having order of inseparability j. By assumption these subfields are equal, and hence are contained in $D(b_1^{p^{e_1}}) \cap D(b_2^{p^{e_2}}) = D(b_1^{p^{e_1+1}})$. But inor $(D(b_1^{p^{e_1+1}})/K) < j$, a contradiction.

An algebraic field extension L/K is called exceptional [5] if L is inseparable over K and $K^{p^{-\infty}} \cap L = K$.

THEOREM 3. *Assume L is algebraic over K with order of inseparability $n > 0$ and let S be the maximal separable extension of K in L. Then L/K has a unique subfield of inor $n - j$, $0 \leq j < n$, if and only if for any S_l, $K \subseteq S_l \subset S$, L is exceptional over S_l and insep$(L/K) = 1$.*

PROOF. If L/K has a unique subfield of inor $n - j$, $0 \leq j < n$, then L/K has a unique minimal subfield of inor $n - j$, $0 \leq j \leq n$. Thus by Theorem 2, insep $(L/K) = 1$.

Assume there exists S_1, $K \subset S_1 \subset S$ and L is not exceptional over S_1. Then $S^{p-1} \cap L \neq S_1$. Let $b \in (S_1^{p-1} \cap L) \setminus S_1$. Then $S_1(b)$ and $S(b)$ both have order of inseparability one over K. Conversely, suppose there exist L_1 and L_2 subfields of L/K both with order of inseparability $j > 0$ and $L_1 \neq L_2$. Let S_1 and S_2 be the maximal separable extensions of K in L_1 and L_2 respectively. If $S_1 \neq S_2$, then since L is not exceptional over either, we have a proper subfield of S over which L is not exceptional. If $S_1 = S_2$, then since $L_1 \neq L_2$, L_1L_2 must have inseparability at least 2 over K, and hence L has inseparability at least 2 over K.

THEOREM 4. *Assume L/K is not algebraic and has order of inseparability $n > 0$. Then L/K has a unique subfield of inor $n - j$, $0 \leq j < n$, if and only if $n = 1$ and L/K is irreducible.*

PROOF. Clearly if L/K is irreducible and $n = 1$, then L is the unique subfield of inor n. Conversely, assume L/K has a unique subfield of inor $n - j$, $0 \leq j < n$. Then since L^*, the irreducible form of L/K, has inor n, $L^* = L$, i.e. L is irreducible over K. By Theorem 2, insep $(L/K) = 1$. Thus $\text{inor}(K(L^p)/K) = n - 1$. If $n - 1 = 0$, we are finished. Assume $n - 1 > 0$. Since $L/K(L^p)$ is not simple (L/K is not algebraic), there are an infinite number of fields L_i, $L \supset L_i \supset K(L^p)$. Since $K(L^p)/K$ is inseparable, the fields L_i are all inseparable over K and certainly some two must have the same order of inseparability.

PROPOSITION 5. *If L/K has a unique maximal subfield L'_{n-j} of order of inseparability $n - j$, then L/K has a unique minimal subfield L^*_{n-j} of order of inseparability $n - j$.*

PROOF. L^*_{n-j} is the unique irreducible form of L'_{n-j}.

PROPOSITION 6. *Suppose L/K is algebraic. L/K has unique maximal subfields of order of inseparability $n - j$, $0 \leq j \leq n$ iff L/K has unique minimal subfields of order of inseparability $n - j$ for $0 \leq j \leq n$.*

PROOF. Suppose there exist unique minimal subfields. By Theorem 2, $L = S(b)$ where S is the maximal separable subfield of L/K. Now $S(b^{p^j})$ are the unique maximal subfields of order of inseparability $n - j$. The converse follows from Proposition 5.

THEOREM 7. *Suppose L/K is not algebraic. There exist unique maximal subfields of order of inseparability $n - j$, $0 \leq j < n$ if and only if $n = 1$.*

PROOF. Assume there exists unique maximal subfields. Then by Proposition 5 and Theorem 2, insep $(L/K) = 1$. Let $\{x_1, \ldots, x_{d-1}\}$ be part of a separating transcendence basis for a distinguished subfield of L/K, where d is the transcendence degree of L over K. Let $K_1 = K(x_1, \ldots, x_{d-1})$. Then $[L:K_1(L^p)] = p^2$ and L has transcendence degree 1 over K_1. Let $\{x, y\}$ be a relative p-basis of L over $K_1(L^p)$. By [8, Lemma 2, p. 113], $\{x, y\}$ contains a separating transcendence basis for a distinguished subfield of L/K_1. Say it is x. Then $x^{p^n} \notin K_1(L^{p^{n+1}})$. If $y^{p^n} \in K_1(L^{p^{n+1}})$, replace y with $y + x$. Thus we may assume either x or y is a separating transcendence basis for a distinguished

https://doi.org/10.4153/CMB-1986-031-5 Published online by Cambridge University Press

subfield. Thus $K(L^{p^n})(x_1, \ldots, x_d, x)$ and $K(L^{p^n})(x_1, \ldots, x_{d-1}, y)$ are distinct distinguished subfields of L/K. Assume $n > 1$. Then $K(L^{p^n})(x_1, \ldots, x_{d-1}, x, y^p)$ and $K(L^{p^n})(x_1, \ldots, x_{d-1}, y, x^p)$ are maximal of order of inseparability $n - 1$. By hypothesis these fields are equal. Thus $y \in K(L^{p^n})(x_1, \ldots, x_{d-1}, x)(y^p)$ and hence $y \in K(L^{p^n})(x_1, \ldots, x_{d-1}, x)$, a contradiction. Thus $n = 1$. Conversely if $n = 1$, L is the unique maximal subfield of order of inseparability $n - 0$.

COROLLARY 8. *Assume L is not algebraic over K. Then L/K is irreducible and has unique subfields maximal of order of inseparability* $n - j$, $0 \leq j < n$ *iff L/K has unique subfields of order of inseparability* $n - j$, $0 \leq j < n$.

We now want to use the results established regarding uniqueness of intermediate fields to resolve a conjecture in [3] and characterize those field extensions where the set of codegrees of maximal separable subfields consists of a single integer.

THEOREM 9. *Assume L is not algebraic over K. If every maximal separable subfield of L/K is distinguished, then L/K is of exponent one.*

PROOF. Assume L/K is of exponent greater than one and let D be a distinguished subfield. Then there is a b in L such that $D(b)$ is of exponent $n > 1$. Then $D(b^p)$ is of exponent $n - 1$ and the order of inseparability of $D(b^p)$ is also $n - 1$. From Theorem 1, the unique minimal subfield of $D(b)$ of inor $n - 1$ is contained in $K(D^p, b^p)$. Thus $D(b^p)$ has $K(D^p, b^p)$ as a form and $D(b^p)$ is purely inseparable over $K(D^p, b^p)$. Thus $D(b^p)$ is not separable algebraic over its irreducible form. But every maximal separable subfield of $D(b^p)$ is distinguished, since they are for L/K [3, Theorem 10, p. 189]. Thus $D(b^p)$ must be separable algebraic over its irreducible form [3, Corollary 7, p. 188], a contradiction. Thus L/K is of exponent one.

COROLLARY 10. *Let* $d > 0$ *be the transendence degree of L over K. Every maximal separable intermediate field of L/K is distinguished if and only if L/K is of exponent one and every set of d relatively p-independent elements of L/K is a separating transcendence basis for a distinguished subfield.*

PROOF. Apply Theorem 9 to [5, Theorem 8, p. 189].

The above results also give some information about the structure of field extensions where the codegrees of maximal separable subfields are bounded. Heerema [6] has shown that in transcendence degree one the set of codegrees of maximal separable subfields is bounded for L/K if and only if the algebraic closure of K in L is separable over K. Thus there clearly exist field extensions of any exponent which have the set of codegrees bounded. Let L/K have a bound on its set of codegrees of maximal separable subfields. Then [4, Theorem 10, p. 19] shows there is a subfield L_1 of L/K with L purely inseparable over L_1 and L_1 inseparable over K with $[L:L_1]$ as large as possible with respect to having these two properties. Let D_1 be distinguished for L_1 and let $M = K^{p^{-\infty}}(D_1) \cap L$. Then by a degree argument every maximal separable subfield of M is distinguished and hence M is of exponent one over K.

COROLLARY 11. *Assume insep* $(L/K) = 1$. *Let* L_1 *and* L_2 *be intermediate fields of* L/K. *If inor* $(L_1/K) =$ *inor* (L_2/K), *then inor* $(L_1 \cap L_2/K) =$ *inor* (L_1/K).

PROOF. If $\text{inor}(L_1/K) = \text{inor}(L_2/K)$, then the irreducible forms of L_1 and L_2 must both be the unique minimal intermediate field L^* of L/K of $\text{inor}(L_1/K)$. Thus $L_1 \supseteq L_1 \cap L_2 \supseteq L^*$ and since $\text{inor}(L_1/K) = \text{inor}(L^*/K)$, all three fields must have the same order of inseparability.

We note that the above corollary is not true without the assumption insep $(L/K) = 1$. Let $K = P(v_1^p, v_2^p, \mu_1^p, \mu_2^p)$, $L = K(x, \mu_1 x + v_1, \mu_2 x + v_2)$ where P is a perfect field of characteristic $p > 0$ and $\{x, \mu_1, v_1, \mu_2, v_2\}$ is algebraically independent over P. Let $L_1 = K(x, \mu_1 x + v_1)$ and $L_2 = K(x, \mu_2 x + v_2)$. Then $\text{inor}(L_1/K) = 1 = \text{inor}(L_2/K)$ and yet $L_1 \cap L_2 = K(x)$ which is separable over K.

PROPOSITION 12. *Let* L_1 *and* L_2 *be intermediate fields of* L/K. *If* $\textit{insep}(L_1/K) = \textit{insep}(L_2/K) = 1$ *and* $L_1 \cap L_2$ *is separable over* K, *then* $\textit{insep}(L_1L_2/K) \geq \textit{insep}(L_1/K) + \textit{insep}(L_2/K)$.

PROOF. Since $L_1L_2 \supseteq L_1 \supseteq K$, $\text{insep}(L_1L_2/K) \geq 1$. Suppose $\text{insep}(L_1L_2/K) = 1$. Let $\text{inor}(L_1/K) = a$ and $\text{inor}(L_2/K) = b$ where $b \geq a$. Then $\text{inor}(K(L_2^{p^{b-a}})/K) = a = \text{inor}(L_1/K)$. By Corollary 11, $\text{inor}(K(L_2^{p^{b-a}}) \cap L_1/K) = a$. But $K(L_2^{p^{b-a}}) \cap L_1 \subseteq L_2 \cap L_1$ and hence is separable over K, a contradiction. Thus $\text{insep}(L_1L_2/K) \geq 2 = \text{insep}(L_1/K) + \text{insep}(L_2/K)$.

The above proposition should be useful in studying the question of when the codegrees of maximal separable subfields are bounded. The case of insep $(L/K) = 1$ has been done [4, Theorem 7, p. 18]. The conjecture is that if every subfield over which L is not algebraic is separable over K, then the codegrees of the maximal separable subfields is bounded. Suppose L/K satisfies the above condition and has $\text{insep}(L/K) = 2$. Let L^2 be the unique minimal intermediate field with $\text{insep}(L^2/K) = 2$. Then $[L:L^2] = s < \infty$ by the assumption. In order to establish the conjecture it would suffice to show the set of degrees of L over subfields L_1 minimal with respect to having $\text{inor}(L_1/K) = 1 = \text{insep}(L_1/K)$ is bounded. Clearly L is finite dimensional over any such L_1. Moreover, if L_1 and L_2 are two distinct minimal subfields, then $L_1 \cap L_2$ is separable over K. Thus by Proposition 12, $\text{insep}(L_1L_2/K) = 2$ and hence $L_1L_2 \supset L^2$. Thus $\{[L:L_1L_2]\}$ is bounded by $[L:L^2]$.

REFERENCES

1. J. Deveney and J. Mordeson, *The Order of inseparability of fields*, Canad. J. of Math. **31** (1979), pp. 655–662.

2. ———, *Calculating invariants of inseparable field extensions*, Proc. Amer. Math. Soc. **81** (1981), pp. 373–376.

3. ———, *Distinguished subfields*, T.A.M.S. **260** (1980), pp. 185–193.

4. ———, *Maximal separable subfields of bounded codegree*, Proc. Amer. Math. Soc. **88** (1983), pp. 16–20.

5. R. Gilmer and W. Heinzer, *On the existence of exceptional field extensions*, Bull. Amer. Math. Soc. **74** (1968), pp. 545–547.

https://doi.org/10.4153/CMB-1986-031-5 Published online by Cambridge University Press

6. N. Heerema, *Maximal separable intermediate fields of large codegree,* Proc. Amer. Math. Soc. **82** (1981), pp. 351–354.

7. N. Heerema and J. Deveney, *Galois Theory for Fields K/k finitely generated,* T.A.M.S. **189** (1974), pp. 263–274.

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

VIRGINIA COMMONWEALTH UNIVERSITY
RICHMOND, VIRGINIA

CREIGHTON UNIVERSITY
OMAHA, NEBRASKA

https://doi.org/10.4153/CMB-1986-031-5 Published online by Cambridge University Press