ON PURELY INSEPARABLE EXTENSIONS OF UNBOUNDED EXPONENT

G. F. HADDIX, J. N. MORDESON, AND B. VINOGRADE

Let L/K be a field extension of characteristic $p \neq 0$. If L/K is purely inseparable and of bounded exponent, then the property that L has a sub-basis over K (**11**, p. 436) is of significance in the theory of higher derivations (**11**) and in the theory of Hopf algebras (**9**; **10**). In this case, where L/K is of bounded exponent, it has been shown independently in (**1**; **9**; **5**) that L/K having a sub-basis is equivalent to the property that L/K is modular (**9**, p. 401). Our aim in this paper is to extend and apply these properties for L/K purely inseparable and of unbounded exponent.

In Theorem 1, we give several conditions on a p-basis of L which are equivalent to the property that L/K has a sub-basis. In Theorem 2, we give a sequence of implications starting with L/K has a sub-basis. We apply both theorems to the theory of coefficient fields in complete local rings (see Theorem 4 and the Remark following it) and to the following problem: *If every relative p-basis for a purely inseparable extension L/K is a minimal generating set, is L/K necessarily of bounded exponent?*† The converse is known to be true (**8**). Finally, in Theorem 3, we give a partial solution to an open problem posed in (**11**, p. 439) and also show that (**11**, p. 442, Theorem 3) is now directly amenable to Zorn's lemma by using the equivalence mentioned in the first paragraph above; see (**11**, p. 439, § IV).

If B is a p-basis for L, then C always denotes

$$\{b^{p^i} \mid b \in B,\ i \text{ is the exponent of } b \text{ over } K \text{ if } b \text{ is purely inseparable over } K \text{ and } i = 0 \text{ otherwise}\}.$$

1. Modular extensions.

L/K always denotes a field extension of characteristic $p \neq 0$.

THEOREM 1. *Let L/K be a purely inseparable field extension. Then the following conditions are equivalent on a p-basis B of L:*

(0) *$B - K$ (set difference) is a sub-basis for L/K;*

(1) *$K = K^p(C)$;*

Received September 10, 1968.

†*Added in proof.* It has recently been shown that the answer to this question is no (J. N. Mordeson and B. Vinograde, *Note on relative p-bases of purely inseparable extensions*, Proc. Amer. Math. Soc. *22* (1969), 587–590).

(2) *C is a p-basis of K;*
(3) *$L = K(B)$ and $K \subseteq L^{p^i}(C)$, $i = 1, 2, \ldots$.*

Proof. (0) implies (1): Let $\{b_1, \ldots, b_r\}$ be any finite subset of $B - K$ and let e_i be the exponent of b_i over K, $i = 1, \ldots, r$. Then, since

$$K^p(C) \subseteq K,\ p^{e_1} \ldots p^{e_r} \geqq [K^p(C)(b_1, \ldots, b_r) \colon K^p(C)]$$
$$\geqq [K(b_1, \ldots, b_r) \colon K] = p^{e_1} \ldots p^{e_r}.$$

Therefore, K and $K^p(B)$ are linearly disjoint over $K^p(C)$, whence

$$K \cap K^p(B) = K^p(C).$$

Since $L = K(B)$, $K \subseteq L = L^p(B) = K^p(B)$. Thus, $K = K^p(C)$.

(1) implies (2): Since $K = K^p(C)$, there exists a subset C' of C such that C' is a p-basis of K. Let $B' = \{b \mid b \in B,\ b^{p^i} \in C'\}$. Then $(K(B'))^p(B') = K^p(B') = K^p(C')(B') = K(B')$. Hence, B' is a p-basis for $K(B')$. Thus, L over $K(B')$ preserves p-independence, whence $L = K(B')$ by (**2**, p. 378, Theorem 8) and the pure inseparability of L/K. Thus, $B = B'$ whence $C = C'$.

(2) implies (3): Since C is a p-basis of K, we have $K = K^{p^i}(C)$, $i = 1, 2, \ldots$. Therefore, $K \subseteq L^{p^i}(C)$, $i = 1, 2, \ldots$. Now $K = K^p(C)$ implies $K \subseteq K^p(B)$. Hence, $(K(B))^p(B) = K(B)$ and thus B is a p-basis of $K(B)$. Thus, L over $K(B)$ preserves p-independence from which it follows that $L = K(B)$.

(3) implies (0): Let $B_1 \cup \ldots \cup B_r$ be any finite subset of $B - K$ where every element of B_i has exponent i over K, $i = 1, \ldots, r$. Suppose that B_i has $s_i \geqq 0$ elements ($i = 1, \ldots, r$). Since C consists of p^eth powers of elements of the p-basis B of L, it follows that:

$$(*) \qquad [L^{p^{i+1}}(C)(B_{i+1}{}^{p^i}, \ldots, B_r{}^{p^i}) \colon L^{p^{i+1}}(C)] = p^{s_{i+1}} \ldots p^{s_r}.$$

Now

$$[K(B_1, \ldots, B_r) \colon K] = [K(B_1, \ldots, B_r) \colon K(B_1{}^p, \ldots, B_r{}^p)]$$
$$\cdot [K(B_1{}^p, \ldots, B_r{}^p) \colon K(B_2{}^{p^2}, \ldots, B_r{}^{p^2})] \cdot \ldots \cdot [K(B_r{}^{p^{r-1}}) \colon K].$$

Since

$$L^{p^{i+1}}(C) \supseteq K(B_{i+1}{}^{p^{i+1}}, \ldots, B_r{}^{p^{i+1}}),$$

we have

$$[K(B_{i+1}{}^{p^i}, \ldots, B_r{}^{p^i}) \colon K(B_{i+1}{}^{p^{i+1}}, \ldots, B_r{}^{p^{i+1}})] = p^{s_{i+1}} \ldots p^{s_r},$$

otherwise we contradict equation $(*)$. Thus,

$$[K(B_1, \ldots, B_r) \colon K] = p^{s_1} \ldots p^{s_r} p^{s_2} \ldots p^{s_r} \ldots p^{s_r} = p^{s_1} p^{2s_2} \ldots p^{rs_r}.$$

Hence, $B - K$ is a sub-basis for L/K.

In the following theorem, (3) shows that the simplest kind of purely inseparable extension of unbounded exponent may have a relative p-basis which is not a minimal generating set.

THEOREM 2. *Let L/K be an arbitrary field extension of characteristic $p \neq 0$. Then* (0) *implies* (1) *which implies* (2) *which implies* (3), *where:*

(0) *L/K is purely inseparable and has a sub-basis;*

(1) *L/K is modular; that is, L^{p^i} and K are linearly disjoint* ($i = 1, 2, \ldots$);

(2) *There exists a p-basis B of L such that $K \subseteq L^{p^i}(C)$* ($i = 1, 2, \ldots$).

(3) *There exists a relative p-basis M of L/K such that $L \supset K(M)$* (*strict inclusion*), *when L/K is purely inseparable and of unbounded exponent.*

Proof. (0) implies (1): Let M be a sub-basis for L/K. Then for all $i = 1, 2, \ldots, M = M_i' \cup M_i$, where every element of M_i' has exponent at most i over K and every element of M_i has exponent greater than i over K. Since $L = K(M_i', M_i)$,

$$L^{p^i} = K^{p^i}(M_i'^{p^i}, M_i^{p^i}) = (L^{p^i} \cap K)(M_i^{p^i}), \qquad i = 1, 2, \ldots .$$

For any finite subset $\{b_1, \ldots, b_r\} \subseteq M_i$, let e_j be the exponent of b_j over K, $j = 1, \ldots, r$. Then

$$p^{e_1 - i} \ldots p^{e_r - i} \geqq [(L^{p^i} \cap K)(b_1^{p^i}, \ldots, b_r^{p^i}) : L^{p^i} \cap K]$$
$$\geqq [K(b_1^{p^i}, \ldots, b_r^{p^i}) : K] = p^{e_1 - i} \ldots p^{e_r - i}.$$

Thus, L^{p^i} and K are linearly disjoint over $L^{p^i} \cap K$, $i = 1, 2, \ldots$. That is, L/K is modular.

(1) implies (2): Since L^p and K are linearly disjoint over $L^p \cap K$, there exists a set C_0 in K such that $K = (L^p \cap K)(C_0)$ and C_0 is p-independent in L. Suppose that there exist sets C_j, $j = 0, \ldots, i-1$, such that $C_j \subseteq L^{p^j} \cap K$, $L^{p^{i-1}} \cap K = (L^{p^i} \cap K)(C_0^{p^{i-1}}, C_1^{p^{i-2}}, \ldots, C_{i-1})$ and

$$C_0^{p^{i-1}} \cup C_1^{p^{i-2}} \cup \ldots \cup C_{i-1}$$

is p-independent in $L^{p^{i-1}}$. Then $C_0^{p^i} \cup C_1^{p^{i-1}} \cup \ldots \cup C_{i-1}^p \subseteq L^{p^i} \cap K$ and is p-independent in L^{p^i}. Since $L^{p^{i+1}}$ and K are linearly disjoint over $L^{p^{i+1}} \cap K$, $L^{p^{i+1}}$ and $L^{p^i} \cap K$ are linearly disjoint over $L^{p^{i+1}} \cap K$. Thus, there exists $C_i \subseteq L^{p^i} \cap K$ such that

$$L^{p^i} \cap K = (L^{p^{i+1}} \cap K)(C_0^{p^i}, C_1^{p^{i-1}}, \ldots, C_i)$$

and $C_0^{p^i} \cup C_1^{p^{i-1}} \cup \ldots \cup C_i$ is p-independent in L^{p^i}. Hence, there exists sets C_i ($i = 0, 1, \ldots$) such that

$$C_i \subseteq L^{p^i} \cap K, \qquad L^{p^i} \cap K = (L^{p^{i+1}} \cap K)(C_0^{p^i}, C_1^{p^{i-1}}, \ldots, C_i)$$

and $C_0^{p^i} \cup C_1^{p^{i-1}} \cup \ldots \cup C_i$ is p-independent in L^{p^i}, $i = 0, 1, \ldots$. Thus, $K = (L^{p^i} \cap K)(C_0, \ldots, C_{i-1})$, whence $K = (L^{p^i} \cap K)(C_0, C_1, \ldots)$, $i = 1, 2, \ldots$. Furthermore, $\bigcup_{i=0}^{\infty} C_i^{1/p^i}$ is p-independent in L. Augment $\bigcup_{i=0}^{\infty} C_i^{1/p^i}$ to a p-basis B of L. Then for $C = \{b^{p^i} \mid b \in B, i$ is the exponent of b over K if b is purely inseparable over K and $i = 0$ otherwise$\}$,

$$(**) \qquad K = (L^{p^i} \cap K)(C^*), \qquad i = 1, 2, \ldots, \quad C^* = C \cap K,$$

since $C^* \supseteq \bigcup_{i=0}^{\infty} C_i$. Thus, $K \subseteq L^{p^i}(C)$, $i = 1, 2, \ldots$.

(2) implies (3): Let B be a p-basis of L satisfying (2), where L/K is purely inseparable and of unbounded exponent. Suppose that $L \supset K(B)$. Then since $L = K(L^p)(B)$, there exists a relative p-basis M of L/K such that $M \subseteq B$. Hence, $K(M) \subseteq K(B) \subset L$. Suppose that $L = K(B)$. Then by Theorem 1, $M = B - K$ is a sub-basis for L/K. Hence, there exists $m_1, m_2, \ldots \in M$ such that m_i has exponent e_i $(e_i < e_{i+1})$ over $K' = K(M')$, where $M' = M - \{m_1, m_2, \ldots\}$, $i = 1, 2, \ldots$. Now

$$M^* = M' \cup M'', \qquad M'' = \{m_i m_{i+1}{}^{p^{e_{i+1}-e_i}} \mid i = 1, 2, \ldots\},$$

is a relative p-basis for L/K and we show $L \supset K(M^*)$ by showing $L \supset K'(M'')$. If $L = K'(M'')$, then there exists a positive integer r such that

$$m_1 \in L_r = K'(m_1 m_2{}^{p^{e_2-e_1}}, \ldots, m_r m_{r+1}{}^{p^{e_{r+1}-e_r}}).$$

Hence, $m_{i+1}{}^{p^{e_{i+1}-e_1}} \in L_r$, $i = 0, \ldots, r$. Let

$$L_{r+1} = K'(m_1, m_2{}^{p^{e_2-e_1}}, \ldots, m_{r+1}{}^{p^{e_{r+1}-e_1}}).$$

Then $L_{r+1} \subseteq L_r$ and

$$\{m_1 m_2{}^{p^{e_2-e_1}}, \ldots, m_r m_{r+1}{}^{p^{e_{r+1}-e_r}}\} \quad \text{and} \quad \{m_1, m_2{}^{p^{e_2-e_1}}, \ldots, m_{r+1}{}^{p^{e_{r+1}-e_1}}\}$$

are sub-bases (whence relative p-bases) for L_r/K' and L_{r+1}/K', respectively. Thus, the intermediate field L_{r+1} of L_r/K' has $r + 1$ minimal generators over K' while L_r has r. This contradicts (**7**, p. 103, *Satz* 28). However, this contradiction can also be shown as follows: There exists $G \subseteq K'$ such that $G \cup \{m_1 m_2{}^{p^{e_2-e_1}}, \ldots, m_r m_{r+1}{}^{p^{e_{r+1}-e_r}}\}$ is a p-basis for L_r. By Theorem 1, $G \cup \{m_1{}^{p^{e_1}} m_2{}^{p^{e_2}}, \ldots, m_r{}^{p^{e_r}} m_{r+1}{}^{p^{e_{r+1}}}\}$ is a p-basis for K'. Since $L_{r+1} \subseteq L_r$, G is p-independent in L_{r+1}. Since $G \subseteq K'$ and $\{m_1, m_2{}^{p^{e_2-e_1}}, \ldots, m_{r+1}{}^{p^{e_{r+1}-e_1}}\}$ is a relative p-basis of L_{r+1}/K', it follows that $G \cup \{m_1, m_2{}^{p^{e_2-e_1}}, \ldots, m_{r+1}{}^{p^{e_{r+1}-e_1}}\}$ is p-independent in L_{r+1} and that $G \cup \{m_1{}^{p^{e_1}}, m_2{}^{p^{e_2}}, \ldots, m_{r+1}{}^{p^{e_{r+1}}}\}$ is p-independent in K' by Theorem 1. Thus, $p^r = [K' : K'^p(G)] \geqq p^{r+1}$ which is impossible. Hence, $L \supset K(M^*)$.

Example. Let L/K be a purely inseparable extension. If L/K is modular, then L/K does not necessarily have a sub-basis. Let L be perfect. Then L/K is clearly modular since $L = L^p$. Since $L = K(L^p)$, every relative p-basis of L/K is empty. Hence, L/K does not have a minimal generating set, let alone a sub-basis.

THEOREM 3. *Let L/K be a field extension of characteristic $p \neq 0$. Then* (1) *there exists a maximal intermediate field K^* of L/K such that K^*/K is modular and* (2) *there exists a minimal intermediate field K^* of L/K such that L/K^* is modular.*

Proof. (1) Let $S = \{K_j \mid K_j$ is an intermediate field of L/K and K_j/K is modular$\}$. Then S is partially ordered under set inclusion. Now $K \in S$ whence $S \neq \emptyset$. Let S' be any simply ordered subset of S. Let $K^* = \bigcup_{K_j \in S'} K_j$. Let i be a fixed but arbitrary positive integer. Let $X \subseteq K$ be a linear basis of K

over $K^{*p^i} \cap K$. Suppose that $0 = \sum_{t=1}^{r} k_t^{*p^i} x_t$, where $x_1, \ldots, x_r \in X$ and $k_1^*, \ldots, k_r^* \in K^*$. Now there exists $K_j \in S'$ such that $k_1^*, \ldots, k_r^* \in K_j$. Since X is linearly independent over $K^{*p^i} \cap K$, X is linearly independent over the smaller field $K_j^{p^i} \cap K$. Since $K_j \in S$, X is linearly independent over $K_j^{p^i}$, whence $k_t^{*p^i} = 0$ $(t = 1, \ldots, r)$. Thus, K^{*p^i} and K are linearly disjoint. Hence, $K^* \in S$ whence S has a maximal element.

(2) Let $S = \{K_j \mid K_j$ is an intermediate field of L/K and L/K_j is modular$\}$. Then S is partially ordered under set containment. Now $L \in S$ whence $S \neq \emptyset$. Let S' be any simply ordered subset of S. Let $K^* = \bigcap_{K_j \in S'} K_j$. Let i be a fixed but arbitrary positive integer. Let $X \subseteq L^{p^i}$ be a linear basis of L^{p^i} over $L^{p^i} \cap K^*$. Suppose that $0 = \sum_{t=1}^{r} k_t^* x_t$, where $k_t^* \in K^*$ and $x_t \in X$, $t = 1, \ldots, r$. Clearly x_1 is linearly independent over $L^{p^i} \cap K_j$ for any $K_j \in S'$. Make the induction hypothesis that $\{x_1, \ldots, x_m\}$, $1 \leqq m < r$, is linearly independent over $L^{p^i} \cap K_{j_0}$ for some $K_{j_0} \in S'$. Let $S_0' = \{K_j \mid K_j \in S', K_j \subseteq K_{j_0}\}$. Then $\{x_1, \ldots, x_m\}$ is clearly linearly independent over $L^{p^i} \cap K_j$ for all $K_j \in S_0'$. If x_{m+1} is in the linear span of $\{x_1, \ldots, x_m\}$ over $L^{p^i} \cap K_j$ for all $K_j \in S_0'$, then x_{m+1} is a linear combination of $x_1, \ldots, x_m$ over $L^{p^i} \cap K_j$ for all $K_j \in S_0'$. Equating these linear combinations, we find that the coefficients all lie in $\bigcap_{K_j \in S_0'} (L^{p^i} \cap K_j) = L^{p^i} \cap K^*$. However, this contradicts the linear independence of $\{x_1, \ldots, x_r\}$ over $L^{p^i} \cap K^*$. Hence, there exists $K_{j_1} \in S_0' \subseteq S'$ such that $\{x_1, \ldots, x_{m+1}\}$ is linearly independent over $L^{p^i} \cap K_{j_1}$. Therefore, by induction, there exists $K_j \in S'$ such that $\{x_1, \ldots, x_r\}$ is linearly independent over $L^{p^i} \cap K_j$. Since $K_j \in S$, $\{x_1, \ldots, x_r\}$ remains linearly independent over K_j. Since $k_1^*, \ldots, k_r^* \in K^* \subseteq K_j$, $k_1^* = \ldots = k_r^* = 0$. Thus, X is linearly independent over K^*. Therefore, $K^* \in S$ whence S has a minimal element.

Since the existence of a sub-basis for a purely inseparable extension L/K is equivalent to the modularity of L/K in the bounded exponent case, Theorem 3 (1) establishes the existence of a maximal intermediate field with a sub-basis over K by use of Zorn's lemma. When L/K is purely inseparable, but of unbounded exponent, then Theorem 3 (1) yields a partial solution to the problem posed in (**11**, p. 439).

2. Coefficient fields. Let (A, K, N, g) denote a complete local algebra A (not necessarily Noetherian) over a subfield K of characteristic $p \neq 0$ where N is the unique maximal ideal of A and g is the natural homomorphism of A onto the residue class field A/N. Identify K and gK in A/N.

THEOREM 4. *Suppose that (A, K, N, g) is a complete local algebra (not necessarily Noetherian). If A/N is modular over K, then A has a coefficient field containing K if and only if $g(A^{p^i} \cap K) = (A/N)^{p^i} \cap K$, $i = 1, 2, \ldots$.*

Proof. Suppose that $g(A^{p^i} \cap K) = (A/N)^{p^i} \cap K$, $i = 1, 2, \ldots$. Since A/N is modular over K, there exists a p-basis B of A/N such that

$$K = ((A/N)^{p^i} \cap K)(C^*), \qquad i = 1, 2, \ldots,$$

by (**). Since $g(A^{p^i} \cap K) = (A/N)^{p^i} \cap K$, there exists a set of representatives B' in A of B such that $A^{p^i}[B']$ contains C^* (K and gK being identified). Since

$$g(A^{p^i} \cap K) = (A/N)^{p^i} \cap K, \qquad K \subseteq (A^{p^i} \cap K)(C), \quad i = 1, 2, \ldots .$$

Thus, $A^{p^i}[B'] \supseteq K$, $i = 1, 2, \ldots$, whence with respect to the N-adic topology of A, $\bigcap_{i=1}^{\infty}$ (closure $A^{p^i}[B']$) is a coefficient field of A containing K (**12**, p. 306). The converse is immediate.

When A/N has no purely inseparable elements over K, then the condition $g(A^{p^i} \cap K) = (A/N)^{p^i} \cap K$ always holds since $(A/N)^{p^i} \cap K = K^{p^i}$ in this case. Also, if A/N is separable over K, then A/N is modular over K.

In view of Theorem 1 above and the fact that the existence of a sub-basis for L/K is equivalent to the modularity of L/K in the bounded exponent case, the following remark consolidates many of the results of (**3**; **4**; **6**).

Remark. Let A be a commutative ring with identity, N a maximal ideal of A, and g the natural homomorphism of A onto A/N. Let R be a complete local ring (not necessarily Noetherian) of prime characteristic p such that $R \subseteq A$, the identities of A and R coincide and $M = R \cap N$ is the unique maximal ideal of R. If A/N is purely inseparable and has a sub-basis over R/M, then there exists a coefficient field of R which is extendable to one of A if and only if $g(A^{p^i} \cap R) = (A/N)^{p^i} \cap R/M$, $i = 1, 2, \ldots$. By Theorem 1, there exists a p-basis B of A/N such that C is a p-basis of R/M. If

$$g(A^{p^i} \cap R) = (A/N)^{p^i} \cap R/M, \qquad i = 1, 2, \ldots,$$

then there exists a set of representatives B' in A of B such that $R \supseteq C'$ where $C' = \{b'^{p^i} \mid b' \in B', i \text{ is the exponent of } b = gb' \text{ over } R/M\}$. Since C is a p-basis of R/M, R has a coefficient field $K \supseteq C'$ by the existence lemma as stated in (**6**). Since $B - (R/M)$ is a sub-basis of A/N over R/M and $b' \in B'$ has the same exponent over K that gb' has over R/M, we see that $K[B']$ is a coefficient field of A.

That this remark consolidates some of the results of (**3**; **4**; and **6**) comes about by varying A and R. That is, for (**3**; **6**), we let A be a complete local ring (not necessarily Noetherian) and for (**4**), we let R be a field.

References

1. G. Haddix, *The existence of K-coefficient fields in commutative algebras*, unpublished thesis, Creighton University, Omaha, Nebraska, 1966.

2. S. MacLane, *Modular fields*, Duke Math. J. *5* (1939), 372–393.

3. J. Mordeson, *Remark on coefficient fields in complete local rings*, J. Math. Kyoto Univ. *4* (1965), 637–639.

4. J. Mordeson and B. Vinograde, *Extension of certain subfields to coefficient fields in commutative algebras*, J. Math. Soc. Japan *17* (1965), 47–51.

5. ——— *Generators and tensor factors of purely inseparable fields*, Math. Z. *107* (1968), 326–334.

6. M. Nagata, *Note on coefficient fields of complete local rings*, Mem. Coll. Sci. Univ. Kyoto *32* (1959-60), 91–92.
7. G. Pickert, *Inseparable Korpererweiterungen*, Math. Z. *52* (1949), 81–136.
8. P. Rygg, *On minimal sets of generators of purely inseparable field extensions*, Proc. Amer. Math. Soc. *14* (1963), 742–745.
9. M. Sweedler, *Structure of inseparable extensions*, Ann. of Math. (2) *87* (1968), 401–410.
10. ——— *The Hopf algebra of an algebra applied to field theory*, J. Algebra *8* (1968), 262–276.
11. M. Weisfeld, *Purely inseparable extensions and higher derivations*, Trans. Amer. Math. Soc. *116* (1965), 435–450.
12. O. Zariski and P. Samuel, *Commutative algebra*, Vol. 2 (Van Nostrand, Princeton, N.J., 1960).

Iowa State University,
Ames, Iowa;
Creighton University,
Omaha, Nebraska

https://doi.org/10.4153/CJM-1969-167-1 Published online by Cambridge University Press