EXTENSIONS OF NORMAL BASES AND COMPLETELY BASIC FIELDS

BY

CARL C. FAITH

A finite, separable, normal extension $\mathfrak{N}/\mathfrak{F}$, with Galois group $\mathfrak{G} = (S_1, S_2, \cdots, S_n)$ always possesses a basis of the form $w^{S_1}, w^{S_2}, \cdots, w^{S_n}$, $w \in \mathfrak{N}$, called a *normal basis of* $\mathfrak{N}/\mathfrak{F}$. Then, *$w$ generates a normal basis of* $\mathfrak{N}/\mathfrak{F}$, or w is a *normal basis element of* $\mathfrak{N}/\mathfrak{F}$. Many proofs of the existence of such a basis are available(1).

Now let Δ be any intermediate field, $\mathfrak{N} \supseteq \Delta \supseteq \mathfrak{F}$. We raise the following question: Does there exist a normal basis of $\mathfrak{N}/\Delta$ which is extendable to a normal basis of $\mathfrak{N}/\mathfrak{F}$, or equivalently, is it possible for an element w to generate a normal basis in both extensions? It is shown in Chapter I that the answer to this question is in the affirmative. Moreover, we show (Theorem 1.1) that one may choose w (when $\mathfrak{F}$ is infinite) independently of the intermediate field Δ, i.e., so that w generates a normal basis of $\mathfrak{N}/\Gamma$, for every intermediate field Γ. We call elements having this latter property *completely basic elements of* $\mathfrak{N}/\mathfrak{F}$.

Every completely basic element of $\mathfrak{N}/\mathfrak{F}$ is a normal basis element of this extension. It is natural to inquire into the special character of normal basis elements by asking whether each normal basis element is completely basic. Although in general the answer to this question is negative (certain cyclotomic extensions provide counterexamples), we are able to establish the existence of a significant class $\mathfrak{C}$ of those normal extensions, called *completely basic extensions*, for which every normal basis element is completely basic. For these extensions every normal basis element of $\mathfrak{N}/\mathfrak{F}$ is the extension of a normal basis of $\mathfrak{N}/\Delta$, for any intermediate field Δ. However, not every normal basis of $\mathfrak{N}/\Delta$ is extendable to normal basis of $\mathfrak{N}/\mathfrak{F}$ when $\Delta \neq \mathfrak{F}$ (Theorem 1.7).

In Chapter I, a new characterization of the normal basis elements in cyclic extensions is used, with practically no additional machinery, to establish the existence of various completely basic extensions, including the cyclic Kummer extensions. The extension of this latter result to an arbitrary Kummer extension $\mathfrak{K}/\mathfrak{F}$ is the main ingredient of Chapter II. The proof that $\mathfrak{K}/\mathfrak{F} \in \mathfrak{C}$ does not use the fact that every cyclic Kummer extension $\mathfrak{Z}/\mathfrak{F}$ belongs to $\mathfrak{C}$, even though it is known that $\mathfrak{K}$ is the direct product over $\mathfrak{F}$ of

Presented to the Society, April 14, 1956; received by the editors February 27, 1956.

(1) For example: Artin [2; 3] proves it when $\mathfrak{F}$ is infinite; Cassels and Wall [5] present a proof when $\mathfrak{F}$ is finite; During [6] and Stauffer [10] have proofs under the hypothesis that the characteristic of $\mathfrak{F}$ is not a prime dividing n. Nakayama [8] extends the results of Stauffer to the general case.

finitely many of the $\mathfrak{Z}$'s. What is lacking is a general theorem (α) which states: If every factorization of a normal extension $\mathfrak{N}/\mathfrak{F}$

$$(*) \qquad \mathfrak{N} = \mathfrak{N}_1 \times \mathfrak{N}_2 \times \cdots \times \mathfrak{N}_t \text{ over } \mathfrak{F}$$

has the property that $\mathfrak{N}_i/\mathfrak{F} \in \mathfrak{C}$, $i = 1, \cdots, t$, then $\mathfrak{N}/\mathfrak{F} \in \mathfrak{C}$. Hence, our proof that $\mathfrak{K}/\mathfrak{F} \in \mathfrak{C}$ uses properties of Kummer extensions in an essential way. One such property vital to our proof is the existence of a basis of elements of $\mathfrak{K}/\mathfrak{F}$ such that every linear combination of the basis elements (with coefficients in $\mathfrak{F}$) is a normal basis element of $\mathfrak{K}/\mathfrak{F}$ if and only if each coefficient is nonzero.

The Kummer extensions are examples of Abelian extensions which belong to $\mathfrak{C}$. One would like to obtain a determination (β) of all Abelian extensions $\mathfrak{A}/\mathfrak{F}$ which are members of $\mathfrak{C}$. $\mathfrak{A}/\mathfrak{F}$ has a factorization (*) where the factors are cyclic extensions $\mathfrak{Z}_e/\mathfrak{F}$ of prime power degrees. Theorem 2.3 (the converse of (α)) implies that in order that $\mathfrak{A}/\mathfrak{F} \in \mathfrak{C}$, it is necessary that each of the factors $\mathfrak{Z}_e/\mathfrak{F} \in \mathfrak{C}$. Thus, if ($\alpha$) were available, the determination (β) would be reduced to that of (γ) all cyclic extensions $\mathfrak{Z}_e/\mathfrak{F}$ of prime power degree p^e which belong to $\mathfrak{C}$. In fact, it is entirely possible that the result (α) for Abelian $\mathfrak{N}/\mathfrak{F}$ would be forthcoming, if (γ) were achieved.

Accordingly, Chapter III is aimed at the classification of (γ). This is achieved (Theorem 3.2) in the case where $\mathfrak{F}$ contains all roots of the polynomial $x^p - 1$. The determination of (γ) in the remaining case is an open problem.

I. Completely basic elements and fields

0. **Definitions.** For any two fields K and F, $K \supset F$ will mean $K \supseteq F$ but $K \neq F$. If Δ is any subfield of K containing F, then occasionally we shall say that Δ is a *subfield of* K/F. The group of all automorphisms of K which leave fixed each element of F is denoted by $\mathfrak{G}(K/F)$, or simply by $\mathfrak{G}(F)$, when there is no confusion concerning the containing field K. For each $x \in K$, and $S \in \mathfrak{G}(F)$, x^S denotes the image of x under the automorphism S. The *trace of* x *in* K/F is the sum $\sum x^S$, S ranging over $\mathfrak{G}(F)$. When K/F has degree n, and $\mathfrak{G}(F) = (S_1, S_2, \cdots, S_n)$, then K/F is *normal*.

1. **A characterization of normal bases in cyclic fields.** If K/F is an arbitrary normal extension with Galois group $\mathfrak{G} = (S_1, S_2, \cdots, S_n)$, it is known (see, for example, [4, p. 158, Proposition 13]) that

(1.1) *$u \in K$ generates a normal basis in K/F if and only if the matrix $(u^{S_i S_j})$ is nonsingular.*

However, when K/F is cyclic, (1.1) may be used to obtain the following characterization of normal bases which we believe is new.

Lemma 1.1. *Let K/F be cyclic of degree n, and let S denote a generating auto-*

morphism of K/F. Then, u is a normal basis element in K/F if and only if the roots of the polynomial

$$u(x) = u + u^S x + \cdots + u^{S^{n-1}} x^{n-1} \tag{1.2}$$

do not include an n root of unity.

Proof. One easily observes that the matrix $A = (u^{S^{i+j}})$ is equivalent to the matrix

$$\begin{pmatrix} u, & u^S, \cdots, & u^{S^{n-1}} \\ u^{S^{n-1}}, & u, & \cdots, & u^{S^{n-2}} \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ u^S, & u^{S^2}, & \cdots, & u \end{pmatrix}, \tag{1.3}$$

so that A is nonsingular if and only if the polynomial

$$u(\zeta) = u + u^S \zeta + \cdots + u^{S^{n-1}} \zeta^{n-1} \tag{1.4}$$

in the algebraic closure $\overline{K}$ of K is nonzero for every $\zeta \in \overline{K}$ satisfying $\zeta^n = 1$.

We mention in passing that the quantities $u(\zeta^i)$, $i = 0, 1, \cdots, n-1$, where ζ is a primitive n root of unity, are the *Lagrange resolvents* of the equation $\prod_{i=0}^{n-1} (x - u^{S^i}) = 0$. Thus, when the characteristic of K does not divide n, the condition of Lemma 1.1 is that the n Lagrange resolvents $u(\zeta^i)$ are nonvanishing.

2. **Reduction theorems for modular fields.** Lemma 1.1 has several immediate implications when F has prime characteristic p dividing n. In this case, the fact that the algebraic closure of K contains fewer than n distinct n roots of unity, enables us to obtain the reduction criterion for a normal basis given by Lemma 1.3. The following lemma, however, is valid in an arbitrary cyclic field.

LEMMA 1.2. *Let K/F be cyclic of degree m, and let N be the unique subfield of K/F of degree n over F, where n is any integer dividing m. Then, $v = T_{K/N}(u)$ is a normal basis element of N/F if and only if the polynomial $u(x)$ defined by* (1.2) *for K/F has no root which is an n root of unity.*

Proof. Let $\mathfrak{G}(F) = (S)$, $u(x) = u + u^S x + \cdots + u^{S^{m-1}} x^{m-1}$, and let ζ be an n root of unity in some field containing K. Also let $T = S^n$. Then, $u(\zeta) = v + v^S \zeta + \cdots + v^{S^{t-1}} \zeta^{t-1}$, where $v = T_{K/N}(u) = u + u^T + \cdots + u^{T^{n-1}}$, and $t = m/n$. Since S induces a generating automorphism of N/F, $u(\zeta) = v(\zeta)$, where $v(x)$ is the polynomial (1.2) defined for $v \in N$ and the extension N/F. An application of Lemma 1.1 then concludes the proof.

Since the np^e roots of unity coincide with the n roots of unity in a field of characteristic p, Lemmas 1.1 and 1.2 may be employed to yield

LEMMA 1.3. *Let K/F be cyclic of degree $m = np^e$, where F has prime char-*

acteristic p, and let N be the unique subfield of K/F of degree n over F. Then, u is a normal basis element of K/F if and only if $T_{K/N}(u)$ is a normal basis element of N/F.

The normal basis elements of N/F when $N=F$ are precisely the nonzero elements of F. Thus, Lemma 1.3 gives an exact generalization of the striking lemma below. Our proof, however, does not require the existence of a normal basis for the extension as did Perlis' [9, Theorem 1].

LEMMA 1.4. *If K is cyclic of degree $n=p^e$ over a field F having prime characteristic p, then u is a normal basis element of K/F if and only if $T_{K/F}(u)\neq 0$*(2).

3. **Completely basic elements.** If Δ is any subfield of the normal extension K/F, then for any $u\in K$, $T_{K/F}(u)=T_{\Delta/F}(T_{K/\Delta}(u))\neq 0$ implies $T_{K/\Delta}(u)\neq 0$. Thus, for the extensions of Lemma 1.4, when u is a normal basis element of K/F, u is also a normal basis element of K/Δ. Accordingly we define a *completely basic element of K/F* to be a normal basis element of K/F which is also a normal basis element of K/Δ, for any intermediate field Δ. A modification of Artin's proof of the existence of a normal basis in K/F yields the existence of completely basic elements of K/F, when F is infinite.

THEOREM 1.1. *Each normal extension of an infinite field possesses a completely basic element.*

Proof. Let $K=F(\theta)$ be a normal extension of an infinite field F, let $\mathfrak{G}(F)=(S_1, S_2, \cdots, S_n)$, where $S_1=I$ is the identity automorphism, and let $f(x)$ be the minimal polynomial of θ over F. Also let

$$g_i(x) = g_1(x)^{S_i} = f(x)\left[(x-\theta^{S_i})f'(\theta^{S_i})\right]^{-1} \qquad (i=1, 2, \cdots, n),$$

$$g_{ij}(x) = g_i(x)^{S_j} = f(x)\left[(x-\theta^{S_iS_j})f'(\theta^{S_iS_j})\right]^{-1} \qquad (i, j=1, 2, \cdots, n),$$

where $f'(x)$ is the derivative of $f(x)$. Then, following Artin [2, Theorem 28],

$$g_i(\theta^{S_j}) = \delta_{ij} \qquad \text{(Kronecker } \delta\text{)},$$

and $\sum_{i=1}^{n} g_i(x)=1$. Then, for every i and j,

$$g_i(x)g_j(x) \equiv \delta_{ij}g_i(x) \qquad \text{(modulo } f(x)\text{)}. \tag{1.5}$$

Now let $\mathfrak{G}(\Delta)=(S_1, S_2, \cdots, S_t)$ denote the Galois group of K/Δ, where Δ is any intermediate field, and let $p(x)$ be the polynomial which is the determinant of the matrix $A(x)=(g_{ij}(x))$ with elements in $K[x]$. Using the fact that $p^2(x)=\det(AA')$, where A' denotes the transpose of $A=A(x)$, one determines (via congruences (1.5)) that $p^2(x)$ is congruent to the polynomial $h(x)\equiv\sum_{i=1}^{t} g_i(x)$ modulo $f(x)$.

(2) This result is extended in a following paper by the author [7] to the case where K is an arbitrary normal extension of F of degree p^e, and F has characteristic p. Moreover, it is shown there that these are the most general proper normal extensions for which every element with nonzero trace is a normal basis element.

Let $R_1, R_2, \cdots, R_s$ be a complete set of right coset representatives of $\mathfrak{G}(F)$ relative to $\mathfrak{G}(\Delta)$. Then, the fact that

$$\sum_{i=1}^{s} h(x)^{R_i} = \sum_{i=1}^{n} g_i(x) = 1$$

implies that $h(x)$ is not the zero polynomial. On the other hand, if $p(x)$ were the zero polynomial, $h(x)$ would be divisible by $f(x)$, which is impossible since the degree of $f(x)$ is equal to n, whereas $h(x)$ has degree less than n. Thus, $p(x)$ has only finitely many roots in F.

The normal extension K/F has only finitely many intermediate fields $\Delta_1, \Delta_2, \cdots, \Delta_q$. For each Δ_k define $p_k(x)$ in the manner $p(x)$ was defined for Δ, and choose $\alpha \in F$ such that $p_1(\alpha)p_2(\alpha) \cdots p_q(\alpha) \neq 0$. Let $u = g_1(\alpha)$, and let $\mathfrak{G}(\Delta_k) = (S_{1k}, S_{2k}, \cdots, S_{tk})$, $t = t(k)$. Then, the determinant of the matrix $A_k(\alpha) = (u^{S_{ik}S_{jk}})$ is equal to $\pm p_k(\alpha) \neq 0$, and hence u is a completely basic element of K/F according to (1.1).

When a normal extension K/F possesses a completely basic element a natural problem is the determination of all others, much in the manner the most general normal basis element is known when an arbitrary normal basis element is given in advance [10, Theorem 5]. Although we have not been able to do this, we have

THEOREM 1.2. *If u is any completely basic element of K/F, then so is each conjugate of u in K/F.*

Proof. If Δ is any intermediate field, and if S is any automorphism of K/F, one may show that u^S is a normal basis element of K/Δ if and only if u is a normal basis element of K over $\Delta^{S^{-1}}$. If u is completely basic in K/F, then u generates a normal basis in $K/\Delta^{S^{-1}}$, and hence u^S is a normal basis element of K/Δ, i.e., u^S is a completely basic element of K/F.

REMARK. If w is a normal basis element of K/Δ, then so is each conjugate of w in K/Δ. However, when in addition w is a completely basic element of K/F, the above theorem shows that each conjugate of w in K/F is a normal basis element of K/Δ.

4. **Composites and direct product fields.** In this section certain results on normal bases in fields which are direct products of subfields are established for later use.

First, however, let K/F be normal, and let F' be any extension of F. It is known that the composites(3) over F of K and F' are isomorphic over F, and hence are essentially unique. We now summarize some facts about the *composite $K' = KF'$ over F of K and F* which we need(4):

(1.6) *K'/F' is normal.*

(3) See [1, p. 161, Theorem 16] and the definitions, and [1, p. 180, Theorem 10].

(4) See [4, p. 149, Theorem 1] for proof of these facts.

(1.7) *The automorphisms of K'/F' induce distinct automorphisms of K/Q, where $Q=K\cap F'$, so that the Galois group of K'/F' is isomorphic to that of K/Q under the natural mapping.*

(1.8) *There is a* 1-1 *correspondence $\Delta\leftrightarrow\Delta'$ between the intermediate fields Δ of K/Q and those Δ' of K'/F': $\Delta'=\Delta F'=\Delta\times F'$ over Q; $\Delta=K\cap\Delta'$.*

The next theorem reduces the construction of a normal basis of a normal extension which is the direct product of subextensions to that of the subextensions. More explicitly one has

THEOREM 1.3. *Let K/F be a normal extension which is the direct product over F of t subfields K_i. Let $u=\prod_{i=1}^{t}u_i$, where each $u_i\in K_i$. Then, u generates a normal basis of K/F if and only if each u_i generates a normal basis of K_i/F. Moreover, each normal basis element of K_i/F is the trace in K/K_i of a normal basis element of K/F, $i=1, 2, \cdots, t$.*

Proof. An obvious induction reduces the proof to the case $t=2$. Let u_i be a normal basis element of K_i/F, $i=1, 2$. The Galois group $\mathfrak{G}(K/F)$ is the direct product of $\mathfrak{G}(K/K_1)$ and $\mathfrak{G}(K/K_2)$, and $\mathfrak{G}(K/K_i)$ coincides with $\mathfrak{G}(K_j/F)$, $i\neq j$, on elements of K_j. Since the set $\mathfrak{s}_j$ of conjugates of u_j in K_j/F, $j=1, 2$, forms a basis of K_j/F, the set $\mathfrak{s}$ of elements of K consisting of all possible products $\{\alpha\beta\}$, $\alpha\in\mathfrak{s}_1$, $\beta\in\mathfrak{s}_2$, is a basis of K/F. Moreover, $\mathfrak{s}$ is a normal basis generated by $u=u_1u_2$.

Conversely, suppose $u=u_1u_2$ generates a normal basis of K/F. Since

$$v_i = T_{K/K_i}(u) = u_i\cdot T_{K/K_i}(u_j) = u_i\cdot T_{K_j/F}(u_j) \qquad (i\neq j)$$

generates a normal basis([5]) of K_i/F, one observes that $u_i=\alpha_i^{-1}v_i$ generates a normal basis of K_i/F, where $\alpha_i=T_{K_j/F}(u_j)\in F$, $i\neq j$.

For the last statement in Theorem 1.3, suppose u_i is a normal basis element of K_i/F, $i=1, 2$. Then,

$$u_i = T_{K/K_i}(\alpha_i^{-1}u) \qquad (\alpha_i = T_{K_j/F}(u_j),\ i\neq j),$$

where $u=u_1u_2$, and $\alpha_i^{-1}u$ are clearly normal basis elements of K/F.

The proof of the above theorem has the following corollary which we shall use later.

THEOREM 1.4. *Let $K=K_1\times K_2$ over F be normal. If $u\in K_i$ generates a normal basis of K_i/F, then u also generates a normal basis of K/K_j, $i\neq j$.*

5. **Completely basic fields.** The extensions K/F of Lemma 1.4 have the property that every normal basis element of the extension is a normal basis element of K/Δ, where Δ is any intermediate field. We call normal extensions possessing this latter property *completely basic extensions*. Thus, for these ex-

([5]) A more general statement is that $T_{K/\Delta}(u)$ generates a normal basis of Δ/F whenever u generates a normal basis of K/F, where Δ is any intermediate field which is normal over F [9, Lemma 4].

tensions the set of completely basic elements coincides with the set of normal basis elements.

In this section, we derive conditions which are sufficient to show the existence of completely basic extensions other than those of Lemma 1.4. We begin with a lemma which contains a criterion for a normal basis element in a cyclic extension K/F to generate a normal basis in K over certain subfields.

THEOREM 1.5. *Let K/F be cyclic of degree $n=tr$. Let P denote the root field over F of the equation $x^t-1=0$, constructed to lie in a common field with K, and suppose $K\cap P=F$. Let T be the unique subfield of K/F of degree r over F. Then, every normal basis element of K/F generates a normal basis in K/Δ, for every subfield Δ of K/T.*

Proof. Suppose $u\in K$ is not a normal basis element of K/Δ. Let m be the degree of K/Δ so that m divides t. By Lemma 1.1 the polynomial $u(x)$ defined by (1.2) has a root $\zeta\in P$ obeying $\zeta^m=1$. Let $K'=K(\zeta)$, and $\Delta'=\Delta(\zeta)$. Since the Galois group of K'/Δ' coincides with that of K/Δ on K, the equation $u(\zeta)=0$ is a nontrivial relation, with coefficients in P, among the conjugates of u in K'/P. Thus, u is not a normal basis element of K'/P. By the Theorem 1.4, the element u cannot be a normal basis element of K/F. This completes the proof.

Putting $t=n$, we get $T=F$, and the corollaries

COROLLARY. *Let K/F be cyclic of degree n, and let P be as in Theorem* 1.5 *with $t=n$. Then, K/F is completely basic.*

COROLLARY. *If K/F is cyclic of degree n, and if F contains all of the roots of the equation $x^n-1=0$, then K/F is completely basic.*

This corollary implies that every cyclic Kummer extension([6]) is completely basic (a fact contained in Theorem 2.2), and is one indication of the extensiveness of the class of all completely basic extensions.

When $n=p^e$, and F has characteristic p, one deduces anew the

COROLLARY. *If K is cyclic of degree p^e over a field F of characteristic p, then K/F is completely basic*([7]).

The condition of the above corollaries which assures that the cyclic extension K/F of degree n is completely basic is that K contain no more of the n roots of unity that F does. This is the condition $K\cap F(\zeta)=F$. The next corollary is a further illustration of this principle.

COROLLARY. *Let K/F be cyclic of degree n, and suppose the cyclotomic polynomial $\Phi_n(x)$ is irreducible over K. Then K/F is completely basic.*

([6]) A definition of Kummer extension may be found in Chapter II.

([7]) This result has been extended by the author [7] to the case given in footnote 2. In this case, the Galois group of K/F may be even non-Abelian, hence establishing the existence of completely basic extensions which are non-Abelian.

Proof. Let ζ be a primitive n root of unity and let $K'=K(\zeta)$, $F'=F(\zeta)$. Since K'/K, $F'/K\cap F'$, and F'/F all have degree equal to $\phi(n)$, it follows that $K\cap F'=F$. The first corollary to Theorem 1.5 now asserts that K/F is completely basic.

The next theorem is the result of an attempt to obtain an analog of Lemma 1.4, under suitable hypotheses, in the case $\mathfrak{Z}_e$ is cyclic of degree p^e, p a prime, over a field $\mathfrak{F}$ of characteristic not p. We let $\mathfrak{Z}_i$ denote a subfield of $\mathfrak{Z}_e/\mathfrak{F}$ of degree p^i over $\mathfrak{F}$.

THEOREM 1.6. *Let $\Phi_n(x)$ be irreducible in $\mathfrak{Z}_e$, $n=p^e$, and suppose $u\in\mathfrak{Z}_e$ does not lie*(8) *in $\mathfrak{Z}_{e-1}$. Then, u generates a normal basis of $\mathfrak{Z}_e/\mathfrak{F}$ if and only if $T_{\mathfrak{Z}_e/\mathfrak{Z}_{e-1}}(u)$ generates a normal basis of $\mathfrak{Z}_{e-1}/\mathfrak{F}$.*

Proof. The necessity is evident. Now suppose u does not generate a normal basis of $\mathfrak{Z}_e/\mathfrak{F}$ while $T_{\mathfrak{Z}_e/\mathfrak{Z}_{e-1}}(u)$ generates a normal basis of $\mathfrak{Z}_{e-1}/\mathfrak{F}$. Then, by Lemmas 1.1 and 1.2, $u(x)$ has a root which is a primitive p^e root of unity. Since $\Phi_n(x)$ is irreducible in $\mathfrak{Z}_e$, $\Phi_n(x)$ divides $u(x)$. Then, necessarily $u=u^{S^t}=\cdots=u^{S^{(p-1)t}}$, where $t=p^{e-1}$. Hence, u must lie in $\mathfrak{Z}_{e-1}$. This contradiction completes the proof.

6. **Extensions of normal bases.** Let Δ be any intermediate field of the normal extension $\mathfrak{K}/\mathfrak{F}$. The existence of a completely basic element in $\mathfrak{K}/\mathfrak{F}$ implies the existence of a normal basis of $\mathfrak{K}/\Delta$ which is extendable to a normal basis of $\mathfrak{K}/\mathfrak{F}$. When $\mathfrak{K}/\mathfrak{F}$ is completely basic, every normal basis of $\mathfrak{K}/\mathfrak{F}$ is the extension of a normal basis of $\mathfrak{K}/\Delta$. We now show that not every normal basis of $\mathfrak{K}/\Delta$ is extendable to a normal basis of $\mathfrak{K}/\mathfrak{F}$ when Δ properly contains $\mathfrak{F}$.

THEOREM 1.7. *Let Δ be any intermediate field of the normal extension $\mathfrak{K}/\mathfrak{F}$, $\Delta\neq\mathfrak{F}$. If w is a normal basis element of $\mathfrak{K}/\Delta$, the element $\alpha^{-1}w$ is also, but $\alpha^{-1}w$ is not a normal basis element of $\mathfrak{K}/\mathfrak{F}$, where $\alpha=T_{\mathfrak{K}/\Delta}(w)$.*

Proof. The element $\alpha^{-1}w$ is clearly a normal basis element of $\mathfrak{K}/\Delta$, since $\alpha\neq 0\in\Delta$. Now let R_i, $i=1,\cdots,q$, be a complete set of right coset representatives of the Galois group of $\mathfrak{K}/\mathfrak{F}$ relative to the Galois group of $\mathfrak{K}/\Delta$. If x is any normal basis element of $\mathfrak{K}/\mathfrak{F}$, one may show quite in general that the elements $v_i=v^{R_i}$, $i=1,\cdots,q$, are linearly independent in $\mathfrak{F}$, where $v=T_{\mathfrak{K}/\Delta}(x)$. In the present case $x=\alpha^{-1}w$, so that the quantities $v^{R_i}=(\alpha\alpha^{-1})^{R_i}=1$ cannot be linearly independent in $\mathfrak{F}$, when $\Delta\supset\mathfrak{F}$. Thus, $\alpha^{-1}w$ is not a normal basis element of $\mathfrak{K}/\mathfrak{F}$.

II. KUMMER EXTENSIONS

1. **A characterization of Kummer extensions.** It may be recalled that a Kummer extension is an extension K which is the root field of a polynomial of the form $(x^n-a_1)(x^n-a_2)\cdots(x^n-a_k)$, for a fixed n, with the a_i in a field

(8) In other words, u is any generator of the extension $\mathfrak{Z}_e/\mathfrak{F}$. See [1, p. 193, Lemma 1].

F which contains a primitive n root of unity. However, it is more convenient for our purposes to use the following equivalent definition([9]):

DEFINITION. *A Kummer extension* K/F is an Abelian extension such that F contains a primitive r root of unity, where r is the least common multiple of the orders of the automorphisms of K/F.

A Kummer extension K/F has a factorization $K=\prod_{i=1}^{t} K_i$ over F into a direct product of cyclic subfields K_i of degrees $p_i^{e_i}$ over F, where each p_i is prime. The structure theory for cyclic extensions of prime power degrees([10]) asserts the existence of ξ_i, $\beta_i \in K_i$ such that $\xi_i^{\overline{S}_i}=\beta_i\xi_i$, $\xi_i^{p_i}\in N_i$, where $\overline{S}_i$ is a generating automorphism of K_i/F, and N_i is the unique subfield of K_i of degree $p_i^{e_i-1}$ over F. However, when F contains a primitive $p_i^{e_i}$ root of unity ζ_i it is known (e.g. [9, p. 512]) that we may take ξ_i such that

$$(2.1) \qquad K_i = F(\xi_i), \qquad \xi_i^{p_i^{e_i}} \in F, \qquad \xi^{\overline{S}_i} = \zeta_i\xi_i, \qquad (i = 1, \cdots, t).$$

Let $L_i=\prod_{i\neq j} K_i$, and $\mathfrak{G}_i$ denote the Galois group of K/L_i, $i=1, \cdots, t$. Then, the Galois group $\mathfrak{G}$ of K/F is the direct product $\prod_{i=1}^{t} \mathfrak{G}_i$; $\mathfrak{G}_i$ coincides with the Galois group $\overline{\mathfrak{G}}_i$ of K_i/F; and $\mathfrak{G}_i$ is the identity on K_j, $i\neq j$. With these preliminary considerations aside one may now prove

LEMMA 2.1. *A normal extension* K/F *with Galois group* $\mathfrak{G}=(R_1, R_2, \cdots, R_n)$ *is a Kummer extension if and only if* K/F *has a basis* $\theta_1, \theta_2, \cdots, \theta_n$ *such that the* n^2 *elements* $\gamma_{ij}=\theta_i^{-1}\theta_i^{R_j}$ *lie in* F.

Proof. If K/F is Kummer, let $K=\prod_{i=1}^{t} K_i$ over F, $K_i=F(\xi_i)$ as in (2.1). Any automorphism T of K/F has the form $T=\prod_{i=1}^{t} S_i^{\pi_i}$, where S_i is any automorphism of K/L_i which induces the generating automorphism $\overline{S}_i$ of K_i/F, $0\leqq\pi_i\leqq p_i^{e_i}-1$. Since

$$\prod_{i=1}^{t} (\xi_i^{\lambda_i})^T = \prod_{i=1}^{t} (\xi_i^T)^{\lambda_i} = \prod_{i=1}^{t} (\xi_i\zeta_i^{\pi_i})^{\lambda_i} = \left(\prod_{i=1}^{t} \xi_i^{\lambda_i}\right)\alpha$$

where $\alpha=\prod_{i=1}^{t} \zeta_i^{\lambda_i\pi_i}\in F$, one sees that the n elements $\{\xi_1^{\lambda_1}\xi_2^{\lambda_2}\cdots\xi_t^{\lambda_t}\}$ form the desired basis, $0\leqq\lambda_i<p_i^{e_i}$, $i=1, 2, \cdots, t$.

The converse may be deduced from the fact that γ_{ij} is a primitive k root of unity in F if the automorphism R_j has order k, and if $x=\sum_{i=1}^{n} \alpha_i\theta_i$ is an arbitrary element in K, then $x^{R_pR_q}=x^{R_qR_p}$, for any p, q.

Lemma 2.1 enables us to prove the following useful characterization of normal basis elements in Kummer fields.

LEMMA 2.2. *Let* K/F *be a Kummer extension with a basis* $\theta_1, \theta_2, \cdots, \theta_n$ *as in Lemma* 2.1. *Then,* $u=\sum_{i=1}^{n} \alpha_i\theta_i$ *is a normal basis element if and only if each* $\alpha_i\neq 0$, $i=1, 2, \cdots, n$.

([9]) Cf. definitions [2, p. 59] and [2, Theorem 25].

([10]) E.g. [1, Theorem 10].

Proof. The n conjugates $u^{R_j} = \sum_{i=1}^{n} \alpha_i \gamma_{ij} \theta_i$ form a basis of K/F if and only if the coefficient matrix $A = (\alpha_i \gamma_{ij})$ is nonsingular. Then, $\det A = (\prod_{i=1}^{n} \alpha_i) \cdot \det(\gamma_{ij}) \neq 0$. The existence of a normal basis of K/F for some choice of $\alpha_1, \alpha_2, \cdots, \alpha_n$ implies that $\det(\gamma_{ij}) \neq 0$. Thus, u is a normal basis element if and only if $\prod_{i=1}^{n} \alpha_i \neq 0$. This completes the proof.

2. **Intermediate fields of prime degree.** Let Δ be any intermediate field of the Kummer extension K/F. Since K/F is Abelian one can find a sequence of intermediate fields

$$F = \Delta_0 \subset \Delta_1 \subset \cdots \subset \Delta_{\lambda-1} \subset \Delta = \Delta_\lambda \subset \cdots \subset \Delta_m = K$$

such that Δ_i/Δ_{i-1} has prime degree, $i = 1, 2, \cdots, m$. Since each extension K/Δ_i, $i = 0, 1, 2, \cdots, m$, is also a Kummer extension, in order to prove that K/F is completely basic, it suffices to prove that every normal basis element of K/F generates a normal basis of K/Γ, where Γ is any intermediate field of prime degree over F. The lemma below is a start in this direction.

LEMMA 2.3. *Let K/F be a Kummer extension, and let $K = K_1 \times K_2 \times \cdots \times K_t$ over F as in the paragraph preceding Lemma 2.1. Then, every normal basis element of K/F generates a normal basis of K/Δ, where Δ is any subfield of some K_i/F of prime degree over F.*

Proof. Let $K_1 \supseteq \Delta$, say, so that Δ/F has degree $p = p_1$, K_1/F has degree p^e. Let $\theta_1, \theta_2, \cdots, \theta_m$ be the basis, and $\overline{R}_1, \overline{R}_2, \cdots, \overline{R}_m$ be the automorphisms, of K^*/F given by Lemma 2.1, where $K^* = K_2 \times \cdots \times K_t$ over F. Let S be an automorphism of K/K^* which induces the generating automorphism $\overline{S}$ of K_1/F, where $K_1 = F(\xi)$, $\xi^{\overline{S}} = \zeta\xi$, $\xi^{p^e} \in F$, as before, and ζ is a primitive p^e root of unity in F. Then the set

$$\xi^i \theta_j \qquad (i = 0, 1, \cdots, p^e - 1, j = 1, 2, \cdots, m) \tag{2.2}$$

is a basis of K/F. Moreover, since the automorphism group of K/F consists of

$$S^i R_j \qquad (i = 0, 1, \cdots, p^e - 1, j = 1, 2, \cdots, m),$$

where R_j is the automorphism of K/K_1 which induces the automorphism $\overline{R}_j$ of K^*, $j = 1, 2, \cdots, m$, one notes that the basis (2.2) satisfies the hypothesis of Lemma 2.2.

Now let $u = \sum_{i,j} \alpha_{ij} \xi^i \theta_j$, $\alpha_{ij} \in F$, $i = 0, 1, \cdots, p^e - 1$, $j = 1, 2, \cdots, m$, be any element in K, and write i in the form

$$i = \lambda s + \pi \qquad (0 \leqq \lambda < p, s = p^{e-1}, 0 \leqq \pi < s).$$

Then, $u = \sum_{i=0}^{s-1} \sum_{j=1}^{m} \delta_{ij} \xi^i \theta_j$, where

$$\delta_{ij} = \sum_{\lambda=0}^{p-1} \alpha_{\lambda s+\pi, j} \xi^{\lambda s} \qquad (i = 0, 1, \cdots, s - 1, j = 1, 2, \cdots, m). \tag{2.3}$$

Since ξ^s is left fixed by S^p, and since the set $\{\xi^{\lambda s}\}$ is linearly independent over

F, one observes that set $\{\xi^{\lambda s}\}$, $\lambda = 0, 1, \cdots, p-1$, is a basis of Δ/F, and the elements (2.3) lie in Δ. If u is a normal basis element of K/F, the coefficients α_{ij}, $i = 0, 1, 2, \cdots, p^e-1$, $j = 1, 2, \cdots, m$, are all nonzero so that the coefficients δ_{ij} of (2.3) are nonzero also. Inasmuch as the basis of K/Δ consisting of the elements $\{\xi^i\theta_j\}$, and the automorphisms $\{S^{ip}R_j\}$, $i = 0, 1, \cdots, s-1$, $j = 1, 2, \cdots, m$, satisfy the conditions of Lemma 2.2, one readily observes that u generates a normal basis of K/Δ also.

3. **Direct factorizations of certain subgroups of Abelian groups.** The problem of showing that each Kummer extension K/F is completely basic has been reduced to that of showing every intermediate field Δ of prime degree over F is obtainable as in Lemma 2.3. This latter problem may be generalized: If Δ is any intermediate field of an Abelian extension K/F, does there exist a factorization of K

$$K = K_1 \times K_2 \times \cdots \times K_t \text{ over } F, \tag{2.4}$$

where each K_i/F is cyclic of degree $p_i^{e_i}$, p_i prime, $i = 1, 2, \cdots, t$, such that

$$\Delta = (\Delta \cap K_1) \times (\Delta \cap K_2) \times \cdots \times (\Delta \cap K_t) \text{ over } F? \tag{2.5}$$

(Of course, when the primes p_i are distinct, K and Δ have unique factorizations satisfying (2.4) and (2.5)).

One obtains, via the Galois theory, a similar consideration in the setting of groups, namely: If $\mathfrak{G}$ is any subgroup of an Abelian group G of finite order, does there exist a factorization of G into the direct product

$$G = (g_1) \otimes (g_2) \otimes \cdots \otimes (g_t) \tag{2.6}$$

where g_i has order $p_i^{e_i}$, p_i prime, $i = 1, 2, \cdots, t$, such that for suitable integers x_i, $i = 1, 2, \cdots, s$, $s \leqq t$,

$$\mathfrak{G} = (g_1^{x_1}) \otimes (g_2^{x_2}) \otimes \cdots \otimes (g_s^{x_s})? \tag{2.7}$$

((g) denotes the cyclic group generated by $g \in G$.)

Unfortunately, one's aesthetic inclinations toward an affirmative answer to this latter problem, and hence to the former, is disallowed in general([11]). Nevertheless, certain subgroups $\mathfrak{G}$ do have the desired factorization property, and these have been called *regular* subgroups by Kaplansky([12]) in the more general setting of modules (see Kaplansky's *Infinite Abelian groups*, Ann

([11]) Professor Kaplansky has pointed out to me that if $G = Z_2 \otimes Z_8$, where $Z_2 = (a)$ is cyclic of order 2, and $Z_8 = (b)$ is cyclic of order 8, then the cyclic subgroup generated by ab^2 is not regular, in the sense below.

([12]) If M is a module over a discrete valuation ring R possessing the unique prime p, a submodule S is *regular* provided $p^n S \cap p^{n+k}M = p^n(S \cap p^k M)$, for every n, k. When the elements of M have bounded orders, Ex. 78 (loc. cit.) asserts that a submodule S is regular if and only if M has a basis $\{x_i\}$ such that for suitable $c_i \in R$, $\{c_i x_i\}$ is a basis of S.

Arbor, University of Michigan Press, 1951, Exercises 78 and 79.) In fact, if G is p-primary, Exercise 79 (loc. cit.) implies that every subgroup of G is regular if and only if, for suitable α, G is the direct product of cyclic subgroups of orders p^α and $p^{\alpha+1}$.

DEFINITION. Let G be an Abelian group of finite order. Then a subgroup $\mathfrak{H}$ of G is *regular* provided G and $\mathfrak{H}$ have the factorizations of (2.6) and (2.7) respectively.

In this section we develop sufficient conditions for a subgroup $\mathfrak{H}$ to be regular which will be suitable for our purposes.

LEMMA 2.4. *Let G be a p-primary Abelian group of finite order n. If $\mathfrak{H}$ is any subgroup of G containing G^p, then there exist factorizations* (2.6) *and* (2.7) *of G and $\mathfrak{H}$ with $p_i=p$, such that $(g_i)\geqq(g_i^{x_i})\geqq(g_i^p)$, $i=1, 2, \cdots, s$.*

Proof. Let $n=p^\alpha$. The proof is by induction on α. The cases $\alpha=0$ and 1 being trivial, we assume the theorem for all p-primary groups of orders less than p^e, $e>1$. Now suppose G has order p^e, and $\mathfrak{H}$ is any subgroup containing G^p. Since $\mathfrak{H}\geqq G^p\geqq\mathfrak{H}^p$, we may apply the induction hypothesis to $\mathfrak{H}$ and the subgroup G^p in order to obtain the existence of direct factorizations

$$\mathfrak{H} = (k_1)\otimes(k_2)\otimes\cdots\otimes(k_s),$$
$$H = G^p = (h_1)\otimes(h_2)\otimes\cdots\otimes(h_r) \qquad (r\leqq s),$$

where $(k_i)\geqq(h_i)\geqq(k_i^p)$, $i=1, 2, \cdots, r$, and h_i has order $p^{e_i-1}\neq 1$, $i=1, 2, \cdots, r$. Since the group (k_i) modulo (k_i^p) has prime order p, it follows that $(k_i)=(h_i)$, or $(k_i^p)=(h_i)$, $i=1, 2, \cdots, r$. Let $\mathfrak{S}=(k_i)$, for some $i>r$. Then, since $\mathfrak{S}^p\subseteq H$, $\mathfrak{S}^p$ must be the identity subgroup, i.e., k_i has order p for any $i>r$.

We now define s elements $g_i\in G$ as follows:

(2.8) If $(k_i)=(h_i)$, g_i is any solution of the equation $x^p-h_i=0$.

(2.9) If $(k_i)\neq(h_i)$, or if $i>r$, g_i is any generator of the group (k_i).

When g_i is defined by (2.8), g_i has order p^{e_i}. When g_i is defined by (2.9) and $i\leqq r$, g_i has order p^{e_i}. Otherwise, g_i has order p when $i>r$. We define $e_i=1$, when $i>r$, and summarize: g_i has order p^{e_i}, $i=1, 2, \cdots, s$.

Let $G^*=(g_1)(g_2)\cdots(g_s)$, and assume for $g_i^{x_i}\in(g_i)$, $i=1, 2, \cdots, s$, that

$$g_1^{x_1}g_2^{x_2}\cdots g_s^{x_s} = 1 \qquad (0\leqq x_i<p^{e_i}), \tag{2.10}$$

where 1 denotes the identity element. Then,

$$g_1^{px_1}\cdot g_2^{px_2}\cdots g_r^{px_r}\cdot g_{r+1}^{px_{r+1}}\cdots g_s^{px_s} = h_1^{x_1}h_2^{x_2}\cdots h_r^{x_r} = 1.$$

This, and the fact that the product $(h_1)(h_2)\cdots(h_r)$ is direct, implies $h_i^{x_i}=1$, $i=1, 2, \cdots, r$. Since h_i has order p^{e_i-1}, x_i is divisible by p^{e_i-1} for $i\leqq r$. Since

$e_i-1\geqq 1$, for any $i\leqq r$, p divides x_i. Let $x_ip^{-1}=y_i$, $i=1, 2, \cdots, r$, so that $0\leqq y_i<p_i^{e_i-1}$. Then, (2.10) implies

$$g_1^{py_1}\cdots g_r^{py_r}g_{r+1}^{x_{r+1}}\cdots g_s^{x_s}=h_1^{y_1}\cdots h_r^{y_r}g_{r+1}^{x_{r+1}}\cdots g_s^{x_s}=1.$$

Since the product $(h_1)\cdots(h_r)(g_{r+1})\cdots(g_s)$ is direct, $h_i^{y_i}=1$, $i=1, 2, \cdots, r$, and $g_j^{x_j}=1$, $j=r+1, \cdots, s$. Thus, $y_i=0$, $i=1, 2, \cdots, r$, and $x_j=0$, $j=r+1, \cdots, s$. Hence, $x_i=0$, $i=1, \cdots, s$; and G^* is the direct product of the subgroups (g_i), $i=1, \cdots, s$.

If $G=G^*$, the lemma is proved already. Otherwise, let g be any element in G not in G^*. Then, $h=g^p$ and h^{-1} are elements in G^p, so that $h^{-1}=h_1^{x_1}\cdots h_r^{x_r}$, for suitable integers x_i. Since $h_i=g_i^p$, $i=1, 2, \cdots, r$, it follows that $h^{-1}=k^p$ for some $k\in G^*$. The element $q=kg$ has order p, since $q^p=1$, and since the assertion $q=kg=1$ implies $g=k^{-1}\in G^*$, contrary to the choice of g. It easily follows that the product $G^*(q)$ is direct. If $G\neq G^*\otimes(q)$, an obvious induction completes the proof([13]).

LEMMA 2.5. *Let G be a p-primary Abelian group of finite order. Then, given a factorization of G^{p^α},*

$$G^{p^\alpha}=(h_1)\otimes(h_2)\otimes\cdots\otimes(h_s), \tag{2.11}$$

there exists a factorization of G

$$G=(g_1)\otimes(g_2)\otimes\cdots\otimes(g_t), \tag{2.12}$$

such that $h_i=g_i^{p^\alpha}$, $i=1, 2, \cdots, s$.

Proof. The proof is by induction on α. Let (2.11), with $\alpha=1$, denote the factorization of G^p, and let g_i be an arbitrary solution in G of the equation $x^p-h_i=0$, $i=1, 2, \cdots, s$. By the proof of the previous lemma, the product $G^*=(g_1)(g_2)\cdots(g_s)$ is direct, $G^*=(g_1)\otimes(g_2)\otimes\cdots\otimes(g_s)$. If $G=G^*$, the proof is complete. Otherwise, one may continue as in the proof of Lemma 2.4 to obtain elements $g_{s+1}, \cdots, g_t$, each having order p, and such that G is the direct product of the (g_i), $i=1, 2, \cdots, t$. Then G has the desired factorization in case $\alpha=1$.

Now assume the theorem for all G^{p^β} with $\beta<\alpha$, and suppose G^{p^α} has the factorization (2.11). Then, since $G^{p^\alpha}=(G^{p^{\alpha-1}})^p$, there exists a factorization

$$G^{p^{\alpha-1}}=(k_1)\otimes(k_2)\otimes\cdots\otimes(k_r) \qquad (r\geqq s)$$

such that $k_i^p=h_i$, $i=1, 2, \cdots, s$. By the induction hypothesis, G has a factorization (2.12) such that $g_i^{p^{\alpha-1}}=k_i$, $i=1, 2, \cdots, r$. Then, $g_i^{p^\alpha}=h_i$, $i=1, 2, \cdots, s$, and the proof is complete.

THEOREM 2.1. *Let G be a p-primary Abelian group of finite order, and suppose $\mathfrak{S}$ is any subgroup satisfying*

([13]) The proof of this lemma is a modification of the proof of the Fundamental Theorem of Abelian Groups given in Speiser's, *Die Theorie der Gruppen*, New York, 1945, p. 47.

$$G^{p^\alpha} \supseteq \mathfrak{H} \supseteq G^{p^{\alpha+1}},$$

for suitable α. Then, $\mathfrak{H}$ is regular.

Proof. By Lemma 2.4, there exist factorizations

$$G^{p^\alpha} = (h_1) \otimes (h_2) \otimes \cdots \otimes (h_s),$$
$$\mathfrak{H} = (k_1) \otimes (k_2) \otimes \cdots \otimes (k_r) \qquad (r \leqq s),$$

such that $(h_i) \supseteq (k_i)$, i.e., $k_i = h_i^{x_i}$, for suitable integers x_i, $i = 1, 2, \cdots, r$. By Lemma 2.5, G has a factorization (2.12) such that $g_i^{p^\alpha} = h_i$, $i = 1, 2, \cdots, s$. Since, $k_i = g_i^{x_i p^\alpha}$, $i = 1, 2, \cdots, r$, the proof is complete.

4. **Kummer extensions are completely basic.** The lemma below is an application of Theorem 2.1.

LEMMA 2.6. *Let K/F be Abelian of degree p^e, p a prime. Let $\mathfrak{G}$ denote the Galois group of K/F, let Δ_λ be the intermediate field of K/F corresponding to $\mathfrak{G}^{p^\lambda}$, $\lambda = 0, 1, \cdots, e$. Let Γ be an intermediate field satisfying $\Delta_\alpha \subseteq \Gamma \subseteq \Delta_{\alpha+1}$, for a suitable α. Then, there exists a factorization $K = K_1 \times K_2 \times \cdots \times K_t$ over F, K_i/F cyclic, $i = 1, 2, \cdots, t$, such that $\Gamma = \Gamma_1 \times \Gamma_2 \times \cdots \times \Gamma_t$ over F, where $\Gamma_i = \Gamma \cap K_i$, $i = 1, 2, \cdots, t$.*

Proof. Let $\mathfrak{H}$ denote the Galois group of K/Γ. Since $\mathfrak{G}^{p^\alpha} \supseteq \mathfrak{H} \supseteq \mathfrak{G}^{p^{\alpha+1}}$, there exists a factorization $\mathfrak{G} = G_1 \otimes G_2 \otimes \cdots \otimes G_t$, G_i cyclic, $i = 1, 2, \cdots, t$, such that $\mathfrak{H} = \mathfrak{H}_1 \otimes \mathfrak{H}_2 \otimes \cdots \otimes \mathfrak{H}_t$, $\mathfrak{H}_i = \mathfrak{H} \cap G_i$, $i = 1, 2, \cdots, t$. Let H_i denote the group $\prod_{j \neq i} G_j$, $\mathfrak{K}_i = H_i \mathfrak{H}_i$, and let K_i and Γ_i be the corresponding subfields respectively, $i = 1, 2, \cdots, t$. Then, $K = K_1 \times K_2 \times \cdots \times K_t$ over F, and $\Gamma = \Gamma_1 \times \Gamma_2 \times \cdots \times \Gamma_t$ over F are the desired factorizations.

We now prove our main result on completely basic extensions.

THEOREM 2.2. *Every Kummer extension is completely basic.*

Proof. It suffices to prove that every subfield Δ of the Kummer extension K/F having prime degree p over F is obtainable as in Lemma 2.3. To do this, we only need assume K/F has degree p^e. Let $\mathfrak{H}$ denote the Galois group of K/Δ. Since $\mathfrak{H}$ has index p in the Galois group $\mathfrak{G}$ of K/F, $\mathfrak{H} \supseteq \mathfrak{G}^p$. The proof now follows from Lemma 2.6 in the case $\alpha = 0$.

That not every completely basic extension is a Kummer extension is emphasized by the

COROLLARY. *Let K/F be Abelian, and let n be the least common multiple of the orders of the automorphisms of K/F. Let ζ be a primitive n root of unity in some field containing K. Then, K/F is completely basic in case $K \cap F(\zeta) = F$.*

Proof. Let Δ be any intermediate field of K/F. Since $K \cap \Delta(\zeta) = \Delta$, i.e., $K(\zeta) = K \times \Delta(\zeta)$ over Δ, every normal basis element of K/Δ is a normal basis element of $K(\zeta)/\Delta(\zeta)$ by Theorem 1.4. Then, since $K(\zeta)/F(\zeta)$ is completely basic, K/F is completely basic.

Let $\mathfrak{N}/\mathfrak{F}$ be an arbitrary normal extension, and suppose for every factorization $\mathfrak{N}=\mathfrak{N}_1\times\mathfrak{N}_2\times\cdots\times\mathfrak{N}_t$ over $\mathfrak{F}$, each $\mathfrak{N}_i/\mathfrak{F}$ is completely basic, $i=1, 2, \cdots, t$. The answer to the following question is unknown in general: Is $\mathfrak{N}/\mathfrak{F}$ completely basic? However, one has the converse

THEOREM 2.3. *If $\mathfrak{N}/\mathfrak{F}$ is completely basic, and if $\mathfrak{N}=\mathfrak{N}_1\times\mathfrak{N}_2\times\cdots\times\mathfrak{N}_t$ over F, then $\mathfrak{N}_i$ is completely basic over $\mathfrak{F}$, $i=1, 2, \cdots, t$.*

Proof. Theorem 1.3 shows that every normal basis element v_i of $\mathfrak{N}_i/\mathfrak{F}$ is the trace in $\mathfrak{N}/\mathfrak{N}_i$ of a normal basis element u_i of $\mathfrak{N}/\mathfrak{F}$, $i=1, 2, \cdots, t$. Let Δ_i be any intermediate field of $\mathfrak{N}_i$, $i=1, 2, \cdots, t$. Then, u_i is a normal basis element of $\mathfrak{N}/\Delta_i$, so that v_i is a normal basis element of $\mathfrak{N}_i/\Delta_i$, $i=1, 2, \cdots, t$.

III. A DETERMINATION OF COMPLETELY BASIC FIELDS

In the preceding chapters, various kinds of normal extensions were demonstrated to be members of the class $\mathfrak{C}$ of completely basic extensions. The first purpose of this chapter is to establish that not every normal extension is a member of $\mathfrak{C}$. This is accomplished in Lemma 3.4 with the aid of certain cyclotomic extensions (although some cyclotomic extensions are members of $\mathfrak{C}$). The broader aim of this chapter is the determination of those cyclic extensions $\mathfrak{Z}_e/\mathfrak{F}$ of prime power degree p^e which are members of $\mathfrak{C}$. This determination is achieved in the case where $\mathfrak{F}$ contains a primitive p root of unity. When $\mathfrak{F}$ does not contain a primitive p root of unity, the situation is complicated by a less satisfactory structure theory for $\mathfrak{Z}_e/\mathfrak{F}$ [1, pp. 209–216]. We were unable to achieve a classification of those extensions $\mathfrak{Z}_e/\mathfrak{F}$ which are members of $\mathfrak{C}$ in this latter case.

1. **Background material.** In this section definitions, notational hypotheses, and certain known results are cited which will be used throughout. Usually our notation conforms with that of [1] and [9].

The symbol $\mathfrak{Z}_e/\mathfrak{F}$ always denotes a cyclic extension of degree p^e, for the prime p; $\mathfrak{Z}_\lambda/\mathfrak{F}$ designates the unique intermediate field of $\mathfrak{Z}_e/\mathfrak{F}$ of degree p^λ over $\mathfrak{F}$, $0\leqq\lambda\leqq e$. The symbol $i\in(k, k+m)$ is reserved for the statement that the integer i is on the range $k, k+1, \cdots, k+m$.

When $\mathfrak{F}$ contains a primitive p root of unity ζ_0 the known structure theory for the extension $\mathfrak{Z}_e/\mathfrak{F}$ [1, pp. 206–208] asserts the existence of $\xi\in\mathfrak{Z}_e$ and $\beta\in\mathfrak{Z}_{e-1}$ such that $\mathfrak{Z}_e/\mathfrak{F}$ has the *generation*

$$(3.1)\qquad \mathfrak{Z}_e=\mathfrak{F}(\xi),\qquad \xi^p\in\mathfrak{Z}_{e-1},\qquad N_{\mathfrak{Z}_{e-1}/\mathfrak{F}}(\beta)=\zeta_0,\qquad \xi^S=\beta\xi,$$

where S is a generating automorphism of $\mathfrak{Z}_e/\mathfrak{F}$. (For any $x\in\mathfrak{Z}_\lambda$, $N_{\mathfrak{Z}_\lambda/\mathfrak{F}}(x)=xx^S\cdots x^{S^{s-1}}$, where $s=p^\lambda$, $\lambda\in(0, e)$).

In case $\mathfrak{F}$ contains a primitive p^g root of unity ρ, $g\in(1, e)$, it is known [9, p. 512] that there exist $\xi\in\mathfrak{Z}_e$ and $\beta\in\mathfrak{Z}_{e-g}$ such that $\mathfrak{Z}_e/\mathfrak{F}$ has the *normalized generation*

$$(3.2) \qquad \mathfrak{Z}_e = \mathfrak{F}(\xi), \qquad \xi^{p^g} \in \mathfrak{Z}_h, \qquad N_{\mathfrak{Z}_h/\mathfrak{F}}(\beta) = \rho, \qquad \xi^S = \beta\xi,$$

where $h = e - g$.

Of particular use to us is a result of Perlis' [9, Theorem 4] which characterizes the normal basis elements of $\mathfrak{Z}_e/\mathfrak{F}$, when $\mathfrak{Z}_e/\mathfrak{F}$ has the normalized generation (3.2), in terms of linear sets. Let $[L_k\gamma(\delta)]$ denote the linear space over $\mathfrak{F}$ spanned by the elements of the set

$$(3.3) \qquad L_k^{\gamma}(\delta) = \{\delta, \delta^S\beta^k, \cdots, \delta^{S^{s-1}}(\beta\beta^S \cdots \beta^{S^{s-2}})^k\}$$

where $\delta \in \mathfrak{Z}_\gamma$, $\gamma \in (e-g, e-1)$, $k \in (0, p^{e-\gamma}-1)$, and $s = p^\gamma$. This theorem states that *an arbitrary element u in $\mathfrak{Z}_e$*

$$(3.4) \qquad u = \delta_0 + \delta_1\xi + \cdots + \delta_{r-1}\xi^{r-1} \qquad (\delta_k \in \mathfrak{Z}_\gamma,\ r = p^{e-\gamma})$$

generates a normal basis of $\mathfrak{Z}_e/\mathfrak{F}$ if and only if, for $k = 0, 1, 2, \cdots, r-1$,

$$[L_k^{\gamma}(\delta_k)] = \mathfrak{Z}_\gamma.$$

2. **The hereditary property.** In determining that $\mathfrak{Z}_e/\mathfrak{F}$ is not completely basic, it suffices in some cases to show that $\mathfrak{Z}_i/\mathfrak{F}$ is not completely basic for some $i < e$. This is a consequence of Theorem 3.1 which establishes a hereditary property of certain completely basic extensions. First, we make an immediate inference from the Perlis criterion (3.4).

LEMMA 3.1. *Let $\mathfrak{Z}_e/\mathfrak{F}$ have normalized generation* (3.2), *and let u be the element defined by* (3.4). *Then,*

$$w = u + (\delta - \delta_\pi)\xi^\pi \qquad (\delta \in \mathfrak{Z}_\gamma,\ \pi \in (0, r-1))$$

generates a normal basis in $\mathfrak{Z}_e/\mathfrak{F}$ if and only if $[L_\pi^{\gamma}(\delta)] = \mathfrak{Z}_\gamma$.

LEMMA 3.2. *If $\mathfrak{Z}_e/\mathfrak{F}$ has generation* (3.1), *then each normal basis element v of $\mathfrak{Z}_\gamma/\mathfrak{F}$, $\gamma \in (0, e)$, is the trace in $\mathfrak{Z}_e/\mathfrak{Z}_\gamma$ of some normal basis element u of $\mathfrak{Z}_e/\mathfrak{F}$.*

Proof. The proof follows from that of the case $\gamma = e-1$, followed by an obvious induction. Accordingly, let v be a normal basis element of $\mathfrak{Z}_{e-1}/\mathfrak{F}$ so that $[L_0^{e-1}(v)] = \mathfrak{Z}_{e-1}$. If

$$w = \delta_0 + \delta_1\xi + \cdots + \delta_{p-1}\xi^{p-1} \qquad (\delta_i \in \mathfrak{Z}_{e-1})$$

is any normal basis element of $\mathfrak{Z}_e/\mathfrak{F}$, then (by the lemma) $u^* = w + (v - \delta_0)$ is also. Moreover, $pv = T_{\mathfrak{Z}_e/\mathfrak{Z}_{e-1}}(u^*)$. Hence, $v = T_{\mathfrak{Z}_e/\mathfrak{Z}_{e-1}}(p^{-1}u^*)$, where $p^{-1}u^*$ is clearly a normal basis element of $\mathfrak{Z}_e/\mathfrak{F}$.

THEOREM 3.1. *Let $\mathfrak{F}$ contain all of the roots of $x^p - 1 = 0$. Then, if $\mathfrak{Z}_e/\mathfrak{F}$ is completely basic, so is $\mathfrak{Z}_\gamma/\mathfrak{F}$, $\gamma \in (0, e)$.*

Proof. If $\mathfrak{F}$ has characteristic p, the first corollary to Theorem 1.5 does it. Otherwise, $\mathfrak{F}$ has generation (3.1) and Lemma 3.2 applies. Accordingly, let

$v = T_{\mathfrak{Z}_e/\mathfrak{Z}_\gamma}(u)$ as in Lemma 3.2, and let Δ be any intermediate field of $\mathfrak{Z}_\gamma/\mathfrak{F}$. If $\mathfrak{Z}_e/\mathfrak{F}$ is completely basic, then u generates a normal basis of $\mathfrak{Z}_e/\Delta$. Hence, v generates a normal basis of $\mathfrak{Z}_\gamma/\Delta$, i.e., $\mathfrak{Z}_\gamma/\mathfrak{F}$ is completely basic.

3. **A sufficient condition.** For convenience we list a lemma which gives a sufficient condition for $\mathfrak{Z}_e/\mathfrak{F}$ to be completely basic. The proof follows from Theorem 1.5 in the case $n = p^e$, $t = p^{e-1}$.

LEMMA 3.3. *Let C be the root field over $\mathfrak{F}$ of the equation $x^{p^{e-1}} - 1 = 0$, constructed to lie in a common field with $\mathfrak{Z}_e$. If $\mathfrak{Z}_e \cap C = \mathfrak{F}$, then $\mathfrak{Z}_e/\mathfrak{F}$ is completely basic.*

4. **Noncompletely basic fields.** The following is the key lemma in the proof of our main result (Theorem 3.2) concerning cyclic fields of prime power degrees which are completely basic. Of interest in its own right, however, is the construction in certain normal extensions of arbitrarily high degree of normal basis elements which are not completely basic.

LEMMA 3.4. *Let $\mathfrak{F}$ be a field which contains a primitive p^g root of unity but which does not contain a primitive p^{g+1} root of unity, for the prime p, and an integer $g \geqq 1$. Let C_g be the root field over $\mathfrak{F}$ of the equation*

$$x^{p^{g+1}} - 1 = 0; \tag{3.5}$$

let ρ denote a primitive p^{g+1} root of unity in C_g, and define $\zeta_i = \rho^{p^{g-i}}$, $i \in (0, g)$. Then,

(I) *$C_g/\mathfrak{F}$ is cyclic of degree p.*

Let $\mathfrak{Z}_{g+2}$ be a superfield of C_g of degree p^{g+2} over $\mathfrak{F}$. Then,

(II) *$\mathfrak{Z}_{g+2}/\mathfrak{F}$ has the normalized generation*

$$\mathfrak{Z}_e = \mathfrak{F}(\xi), \qquad \xi^{p^g} \in \mathfrak{Z}_2, \qquad N_{\mathfrak{Z}_2/\mathfrak{F}}(\beta) = \zeta_{g-1},$$

$$\xi^S = \beta\xi, \quad \text{with} \quad \beta\beta^S \cdots \beta^{S^{p-1}} = \rho.$$

(III) *$\mathfrak{Z}_2/\mathfrak{F}$ has the generation*

$$\mathfrak{Z}_2 = \mathfrak{F}(\beta), \ \beta^p \in \mathfrak{Z}_1, \ N_{\mathfrak{F}_1/\mathfrak{F}}(\gamma) = \zeta_0^t, \ \beta^S = \gamma\beta,$$

where $0 < t < p$, and β as in (II).

Let the element

$$u^* = \delta_0 + \delta_1\xi + \cdots + \delta_{r-1}\xi^{r-1} \qquad (\delta_i \in \mathfrak{Z}_2, \ r = p^g)$$

represent an arbitrary normal basis element of $\mathfrak{Z}_{g+2}/\mathfrak{F}$. Then,

(IV) *the element $u = u_+^*(1 - \delta_1)\xi$ generates a normal basis of $\mathfrak{Z}_{g+2}/\mathfrak{F}$, but*

(V) *u is not a normal basis element of $\mathfrak{Z}_{g+2}/\mathfrak{Z}_1$.*

Proof of (I). By hypothesis $\mathfrak{F}$ contains the primitive p^g root of unity ζ_{g-1}. The element $\rho \in C_g$ is a root of the equation

$$x^p - \zeta_{g-1} = 0. \tag{3.6}$$

The field $\mathfrak{F}$ contains the primitive p root of unity ζ_0 by our hypothesis that $g \geqq 1$. Then, $C_g = \mathfrak{F}(\rho)$ is cyclic of degree p over $\mathfrak{F}$ with generating automorphism R defined by

$$\rho \longrightarrow \rho\zeta_0 = \rho^R \tag{3.7}$$

as in [1, Theorem 22, p. 188].

Proof of (II). Since ζ_{g-1} is a primitive p^g root of unity in $\mathfrak{F}$, $\mathfrak{Z}_{g+2}/\mathfrak{F}$ has a normalized generation

$$\mathfrak{Z}_{g+2} = \mathfrak{F}(\xi_0), \qquad \xi_0^{p^g} \in \mathfrak{Z}_2, \qquad N_{\mathfrak{Z}_2/\mathfrak{F}}(\beta_0) = \zeta_{g-1}, \qquad \xi_0^S = \beta_0\xi_0.$$

If $\theta_0 = \beta_0\beta_0^S \cdots \beta_0^{S^{p-1}}$, then $N_{\mathfrak{Z}_2/\mathfrak{Z}_1}(\theta_0) = N_{\mathfrak{Z}_2/\mathfrak{F}}(\beta_0) = \zeta_{g-1} = \rho^p$. Since C_g has degree p over $\mathfrak{F}$, $C_g = \mathfrak{Z}_1$. Since $\rho \in \mathfrak{Z}_1$, $N_{\mathfrak{Z}_2/\mathfrak{Z}_1}(\theta_0\rho^{-1}) = 1$. By a theorem([14]) of Hilbert, there exists an element δ in $\mathfrak{Z}_2$ such that $\theta_0\rho^{-1} = \delta(\delta^{S^p})^{-1}$. The element $\beta = \delta^{-1}\delta^S\beta_0 \in \mathfrak{Z}_2$; $N_{\mathfrak{Z}_2/\mathfrak{F}}(\beta) = N_{\mathfrak{Z}_2/\mathfrak{F}}(\beta_0) = \zeta_{g-1}$; and $\beta\beta^S \cdots \beta^{S^{p-1}} = \delta^{S^p}\delta^{-1}\theta_0 = \rho \in \mathfrak{Z}_1$. Since $N_{\mathfrak{Z}_{g+1}/\mathfrak{F}}(\beta) = \zeta_{g-1}^s = \zeta_0$, $s = p^{g-1}$, there exists $\xi \in \mathfrak{Z}_{g+2}$ such that $\mathfrak{Z}_{g+2}/\mathfrak{F}$ has the desired generation by [1, p. 208, Theorem 12].

Proof of (III). Since $\xi^S = \beta\xi$, it follows that $a = \xi^p \in \mathfrak{Z}_{g+1}$ satisfies the equation $a^S = \beta^p a$. Consequently,

$$a^T = a^{S^p} = (\beta^{S^{p-1}} \cdots \beta)^p a = \rho^p a = \zeta_{g-1}a \qquad (T = S^p).$$

Thus $\beta^p \in \mathfrak{Z}_1$ as can be verified as follows:

$$(\beta^p)^T = (a^T)^S/a^T = (\zeta_{g-1}a)^S/(\zeta_{g-1}a) = (\zeta_{g-1}a^S)/(\zeta_{g-1}a) = a^S/a = \beta^p.$$

If β were in $\mathfrak{Z}_1$, then $N_{\mathfrak{Z}_2/\mathfrak{F}}(\beta) = N_{\mathfrak{Z}_1/\mathfrak{F}}(\beta^p) = (N_{\mathfrak{Z}_1/\mathfrak{F}}(\beta))^p = \zeta_{g-1}$, and $N_{\mathfrak{Z}_1/\mathfrak{F}}(\beta)$ would be in $\mathfrak{F}$, contrary to our hypothesis that $\mathfrak{F}$ does not contain a primitive p^{g+1} root of unity. Thus $\mathfrak{Z}_1(\beta) \supset \mathfrak{Z}_1$. On the other hand, $\mathfrak{Z}_2 \supseteq \mathfrak{Z}_1(\beta)$, since $\beta \in \mathfrak{Z}_2$. Hence $\mathfrak{Z}_2 = \mathfrak{Z}_1(\beta)$; β has degree p over $\mathfrak{Z}_1$; $x^p - \beta^p$ is the minimal polynomial of β over $\mathfrak{Z}_1$. The automorphism $T = S^p$ of $\mathfrak{Z}_{g+2}/\mathfrak{Z}_1$ maps β onto one of its conjugates over $\mathfrak{Z}_1$, and since T induces a generating automorpism of $\mathfrak{Z}_2/\mathfrak{Z}_1$, $\beta^T = \beta\zeta_t^0$ for some t prime to p.

We verify that $\gamma = \beta^{-1}\beta^S$ is in $\mathfrak{Z}_1$ as follows:

$$\gamma^T = (\beta^{-1}\beta^S)^T = (\beta^T)^{-1}(\beta^T)^S = (\beta\zeta_0^t)^{-1}(\beta\zeta_0^t)^S = \beta^{-1}\beta^S = \gamma.$$

Thus $\mathfrak{Z}_2/\mathfrak{F}$ has the desired generation.

Proof of (IV). Applying Lemma 3.1 to this case when $g = e-2$, $r = p^g$, $\gamma = 2$, we see that u is a normal basis element of $\mathfrak{Z}_{g+2}/\mathfrak{F}$ if and only if the vector space over $\mathfrak{F}$ spanned by the $s = p^2$ quantities of the set

$$L_1^2(1) = \{1, \beta, \beta\beta^S, \cdots, \beta\beta^S \cdots \beta^{S^{s-2}}\} \text{ is equal to } \mathfrak{Z}_2.$$

([14]) See [4, p. 171, Theorem 3] for the statement and proof of this theorem.

Consider

$$\beta_\pi = \beta\beta^S \cdots \beta^{S^{\pi-1}} \qquad (\pi = fp + c,\ 0 \leqq c < p,\ 0 \leqq f).$$

Then $\beta_1 = \beta$, $\beta_p = \rho$, and

$$\beta_\pi = \beta\beta^S \cdots \beta^{S^{c-1}} \rho^{S^c} \rho^{S^{p+c}} \cdots \rho^{S^{(f-1)p+c}}$$

Since $\rho^{-1}\rho^S = \zeta_0^h$ is in $\mathfrak{F}$ by (3.7), $\rho^{-1}\rho^{S^i}$ is in $\mathfrak{F}$ for any i, so that the quantity

$$\beta'_\pi = (\beta\beta^S \cdots \beta^{S^{c-1}})\rho^{f-1} \qquad (\pi = 1, 2, \cdots, s-1)$$

differs from β_π by a nonzero scalar multiple in $\mathfrak{F}$. Thus

$$[L_1^2(1)] = (1, \beta, \beta_2, \cdots, \beta_{p-1}, \rho, \beta\rho, \cdots, \beta_{p-1}\rho, \cdots, \rho^{p-1}, \beta\rho^{p-1}, \cdots, \beta_{p-1}\rho^{p-1}) \text{ over } \mathfrak{F}.$$

Let U be the vector space over $\mathfrak{F}$ spanned by unity and the quantities β_i $(i = 1, 2, \cdots, p-1)$. The vector space over $\mathfrak{F}$ spanned by the ρ^i $(i = 1, 2, \cdots, p-1)$ is $\mathfrak{Z}_1$, since $\mathfrak{Z}_1 = \mathfrak{F}(\rho)$. Therefore,

$$[L_1^2(1)] = (U, U\rho, \cdots, U\rho^{p-1}) \qquad \text{over } \mathfrak{F}$$

is the vector space spanned by the p generating quantities of U over $\mathfrak{Z}_1$. Since $\beta^S = \gamma\beta$, $\gamma \in \mathfrak{Z}_1$ ((III) above), it follows that

$$\beta\beta^S \cdots \beta^{S^{\pi-1}} = \beta^\pi\gamma_\pi \qquad (\gamma_\pi \neq 0 \in \mathfrak{Z}_1;\ \pi = 1, 2, \cdots, p-1).$$

Since $[L_1^2(1)]$ is the vector space over $\mathfrak{Z}_1$ spanned by unity and the $p-1$ quantities $\beta^\pi\gamma_\pi$, it follows that

$$[L_1^2(1)] = (1, \beta, \beta^2, \cdots, \beta^{p-1}) \text{ over } \mathfrak{Z}_1,$$

which is equal to $\mathfrak{Z}_2$ since $\mathfrak{Z}_2 = \mathfrak{Z}_1(\beta)$ by (III). This completes the proof of (IV).

Proof of (V). Since $\mathfrak{Z}_{\sigma+2}$ has the generation (II), with $\sigma = \xi^r \in \mathfrak{Z}_2$, $r = p^\sigma$, it follows that $\mathfrak{Z}_2 = \mathfrak{Z}_1(\sigma)$. Thus, the coefficients δ_i of u, $i \neq 1$, are expressible

$$\delta_i = \sum_{j=0}^{p-1} \alpha_{ij}\sigma^j = \sum_{j=0}^{p-1} \alpha_{ij}\xi^{jr} \qquad (\alpha_{ij} \in \mathfrak{Z}_1,\ r = p^\sigma).$$

Therefore u has the form

$$u = \sum_{i \neq 1} \sum_{j=0}^{p-1} \alpha_{ij}\xi^{jr+i} + \xi,$$

where the coefficient of ξ^{r+1} is zero. $T = S^p$ is a generating automorphism of $\mathfrak{Z}_{\sigma+2}/\mathfrak{Z}_1$, and the $p^{\sigma+1}$ elements

$$\rho^\lambda = \xi^{-1}\xi^{T^\lambda} \qquad (\lambda = 0, 1, \cdots, p^{\sigma+1} - 1) \tag{3.8}$$

lie in $\mathfrak{Z}_1$. Since ρ is a primitive p^{g+1} root of unity in $\mathfrak{Z}_1$ and since $\mathfrak{Z}_{g+2}/\mathfrak{Z}_1$ is cyclic of degree p^{g+1}, this extension is Kummer. By (3.8) the basis of $\mathfrak{Z}_{g+2}/\mathfrak{Z}_1$ consisting of the ξ^i, $i=0, 1, \cdots, p^{g+1}-1$, is seen to satisfy the condition of Lemma 2.2. Hence, u does not generate a normal basis of $\mathfrak{Z}_{g+2}/\mathfrak{Z}_1$. This simultaneously completes the proofs of (V) and Lemma 3.4.

5. **A determination of completely basic fields.** We now give a classification of all completely basic fields $\mathfrak{Z}_e$ which are cyclic of prime power degree p^e over a field $\mathfrak{F}$ in which the polynomial x^p-1 factors linearly. If $\mathfrak{F}$ does not contain the roots of the equation $x^p-1=0$, this equation defines a field $\mathfrak{F}'=\mathfrak{F}(\zeta_0)$, where ζ_0 is a primitive p root of unity, and $\mathfrak{F}'/\mathfrak{F}$ has degree $<p$. The composite $\mathfrak{Z}_e'=\mathfrak{Z}_e(\zeta_0)$ is the direct product over $\mathfrak{F}$ of $\mathfrak{Z}_e$ and $\mathfrak{F}'$. Therefore, $u\in\mathfrak{Z}_e$ is a normal basis element of $\mathfrak{Z}_e/\mathfrak{F}$ if and only if u is a normal basis element in $\mathfrak{Z}_e'/\mathfrak{F}'$. If $\mathfrak{Z}_e'/\mathfrak{F}'$ is completely basic, so is $\mathfrak{Z}_e/\mathfrak{F}$. Hence, our determination will provide a sufficient condition in some cases where x^p-1 does not factor linearly in the base field $\mathfrak{F}$.

Let $g=g(\mathfrak{F}, p)$ denote the largest integer, if such exists, for which the polynomial

$$x^{p^g}-1$$

factors linearly in the field $\mathfrak{F}$. If there is no such maximal g, we define $g=g(\mathfrak{F}, p)$ to be ∞, which is regarded as being larger than any integer.

THEOREM 3.2. *Let $\mathfrak{Z}_e$ be cyclic of prime power degree p^e, p a prime, over a field $\mathfrak{F}$ in which the polynomial x^p-1 factors linearly. If $g(\mathfrak{F}, p)\geqq e-1$, then $\mathfrak{Z}_e/\mathfrak{F}$ is completely basic. Otherwise, $\mathfrak{Z}_e/\mathfrak{F}$ is completely basic if and only if $g(\mathfrak{Z}_e, p)=g(\mathfrak{F}, p)$.*

Proof. If the invariant g defined above for the field $\mathfrak{F}$ and the prime p obeys $g\geqq e-1$, then $\mathfrak{Z}_e/\mathfrak{F}$ is completely basic by Lemma 3.3.

Now assume that $e\geqq g+2$, so that $\mathfrak{F}$ has characteristic not p, and the root field C over $\mathfrak{F}$ of the equation $x^{p^{e-1}}-1=0$ contains a primitive p^{e-1} root of unity, and hence contains a primitive p^{g+1} root of unity ρ. Lemma 3.4 (I) asserts that $C_g=\mathfrak{F}(\rho)$ is then cyclic of degree p over $\mathfrak{F}$. Let K be the composite over $\mathfrak{F}$ of C and $\mathfrak{Z}_e$, and $Q=C\cap\mathfrak{Z}_e$. If $\mathfrak{Z}_e/\mathfrak{F}$ is not completely basic, then $Q\supset\mathfrak{F}$ by Lemma 3.3. Necessarily then $\mathfrak{Z}_e\supseteq Q\supseteq\mathfrak{Z}_1=C_g=\mathfrak{F}(\rho)\supset\mathfrak{F}$. The field $\mathfrak{Z}_e$ contains a primitive p^{g+1} root of unity ρ and $g(\mathfrak{Z}_e, p)\geqq g+1>g$ since $x^{p^{g+1}}-1$ factors linearly in $C_g\subseteq\mathfrak{Z}_e$.

Conversely, suppose $g(\mathfrak{Z}_e, p)\doteq g_e>g$. Then, $\mathfrak{Z}_e$ contains the root field C_g over $\mathfrak{F}$ of the equation (3.5), and hence contains a primitive p^{g+1} root of unity ρ. Thus, $\mathfrak{Z}_{g+2}$ is a superfield of $C_g=\mathfrak{F}(\rho)$ of degree p^{g+2} over $\mathfrak{F}$. The extension $\mathfrak{Z}_{g+2}/\mathfrak{F}$ satisfies the hypotheses of Lemma 3.4 and therefore is not completely basic by parts (IV) and (V) of this lemma. Since $\mathfrak{Z}_e$ is a superfield of $\mathfrak{Z}_{g+2}$ cyclic of prime power degree over $\mathfrak{F}$, $\mathfrak{Z}_e/\mathfrak{F}$ is not completely basic by Theorem 3.1.

If $\mathfrak{Z}_e/\mathfrak{F}$ is completely basic and cyclic of degree p^e, p a prime with $g(\mathfrak{F}, p) \geqq 1$, we say that the extension has *type* I if $g(\mathfrak{F}, p) \geqq e-1$, and has *type* II, otherwise.

We now cite two corollaries, and a theorem which illustrates the special character of completely basic extensions of type II.

COROLLARY. *Let $\mathfrak{Z}_e/\mathfrak{F}$ be cyclic of degree p^e, p a prime with $e-1 > g(\mathfrak{F}, p) \geqq 1$, and let C be the root field over $\mathfrak{F}$ of the equation $x^{p^{e-1}}-1=0$, constructed to lie in a common field with $\mathfrak{Z}_e$. Then:*

(i) *If $\mathfrak{Z}_e \cap C = \mathfrak{F}$, $\mathfrak{Z}_e/\mathfrak{F}$ has type* II;

(ii) *If p is an odd prime, and if $\mathfrak{Z}_e/\mathfrak{F}$ has type* II, *then $\mathfrak{Z}_e \cap C = \mathfrak{F}$.*

Proof. First we prove (i). If the extension does not have type II, then $g(\mathfrak{Z}_e, p) > g(\mathfrak{F}, p) = g$, so that $x^{p^{g+1}}-1$ factors linearly in $\mathfrak{Z}_e$. The fact that g is finite implies $\mathfrak{F}$ has characteristic not p, and hence, $\mathfrak{Z}_e$ contains a primitive p^{g+1} root of unity ρ. It follows that $\mathfrak{Z}_e \supseteq \mathfrak{F}(\rho) \supset \mathfrak{F}$ and that $C \supseteq \mathfrak{F}(\rho) \supset \mathfrak{F}$, completing the proof of (i).

Now suppose p is odd, and suppose $C \cap \mathfrak{Z}_e \supset \mathfrak{F}$. It is known for cyclotomic extensions of the type we are considering that $C/\mathfrak{F}$ is cyclic. Hence $C \cap \mathfrak{Z}_e$ contains a unique field of degree p over $\mathfrak{F}$. If ρ is a primitive p^{g+1} root of unity in C, ρ has degree p over $\mathfrak{F}$. Then $C \cap \mathfrak{Z}_e \supseteq \mathfrak{F}(\rho) \supset \mathfrak{F}$ so that $x^{p^{g+1}}-1$ factors linearly in $\mathfrak{Z}_e$; $g(\mathfrak{Z}_e, p) > g(\mathfrak{F}, p)$, and $\mathfrak{Z}_e/\mathfrak{F}$ does not have type II.

COROLLARY. *Let $\mathfrak{Z}_e/\mathfrak{F}$ be cyclic of degree p^e, p a prime with $g(\mathfrak{F}, p) = g \geqq 1$. If $\mathfrak{Z}_e/\mathfrak{F}$ is completely basic, so is $\mathfrak{Z}_e/\mathfrak{Z}_\gamma$, for every γ.*

Proof. Let $g_\gamma = g(\mathfrak{Z}_\gamma, p)$. If

(1) $g \geqq e-1$, then

$$g_\gamma \geqq g \geqq e-1 \geqq (e-\gamma)-1$$

so that $\mathfrak{Z}_e/\mathfrak{Z}_\gamma$ has type I. Otherwise

(2) $e-1 > g(\mathfrak{Z}_e, p) = g_\gamma = g \geqq 1$. If

(i) $(e-\gamma)-1 > g_\gamma = g$, then $\mathfrak{Z}_e/\mathfrak{Z}_\gamma$ has type II. Otherwise

(ii) $g = g_\gamma \geqq (e-\gamma)-1$ so that $\mathfrak{Z}_e/\mathfrak{Z}_\gamma$ has type I.

Theorem 3.1 shows that if $\mathfrak{Z}_e/\mathfrak{F}$ is not completely basic, then no superfield of $\mathfrak{Z}_e$ which is cyclic of prime degree over $\mathfrak{F}$ can be completely basic over $\mathfrak{F}$. However,

THEOREM 3.3. *If $\mathfrak{Z}_e/\mathfrak{F}$ has type* II, *any superfield of $\mathfrak{Z}_e$ cyclic of prime power degree over $\mathfrak{F}$ is completely basic over $\mathfrak{F}$, and has type* II.

Proof. Since $\mathfrak{Z}_e/\mathfrak{F}$ has type II,

$$e-1 > g(\mathfrak{Z}_e, p) = g(\mathfrak{F}, p) = g > 0$$

by Theorem 3.2. Let K be any superfield of $\mathfrak{Z}_e$ cyclic of prime power degree over $\mathfrak{F}$, say $p^{e+\pi}$, and assume $g(K, p) > g$. Let ρ be a primitive p^{g+1} root of

unity in K. By Lemma 3.4 (I), the subfield $\mathfrak{F}(\rho)$ of K has degree p over $\mathfrak{F}$. Thus $\mathfrak{F}(\rho) = \mathfrak{Z}_1 \subset \mathfrak{Z}_e$, since $e \geqq 3$. This contradicts the fact that $g(\mathfrak{Z}_e, p) = g$, since $x^{p^g+1} - 1$ factors linearly over $\mathfrak{Z}_1$. Therefore,

$$(e + \pi) - 1 \geqq e - 1 > g(K, p) = g > 0,$$

and $K/\mathfrak{F}$ has type II by Theorem 3.2.

Bibliography

1. A. A. Albert, *Modern higher algebra*, Chicago, 1937, pp. 146–216.

2. Emil Artin, *Galois theory*, Notre Dame Mathematical Lectures, No. 2, 2d ed., 1948.

3. ———, *Linear mappings and the existence of a normal basis*, Studies and Essays presented to R. Courant on his 60th birthday, New York, 1948.

4. N. Bourbaki, *Éléments de mathématique*, Livre II-Algèbre, Chapitres, IV and V, Actualités Scientifiques et Industrielles, no. 1102.

5. J. W. S. Cassels and G. E. Wall, *The normal basis theorem*, J. London Math. Soc. vol. 25 (1950) p. 259.

6. M. Deuring, *Galoissche Theorie und Darstellungstheorie*, Math. Ann. vol. 107 (1932) p. 140.

7. C. C. Faith, *Normal extensions in which every element with nonzero trace is a normal basis element*, unpublished.

8. T. Nakayama, *On Frobeniusean algebras* II, Ann. of Math. vol. 42 (1941) pp. 1–21.

9. Sam Perlis, *Normal bases of cyclic fields of prime power degree*, Duke Math. J. vol. 9 (1942) pp. 507–517.

10. R. Stauffer, *The construction of a normal basis in a separable normal extension field*, Amer. J. Math. vol. 58 (1936) pp. 585–597.

Michigan State University,
East Lansing, Mich.
Purdue University,
Lafayette. Ind.