Can. J. Math., Vol. XXVII, No. 5, 1975, pp. 1176–1182

MODULARITY vs. SEPARABILITY FOR FIELD EXTENSIONS

H. F. KREIMER AND N. HEEREMA

1. Introduction. In this paper we compare the properties separability and modularity for field extensions. Let $K \supset k$ be fields of characteristic $p \neq 0$. K is separable over k if K and $k^{p^{-1}}$ are linearly disjoint over k. K is modular over k if K and $k^{p^{-n}}$ are linearly disjoint over their intersection for all $n > 0$. The latter definition is due to Sweedler [**12**] and is important particularly for Galois theories of purely inseparable extensions [**2**; **3**; **4**; **7**].

The similarity between the two definitions suggests they may give rise to similar theories. It is a familiar fact that a separable extension is modular whereas the converse is not true since, for example the perfect closure of any field k is modular over k. Our point of departure is a theorem of Heerema and Tucker [**8**, Lemma 4] which states that K/k is modular if and only if K is a separable extension of a purely inseparable modular extension of k. Using this result we extend to the modular case the characterization of separable extensions as p-independence preserving. The result is that if K/k has finite exponent (i.e., $k(K^{p^n})/k$ separable for some n) then K is a modular extension of k if and only if there is a p-basis $\mathscr{S}$ of k such that the set

$$\{s^{p^{-n}}, s \in \mathscr{S} | s^{p^{-n}} \in K, s^{p^{-n-1}} \notin K\}$$

is p-independent in K. This characterization is then used to show (Theorem 4) that if $K \supset M \supset k$ where M/k is purely inseparable with finite exponent and K/M is separable then $K = S \otimes_k M$ with S/k separable extending an observation of Heerema [**6**, Proposition 2.7; also see reference **8**, Proposition 1].

In Section 3 we bring together a number of characterizations of modularly perfect fields, that is, fields k with the property that every field extension of k is a modular extension. We find that modularly perfect fields are almost perfect, that is, k is modularly perfect if and only if $[k : k^p] \leqq p$. Thus k is modularly perfect if and only if every finite extension of k is simple [**1**; p. 134, Ex. 6]. Theorem 1 states that a modular extension cannot be exceptional where in the terminology introduced by Reid [**11**] an exceptional extension K of k is an inseparable extension with the property that $k^{p^{-1}} \cap K = k$. This suggests the characterization of modularly perfect fields as those fields which have no exceptional extensions. Other characterizations are obtained.

A question suggested by this paper, and one which the writers have been unable to resolve is the following. Is every field extension which is a purely

Received October 7, 1974 and in revised form, January 7, 1975.

inseparable extension followed by a separable extension, a tensor product of purely inseparable and separable factors?* Theorem 4 gives an affirmative answer if the extension has finite exponent.

2. Modularity and separability. We begin by setting down two results, due to Sweedler, which we will need. Part (c) of the first result quoted is stated a bit differently but is easily seen to be equivalent to the corresponding Part (f) of the original

THEOREM A [**12**, p. 403, Theorem 1]. *Let K be a purely inseparable extension of k having finite exponent. The following are equivalent.*

(a) $K = \bigotimes_{k, x \in \mathcal{N}} k(x)$ *for some subset* $\mathcal{N}$ *of* K.

(b) *K is a modular extension of k.*

(c) *For some set* $\mathcal{N}$ *which generates K over k, the set* $\{x^{p^n}, x \in \mathcal{N} | p^n = \text{degree of } x \text{ over } k\}$ *is a p-independent subset of k.*

THEOREM B [**12**, p. 407, Lemma 5, Part 3]. *Given fields* $K \supset M \supset k$, *if K is separable over M then K is modular over k if and only if M is modular over k.*

The following characterization of modular extensions is due to Heerema and Tucker. We prove it here since the proof is short and the result is basic to this paper.

THEOREM 1 [**8**, Lemma 4]. *A field K is a modular extension of a subfield k if and only if there is an intermediate field M such that K/M is separable and M/k is purely inseparable modular.*

Proof. If there is such an intermediate field then by Theorem B, K is modular over k. Conversely, let $M = k^* \cap K$ where k^* is the perfect closure of k. Since, by assumption K and $k^{p^{-n}}$ are linearly disjoint over $K \cap k^{p^{-n}}$ and since $K \cap k^{p^{-n}} = M \cap k^{p^{-n}}$ it follows that M and $k^{p^{-n}}$ are linearly disjoint over their intersection. Thus M/k is modular.

To show K separable over M let $\rho_1, \ldots, \rho_n$ be elements of K linearly dependent over $k^* = M^*$ and hence over $k^{p^{-n}}$ for some n. Since K is modular over k they are linearly dependent over $k^{p^{-n}} \cap K \subset M$. Thus K is separable over M.

The following theorem generalizes to modular extensions the p-independence preserving characterization of separable extensions. It is based on Theorems A and 1.

THEOREM 2. *An extension K of k having finite exponent over k is modular over k if and only if there is a p-basis* $\mathcal{S}$ *of k such that* $\mathcal{S}' = \{s^{p^{-n}}, s \in \mathcal{S} | s^{p^{-n}} \in K, s^{p^{-n-1}} \notin K\}$ *is p-independent in K.*

*James Deveney has settled the matter with a counter example.

https://doi.org/10.4153/CJM-1975-123-2 Published online by Cambridge University Press

Proof. By Theorem 1, if K is modular over k then there is an intermediate field M such that K/M is separable and M/k is purely inseparable modular with finite exponent. By Part (c) of Theorem A there is a set $\mathscr{N}'$ such that $M = \bigotimes_{k,\, x \in \mathscr{N}} k(x)$ and

$$\mathscr{N} = \{x^{p^n}, x \in \mathscr{N}' | p^n = \text{degree of } x \text{ over } k\}$$

is a p-independent subset of k. We choose $\mathscr{T}$ in k so that $\mathscr{S} = \mathscr{N} \cup \mathscr{T}$ is a p-basis for k. Then $\mathscr{S}' = \mathscr{N}' \cup \mathscr{T}$ is a p-basis for M which, since K is separable over M, is a p-independent subset of K.

Conversely, if there is a p-basis $\mathscr{S}$ of k such that $\mathscr{S}'$ is p-independent in K we choose $M = k(\mathscr{S}')$. M is purely inseparable over k and by Theorem A, Part (c), M is modular over k. Also, $\mathscr{S}'$ is a p-base for M. Since $\mathscr{S}'$ is p-independent in K, K is a separable extension of M and thus by Theorem B, K is modular over k.

We now use Theorem 2 to obtain a rather general result on the splitting of a purely inseparable extension followed by a separable extension.

THEOREM 3. *An extension K of k having finite exponent over k is a modular extension of k if and only if $K = S \otimes_k M$ where M is a modular purely inseparable extension of k having finite exponent and S is separable over k.*

Proof. If $K = S \otimes_k M$ as in the theorem then K is modular over k by Theorem B. Conversely, assume K modular over k and let M be the intermediate field of Theorem 1. We choose a tensor generating set $\mathscr{N}'$ of M over k, as in Part (a) of Theorem A, and let

$$\mathscr{N}' = \{s^{p^n}, s \in \mathscr{N}' | p^n = \text{degree of } s \text{ over } k\}.$$

Let $\mathscr{T}$ be a subset of k chosen so $\mathscr{T} \cup \mathscr{N}$ is a p-basis for k. Then $\mathscr{T} \cup \mathscr{N}'$ is a p-basis for M which we extend to a p-basis $\mathscr{S} = \mathscr{T} \cup \mathscr{N}' \cup \mathscr{Q}$ for K. Let $S = K^{p^{n+1}}(\mathscr{T} \cup \mathscr{N} \cup \mathscr{Q})$ where n is the exponent of K over k. Clearly, $\mathscr{T} \cup \mathscr{N} \cup \mathscr{Q}$ is a p-basis for S so S is a separable extension of k. Since $K = K^{p^{n+1}}(\mathscr{T} \cup \mathscr{N}' \cup \mathscr{Q})$ it follows that $SM = K$ or $K = S \otimes_k M$.

Using the concept of modular closure of a purely inseparable extension we can drop the modularity condition from Theorem 3 as follows.

THEOREM 4. *Let $K \supset M \supset k$ be fields such that K is separable over M and for some $n \geqq 0$, $M^{p^n} \subset k$. Then $K = S \otimes_k M$ where S is a separable extension of k.*

Proof. Let L be the modular closure of M over k. We note that $L^{p^n} \subset k$ [**12**, p. 408, Theorem 6 and Definition]. Then $K' = K(L) = K \otimes_M L$. As in the proof of Theorem 3 we choose a tensor generating set, $\mathscr{N}'$ for L over k and let

$$\mathscr{N} = \{s^{p^n}, s \in \mathscr{N} | p^n = \text{degree } s \text{ over } k\}.$$

Let $\mathscr{T}$ be a subset of k such that $\mathscr{N} \cup \mathscr{T}$ is a p-basis for k. As before $\mathscr{N}' \cup \mathscr{T}$ is a p-basis for L. Let $\mathscr{Q}$ be a p-basis for K over M. Then, since $K' = K \otimes_M L$,

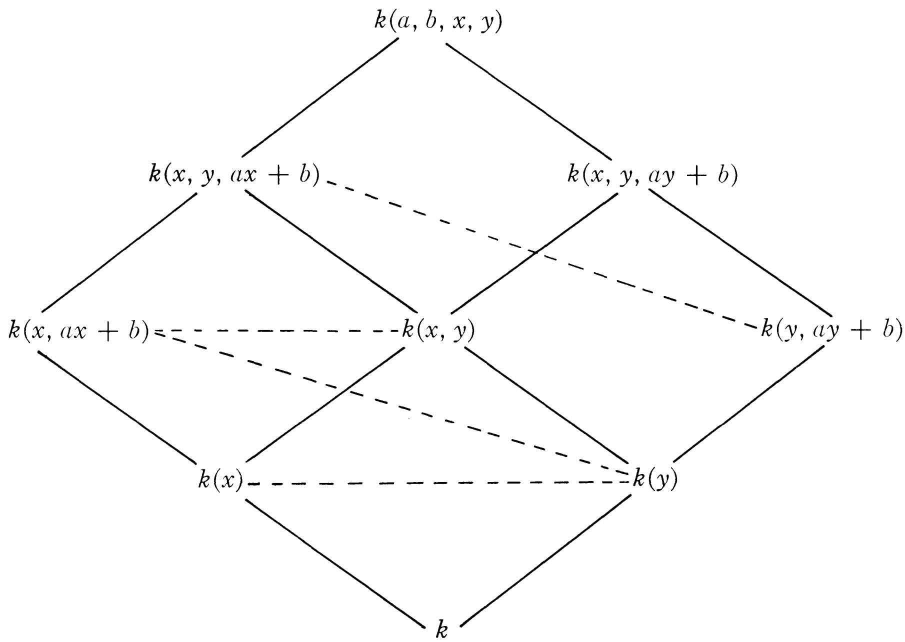
$\mathscr{S} = \mathscr{N}' \cup \mathscr{T} \cup \mathscr{Q}$ is a p-basis for K'. Then $S = K'^{p^{n+1}}(\mathscr{N} \cup \mathscr{T} \cup \mathscr{Q})$ is separable over k. Since $K = MK^{p^{n+1}}(\mathscr{Q}) \subseteq MS$ and $S \subseteq K$, we have $K = S \otimes_k M$.

In connection with Theorem 4, Heerema and Tucker [**8**, Lemma 4] have given a simple proof that any purely inseparable extension followed by a separably generated extension splits as above.

3. Modularly perfect fields. The purpose of this section is to discover and characterize fields for which every field extension is modular. Any exceptional field extension fails to be modular according to Theorem 1, and so we shall find it useful to know when exceptional field extensions exist. The following proposition generalizes Exercise 3 in reference [**1**, p. 144].

PROPOSITION 5. *Let k be a field of characteristic $p \neq 0$ such that $[k : k^p] > p$. There exists an exceptional field extension K of k such that $K \otimes_k K$ is a ring with zero nil radical.*

Proof. Since $[k^{p^{-1}} : k] = [k : k^p] > p$, there exist elements a, b in $k^{p^{-1}}$ such that $[k(a, b) : k] = p^2$. Let x and y be elements which are algebraically independent over k, and let $K = k(x, ax + b)$. There is a homomorphism of $K \otimes_k K$ over k into $k(a, b, x, y)$ which maps $x \otimes 1$ onto x, $1 \otimes x$ onto y, $(ax + b) \otimes 1$ onto $ax + b$, and $1 \otimes (ax + b)$ onto $ay + b$. If the subfields $K = k(x, ax + b)$ and $k(y, ay + b)$ of $K(a, b, x, y)$ are linearly disjoint over k, then this homomorphism is monic and there can be no non-zero nilpotent element in $K \otimes_k K$. Consider the following diagram.



Because $k(x, y)$ is a separable extension of k, $k(x, y)$ and $k(a, b)$ are linearly disjoint over k and $[k(a, b, x, y) : k(x, y)] = p^2$. Consequently, each of the dimensions $[k(a, b, x, y) : k(x, y, ax + b)]$, $[k(x, y, ax + b) : k(x, y)]$, $[k(x, ax + b) : k(x)]$ and $[k(y, ay + b) : k(y)]$ must equal p. In particular, $k(x, y, ax + b)$ and $k(y, ay + b)$ are linearly disjoint over $k(y)$. Also $k(x, ax + b)$ and $k(x, y)$ are linearly disjoint over $k(x)$, while $k(x)$ and $k(y)$ are linearly disjoint over k since x and y are algebraically independent over k. Therefore $k(x, ax + b)$ and $k(y)$ are linearly disjoint over k, and it now follows that $k(x, ax + b)$ and $k(y, ay + b)$ are linearly disjoint over k.

Because $\{1, x, ax + b\}$ is a linearly independent set over k, but not over $k(a, b) \subseteq k^{p^{-1}}$, K is not a separable extension of k. To verify that K is an exceptional extension of k, we show that k is algebraically closed in K. Thus suppose $c \in K$ and c is algebraic over k. Then $c^p \in k(x)$ and c^p is algebraic over k. Since $k(x)$ is a purely transcendental extension of k, $c^p \in k$. If c were not an element of k, $c \otimes 1 - 1 \otimes c$ would be a non-zero nilpotent element of $K \otimes_k K$, in contradiction with what has already been proved.

If in addition to the hypotheses of the preceding proposition, k is not separable algebraically closed, then a finite dimensional exceptional extension of k can be constructed. Such a construction has been given by Kreimer and appears in [**5**].

THEOREM 6. *Let k be a field of characteristic $p \neq 0$ and let k^* be the perfect closure of k. The following statements are equivalent.*

(i) $[k : k^p] \leqq p$.

(ii) *Every field extension of k is modular.*

(iii) *For every field extension K of k, there exists a separable field extension S of k such that $K \subseteq S \otimes_k (k^* \cap K)$.*

(iv) *Every field extension K of k is separable over $k^* \cap K$.*

(v) *There exist no exceptional field extensions of k.*

(vi) *A field extension K of k is separable if, and only if, the nil radical of the ring $K \otimes_k K$ is zero.*

(vii) *Every finite dimensional field extension of k is simple.*

Proof. Suppose $[k : k^p] \leqq p$. Then k must be a simple extension of k^p; and if a is an element of k such that $k = k^p(a)$, then $k^{p^{-1}} = k(a^{p^{-1}})$. An easy argument by induction will establish that $k^{p^{-n}} = k(a^{p^{-n}})$ for every positive integer n. Now let K be any field extension of k and let n be any positive integer. Since $K(k^{p^{-n}}) = K(a^{p^{-n}})$, the dimensions $[K(k^{p^{-n}}) : K]$ and $[k^{p^{-n}} : k^{p^{-n}} \cap K]$ must both equal p^m where m is the smallest non-negative integer for which $a^{p^{m-n}} \in K$; and therefore K and $k^{p^{-n}}$ are linearly disjoint over their intersection. Thus statement (i) implies statement (ii).

Next we shall show that statement (i) implies statement (iii). If K is a modular field extension of k having finite exponent over k, then $K = S \otimes_k (k^* \cap K)$ for some subfield S of K which is a separable extension of k according to Theorem 3. Thus we shall assume $[k : k^p] \leqq p$ and K is a field extension of k having unbounded exponent over k. It has already been observed that $k^{p^{-n}}$ is a simple extension of k, whence $[k^{p^{-n}} : k] \leqq p^n$ for every positive integer n; so if $b \in k^* \cap K$ has positive exponent n over k, then $[k^{p^{-n}} : k] = p^n$ and $k^{p^{-n}} = k(b) \subseteq k^* \cap K$. Therefore $k^* = k^* \cap K \subseteq K$. Let K^* be the perfect closure of K. By Zorn's Lemma there exists among the subfields of K^* which are separable extensions of k, some maximal element S, and we shall prove that $K^* = S \otimes_k k^*$. Let c be an element of K^* which is not an element of S. Since $S(c)$ cannot be a separable extension of k, $S(c)$ is not a separable extension of S and c is neither separable algebraic nor transcendental over S. Therefore K^* is algebraic and purely inseparable over S and K^* must be the perfect closure of S. Suppose $[S(c) : S] = p$. Because S is a separable extension of k, $[S(k^{p^{-1}}) : S] = [k^{p^{-1}} : k] = p$. But $S(c)$ and $k^{p^{-1}}$ are not linearly disjoint over k, and so $k^{p^{-1}}$ must be a subfield of $S(c)$ and $S(c) = S(k^{p^{-1}})$. Consequently $S^{p^{-1}} = S(k^{p^{-1}})$, and it follows by induction that $S^{p^{-n}} = S(k^{p^{-n}})$ for every positive integer n. Therefore $K^* = S(k^*) = S \otimes_k k^*$.

Statement (ii) implies statement (iv) by Theorem 1. Now let K and S be field extensions of k such that S is separable over k and $K \subseteq S \otimes_k (k^* \cap K)$. Then S and k^* are linearly disjoint over k, and so $S \otimes_k (k^* \cap K)$ and k^* must be linearly disjoint over $k^* \cap K$. Therefore $S \otimes_k (k^* \cap K)$ and its subfield K are separable field extensions of $k^* \cap K$. Thus statement (iii) implies statement (iv), and clearly statement (iv) implies statement (v). It is well known that if K and L are field extensions of k and K is separable over k then the nil radical of the ring $K \otimes_k L$ is zero [**9**, Chapter IV, Theorem 23]. But if K is a field extension of k which is neither separable nor exceptional, then there exists an element c of K which is algebraic and purely inseparable of positive exponent over k and $c \otimes 1 - 1 \otimes c$ is a non-zero nilpotent element of $K \otimes_k K$. Therefore statement (v) implies statement (vi). Statement (vi) implies statement (i) by Proposition 5, and the equivalence of statements (i) and (vii) is well known and appears as an exercise in reference [**1**, p. 134].

A field which satisfies any of the equivalent statements of the preceding theorem will be called modularly perfect. In regard to statement (iii) of the theorem, note that if the field extension K has finite exponent over k or if K is perfect, then the field S can be chosen to be a subfield of K and $K = S \otimes_k (k^* \cap K)$. This conclusion is also valid if K is algebraic over k. In that case take S to be the subfield of elements of K which are separable algebraic over k, and each element of K being separable over $k^* \cap K$ and purely inseparable over S will be both separable and purely inseparable over $S(k^* \cap K) = S \otimes_k (k^* \cap K)$. Therefore $K = S \otimes_k (k^* \cap K)$. The writers know of no example of a field extension of a modularly perfect field which is not a tensor product of separable and purely inseparable factors.

In analogy with perfect fields, we have the following theorem.

THEOREM 7. *Any algebraic field extension of a modularly perfect field is again modularly perfect.*

https://doi.org/10.4153/CJM-1975-123-2 Published online by Cambridge University Press

Proof. Let k be a modularly perfect field, let K be an algebraic field extension of k, and let $M = k^* \cap K$. Since K is separable algebraic over M, $K = M(K^p)$. Therefore

$$[K : K^p] = [M(K^p) : M^p(K^p)] \leqq [M : M^p],$$

and it remains only to prove that M is modularly perfect. But any field extension L of M is also an extension of k, and therefore L is separable over $k^* \cap L = M^* \cap L$. Thus M is modularly perfect.

If k is perfect or is a simple transcendental extension of a perfect field, then clearly $[k : k^p] \leqq p$. By the preceding theorem, any field extension of transcendence degree one over a perfect field is modularly perfect; but these are not the only modularly perfect fields. In Section 10 of reference [**10**] there is given an example of a field k which has a p-basis of one element, hence $[k : k^p] = p$, and transcendence degree two over its maximal perfect subfield.

References

1. N. Bourbaki, *Elements de mathematique, Chapter 5, Corps commutatifs* (Actualites Sci. et Ind., No. 1102, Hermann, Paris, 1950).

2. S. U. Chase, *On inseparable Galois theory*, Bull. Amer. Math. Soc. *77* (1971), 413–417.

3. R. L. Davis, *A Galois theory for a class of purely inseparable field extensions*, Dissertation, Florida State University, Tallahassee, Fla., 1969.

4. M. Gerstenhaber and A. Zaromp, *On the Galois theory of purely inseparable field extensions*, Bull. Amer. Math. Soc. *76* (1970), 1011–1014.

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

6. N. Heerema, *A Galois theory for inseparable field extensions*, Trans. Amer. Math. Soc. *154* (1971), 193–200.

7. N. Heerema and J. Deveney, *Galois theory for fields K/k finitely generated*, Trans. Amer. Math. Soc. *189* (1974), 263–274.

8. N. Heerema and D. Tucker, *Modular field extensions*, preprint.

9. N. Jacobson, *Lectures in abstract algebra III, Theory of fields and Galois theory* (D. Van Nostrand Company, Princeton, N.J., 1964).

10. S. MacLane, *Modular fields I, Separating transcendence bases*, Duke Math. J. *5* (1939), 372–393.

11. J. D. Reid, *A note on inseparability*, Michigan Math. J. *13* (1966), 219–223.

12. M. E. Sweedler, *Structure of inseparable extensions*, Ann. of Math. *87* (1968), 401–410.

Florida State University,
Tallahassee, Florida

https://doi.org/10.4153/CJM-1975-123-2 Published online by Cambridge University Press