PACIFIC JOURNAL OF MATHEMATICS
Vol. 128, No. 1, 1987

SPECIAL GENERATING SETS OF PURELY INSEPARABLE EXTENSION FIELDS OF UNBOUNDED EXPONENT

B. I. EKE

The present paper considers the problem of choosing a maximum subfield having a subbasis over K among subextensions of L/K, when L/K is purely inseparable but of unbounded exponent.

Throughout L will be a purely inseparable extension field of a field K of characteristic $p \neq 0$. For the case when L/K is of bounded exponent $e > 0$ Weisfeld [**6**, Theorem 3, p. 442] has shown that among the subfields of L having a subbasis over K there is a maximal subfield with respect to set inclusion. This theorem fails in the unbounded exponent case since such a maximal subfield would not always exist [**6**, p. 442]. An open problem was, therefore, posed in Weisfeld's paper regarding a necessary and sufficient condition for the theorem to hold for extensions L/K of unbounded exponent. The present paper seeks to provide a solution to this problem.

Let M be a given subset of L. The subset M will be said to be in *canonical form* when M is put in the form $M = A_1 \cup A_2 \cup \cdots$ where A_i consists of the elements of M having exponent i over K. M is called a *canonical generating set over* K if M is a minimal generating set for $K(M)$ and when $M = A_1 \cup A_2 \cup \cdots$ in canonical form, then the subsets M_i defined by $M_i = \bigcup_{j=i+1}^{\infty} A_j$, $i = 0, 1, \ldots$, $M_0 = M$, satisfy $M_i^{p^i}$ is a minimal generating set for $K(M^{p^i})/K$. The set M is called a *distinguished subset of* L/K if M is a canonical generating set over K and, for each nonnegative integer n, $K \cap L^{p^n} \subseteq K^p(A_n^p \cup A_{n+1}^p \cup \cdots)$ where $M = A_1 \cup A_2 \cup \cdots$ in canonical form. Finally, M is called a *subbasis over* K if for every finite subset $\{a_1, \ldots, a_r\}$ of M, $K(a_1, \ldots, a_r)$ is the tensor product of the simple extensions $K(a_i)$, $i = 1, \ldots, r$, and when this happens, the extension $K(M)$ is called an extension having a subbasis over K.

The main result is that if L/K is any purely inseparable extension, then L/K has a maximal subfield J having a subbasis over K if and only if L/K has a distinguished subset M.

LEMMA 1. *If L/K has a subbasis, then every subbasis for L/K is distinguished.*

Proof. Let L/K have a subbasis $B = B_1 \cup B_2 \cup \cdots$ in canonical form. Let u be any element of L with exponent n over K. Then $u^{p^{n-1}} \in K(B^{p^{n-1}}) = K(\bigcup_{i=n}^{\infty} B_i^{p^{n-1}})$ which shows that the exponent of u over $K(\bigcup_{i=n}^{\infty} B_i)$ is less than n. Hence B is distinguished.

LEMMA 2. *If the subset M of L is a canonical generating set over K, then M is a subbasis over K.*

Proof. Suppose M is a canonical generating set over K but M is not a subbasis over K. Let $M = A_1 \cup A_2 \cup \cdots$ in canonical form and let e be the smallest positive integer such that there exists an element $b \in A_e$ for which $b^{p^{e-1}} \in K(M - b)$. Clearly $e \neq 1$ otherwise we contradict the minimality of M over K. There exists a smallest positive integer t such that

$$b^{p^{e-1}} \in K(M_{t-1} - b) \tag{1}$$

where $M_{t-1} = \bigcup_{j=t}^{\infty} A_j$. Also there exists an element $a \in A_t$ such that $b^{p^{e-1}} \in K(M_{t-1} - b)$ but

$$b^{p^{e-1}} \notin K(M_{t-1} - \{a, b\}). \tag{2}$$

Let s be the highest integer such that

$$b^{p^{e-1}} \in K\left(M_{t-1} - \{a, b\}, a^{p^s}\right). \tag{3}$$

Then $a^{p^s} \in K(M_{t-1} - \{a, b\}, a^{p^{s+1}}, b^{p^{e-1}})$. Consequently a^{p^s} is separable and purely inseparable over $K(M_{t-1} - \{a, b\}, b^{p^{e-1}})$ which says that

$$a^{p^s} \in K\left(M_{t-1} - \{a, b\}, b^{p^{e-1}}\right). \tag{4}$$

In expression (1) above it must be the case that $e > t$ and in (4) it is the case that $s \geq t$ both because of [3, Cor. 1.31, p. 28]. But if $s > t$, then in expression (3) we have $K(M_{t-1} - \{a, b\}, a^{p^s}) = K(M_{t-1} - \{a, b\})$ so that $b^{p^{e-1}} \in K(M_{t-1} - \{a, b\})$ contradicting the expression (2). Therefore $s = t$. So, we have $s = t < e$. But then (4) implies that $a^{p^t} \in K(M_{t-1} - a) \subseteq K(M - a)$ where $t < e$ contradicting the minimality of e for this purpose. This contradiction proves the assertion.

THEOREM 3 (*Main result*). *The extension L/K has a maximal subfield J having a subbasis over K if and only if L/K has a distinguished subset M.*

Proof. Suppose L/K has a distinguished subset M. By Lemma 2 M is a subbasis over K. Moreover, M is distinguished in L/K implies that any element of L having exponent r over K must have exponent less than r over $K(\bigcup_{i=r}^{\infty} A_i)$ where $M = A_1 \cup A_2 \cup \cdots$ in canonical form.

Denote $K(M)$ by J. Let F be any modular subfield of L over K containing J and suppose $u \in F - J$ has exponent r over k. Then one can write

$$u^{p^s} = a_1 u_1^{p^s} + \cdots + a_n u_n^{p^s} \tag{5}$$

where $a_1, \ldots, a_n \in K$, $u_1, \ldots, u_n \in J$, $s < r$, and n is chosen minimal. Using arguments similar to those of Weisfeld in [**6**, Theorem 4, p. 442] and the concept of p-freedom as defined in that paper one can get a maximal p-free subset $\{a_1, \ldots, a_k\}$ of $\{a_1, \ldots, a_n\}$ relative to J^p and a maximal p-free subset $\{a_1, \ldots, a_j\}$ of $\{a_1, \ldots, a_k\}$ relative to F^p where $j < k$. Consequently we have a relation

$$a_{j+1} = \sum \Big\{ y^p_{i_1 \cdots i_j} a_1^{i_1} \cdots a_j^{i_j} \,|\, y_{i_1 \cdots i_j} \in F, \qquad 0 \le i_m < p, m = 1, \ldots, j \Big\}. \tag{6}$$

Let B be the set consisting of the coefficients $y_{i_1 \cdots i_j}$. Let F_1 be the modular closure of $K(B)$ as defined in [**4**, p. 408], and let $F_2 = F \cap F_1$. Then F_2 must have a subbasis over K. Therefore by [**4**, Theorem 1, p. 403] there exists a higher derivation D of F_2 relative to which K is the field of constants. Using this in (6), one can violate the p-freedom of $\{a_1, \ldots, a_j\}$ relative to F^p. Therefore $J = F$.

Conversely let N be a maximal subfield of L/K having a subbasis over K and let $M = A_1 \cup A_2 \cup \cdots$ (in canonical form) be any subbasis for N/K. As usual, for $i = 0, 1, \ldots$ we let $M_i = \cup_{j=i+1}^{\infty} A_j$. We must show that M is a distinguished subset of L/K. Clearly M is a canonical generating set over K. We shall prove, by induction, the statement $P(n)$: If u is any element of L having exponent n over K, then the exponent of u over $K(M_{n-1})$ is less than n. Now $P(1)$ is trivial. Hence assume $P(n-1)$ holds and suppose an element $u \in L$ has exponent n over K and same exponent over $K(M_{n-1})$. Let $A = \{u\} \cup M_{n-1}$. Then A is a subbasis over K. Let $T^{(n-1)} = \{B \subseteq A_{n-1} \cup A \,|\, B \supseteq A$ and B is a subbasis over $K\}$. Clearly A is in $T^{(n-1)}$. So, $T^{(n-1)} \neq \varnothing$. Let $M^{(n-1)}$ be a maximal element (with respect to set inclusion) of the set $T^{(n-1)}$. We now proceed to let $M^{(n-2)}$ be a maximal element of

$$T^{(n-2)} = \Big\{ B \subseteq A_{n-2} \cup M^{(n-1)} \,|\, B \supseteq M^{(n-1)} \text{ and } B \text{ is a subbasis over } K \Big\}.$$

In general, for $1 \le k < n-1$, we let $M^{(k)}$ be a maximal element of

$$T^{(k)} = \Big\{ B \subseteq A_k \cup M^{(k+1)} \,|\, B \supseteq M^{(k+1)} \text{ and } B \text{ is a subbasis over } K \Big\}.$$

It is our ambition to show that $K(M^{(1)}) = N$.

Let v be an element of M and suppose $v \in A_r$ $(1 \leq r < n)$. If $v \notin K(M^{(r)})$, then it must be the case that v has an exponent $s < r$ over $K(M^{(r)})$ by the definition of $M^{(r)}$. Consequently we can write

$$(7) \qquad v^{p^s} = c_1 v_1^{p^s} + \cdots + c_m v_m^{p^s}$$

where $c_1, \ldots, c_m \in K$, $v_1, \ldots, v_m \in K(M^{(r)})$, $s < r$, and m is minimal. This relation now allows us to apply an argument similar to that in the first part of this proof between $K(M^{(r)})$ as J and the modular closure of $K(M^{(r)}, v)$ as F (F and J in this case both contained in their composite $F(J)$ as L). The contradiction which will then arise as in the first part shows that $v \in K(M^{(r)})$. Consequently, $K(M^{(1)})$ contains $K(M) = N$, and, by the maximality of N, $K(M^{(1)}) = N$. This shows that $u \in N$. By Lemma 1 the exponent of u over $K(M_{n-1})$ is less than n. This shows that M is a distinguished subset of L/K.

COROLLARY 4. *Let J be a subfield of L/K having a subbasis over K. Then J is a maximal subfield of L/K having a subbasis over K if and only if $J \cap K^{p^{-i}}$ is a maximal subfield of $L \cap K^{p^{-i}}$ having a subbasis over K, $i = 1, \ldots$.*

Proof. Let J be a maximal subfield of L/K having a subbasis over K, and let $B = B_1 \cup B_2 \cup \cdots$ (in canonical form) be a subbasis for J/K. Fix the integer $i \geq 1$ and let $B_{(i)} = \{a^{p^{s-i}} \mid a \in B_s \text{ and } s > i\}$. Then $W = B_1 \cup \cdots \cup B_i \cup B_{(i)}$ is a subset of $J \cap K^{p^{-i}}$ which is also a subbasis over K. We shall show that W is a distinguished subset of $L \cap K^{p^{-i}}/K$. Let $u \in L \cap K^{p^{-i}}$ have exponent $e \leq i$ over K. We note that by Theorem 3 the subbasis B is a distinguished subset of L/K. Let

$$u^{p^{e-1}} = \sum c_{i_1 \cdots i_n} u_1^{i_1} \cdots u_n^{i_n}$$

where $0 \leq i_k < p^{e_k}$, $e_k =$ exponent of u_k over K, and $u_k \in \bigcup_{j=e}^{\infty} B_j$. Since $u^{p^e} \in K$ it must be the case that $i_k \geq p^{e_k - 1}$, and since $e_k - i \leq e_k - 1$, it must be the case that $p^{e_k - i} \leq p^{e_k - 1} \leq i_k < p^{e_k}$ whenever $e_k > i$. Hence $u_k^{i_k} \in K(B_{(i)})$ when $e_k > i$ and, of course, $u_k \in B_{e_k}$ if $e_k \leq i$. This shows that if $W = \tilde{B}_1 \cup \cdots \cup \tilde{B}_i$ in canonical form, then $u^{p^{e-1}} \in K(\tilde{B}_e \cup \cdots \cup \tilde{B}_i)$. Consequently W is distinguished in $L \cap K^{p^{-i}}/K$ and, by Theorem 3, $K(W)$ is a maximal subfield of $L \cap K^{p^{-i}}$ having a subbasis over K. Now it is obvious that $K(W) \subseteq J \cap K^{p^{-i}}$. Now let $x \in J \cap K^{p^{-i}}$. Then $x = \sum a_{i_1 \cdots i_m} v_1^{l_1} \cdots v_m^{l_m}$ where $0 \leq l_j < p^{e_j}$, $e_j =$ exponent of v_j over K, and $v_j \in B$, $1 \leq j \leq m$. Since $x^{p^i} \in K$ we must have, for each j, $l_j \geq p^{e_j - i}$ and hence $v_j^{l_j} \in K(W)$. This shows $J \cap K^{p^{-i}} \subseteq K(W)$, and equality follows.

Conversely suppose $J \cap K^{p^{-i}}$ is a maximal subfield of $L \cap K^{p^{-i}}$ having a subbasis over K. Let T be any subfield of L/K having a subbasis over K and suppose $T \supseteq J$. Then for each i $T \cap K^{p^{-i}} \supseteq J \cap K^{p^{-i}}$. If $T \cap K^{p^{-i}} \neq J \cap K^{p^{-i}}$ we contradict the maximality of $J \cap K^{p^{-i}}$ as stated earlier since $T \cap K^{p^{-i}}$ is also a subfield of $L \cap K^{p^{-i}}$ having a subbasis over K. Consequently $J = T$. □

It was shown in Lemma 1 that if L/K has a subbasis over K, then that subbasis must be a distinguished subset of L/K. It is not true, however, that an extension L/K must be modular in order to have a distinguished subset as the following example shows.

EXAMPLE. Let $K = Z_p(x_1, x_2, \dots)$ where the x_i are algebraically independent indeterminates over Z_p. Let

$$L = K\left(x_1^{p^{-1}}x_3^{p^{-2}} + x_2^{p^{-1}}, x_3^{p^{-2}}, x_3^{p^{-3}}, x_4^{p^{-3}}, x_5^{p^{-4}}, \dots\right).$$

First, we show that L/K is not modular. We note that

$$\begin{aligned} L^p &= K^p\left(x_1 x_3^{p^{-1}} + x_2, x_3^{p^{-1}}, x_4^{p^{-2}}, x_5^{p^{-3}}, \dots\right) \\ &= Z_p\left(x_1^p, x_2^p, x_1 x_3^{p^{-1}} + x_2, x_3^{p^{-1}}, x_4^{p^{-2}}, x_5^{p^{-3}}, \dots\right). \end{aligned}$$

$$K \cap L^p = Z_p(x_1^p, x_2^p, x_3, x_4, \dots) = K^p(x_3, x_4, x_5, \dots).$$

Now the set $\{1, x_3^{p^{-1}}, x_1 x_3^{p^{-1}} + x_2\}$ is a subset of L^p which is linearly independent over $K \cap L^p$. For suppose $c_0 + c_1 x_3^{p^{-1}} + c_2 x_1 x_3^{p^{-1}} + c_2 x_2 = 0$, $c_i \in K \cap L^p$ and not both c_1 and c_2 are zero. We have

$$c_0^p + c_1^p x_3 + c_2^p x_1^p x_3 + c_2^p x_2^p = 0$$

or

$$(c_1^p + c_2^p x_1^p) x_3 = -(c_2^p x_2^p + c_0^p).$$

If $c_1^p + c_2^p x_1^p \neq 0$, then

$$x_3 = \frac{-(c_2^p x_2^p + c_0^p)}{c_1^p + c_2^p x_1^p} \in K^p = Z_p(x_1^p, x_2^p, x_3^p, \dots).$$

There exists a finite n such that

$$x_3 \in Z_p(x_1^p, \dots, x_n^p) \subseteq Z_p(x_1, x_2, x_3^p, x_4, \dots, x_n).$$

Consequently x_3 is separable algebraic over $Z_p(x_1, x_2, x_4, \dots, x_n)$ violating the algebraic independence of the x_i over Z_p. Therefore $c_1^p + c_2^p x_1^p = 0$. This again leads to a contradiction unless $c_1 = c_2 = 0$. Consequently we must have $c_0 = c_1 = c_2 = 0$ as required. On the other hand, it is obvious that the given set $\{1, x_3^{p^{-1}}, x_1 x_3^{p^{-1}} + x_2\}$ is linearly dependent over K. This shows that L/K is not modular.

Now the set $S = \{x_3^{p^{-2}}, x_4^{p^{-3}}, x_5^{p^{-4}}, \dots\}$ is a subbasis over K. Besides, S is distinguished in L/K.

DEFINITION. An extension field F/K is called Galois if it is modular and $\bigcap_{i=1}^{\infty} K(F^{p^i}) = K$.

LEMMA 5. *If a purely inseparable extension F/K has a subbasis then it is Calois.*

Proof. Let $M = B_1 \cup B_2 \cup \cdots$ (in canonical form) be a subbasis for F/K. Let $x \in \bigcap_{i=1}^{\infty} K(F^{p^i})$. Then $x = g(b_1^{p^1}, \dots, b_n^{p^i})$ for some $b_1, \dots, b_n \in M_i = \bigcup_{j=i+1}^{\infty} B_j$ and n is chosen minimum. Since $M = \bigcup_{j=1}^{\infty} B_j$ is part of a linear basis for F/K the set $\{b_1, \dots, b_n\}$ must be contained in every M_i otherwise we contradict the unique representation of x relative to the said linear basis. This shows that

$$x \in K\left(\bigcap_{i=1}^{\infty} F^{p^i}\right) = K\left(\bigcap_{i=1}^{\infty} M_i^{p^i}\right) = K$$

since $\bigcap_{i=1}^{\infty} M_i = \varnothing$. This shows $\bigcap_{i=1}^{\infty} K(F^{p^i}) = K$ and F/K is Galois. □

THEOREM 6. *The purely inseparable extension L/K has a maximal subfield F having a subbasis over K, if and only if there exist in L a maximal modular subfield F which is Galois over K.*

Proof. Suppose F is a maximal modular subfield of L/K which is also Galois over K. Let $A_1, A_2, \dots$ be subsets of F constructed in the manner of [**2**, Theorem 11, p. 339]. Let

$$Q = \bigcap_{i=1}^{\infty} K(F^{p^i}) \otimes K(A_1 \cup A_2 \cup \cdots)$$

as defined in [**2**, Theorem 13]. Then F is relatively perfect over Q and has a subbasis over Q. By Lemma 5, $F = \bigcap_{i=1}^{\infty} Q(F^{p^i}) = Q$. From the fact that F/K is also Galois we have

$$F = Q = \bigcap_{i=1}^{\infty} K(F^{p^i}) \otimes K(A_1 \cup A_2 \cup \cdots) = K(A_1 \cup A_2 \cup \cdots).$$

Consequently F has a subbasis over K. The converse is immediate.

References

[1] G. F. Haddix, J. N. Mordeson, and B. Vinograde, *On purely inseparable extensions of unbounded exponent*, Canad. J. Math., **XXI** (1969), 1526–1532.

[2] L. A. Kime, *Purely inseparable, modular extensions of unbounded exponent*, Trans. Amer. Math. Soc., **176** (1973), 335–349.

[3] J. N. Mordeson and B. Vinograde, *Structure of Arbitrary Purely Inseparable Extension Fields*, Lecture Notes in Math. Vol. 173, Springer-Verlag, New York (1970).

[4] M. Sweedler, *Structure of inseparable extensions*, Ann. of Math., **87** (1968), 401–410.

[5] _____, *Correction to "Structure of inseparable extensions"*, Ann. of Math., **89** (1969), 206–207.

[6] M. Weisfeld, *Purely inseparable extensions and higher derivations*, Trans. Amer. Math. Soc., **116** (1965), 435–449.

Received January 24, 1985.

INSTITUE OF MANAGEMENT AND TECHNOLOGY
ENUGU, NIGERIA