THE STRUCTURE OF INSEPARABLE FIELD
EXTENTIONS

BY

WILLIAM C. WATERHOUSE[1]

ABSTRACT. The goal of this paper is to introduce some structural ideas into the hitherto chaotic subject of infinite inseparable field extensions. The basic discovery is that the theory is closely related to the well-developed study of primary abelian groups. This analogy undoubtedly has implications beyond those included here. We consider only modular extensions, which are the inseparable equivalent of galois extensions. §§2 and 3 develop the theory of pure independence, basic subfields, and tensor products of simple extensions. The following sections are devoted to Ulm invariants and their computation; the existence of nonzero invariants of arbitrary index is proved by means of a theorem which furnishes an actual connection between primary groups and inseparable fields. The final section displays some complications in the field extensions not occurring in abelian groups.

1. Preliminaries; modular extensions.

Theorem 1.1. *Let K and $\{L_\alpha\}$ be subfields of some common field, and suppose K is linearly disjoint from each L_α. Then K is linearly disjoint from $L = \bigcap L_\alpha$.*

Proof. Suppose that there are $x_1, \cdots, x_n$ in L linearly independent over $L \cap K$ but not over K. We may assume n minimal; then there is a relation $\Sigma a_i x_i = 0$ with $a_i \in K$ and $a_1 = 1$, and this relation is unique. The x_i are in each L_α and are dependent over K, hence dependent over $K \cap L_\alpha$. Since the dependence relation over K is unique, the a_i are in $K \cap L_\alpha$. But this implies $a_i \in K \cap L$, which is impossible.

This theorem is basic and will be used repeatedly, usually without explicit citation.

Definition [5]. A purely inseparable field extension K/k is *modular* if K^{b^n} and k are linearly disjoint, $n = 1, 2, 3, \cdots$. (The concept is defined in [5] for more general extensions, but all the extensions we consider will be purely inseparable.)

If K/k is a finite purely inseparable extension, then it is known

---

[6, p. 433] that $K \otimes_k \bar{k}$ has the form $\bar{k}[X_1, \cdots, X_n]/(X_1^{q_1}, \cdots, X_n^{q_n})$ where the q_i are powers of the characteristic p; note for later reference that this truncated polynomial algebra is simply $\bar{k}[G]$ for G a finite abelian p-group. Say that an extension L *splits* K if $K \otimes_k L \simeq L[G]$. Then there is a unique smallest splitting field $S(K/k)$; it contains K and is itself a finite purely inseparable extension of k. Furthermore, K is its own splitting field if and only if it is a tensor product of simple extensions [6, p. 425], and this condition is equivalent to modularity [5, p. 403]. Thus the finite modular extensions in this theory play a role like that of those finite separable extensions which are their own splitting fields, i.e. the galois extensions.

Proposition 1.2. *Let K/k be a purely inseparable extension, $\{L_\alpha\}$ a family of intermediate fields.*

(a) *If each L_α is modular over k, their intersection is modular over k.*

(b) *If K is modular over each L_α, it is modular over their intersection.*

(c) *If the L_α are directed by inclusion and each is modular over k, their union is modular over k.*

(d) *If the L_α are directed by inclusion and K is modular over each of them, it is modular over their union.*

Proof. Since the pth power map is injective, we have $(\bigcap L_\alpha)^{p^n} = \bigcap (L_\alpha^{p^n})$. Hence (a) as well as (b) follows from 1.1. Statements (c) and (d) are even easier, needing only the fact that linear disjointness is a condition of finite type.

Part of this proposition was proved in a different way in [3].

Proposition 1.3. *Let K/k be purely inseparable. The following are equivalent:*

(a) *K/k is modular.*

(b) *K is a directed union of finite modular extensions of k.*

(c) *For every finite extension F/k contained in K, the splitting field $S(F/k)$ is contained in K.*

Proof. Let F be any finite purely inseparable extension of k, and consider the sequence $S(F/k), S(S(F/k)/k), \cdots$. By [6, p. 429] it stabilizes after finitely many steps, and the result is the smallest modular extension of k containing F. Hence from (c) we can deduce that every finite sub-extension is contained in a finite modular extension, thus getting (b). We can deduce (a) from (b) by 1.2 (c). Finally, assume (a); let F be a finite subextension, and let L be the smallest modular extension containing it. We have $L \cap K$ modular over k by 1.2 (a), and $F \subseteq L$, so by minimality $L = L \cap K$; thus $S(F/k) \subseteq L \subseteq K$.

This proposition shows that modular extensions in general are the inseparable analogue of infinite galois extensions.

We must also put on record the familiar result about linear disjointness in towers [2, p. 162], which we use in the form derived by Sweedler [5, p. 206]:

Proposition 1.4. *Let L/k be purely inseparable, K an intermediate field.*

(a) *The following are equivalent:*

(i) *K and kL^{p^n} are linearly disjoint over $k[K \cap L^{p^n}]$ for all (positive) n, and L is modular over k.*

(ii) *$K \cap L^{p^n}$ and k are linearly disjoint for all n, and L is modular over K.*

(b) *The following are equivalent:*

(i) *K^{p^n} and $L^{p^n} \cap k$ are linearly disjoint for all n, and L is modular over k.*

(ii) *L^{p^n} and kK^{p^n} are linearly disjoint over $K^{p^n}[L^{p^n} \cap k]$ for all n, and K is modular over k.*

Remark 1.5. To illustrate how 1.1 and 1.4 are used, we insert here an argument which will arise later. Let L/k be modular. Then L^{p^r} and $k^{1/p}$ are linearly disjoint, since pth power is an isomorphism. Clearly L^{p^r} and L are linearly disjoint, so L^{p^r} and $L \cap k^{1/p}$ are linearly disjoint. That is, L is modular over $L \cap k^{1/p}$. Also, $(L \cap k^{1/p}) \cap L^{p^n}$ equals $L^{p^n} \cap k^{1/p}$, and by 1.1 this is linearly disjoint from k. Thus by 1.4 (a) we conclude that kL^{p^n} and $L \cap k^{1/p}$ are linearly disjoint over $k[L^{p^n} \cap k^{1/p}]$, and in particular have that field as their intersection.

2. Pure independence and basic subfields.

Definition. Let K/k be modular. A subset $\{x_i\}$ of $K \backslash k$ is *pure independent* if for each n the monomials $\Pi x_i^{e_i}$ with $0 \le e_i < p^n$, almost all $e_i = 0$, and $e_i < |k(x_i):k|$ are linearly independent over kK^{p^n}.

This definition says that no polynomial in the x_i lies in kK^{p^n} unless it obviously does; tensor product generators, for instance, must have this property. If $K^p \subseteq k$, pure independence reduces to the usual concept of p-independence [2, p. 180].

Definition. Let K/k be purely inseparable. An intermediate field F is called *pure* if F and kK^{p^n} are linearly disjoint over kF^{p^n} for all n.

Note that then $k[K^{p^n} \cap F]$ equals kF^{p^n}, and if K/k is modular it follows by 1.4 (a) that K/F is also modular.

Proposition 2.1. *Let K/k be modular. If $\{x_i\}$ is pure independent,*

then the subextension F generated by the x_i is pure and is the tensor product of the simple extensions $k(x_i)$. Conversely, if F is a pure subfield of the form $\bigotimes k(x_i)$, then the x_i are pure independent.

Proof. The definition of pure independence shows that the monomials $\Pi x_i^{e_i}$ with $0 \le e_i < |k(x_i):k|$ and almost all $e_i = 0$ are independent over k; thus the surjection $\bigotimes k(x_i) \to F$ is also injective. We have then $kF^{p^n} = \bigotimes k(x_i^{p^n})$, and a basis for F over kF^{p^n} is given by the monomials with $e_i < |k(x_i):k|$ and $0 \le e_i < p^n$. By definition again these are still independent over kK^{p^n}, and thus F is pure. The converse implication is equally easy.

Proposition 2.2. *Let K/k be modular, and assume $K \cap k^{1/p} = kK^{p^n} \cap k^{1/p}$ for all n. Then K is relatively perfect over k, i.e. $kK^p = K$.*

Proof. We show inductively on r that $K \cap k^{1/p^r} \subseteq kK^{p^n}$ for all n; by hypothesis this is true for $r = 1$. Assume it for r and take $x \in K \cap k^{1/p^{r+1}}$. Then $x^p \in K \cap k^{1/p^r}$, so $x^p \in kK^{p^{n+1}}$ by induction. Say x^p is a k-linear combination of elements $y_i^{p^{n+1}}$ with $y_i \in K$. Then x^p and $(y_i^{p^n})^p$ are in K^p, and x^p is in the k-span of the others; by modularity it is in the $(K^p \cap k)$-span. Taking pth roots we get x as a $(K \cap k^{1/p})$-linear combination of the $y_i^{p^n}$, and hence $x \in (K \cap k^{1/p})K^{p^n} \subseteq (kK^{p^n})K^{p^n} = kK^{p^n}$.

Definition. Let K/k be modular. A *basic subfield* of K/k is an intermediate field F such that

   (i) F is a tensor product of simple extensions of k,
   (ii) F is pure, and
   (iii) K is relatively perfect over F.

Theorem 2.3. *Let K/k be modular. Then the basic subfields are precisely the subextensions generated by maximal pure independent sets.*

Proof. Let F be generated by a maximal pure independent set $\{x_i\}$; in view of 2.1 the problem is only to prove K relatively perfect over F. As remarked after the definition of purity, K/F is automatically modular. If it is not relatively perfect, then 2.2 implies that we can find an n (possibly $n = 1$) such that $K \cap F^{1/p}$ is contained in $FK^{p^{n-1}}$ but not in FK^{p^n}.

Remark 1.5 tells us that $K \cap F^{1/p}$ and $FK^{p^{n-1}}$ have intersection $F[F^{1/p} \cap K^{p^{n-1}}]$, and thus $K \cap F^{1/p}$ is generated over F by elements $x^{p^{n-1}}$ with $x \in K$. We can therefore choose such an x with $x^{p^{n-1}} \notin FK^{p^n}$. By purity, $F \cap kK^{p^n} = kF^{p^n}$; hence x^{p^n} is in kF^{p^n}, say a k-linear combination of $y_j^{p^n}$ with $y_j \in F$. As k is linearly disjoint from K^{p^n}, we can take

this combination with coefficients in $k \cap K^{p^n}$. Taking p^nth roots we get $x = \Sigma b_j y_j$ with $b_j \in K$ and $b_j^{p^n} \in k$. Not all $b_j^{p^{n-1}}$ can be in FK^{p^n}, as then $x^{p^{n-1}}$ would be in FK^{p^n}. Thus we have an element b in K with $b^{p^n} \in k$ and $b^{p^{n-1}} \notin FK^{p^n}$. We now claim that $\{x_i\} \cup \{b\}$ is pure independent.

Suppose there is a relation among the properly restricted monomials $\Pi x_i^{e_i} b^e$ over kK^{p^m}. All of them have $0 \le e < p^m$ and $e < p^n = |k(b):k|$. Grouping the terms with the same e, we apparently have a relation among the b^e over FK^{p^m}. If $m \le n$ this means the degree of b over FK^{p^m} is less than p^m, and so $b^{p^{m-1}} \in FK^{p^m}$; but this is impossible, since raising to the p^{n-m}th power would give $b^{p^{n-1}} \in FK^{p^n}$. For $m > n$ we similarly deduce degree less than p^n and $b^{p^{n-1}} \in FK^{p^m} \subseteq FK^{p^n}$. Thus in either case we see that the coefficients of each power b^e must be zero. But these now are relations among monomials in the x_i, and by pure independence all the coefficients in them must be zero. Thus we have only the trivial relation, and $\{x_i\} \cup \{b\}$ is pure independent, contrary to the assumption of maximality.

Conversely, now, suppose $F = \bigotimes k(x_i)$ is a basic subfield; by 2.1 all we need to show is that $\{x_i\}$ is maximal. Suppose that $\{x_i\} \cup \{b\}$ is pure independent, with $|k(b):k| = p^n$. Then b is in the span of F over kK^{p^n}, since by relative perfection $K = FK^{p^n}$. But by purity $F(b)$ and kK^{p^n} are linearly disjoint over $kF(b)^{p^n} = kF^{p^n}$, so b is in $F[kF^{p^n}] = F$, which is clearly impossible.

Corollary 2.4. *Basic subfields exist.*

Proof. Pure independence is a condition of finite type, and so maximal pure independent sets exist.

Corollary 2.5 (Sweedler). *Let K/k be modular and $K^{p^n} \subseteq k$. Then K is a tensor product of simple extensions.*

Proof. Let F be basic; then $K = FK^{p^n} = F$.

Remarks. (i) We shall see in 4.5 that in any maximal pure independent set the number of x_i of each degree is an invariant. The actual field F, however, is far from unique. This can be shown easily by imitating the corresponding examples for groups, e.g. [1, p. I-147]; indeed, it can be deduced from those examples (see the Remark in §6).

(ii) The process used in [3, §2] appears to be in essence a construction of basic subfields. The nonuniqueness was not noted there, and [3, Theorem 16] might be misleading for that reason.

Proposition 2.6. *Let K/k be modular, B a pure modular subextension*

such that $B^{p^n} \subseteq k$ *for some* n. *Then* B *is a tensor factor of* K *over* k.

Proof. By 2.5 we know B is a tensor product of simple extensions; let X be a set of tensor generators of B over k. By 2.1 the set X is pure independent in K. Let $E = kK^{p^n}$; by purity E is linearly disjoint from B over $kB^{p^n} = k$. It follows that the elements of X are pure independent over E. Extend X to a maximal pure independent set $X \cup Y$ for K over E; as $K^{p^n} \subseteq E$, we have $K = E(X \cup Y)$. Set $H = E(Y)$, so $BH = K$. Since $X \cup Y$ is pure independent over E, the basis of B over k given by monomials in the elements of X is still independent over $E(Y)$. Thus $K = B \otimes_k H$.

The condition $B^{p^n} \subseteq k$ is necessary; indeed, a basic subfield need not be a tensor factor. Again examples to illustrate this can be deduced from those for groups, e.g. [1, p. I-139].

We conclude with a result needed in the next section. Like 2.2, it demonstrates how $K \cap k^{1/p}$ controls the structure of modular extensions.

Proposition 2.7. *Let* K/k *be modular,* E *a pure subfield with* $E \cap k^{1/p} = K \cap k^{1/p}$. *Then* $E = K$.

Proof. Suppose inductively $E \cap k^{1/p^r} = K \cap k^{1/p^r}$, and take an $x \in K \cap k^{1/p^{r+1}}$. Then $x^p \in E$, so by purity $x^p \in kE^p = E \cap kK^p$. Write it as a k-linear combination of y_i^p with $y_i \in E$, so that x is a $k^{1/p}$-linear combination of the y_i. Since K/k is modular, x is a linear combination of the y_i over $K \cap k^{1/p} = E \cap k^{1/p}$; as the y_i are in E, so is x.

3. Tensor products of simple extensions.

Definition. Let K/k be purely inseparable. An element in K has *height* $< n$ if it is not in kK^{p^n}. An intermediate field E has *bounded height* in K/k if its elements not in k have bounded height, i.e. $E \cap kK^{p^n} = k$ for some n.

Theorem 3.1. *Let* K/k *be modular. The following are equivalent:*

(i) K *is a tensor product of simple extensions.*

(ii) K *can be written as an increasing union of intermediate fields* $F_1 \subseteq F_2 \subseteq \cdots$ *where each* F_n *has bounded height in* K *and* K/F_n *is modular.*

(iii) $K \cap k^{1/p}$ *can be written as an increasing union of intermediate fields* $S_1 \subseteq S_2 \subseteq \cdots$ *where each* S_n *has bounded height in* K *and* K/S_n *is modular.*

Proof. If K is a tensor product of simple extensions, let X be a corresponding pure independent set, and let F_n be the intermediate field generated by the elements of X with degree $\leq p^n$; then (ii) is satisfied.

When (ii) holds, let $S_n = F_n \cap k^{1/p}$. Clearly the S_n have bounded height and exhaust $K \cap k^{1/p}$; we know by 1.5 that K is modular over $K \cap k^{1/p}$, so by 1.2 (b) it is modular over S_n.

The problem then is to prove (i) assuming (iii). We do this by inductively constructing pure independent sets $X_1 \subseteq X_2 \subseteq \cdots$ such that $k(X_n) \cap k^{1/p} = S_n$; by 2.7 we will then have $K = k(\bigcup X_n)$. Suppose therefore that we already have X_{n-1}, and expand it to a pure independent set X_n maximal among those for which $k(X_n) \cap k^{1/p} \subseteq S_n$. The induction step will be complete if we can show that $k(X_n) \cap k^{1/p} = S_n$.

Suppose the intersection is smaller. Then as S_n has bounded height we can find an $r \geq 0$ such that $kK^{p^r} \cap S_n \not\subseteq k(X_n)$ but $kK^{p^{r+1}} \cap S_n \subseteq k(X_n)$. Since K is modular over S_n and over k, we deduce from 1.4(a) that $S_n \cap kK^{p^r} = k[S_n \cap K^{p^r}]$, and hence there must be an element b^{p^r} in S_n not in $k(X_n)$. If we can now show $X_n \cup \{b\}$ is pure independent, we will be through. For then $k(X_n \cup \{b\}) = k(b) \otimes k(X_n)$, and the intersection of that with $k^{1/p}$ is $k(b^{p^r}) \otimes [k(X_n) \cap k^{1/p}] \subseteq S_n$, contrary to the maximality of X_n.

For brevity set $F = k(X_n)$ and $L = F \cap k^{1/p} \subseteq S_n$. If $X_r \cup \{b\}$ is not pure independent we get a nontrivial relation among properly restricted monomials $\Pi x_i^{e_i} b^e$; as in the next-to-last paragraph of 2.3 we find $b^{p^r} \in FK^{p^{r+1}}$. Hence there is an element in $FK^{p^{r+1}} \cap S_n$ not in F. We can thus finish the proof by showing that $FK^{p^{r+1}} \cap S_n \subseteq F$.

We begin with the tower $k \subseteq kF^{p^m} \subseteq F$, for any m; by 1.4 (b) we deduce that F^p and $kF^{p^{m+1}}$ are linearly disjoint over $k^p F^{p^{m+1}}[k \cap F^p] = F^{p^{m+1}} L^p$. [For this we need kF^{p^m} modular over k, which is clear here since F is a tensor product of simple extensions – cf. 4.1.] It follows then that F^p and $kK^{p^{m+1}}$ are linearly disjoint over $F^{p^{m+1}} L^p$. For suppose elements f_i^p in F^p are linearly dependent over $kK^{p^{m+1}}$; they are in F, so by the purity of F they are linearly dependent over $kF^{p^{m+1}}$. By the previous step they are then linearly dependent over $F^{p^{m+1}} L^p$.

Now let x be in $FK^{p^m} \cap k^{1/p}$, say $x = \Sigma f_i a_i$ with $f_i \in F$ and $a_i \in kK^{p^m}$. Then $x^p = \Sigma f_i^p a_i^p$. Both x^p and a_i^p are in $kK^{p^{m+1}}$, and x^p is a linear combination of the a_i^p over F^p, whence by linear disjointness it is so over $F^{p^{m+1}} L^p$. Taking pth roots we get x in $F^{p^m} L[kK^{p^m}] = LK^{p^m}$. Thus we have shown $FK^{p^m} \cap k^{1/p} = LK^{p^m} \cap k^{1/p}$, and in particular $FK^{p^{r+1}} \cap S_n = LK^{p^{r+1}} \cap S_n$.

Consider finally the tower $L \subseteq S_n \subseteq K$. By purity we know K is modular over F, whence as we saw earlier K is modular over $L = F \cap k^{1/p}$. Therefore we have $S_n \cap K^{p^m}$ linearly disjoint from L for all m. By assumption also K/S_n is modular. Hence by 1.4 (a) we have $S_n \cap LK^{p^{r+1}} =$

$L[S_n \cap K^{p^r+1}]$. But by choice of r we know $S_n \cap kK^{p^r+1} \subseteq F$, so $S_n \cap LK^{p^r+1} \subseteq F$. Consequently we have $S_n \cap FK^{p^r+1} \subseteq F$, as desired.

This theorem of course gives another proof of 2.5.

4. Ulm invariants of modular extensions. Our first structural analysis, in §2, led us to write a modular K/k as $K/F/k$ with K/F relatively perfect and F/k a tensor product of simple extensions; the two steps are relatively uncomplicated, but the construction is not unique. In this section we will give a decomposition with the relatively perfect extension at the bottom; it is more elaborate but canonical, and will yield numerical invariants.

Definition. Let K/k be purely inseparable. For α an ordinal, the intermediate field $(K/k)^\alpha$ [or kK^{p^α}] is constructed inductively as follows:

(i) $(K/k)^0 = K$,

(ii) $(K/k)^{\alpha+1} = k[(K/k)^\alpha]^p$, and

(iii) $(K/k)^\alpha = \bigcap\{(K/k)^\beta | \beta < \alpha\}$ for α a limit ordinal.

Write $(K/k)^\infty$ for $\bigcap(K/k)^\alpha$. The first α for which $(K/k)^\alpha = (K/k)^\infty$ is the *length* of K over k.

We thus have a descending chain of intermediate fields. The finite stages $(K/k)^n = kK^{p^n}$ are of course familiar, but it seems to have been unconsciously supposed that the chain would always stabilize at $(K/k)^\omega = \bigcap(K/k)^n$. Indeed, this is tacitly assumed in [3, Proposition 9], and I believe it is true for every inseparable extension in the literature. It may therefore be advisable to give at once an example where it is false. Let $K = F_p(y, x_1, x_2, x_3, \cdots)$ where y and the x_i are indeterminates, and let k be $F_p(y^p, x_1^p/y, x_2^{p^2}/y, x_3^{p^3}/y, \cdots)$. Then $(K/k)^\omega = k(y)$ and $(K/k)^{\omega+1} = k$, and thus K/k has length $\omega + 1$. It is in fact true, as we will prove in 6.2, that there are extensions of arbitrary prescribed length.

The definition in §3 can be extended transfinitely: the elements in K of *height* α are those in $(K/k)^\alpha$ but not in $(K/k)^{\alpha+1}$. The elements of $(K/k)^\infty$ must of course be assigned height ∞.

Proposition 4.1. *Let K/k be modular. Then for every α,*

(a) *$(K/k)^\alpha$ is modular over k, and*

(b) *K is modular over $(K/k)^\alpha$.*

Proof. We first prove (a) by induction on α. If α is a limit ordinal, $(K/k)^\alpha$ is an intersection of extensions already known to be modular, and so it is itself modular. Suppose now that $E = (K/k)^\alpha$ is modular over k. By 1.3 we can write E as a directed union $\bigcup E_\lambda$ where the E_λ are finite modular extensions of k. Then $kE^p = \bigcup kE_\lambda^p$, and the kE_λ^p are modular

over k by computation since E_λ is a tensor product of simple extensions. Thus $(K/k)^{\alpha+1} = kE^p$ is modular over k.

For (b) we note that by 1.4 (a) we have K modular over $(K/k)^\alpha$ if and only if $(K/k)^\alpha$ and kK^{p^n} are linearly disjoint over $k[(K/k)^\alpha \cap K^{p^n}]$ for all n. If α is a limit ordinal, the modularity holds by induction and 1.2 (b). Also, the second condition is trivial for $n \geq \alpha$, as there $(K/k)^\alpha \cap K^{p^n} = K^{p^n}$. Thus assuming the result for α we must prove $(K/k)^{\alpha+1} = k[(K/k)^{\alpha+1} \cap K^{p^n}]$ for $1 \leq n < \alpha + 1$. But we have

$$k[(K/k)^{\alpha+1} \cap K^{p^n}] \supseteq k[((K/k)^\alpha)^p \cap K^{p^n}] = k[(K/k)^\alpha \cap K^{p^{n-1}}]^p$$

$$= kk^p[(K/k)^\alpha \cap K^{p^{n-1}}]^p = k((K/k)^\alpha)^p = (K/k)^{\alpha+1}.$$

Definition. Let K/k be modular. The αth *Ulm invariant* of the extension, $f_\alpha(K/k)$, is the p-rank of $(K/k)^\alpha \cap k^{1/p}$ over $(K/k)^{\alpha+1} \cap k^{1/p}$.

Proposition 4.2. *Let K/k be modular.*

(a) *$(K/k)^\infty$ is relatively perfect over k, and is the largest relatively perfect subextension of K.*

(b) *If $f_n(K/k) = 0$ for all finite n, i.e. if all elements of $K \cap k^{1/p}$ have height $\geq \omega$, then K is relatively perfect over k.*

(c) *If for some α one has $f_{\alpha+n}(K/k) = 0$ for all finite n, then the length of K/k is $\leq \alpha$.*

(d) *If K is a tensor product of simple extensions, then K/k has length $\leq \omega$, and $f_n(K/k)$ equals the number of tensor generators of degree p^{n+1}.*

Proof. Statement (a) is obvious, (d) is a straightforward computation, and (b) is a paraphrase of 2.2. Then (c) follows by applying (b) to $(K/k)^\alpha$, which is modular over k by 4.1.

Proposition 4.3. *Let K/k be modular. Let n and r be finite with $r \geq 2$. Then*

(a) *$f_n(K/k) = f_n(K \cap k^{1/p^{n+r}}/k)$ and*

(b) *$f_n(K/k) = f_n(K/(K/k)^{n+r})$.*

Proof. By 1.5 we have $k^{1/p} \cap kK^{p^s} = k[k^{1/p} \cap K^{p^s}]$. But obviously for $n + r > s$ we have $k^{1/p} \cap K^{p^s} = k^{1/p} \cap (K \cap k^{1/p^{n+r}})^{p^s}$. Thus the same fields occur in computing both sides of (a).

Write $L = kK^{p^n}$; then (b) says that

$$|k^{1/p} \cap L : k^{1/p} \cap kL^p| = |(kL^{p^r})^{1/p} \cap L : (kL^{p^r})^{1/p} \cap kL^p|.$$

Thus it suffices to show that $k^{1/p} \cap L$ and $(kL^{p^r})^{1/p} \cap kL^p$ are linearly disjoint with intersection $k^{1/p} \cap kL^p$ and join $(kL^{p^r})^{1/p} \cap L$. Obviously the intersection is right. We have kL^p and $k^{1/p}$ linearly disjoint since the former is modular over k; similarly L and $(kL^{p^r})^{1/p}$ are linearly disjoint. Hence by 1.1 we have the necessary linear disjointness.

To show the join is as large as claimed, we write L as a directed union of finite modular extensions; if the join is large enough for each of them, it is so for their union. Thus we may assume L/k finite. Write it as a tensor product of $k(x_i)$ with x_i of exponent e_i. Then the elements with pth power in kL^{p^r} are generated by $x_i^{d_i}$ where $d_i = p^{e_i-1}$ if $e_i < r$ and $d_i = p^{r-1}$ if $e_i \geq r$. The last type are in $(kL^{p^r})^{1/p} \cap kL^p$, and the others are in $k^{1/p} \cap L$.

Lemma 4.4. *Let K/k be modular, B a pure modular subextension over which K is relatively perfect. Then the Ulm invariants of K over kK^{p^n} equal those of B over kB^{p^n}.*

Proof. By hypothesis B and kK^{p^n} are linearly disjoint with intersection kB^{p^n} and join K. Thus a pure independent set giving tensor generators for B over kB^{p^n} also gives tensor generators for K over kK^{p^n}.

Theorem 4.5. *Let K/k be modular. Let X be any maximal pure independent set. Then the number of elements of X having degree p^{n+1} is $f_n(K/k)$, and thus is independent of the choice of X.*

Proof. By 2.3 we know $B = k(X)$ is a basic subfield, and by 4.2 (d) the number of elements involved is $f_n(B/k)$. But $f_n(B/k) = f_n(B/kB^{p^{n+2}}) = f_n(K/k K^{p^{n+2}}) = f_n(K/k)$.

5. Ulm invariants and group algebras. In this section we will compute the invariants of §4 by a process which explicitly connects them with the usual Ulm invariants for groups. Recall [1, p. I-154] that if G is a p-primary abelian group, the subgroups $p^\alpha G$ are defined inductively by $p^{\alpha+1}G = p(p^\alpha G)$, starting with $p^0 G = G$ and setting $p^\alpha G = \bigcap \{p^\beta G | \beta < \alpha\}$ for α a limit ordinal. If $G[p]$ denotes $\{g \in G | pg = 0\}$, then the groups $p^\alpha G \cap G[p]$ are vector spaces over F_p, and (in Kaplansky's terminology) the codimension of $p^{\alpha+1}G \cap G[p]$ in $p^\alpha G \cap G[p]$ is the αth *Ulm invariant* of G, denoted $f_\alpha(G)$.

Let k now be a field of characteristic p, and A a commutative k-algebra; we can define $(A/k)^\alpha$ inductively just as for field extensions. If L is a larger field, it is easy to show inductively that $(A \otimes_k L/L)^\alpha =$

$(A/k)^{\alpha} \otimes_k L$. If $A = k[G]$, moreover, a simple induction using the standard basis shows that $(A/k)^{\alpha} = k[p^{\alpha}G]$.

With the proper tool, the Ulm invariants of G can now be recovered from $k[G]$. If A is any (commutative) local k-algebra with residue field k, let M be its maximal ideal and J the ideal $\{a \in A | a^p = 0\}$. We define the *Ulm space* $\mathfrak{U}(A)$ to be J/MJ. Clearly $A \mapsto \mathfrak{U}(A)$ is a functor from such algebras to vector spaces over k.

Proposition 5.1. *Let G be a p-primary abelian group, k a field of characteristic p. Then there is a natural isomorphism*

$$G[p] \otimes_{\mathbf{F}_p} k \xrightarrow{\sim} \mathfrak{U}(k[G]).$$

Proof. We show first that J is generated by the elements $g - 1$ for $g \in G[p]$; it is enough to show this for G finite, since any G is a directed union of finite subgroups. If $\{g_i\}$ are basic generators for a finite G, then $k[G]$ has the form $k[X_1, \cdots, X_n]/(X_1^{q_1}, \cdots, X_n^{q_n})$, where $X_i = g_i - 1$ and g_i has order $q_i = p^{e_i}$. Clearly two different monomials here have equal pth powers only if both collapse to zero, and the pth power of a monomial is zero only if it involves a factor $X_i^{q_i/p} = g_i^{q_i/p} - 1$. This yields the desired statement.

We thus have a natural map $G[p] \to \mathfrak{U}$ sending g to the class of $g - 1$. If g and h are in $G[p]$, then $gh - 1 = (g - 1) + (h - 1) + (g - 1)(h - 1)$ and the last term is in MJ; thus $G[p] \to \mathfrak{U}$ is $\mathbf{F}_p$-linear. Any multiple of $(g - 1)$ has the form (scalar)$(g - 1)$ + (element of M)$(g - 1)$, so the image of $G[p]$ spans $\mathfrak{U}$ over k.

When G is finite, the map from $G[p] \otimes k$ is injective as well as surjective; this is clear from direct inspection of $k[G]$, as above. If then $G_1 \subseteq G_2$ are finite, $G_1[p]$ injects into $G_2[p]$, and hence accordingly $\mathfrak{U}(k[G_1])$ injects into $\mathfrak{U}(k[G_2])$. Since $\mathfrak{U}(k[G])$ in general is the direct limit of the Ulm spaces of finite subgroup algebras, it follows that $G[p] \otimes k$ always injects into $\mathfrak{U}(k[G])$.

Corollary 5.2. *Each $\mathfrak{U}((k[G]/k)^{\alpha})$ injects into $\mathfrak{U}(k[G])$, and the co-dimension of $\mathfrak{U}((k[G]/k)^{\alpha+1})$ in $\mathfrak{U}((k[G]/k)^{\alpha})$ is $f_{\alpha}(G)$.*

In particular, of course, the Ulm invariants of G are determined by the algebra $k[G]$; a less transparent proof of this fact was given in [4]. We may note that $\dim_{\mathbf{F}_p} G[p] \cap p^{\infty}G$, which is the number of $Z[p^{\infty}]$ summands in G, is similarly determinable from the Ulm space of $k[G]$.

For arbitrary algebras $\mathfrak{U}(A)$ may be zero, or the $\mathfrak{U}((A/k)^{\alpha})$ may not

inject into $\mathfrak{U}(A)$. When they do, however, it is natural to call the codimensions in 5.2 the *Ulm invariants of* A. The Ulm invariants of §4 can be recovered by precisely this process, as we now show.

Theorem 5.3. *Let* K/k *be modular. Let* L *be the perfect closure of* k, *and let* A *be the* L-*algebra* $K \otimes_k L$. *There is a natural map from* $K \cap k^{1/p}$ *to* $\mathfrak{U}(A)$ *sending* x *to the class of* $x \otimes 1 - 1 \otimes x$. *Under this map a set* $\{x_i\}$ *goes to a basis (resp. an independent set, a spanning set) if and only if* $\{x_i\}$ *is a p-basis (resp. a p-independent set, a generating set) for* $K \cap k^{1/p}$ *over* k.

Proof. Suppose first that K/k is finite and $K \subseteq k^{1/p}$; let $\{x_i\}$ be a p-basis of K over k. Then the x_i are tensor product generators, and $K \otimes L$ is $\bigotimes L[X_i]/X_i^p$ where $X_i = x_i \otimes 1 - 1 \otimes x_i$. Clearly then the images of the x_i are a basis for $\mathfrak{U}(K \otimes L)$. Passing to a direct limit over finite subextensions we see that the same result holds for infinite $K \subseteq k^{1/p}$. Furthermore, any p-independent set can be expanded to a p-basis, and so must go to an independent set; similarly any generating set contains a p-basis, and hence goes to a spanning set. In addition, if F is an intermediate field, then a p-basis of F extends to one of K, and thus $\mathfrak{U}(F \otimes L)$ injects into $\mathfrak{U}(K \otimes L)$.

Still assuming $K \subseteq k^{1/p}$, let $\{x_i\}$ be elements whose images are independent. If the x_i are not p-independent, some one of the x_1 is in the field F generated over k by the others. The images of x_i for $i \neq 1$ then span $\mathfrak{U}(F \otimes L)$, so the image of x_1 is dependent on them there and hence is dependent on them in $\mathfrak{U}(K \otimes L)$. This is impossible, and so the x_i are p-independent. If on the other hand $\{x_i\}$ is a set of elements whose images span $\mathfrak{U}(K \otimes L)$, let F be the subextension they generate. If F is not all of K we can choose a p-basis of F and extend it to a p-basis of K; we get thereby an element in $\mathfrak{U}(K \otimes L)$ not in $\mathfrak{U}(F \otimes L)$, which is impossible since $\mathfrak{U}(F \otimes L)$ contains the images of the x_i. Thus the theorem is completely proved for the case $K \subseteq k^{1/p}$.

Now let K/k be arbitrary finite modular with tensor product generators y_i having degrees $q_i = p^{e_i}$. Then $K \otimes L$ is $\bigotimes L[Y_i]/(Y_i^{q_i})$ where $Y_i = y_i \otimes 1 - 1 \otimes y_i$. The computation in 5.1 shows that the elements $Y_i^{q_i/p}$ give a basis for $\mathfrak{U}(K \otimes L)$. But the elements $y_i^{q_i/p}$ are a p-basis for $K \cap k^{1/p}$, and hence go to a basis for $\mathfrak{U}((K \cap k^{1/p}) \otimes L)$. Since a basis thus goes to a basis, the map $\mathfrak{U}((K \cap k^{1/p}) \otimes L) \to \mathfrak{U}(K \otimes L)$ is an isomorphism. Writing any modular K/k as a direct limit of finite modular extensions, we see that the map is still an isomorphism there. Hence the theorem is reduced to $K \cap k^{1/p}$, where we have proved it.

Porism 5.4. *If F is an intermediate field modular over k, then $\mathfrak{U}(F \otimes L)$ $\rightarrow \mathfrak{U}(K \otimes L)$ is an injection.*

Corollary 5.5. *If K/k is modular, then the Ulm invariants of K/k are the same as the Ulm invariants of the algebra $K \otimes L$.*

Proof. The p-rank of $(K/k)^\alpha \cap k^{1/p}$ over $(K/k)^{\alpha+1} \cap k^{1/p}$ equals the number of elements added to a p-basis of the latter over k to get a p-basis of the former over k. Thus it equals the codimension of $\mathfrak{U}((K/k)^{\alpha+1} \otimes L)$ in $\mathfrak{U}((K/k)^\alpha \otimes L)$. The p-rank is $f_\alpha(K/k)$; the codimension is the Ulm invariant of $K \otimes L$, since $(K/k)^\alpha \otimes L = (K \otimes L/L)^\alpha$.

This need not be true, with the definition of §4, if K/k is not modular. If one wants to define Ulm invariants for nonmodular extensions, they should probably be the invariants of $K \otimes L$.

Corollary 5.6. *If K/k is modular and is a form of a group algebra, i.e. $K \otimes L$ is isomorphic to a group algebra $L[G]$, then $f_\alpha(K/k) = f_\alpha(G)$.*

Theorem 5.7. *Let K/k be modular, L the perfect closure of k, and α a limit ordinal. Then*

$$\mathfrak{U}((K/k)^\alpha \otimes L) = \bigcap \{\mathfrak{U}((K/k)^\beta \otimes L) \,|\, \beta < \alpha\}.$$

Proof. We of course use 5.4 to identify these spaces with subspaces of $\mathfrak{U}(K \otimes L)$. The inclusion $\subseteq$ is obvious. Take then an element v in the right-hand side. It can be expressed using finitely many elements from $K \cap k^{1/p}$; among such expressions choose one using the smallest number of elements not in $(K/K)^\alpha \cap k^{1/p}$. Let M be the intermediate field generated by these elements. We clearly must have M linearly disjoint from $(K/k)^\alpha \cap k^{1/p}$ over k, as otherwise we could drop one of the generators of M and still span the same space together with $\mathfrak{U}((K/k)^\alpha \otimes L)$.

Lemma 5.8. *Let K/k be algebraic. Let $\{E_\beta\}$ be a family of intermediate fields directed by inverse inclusion, and let $E = \bigcap E_\beta$. Suppose M is an intermediate field linearly disjoint from E with $|ME : E|$ finite. Then M is linearly disjoint from all sufficiently small E_β.*

Proof. Let B be a linear basis for M over $M \cap E$; it is then a basis for ME over E, and so is finite. Choose any β; then we choose a subset B_β of B which is a basis for ME_β over E_β. Consider some $E_\gamma \subseteq E_\beta$; if B_β is no longer a basis of ME_γ over E_γ it can be expanded to a larger subset B_γ which is. Since B is finite, successive expansions in this way must eventually stop; thus we get an E_γ and a subset B_γ of B

such that B_γ is a basis of ME_δ over E_δ whenever $E_\delta \subseteq E_\gamma$. Obviously it is enough now to show $B_\gamma = B$. Suppose therefore that there is some b in $B \backslash B_\gamma$. We can write $b = \Sigma a_i b_i$ uniquely with $b_i \in B_\gamma$ and $a_i \in E_\gamma$. The same is true for each smaller E_δ, so the a_i are in $\bigcap \{E_\delta | E_\delta \subseteq E_\gamma\}$. But that intersection is E, since the original intersection was directed; and thus we have a contradiction.

Applying this lemma in our previous situation, we see that M is linearly disjoint from all sufficiently small $(K/k)^\beta \cap k^{1/p}$. Since M is finite, the intersection of the two will also be k eventually. But now we can choose a p-basis X_1 of $(K/k)^\alpha \cap k^{1/p}$, expand it to a p-basis $X_1 \cup X_2$ of $(K/k)^\beta \cap k^{1/p}$, and add in a p-basis X_3 of M while still staying independent. In $\mathfrak{U}(K \otimes L)$ the images $Y_1 \cup Y_2 \cup Y_3$ will then be linearly independent. The set $Y_1 \cup Y_2$ spans $\mathfrak{U}((K/k)^\beta \otimes L)$, so v is in its span; and by definition of M we have v in the span of $Y_1 \cup Y_3$. But that implies v is in the span of Y_1, i.e. v is in $\mathfrak{U}((K/k)^\alpha \otimes L)$.

This is a nontrivial property which $K \otimes L$ shares with group algebras; there are other algebras for which it is false.

6. An existence theorem.

Theorem 6.1. *Let G be a p-primary abelian group. Then there is a modular extension K/k which is a form of $k[G]$, in fact for which $K \otimes_k K \simeq K[G]$.*

Proof. Let F be a field of characteristic p. Let $0 \to R \to P \to G \to 0$ be a resolution of G with P and hence R free abelian groups. Then $F[P]$ is equal to $F[\{X_\alpha, 1/X_\alpha\}]$ where X_α runs over a basis of P; in particular it is an integral domain, and $F[R]$ is a subdomain. Let K and k be their fraction fields. It is easy to verify that $X_\alpha \otimes X_\beta \mapsto \overline{X}_\alpha \otimes X_\alpha X_\beta$ defines an isomorphism

$$F[P] \otimes_{F[R]} F[P] \xrightarrow{\sim} F[G] \otimes_F F[P].$$

Now since G is torsion, $F[P]$ is integral over $F[R]$, and hence $K = F[P] \otimes_{F[R]} k$. Tensoring the above isomorphism with k then yields

$$K \otimes_k K \xrightarrow{\sim} F[G] \otimes_F K = K[G].$$

It now follows automatically that K/k is modular. For if E is a finite subextension, $E \otimes_k K$ is isomorphic to a subalgebra of $K[G_0]$ for some finite subgroup G_0 of G. It follows [6, p. 423] that $E \otimes_k K$ is split, and so K contains the splitting field $S(E/k)$. Hence K/k is modular by 1.3.

Corollary 6.2. *Let λ be any ordinal. Then there is a modular K/k with $(K/k)^\lambda = k$ and length precisely λ.*

Proof. It is known [1, pp. II-57 and II-210] that there is a group G with $p^\lambda G = 0$ and $p^\beta G \neq 0$ for $\beta < \lambda$. Take K/k in the theorem corresponding to this G, noting that we already know $(K/k)^\beta \otimes K = (K[G]/K)^\beta = K[p^\beta G]$.

Corollary 6.3. *If K/k is a countable-dimensional modular extension, then $\alpha \mapsto f_\alpha(K/k)$ is a function from countable ordinals to cardinals $\leq \aleph_0$ with the following properties:*

(i) *it is identically zero from some point on, and*

(ii) *it nowhere has an infinite string of successive zero values followed by a nonzero value.*

Conversely, any such function arises from some countable-dimensional modular extension.

Proof. Condition (ii) is 4.2(c). Since $\mathfrak{U}(K \otimes L)$ is countable-dimensional, clearly all f_α are $\leq \aleph_0$; also there cannot be an uncountable well-ordered chain of subspaces, so (i) holds. The converse follows from combining 6.1, 5.6, and the corresponding existence theorem for countable groups [1, p. II-65], since in 6.1 we clearly have $(K : k) = \#(G)$.

Remark. In the construction of 6.1 any subgroup of G will correspond to an intermediate modular field (though of course there will be many other intermediate fields also). Examples of subgroups with certain properties can often therefore be carried over to examples on fields. For instance, there are well-known examples showing that one basic subgroup may be properly contained in another, and that a pure subgroup of unbounded height need not be a direct summand; as mentioned in §2, these yield corresponding examples for fields.

7. Complications and counterexamples. In this section we show that two analogues of abelian group theorems are false for fields. The first corresponds to the famous theorem of Prüfer[1, p. I-88] that countable primary groups with no elements of infinite height are direct sums of cyclic groups.

Proposition 7.1. *There is a countable-dimensional modular extension K/k with $(K/k)^\omega = k$ which is not a tensor product of simple extensions.*

Proof. Let $k = F_p(b, a_0, a_1, a_2, a_3, \cdots)$ where b and the a_i are indeterminates. Let $y_0 = b^{1/p}$ and $x_n = a_n^{1/p}$. Define inductively $y_n = y_{n-1} + x_{n-1}x_n$ for $n = 1, 2, 3, \cdots$. Let

$$K_n = k(y_n^{1/p^n}, x_0, x_1^{1/p}, x_2^{1/p^2}, x_3^{1/p^3}, \ldots, x_n^{1/p^n}).$$

Since $x_0, x_1, x_2, \cdots, x_n, y_n$ in $k^{1/p}$ are p-independent over k, we see that K_n is modular over k with its listed generators as tensor generators. We have $K_{n-1} \subseteq K_n$, and hence $K = \bigcup K_n$ is a modular extension of k. Since we know tensor generators, it is evident that $kK_n^{p^r} \cap k^{1/p}$ equals k for $r > n$ and equals $k(y_n, x_r, x_{r+1}, \cdots, x_n)$ for $r \leq n$. Hence $kK^{p^r} \cap k^{1/p}$ is $k(y_r, x_r, x_{r+1}, x_{r+2}, \cdots)$.

To show now $(K/k)^\omega = k$ it suffices to show $\bigcap (kK^{p^r} \cap k^{1/p}) = k$, since an extension with no elements of exponent 1 is trivial. Clearly $kK^{p^{n+1}} \cap k(y_0, x_0, \cdots, x_{n+1}) = k(y_{n+1}, x_{n+1})$; if we show $k(y_{n+1}, x_{n+1}) \cap k(y_0, x_0, \cdots, x_n) = k$ that will suffice, since $k^{1/p} = \bigcup k(y_0, x_0, \cdots, x_n)$.

Let E be $k(y_{n+1}, x_{n+1}) \cap k(y_0, x_0, \cdots, x_n)$. Considering dimensions over k and noting that the join of the two fields is $k(y_0, x_0, \cdots, x_{n+1})$, we see that either $E = k$ or $|E : k| = p$; and in the latter case the two fields are linearly disjoint. Now x_{n+1} is not in $k(y_0, x_0, \cdots, x_n)$, so 1 and x_{n+1} are linearly independent over that field. We have the relation $y_{n+1} = (x_n)x_{n+1} + (y_n)1$ over $k(y_0, x_0, \cdots, x_n)$, and by linear independence the coefficients are unique. If the two fields are linearly disjoint, there must be such a relation over E, and by uniqueness it must be the same relation. Hence $x_n, y_n \in E$, an impossibility since they are p-independent over k and $|E : k| \leq p$. This contradiction proves $(K/k)^\omega = k$.

If K/k were a tensor product of simple extensions, then any finite subextension F of $K \cap k^{1/p}$ would be contained in a finite subextension F' of $K \cap k^{1/p}$ with K/F' modular. Thus we can complete the proof as follows. Let $F = k(y_0, x_0)$. We will show that if $F \subseteq F' \subseteq K \cap k^{1/p}$ and K/F' modular, then $F' = K \cap k^{1/p}$. This we do by proving inductively that $k(y_0, x_0, \cdots, x_n) \subseteq F'$ implies $x_{n+1} \in F'$.

By 1.4(a) we have F' and kK^{p^r} linearly disjoint for all r, and hence F' is linearly disjoint from $kK^{p^{n+1}} \cap k^{1/p} = k(y_{n+1}, x_{n+1}, x_{n+2}, \cdots)$. Call the latter field T. Since by induction $y_0, x_0, \cdots, x_n$ are in F', we have y_n also in F'. The relation $y_n = (-x_{n+1})x_n + (y_{n+1})1$ expresses $y_n \in F$ in terms of $x_n, 1 \in F$ over T; since $x_n \notin T$ the expression is unique. By linear disjointness then the coefficients must be in $T \cap F'$, and thus $x_{n+1} \in F'$.

This example illustrates why linear disjointness has to enter as a "straightening condition" in many of the earlier proofs. In particular, it shows that the condition "K/S_n modular" cannot be dropped from 3.1(iii). For in our example the countability of $K \cap k^{1/p}$ automatically makes it a

union of a chain of finite-dimensional intermediate fields S_n; and each S_n has bounded height in K, since it is finite and $\bigcap k K^{p^r} = k$. Yet K/k is not a tensor product of simple extensions.

Theorem 7.2. *Let m be any infinite cardinal. Then there is a modular extension K/k with $|K:k| = m$ having $(K/k)^\omega = k$ and $f_n(K/k) = 1$ for all finite n.*

Proof. We first claim that if F is a field of cardinality m, then $F^{\aleph_0}$ as an F-space has dimension at least m. (It follows easily that its dimension is precisely $m^{\aleph_0}$, but that will not matter.) Suppose indeed that we have a basis of the product containing fewer than m elements; obviously for this to happen m must be uncountable. The entries in the basis vectors then form a set of cardinality less than m, and so generate over the prime field a subfield L of cardinality less than m. Now an F-linear combination of elements in $L^{\aleph_0}$ must have all its entries in a finite-dimensional L-subspace of F. But $\#(F) = m > \#(L)$ certainly implies $|F:L|$ infinite, so we can produce an element in $F^{\aleph_0}$ not having all its entries in such a finite-dimensional space.

Now let F be a perfect field of cardinality m. Choose m linearly independent elements in $F^{\aleph_0}$ starting with the elements e_n which are 1 in the nth place and 0 elsewhere. Let V be the F-space spanned by these m elements. Let V_n be the elements in V with first n entries equal to 0. Then we have a chain of subspaces $V = V_0 \supset V_1 \supset V_2 \supset \cdots$ where $\dim V = m$, $\dim V_n/V_{n+1} = 1$ for all n, and $\bigcap V_n = 0$.

Let $k = F(V)$, the fraction field of the free commutative algebra on the vector space; it is a pure transcendental extension of F with transcendence basis = a linear basis of V = a p-basis of k over k^p. Let K_1 be $k[V^{1/p}]$, that is, $k[\{x^{1/p} | x \in V\}]$; since F is perfect this is the same as adjoining to k the pth roots of the elements in a basis of V. Inductively define

$$K_n = K_{n-1}[V_{n-1}^{1/p^n}] = k[e_0^{1/p}, e_1^{1/p^2}, \ldots, e_{n-2}^{1/p^{n-1}}, V_{n-1}^{1/p^n}].$$

Clearly K_n/k is modular, and hence $K = \bigcup K_n$ is modular over k. Obviously $|K:k| = m$. We have $k K_n^{p^r} \cap k^{1/p} = k[V_r^{1/p}]$ for $n > r$, and thus $(K/k)^r \cap k^{1/p} = k[V_r^{1/p}]$. Therefore $e_r^{1/p}$ is a p-basis for $(K/k)^r \cap k^{1/p}$ over $(K/k)^{r+1} \cap k^{1/p}$, and so $f_r(K/k) = 1$ for all finite r.

Finally, $(K/k)^\omega = k$ follows easily from 5.7. For it is enough to show $\mathfrak{U}((K/k)^\omega \otimes L)$ is trivial, and hence enough to show $\bigcap \mathfrak{U}((K/k)^r \otimes L) = 0$. But clearly $\mathfrak{U}(K \otimes L)$ is isomorphic to $V \otimes_F L$, with the subspaces isomorphic to $V_r \otimes_F L$; thus the result follows from $\bigcap V_r = 0$.

Corollary 7.3. *There are modular extensions K/k which are not forms of group algebras.*

Proof. Let K/k be as in the theorem, with $m > 2^{\aleph_0}$. If $K \otimes_k L$ were isomorphic to some $L[G]$, then by §5 we could conclude $p^\omega G = 0$ and $f_n(G) = 1$ for all finite n. But for abelian groups this implies [1, p. I-146] that $\#(G) \leq 2^{\aleph_0}$.

REFERENCES

1. L. Fuchs, *Infinite abelian groups*. Vols. I, II, Pure and Appl. Math., vol. 36, Academic Press, New York and London, 1970, 1973.   MR 41 #333.
2. N. Jacobson, *Lectures in abstract algebra*. Vol. III: *Theory of fields and Galois theory*, Van Nostrand, Princeton, N. J., 1964.   MR 30 #3087.
3. L. A. Kime, *Purely inseparable, modular extensions of unbounded exponent*, Trans. Amer. Math. Soc. 176 (1973), 335—349.   MR 47 #192.
4. W. May, *Commutative group algebras*, Trans. Amer. Math. Soc. 136 (1969), 139—149.   MR 38 #2224.
5. M. E. Sweedler, *Structure of inseparable extensions*, Ann. of Math. (2) 87 (1968), 401—410; ibid.(2) 89 (1969), 206—207.   MR 36 #6391; 38 #4451.
6. R. Rasala, *Inseparable splitting theory*, Trans. Amer. Math. Soc. 162 (1971), 411—448.   MR 44 #1648.

DEPARTMENT OF MATHEMATICS, CORNELL UNIVERSITY, ITHACA, NEW YORK 14853

Current address: Department of Mathematics, Pennsylvania State University, University Park, Pennsylvania 16802