GALOIS EXTENSIONS IN WHICH EVERY ELEMENT WITH REGULAR TRACE IS A NORMAL BASIS ELEMENT

CARL C. FAITH

1. Introduction. If $\mathfrak{K}/\mathfrak{F}$ is a finite separable normal (or Galois) extension field of degree n, with Galois group $\mathfrak{G}=(G_1, \cdots, G_n)$, then the *theorem of the normal basis* asserts that $\mathfrak{K}/\mathfrak{F}$ always possesses a field basis of the form $w^{G_1}, \cdots, w^{G_n}$ $(w\in\mathfrak{K})$, called a normal basis of $\mathfrak{K}/\mathfrak{F}$. Nakayama [7] has extended the normal basis theorem to Galois division ring extensions of finite dimension n with outer Galois group of order n. More recently Kasch [6] has established the existence of a generalized normal basis for Galois extensions of certain simple rings.

In the present article, if $\mathfrak{G}=(G_1, \cdots, G_n)$ is a finite group of automorphisms of a ring $\mathfrak{K}$, and if $\mathfrak{F}$ is the fixring corresponding to $\mathfrak{G}$, then $\mathfrak{K}/\mathfrak{F}$ has a $\mathfrak{G}$-*normal basis* whenever $\mathfrak{K}$ has an independent $\mathfrak{F}$-basis of the form $u^{G_1}, \cdots, u^{G_n}$ $(u\in\mathfrak{K})$. Then u is a $\mathfrak{G}$-*normal* basis element of $\mathfrak{K}/\mathfrak{F}$. Contained in this article is a characterization of those extensions $\mathfrak{K}/\mathfrak{F}$ possessing a $\mathfrak{G}$-normal basis for which the $\mathfrak{G}$-normal basis elements have the following simple description: *every* $w\in\mathfrak{K}$ *with* $\mathfrak{G}$-*trace* $\sum_{i=1}^{n} w^{G_i}$ *which is regular in* $\mathfrak{F}$ *is a* $\mathfrak{G}$-*normal basis element of* $\mathfrak{K}/\mathfrak{F}$. It will be shown that the only proper Galois extensions (of the kind considered) having this property are those for which $\mathfrak{K}/\mathfrak{F}$ *has dimension* p^e *and* $\mathfrak{K}$ *has characteristic* p.[1] This determination follows as a corollary to the more general Theorem 1.

For the most part the methods of the present note are the same as those announced in [4], namely, when $\mathfrak{K}/\mathfrak{F}$ has a $\mathfrak{G}$-normal basis, essential use is made of the evident $\mathfrak{G}(\mathfrak{F})$-module operator isomorphism between $\mathfrak{G}(\mathfrak{F})$ and $\mathfrak{K}$, where $\mathfrak{G}(\mathfrak{F})$ denotes the group ring defined by $\mathfrak{G}$ and $\mathfrak{F}$.

In §4, the question of the existence of a $\mathfrak{G}$-normal basis is considered. In §5, an application of the foregoing results is given.

I wish to thank the referee for his constructive remarks, and, in particular, for observing that the proof of my earlier result for fields (which had been submitted to this journal for publication) was valid for more general rings.

Presented to the Society January 30, 1958; received by the editors October 18, 1957.

[1] This result contains some previous work in this direction. See [1, Theorem 1; 3, Lemma 1.4; 4] and [9, Theorem 1].

2. **The ring homomorphism ϕ.** If $\mathfrak{G}$ is a group of automorphisms of a ring $\mathfrak{R}$, then $\mathfrak{F}(\mathfrak{G})$ will denote the subring consisting of those elements of $\mathfrak{R}$ left fixed by each automorphism in $\mathfrak{G}$. Then $\mathfrak{R}/\mathfrak{F}$ is $\mathfrak{G}$-*Galois*, where $\mathfrak{F}=\mathfrak{F}(\mathfrak{G})$. If $\mathfrak{F}$ is any subring, $\mathfrak{G}(\mathfrak{R}/\mathfrak{F})$ indicates the group of all automorphisms of $\mathfrak{R}$ which leave fixed each element of $\mathfrak{F}$. When $\mathfrak{G}=(G_1, \cdots, G_n)$ is a finite group of automorphisms of $\mathfrak{R}$, then the $\mathfrak{G}$-*trace of* $x\in\mathfrak{R}$ is the sum $T_{\mathfrak{G}}(x)=x^{G_1}+\cdots+x^{G_n}$.[2]

For brevity, a simple ring with minimum condition will be called a *simple* ring. Let $\mathfrak{R}$ be a ring with identity 1, and suppose $\mathfrak{R}$ is a finitely generated right $\mathfrak{F}$-module, where $\mathfrak{F}$ is a simple subring containing 1. Then $\mathfrak{R}$ has an independent right $\mathfrak{F}$-basis and every right $\mathfrak{F}$-basis of $\mathfrak{R}$ has the same cardinality $[\mathfrak{R}:\mathfrak{F}]$, called the *dimension of* $\mathfrak{R}/\mathfrak{F}$.[3]

DEFINITION. Let $\mathfrak{R}$ be a ring simple with identity, and let $\mathfrak{F}$ be a simple subring of $\mathfrak{R}$ such that $\mathfrak{R}/\mathfrak{F}$ is $\mathfrak{G}$-Galois, $[\mathfrak{R}:\mathfrak{F}]$ is finite, and $\mathfrak{G}=(G_1, \cdots, G_n)$ has order $n=[\mathfrak{R}:\mathfrak{F}]$. If for some $u\in\mathfrak{R}$, $\mathfrak{R}$ has an independent right $\mathfrak{F}$-basis of the form $u^{G_1}, \cdots, u^{G_n}$, then $\mathfrak{R}/\mathfrak{F}$ *has a* $\mathfrak{G}$-*normal basis generated by* u. Then u is a $\mathfrak{G}$-*normal basis element*; a $\mathfrak{G}(\mathfrak{R}/\mathfrak{F})$-*normal basis* [*element*] is simply a *normal basis* [*element*].[4]

Let $\mathfrak{E}=\mathfrak{E}(\mathfrak{R})$ be the ring of all endomorphisms of the right $\mathfrak{F}$-module $\mathfrak{R}$. If $k\in\mathfrak{R}$, k^r signifies the "right multiplication" defined by: $x\to x^{k^r}=xk$ for every $x\in\mathfrak{R}$. The set $\mathfrak{F}^r=\{\alpha^r\in\mathfrak{E}\,|\,\alpha\in\mathfrak{F}\}$ is a subring of $\mathfrak{E}$ isomorphic to $\mathfrak{F}$. $\mathfrak{G}(\mathfrak{F}^r)$ represents the subring of $\mathfrak{E}$ generated by $\mathfrak{F}^r$ and a subgroup $\mathfrak{G}$ of $\mathfrak{G}(\mathfrak{R}/\mathfrak{F})$. When $\mathfrak{R}/\mathfrak{F}$ has a $\mathfrak{G}$-normal basis, and $\mathfrak{G}=(G_1, \cdots, G_n)$, it is trivial to verify that $G_1, \cdots, G_n$ is an independent right $\mathfrak{F}^r$-basis of $\mathfrak{G}(\mathfrak{F}^r)$. Since $\alpha^rG=G\alpha^r$ for every $\alpha^r\in\mathfrak{F}^r$ and every $G\in\mathfrak{G}$, the elements $G_1, \cdots, G_n$ constitute a left $\mathfrak{F}^r$-basis of $\mathfrak{R}$ as well. Since $\mathfrak{F}^r$ is a simple ring, i.e., since $\mathfrak{F}$ may be identified with the full ring of $k\times k$ matrices with elements in a division ring, $\mathfrak{G}(\mathfrak{F}^r)$ has finite dimension over some division subring; for such rings it is known that every element of $\mathfrak{G}(\mathfrak{F}^r)$ is either regular or a zero divisor in $\mathfrak{G}(\mathfrak{F}^r)$, a fact which will be used in the following familiar[5] characterization of normal basis elements of $\mathfrak{R}/\mathfrak{F}$.

LEMMA 1. *Let* $\mathfrak{R}/\mathfrak{F}$ *have a* $\mathfrak{G}$-*normal basis generated by* u. *Then* u^σ *is*

---

[2] If σ is any endomorphism of $\mathfrak{R}$, x^σ will denote the image of $x\in\mathfrak{R}$ under σ.

[3] For this result see [5, p. 134]. I am indebted to the referee for this reference, as well as that given in Footnote 7.

[4] I wish to emphasize that the present definition of a $\mathfrak{G}$-normal basis does not coincide necessarily with Kasch's normal basis defined in [6]. The concepts do coincide, however, when $\mathfrak{G}(\mathfrak{R}/\mathfrak{F})$ is outer. See §4 of the present article.

[5] R. Stauffer, *The construction of a normal basis in a separable normal extension field*, Amer. J. Math. vol. 48 (1936) p. 596, Theorem 5.

also a $\mathfrak{G}$-normal basis element of $\mathfrak{K}/\mathfrak{F}$, $\sigma\in\mathfrak{G}(\mathfrak{F}^r)$, if and only if σ is regular in $\mathfrak{G}(\mathfrak{F}^r)$.

PROOF. Since the automorphisms $G_1, \cdots, G_n$ form an $\mathfrak{F}^r$-basis of $\mathfrak{G}(\mathfrak{F}^r)$, u^σ is a $\mathfrak{G}$-normal basis element of $\mathfrak{K}/\mathfrak{F}$ if and only if σ is not a left divisor of zero in $\mathfrak{G}(\mathfrak{F}^r)$. Then by the argument preceding the lemma, σ must be regular in $\mathfrak{G}(\mathfrak{F}^r)$.

In order that w be a $\mathfrak{G}$-normal basis element in $\mathfrak{K}/\mathfrak{F}$ it is trivially necessary that the trace $T_{\mathfrak{G}}(w)$ be a nonleft divisor of zero in $\mathfrak{F}$. Since $\mathfrak{F}$ is isomorphic to a full ring of $k\times k$ matrices with elements in a division ring, this is the requirement that $T_{\mathfrak{G}}(w)$ be regular in $\mathfrak{F}$. We wish to characterize those extensions for which the converse is true, namely, every w with regular $\mathfrak{G}$-trace is a $\mathfrak{G}$-normal basis element in $\mathfrak{K}/\mathfrak{F}$. To do this we have found it interesting (and expedient) to generalize the problem. We consider intermediate rings Δ, $\mathfrak{K}\supseteq\Delta\supseteq\mathfrak{F}$, for which the extension $\mathfrak{K}/\Delta$ is $\mathfrak{H}$-Galois, where $\mathfrak{H}$ is a normal subgroup of $\mathfrak{G}$. Then if $\mathfrak{P}$ is the subgroup of $\mathfrak{G}(\Delta/\mathfrak{F})$ induced by $\mathfrak{G}$, we show that

(A) *w is a $\mathfrak{G}$-normal basis element of $\mathfrak{K}/\mathfrak{F}$*

implies

(B) *the $\mathfrak{H}$-trace of w is a $\mathfrak{P}$-normal basis element of $\Delta/\mathfrak{F}$.*

In this more general setting (the normal basis elements of the trivial extension $\Delta/\mathfrak{F}$, when $\Delta=\mathfrak{F}$, are precisely the non left zero divisors in $\mathfrak{F}$) we seek a determination of those extensions $\mathfrak{K}/\mathfrak{F}$ for which every w satisfying condition (B) also satisfies (A). The preliminary facts are collected in the following lemma.

LEMMA 2. *Let $\mathfrak{K}/\mathfrak{F}$ have a $\mathfrak{G}$-normal basis generated by u, and let Δ be any simple intermediate ring such that $\mathfrak{K}/\Delta$ is $\mathfrak{H}$-Galois, where $\mathfrak{H}=(H_1, \cdots, H_h)$ is normal in $\mathfrak{G}$, and $h=[\mathfrak{K}:\Delta]$. Then,*

(1) *$\Delta/\mathfrak{F}$ has a $\mathfrak{P}$-normal basis generated by $T_{\mathfrak{H}}(u)$, where $\mathfrak{P}$ is the group of automorphisms of $\Delta/\mathfrak{F}$ induced by $\mathfrak{G}$.*

(2) *The kernel of the (natural) homomorphism ϕ (defined below) of $\mathfrak{G}(\mathfrak{F}^r)$ onto $\mathfrak{P}(\mathfrak{F}^r)$ is the ideal $\mathfrak{B}$ generated by H_i-1, $i=1, 2, \cdots, h$, where $H_1=1$ is the identity automorphism.*

(3) *A necessary and sufficient condition that* (B) *imply* (A) *when $w=u^\sigma$ is for σ to be regular in $\mathfrak{G}(\mathfrak{F}^r)$ whenever $\phi(\sigma)$ is regular in $\mathfrak{P}(\mathfrak{F}^r)$.*

PROOF. (1) Let $P_1, \cdots, P_q$, $q=n/h$, be a complete set of coset representatives of $\mathfrak{G}$ relative to $\mathfrak{H}$. Then the isomorphisms $\overline{P}_1, \cdots, \overline{P}_q$ of Δ in $\mathfrak{K}$ induced by the automorphisms $P_1, \cdots, P_q$, respectively, are distinct. Since $\mathfrak{H}$ is normal in $\mathfrak{G}$ the $\overline{P}_i$ are actually automorphisms of Δ, so that $\mathfrak{P}=(\overline{P}_1, \cdots, \overline{P}_q)$. $\mathfrak{P}$ is actually isomorphic to $\mathfrak{G}/\mathfrak{H}$ under the correspondence $\overline{P}_i\rightarrow P_i\mathfrak{H}$, so that $\Delta/\mathfrak{F}$ is

evidently $\mathfrak{P}$-Galois. The dimension relation (cf. [5, p. 138]) $[\mathfrak{K}:\Delta][\Delta:\mathfrak{F}]=[\mathfrak{K}:\mathfrak{F}]=n$ implies $[\Delta:\mathfrak{F}]=n/h=q$, the order of $\mathfrak{P}$. That $T_{\mathfrak{H}}(u)$ generates a $\mathfrak{P}$-normal basis of $\Delta/\mathfrak{F}$ is quite easily seen.

(2) We have seen that the automorphisms $G_1, \cdots, G_n$ form an independent $\mathfrak{F}^r$-basis of $\mathfrak{G}(\mathfrak{F}^r)$ so that each $\sigma\in\mathfrak{G}(\mathfrak{F}^r)$ is uniquely expressible as

$$\sigma = \sum_{j=1}^{q}\sum_{i=1}^{h} H_iP_j(\alpha_{ij})^r \qquad (\alpha_{ij}\in\mathfrak{F}).$$

The homomorphism ϕ is defined by

$$\phi(\sigma) = \sum_{j=1}^{q}\sum_{i=1}^{h} \overline{P}_i(\alpha_{ij})^r,$$

so that σ is in the kernel $\mathfrak{B}$ of ϕ if and only if $\sum_{i=1}^{h}\alpha_{ij}=0, j=1, \cdots, q$. Then $\sum_{i=1}^{h} H_iP_j(\alpha_{ij})^r=\sum_{i=2}^{h}(H_i-1)P_j(\alpha_{ij})^r$. Thus $\mathfrak{B}$ is the ideal generated by the $\{H_i-1\}$. (Since $\mathfrak{H}$ is normal in $\mathfrak{G}$, $\mathfrak{B}$ is actually the right ideal generated by these elements.)

(3) The center of $\mathfrak{G}(\mathfrak{F}^r)$ contains $\tau=\sum_{i=1}^{h} H_i$; moreover d^r lies in Δ for all d. These two facts combined with the knowledge that $d^\sigma=d^{\phi(\sigma)}$, for all $d\in\Delta$ and $\sigma\in\mathfrak{G}(\mathfrak{F}^r)$ yield:

$$T_{\mathfrak{H}}(x^\sigma) = x^{\sigma\tau} = (x^\tau)^\sigma = (x^\tau)^{\phi(\sigma)} = T_{\mathfrak{H}}(x)^{\phi(\sigma)}.$$

Since u is a $\mathfrak{G}$-normal basis element of $\mathfrak{K}/\mathfrak{F}$, by Lemma 1, u^σ is also if and only if σ is regular in $\mathfrak{G}(\mathfrak{F}^r)$. By (1) of the present lemma $T_{\mathfrak{H}}(u)$ is a $\mathfrak{P}$-normal basis element of $\Delta/\mathfrak{F}$. Moreover $T_{\mathfrak{H}}(u^\sigma)=T_{\mathfrak{H}}(u)^{\phi(\sigma)}$ so that $T_{\mathfrak{H}}(u^\sigma)$ is a $\mathfrak{P}$-normal basis element of $\Delta/\mathfrak{F}$ if and only if $\phi(\sigma)$ is regular in $\mathfrak{P}(\mathfrak{F}^r)$. Thus for $w=u^\sigma$, (B) implies (A) is equivalent to that statement that σ is regular in $\mathfrak{G}(\mathfrak{F}^r)$ whenever $\phi(\sigma)$ is regular in $\mathfrak{P}(\mathfrak{F}^r)$.

3. A lemma on group rings. The condition that (B)$\Rightarrow$(A) is restated as:

(I) *w is a $\mathfrak{G}$-normal basis element of $\mathfrak{K}/\mathfrak{F}$ whenever $T_{\mathfrak{H}}(w)$ is a $\mathfrak{P}$-normal basis element of $\Delta/\mathfrak{F}$.*

From Lemma 2(3) it is clear that (I) is equivalent to:

(i) *σ is regular in $\mathfrak{A}=\mathfrak{G}(\mathfrak{F}^r)$ whenever $\bar{\sigma}$ is regular in the difference ring $\overline{\mathfrak{A}}=\mathfrak{A}-\mathfrak{B}$, where $\bar{\sigma}$ is the image of σ under the canonical homomorphism of $\mathfrak{A}$ onto $\overline{\mathfrak{A}}$.*

That (i) is equivalent to the assertion that $\mathfrak{B}$ is a quasi-regular (q.r.) ideal can be seen easily as follows: If $\bar{\sigma}$ is regular in $\overline{\mathfrak{A}}$, then $\sigma\rho=1+b$, with $\rho\in\mathfrak{A}$, $b\in\mathfrak{B}$. If $\mathfrak{B}$ is q.r., both $y=\sigma\rho$, and σ are regular, and $\sigma^{-1}=\rho y^{-1}$. Conversely (i) implies that $1+b$ is regular for each $b\in\mathfrak{B}$; $\mathfrak{B}$ is q.r.

It is now evident that we actually are seeking to characterize the condition:

(ii) $\mathfrak{B}$ *is contained in the radical of* $\mathfrak{A}$.

When $\mathfrak{F}$ is a field, and $\mathfrak{B} \neq 0$, it is known that (ii) holds (if and) only if:

(II) $\mathfrak{F}$ *has prime characteristic* p, *and* $h = p^e$.

In a routine fashion this result may be extended as follows:

LEMMA 3. *Let* $\mathfrak{G}$ *be a group of finite order, and* $\mathfrak{H} = (H_1, \cdots, H_h)$ *be a normal subgroup of* $\mathfrak{G}$ *different from the identity subgroup* (1). *Let* $\mathfrak{F}$ *be a simple ring (with minimum condition), and let* $\mathfrak{B}$ *be the ideal of the group ring* $\mathfrak{G}(\mathfrak{F})$ *generated by all* $H_i - 1$, $i = 1, \cdots, h$. *Then* $\mathfrak{B}$ *is contained in the radical of* $\mathfrak{G}(\mathfrak{F})$ *if and only if* (II) *holds.* (*Then* $\mathfrak{B}$ *is nilpotent.*)

PROOF. Suppose $\mathfrak{B}$ is contained in the radical $\mathfrak{R}$ of $\mathfrak{G}(\mathfrak{F})$. As was seen before $\mathfrak{G}(\mathfrak{F})$ has finite dimension over a division subring so that $\mathfrak{R}$, and hence $\mathfrak{B}$, is nilpotent. Then the algebra $\mathfrak{H}^*$ over the center $\mathfrak{Z}$ of $\mathfrak{F}$ having $H_i - 1$, $i = 2, \cdots, h$ (where $H_1 = 1$), as a basis is also nilpotent. Since $\mathfrak{Z}$ is a field, this is possible only if both $\mathfrak{Z}$ has characteristic p and $h = p^e$.[6]

Conversely let $\mathfrak{F}$ have prime characteristic p, and $h = p^e$. Then the algebra $\mathfrak{H}^*$ defined above is nilpotent; $(\mathfrak{H}^*)^k = 0$ for some integer k.[7] Since $\mathfrak{B} = \mathfrak{A}\mathfrak{H}^* = \mathfrak{H}^*\mathfrak{A}$, where $\mathfrak{A} = \mathfrak{G}(\mathfrak{F})$, certainly $\mathfrak{B}^k = 0$ also; $\mathfrak{B} \subseteq \mathfrak{R}$.

In view of this lemma, and the remarks preceding, we now have

THEOREM 1. *Let* $\mathfrak{K}$, Δ, *and* $\mathfrak{F}$ *be as in Lemma* 2, *with* $\mathfrak{K} \neq \Delta$. *Then* (I) *and* (II) *are equivalent.*[8]

When Δ is set equal to $\mathfrak{F}$ in Theorem 1, one obtains the

COROLLARY. *Let* $\mathfrak{K}$ *be a simple ring, and* $\mathfrak{F}$ *a proper simple subring such that* $\mathfrak{K}/\mathfrak{F}$ *has a* $\mathfrak{G}$*-normal basis. Then every element in* $\mathfrak{K}$ *with regular* $\mathfrak{G}$*-trace is a* $\mathfrak{G}$*-normal basis element if and only if both* $\mathfrak{F}$ *has prime characteristic* p *and* $[\mathfrak{K} : \mathfrak{F}] = p^e$.

In case $\mathfrak{F}$ is a division ring, the corollary shows, when $\mathfrak{K} \neq \mathfrak{F}$, that *every element of* $\mathfrak{K}$ *with nonzero* $\mathfrak{G}$*-trace is a* $\mathfrak{G}$*-normal basis element if*

---

[6] It is well known that if $\mathfrak{H}^*$ is the radical of $\mathfrak{H}(\mathfrak{Z})$, then $\mathfrak{Z}$ must have prime characteristic p dividing h. If $h \neq p^e$, then $\mathfrak{H}$ contains an element S of prime order $q \neq p$, and such that, for $\mathfrak{L} = (S)$, $\mathfrak{L}(\mathfrak{Z})$ is semi-simple, which is impossible since $\mathfrak{L}(\mathfrak{Z}) \neq 0$ is nilpotent.

[7] An algebra with a nilpotent basis is itself nilpotent. See J. H. M. Wedderburn, Ann. of Math. (2) 38 (1937) p. 854, Theorem 1.

[8] The proof of [3, Lemma 1.3] provides an elementary proof of the implication (II)$\Rightarrow$(I) in the case $\mathfrak{K}/\mathfrak{F}$ is a cyclic field extension.

and only if $\mathfrak{F}$ *has characteristic* p, *and* $[\mathfrak{K}:\mathfrak{F}]=p^e$.[9]

4. Existence of a $\mathfrak{G}$-normal basis. In this section conditions which imply that $\mathfrak{K}/\mathfrak{F}$ possesses a $\mathfrak{G}$-normal basis are noted. First let $\mathfrak{G}$ be a group of finite order n of outer automorphisms of a simple ring $\mathfrak{K}$. If $\mathfrak{K}/\mathfrak{F}$ is $\mathfrak{G}$-Galois, then the results of Nakayama [8] show that (i) $\mathfrak{F}$ is simple, (ii) $\mathfrak{G}=\mathfrak{G}(\mathfrak{K}/\mathfrak{F})$, and (iii) $[\mathfrak{K}:\mathfrak{F}]=n$. Then Kasch's theorem [6, Satz 7] applies—$\mathfrak{K}/\mathfrak{F}$ possesses a $(\mathfrak{G}(\mathfrak{K}/\mathfrak{F})-)$ normal basis. This observation is a special case of the next theorem which is also obtained by application of results of Kasch and Nakayama.

THEOREM 2. *Let* $\mathfrak{K}$ *be a simple ring, and let* $\mathfrak{F}$ *be a simple subring such that* (1) $[\mathfrak{K}:\mathfrak{F}]$ *is finite*, (2) $\mathfrak{K}/\mathfrak{F}$ *is* $\mathfrak{G}$*-Galois, where* $\mathfrak{G}$ *has finite order* $n=[\mathfrak{K}:\mathfrak{F}]$, *and* (3) *the centralizer* $\mathfrak{F}'$ *of* $\mathfrak{F}$ *in* $\mathfrak{K}$ *is simple. Then* $\mathfrak{K}/\mathfrak{F}$ *possesses a* $\mathfrak{G}$*-normal basis*

PROOF. Since $\mathfrak{G}(\mathfrak{F}^r)$ is a ring with minimum condition, by [6, Satz 4], it suffices to show that $\mathfrak{G}(\mathfrak{F}^r)$ is a *right scalar ring* of the endomorphism ring $\mathfrak{E}$ of $\mathfrak{K}/\mathfrak{F}$, and that $[\mathfrak{E}:\mathfrak{G}(\mathfrak{F}^r)]=n$, i.e., that $\mathfrak{E}$ has an independent right $\mathfrak{G}(\mathfrak{F}^r)$-basis of length n. By [8, Theorem 3] the group $\mathfrak{G}=\mathfrak{G}(\mathfrak{K}/\mathfrak{F})$ is regular so that $n=(\mathfrak{G}:\mathfrak{J})[\mathfrak{F}':\mathfrak{C}]$, where $q=(\mathfrak{G}:\mathfrak{J})$ is the index in $\mathfrak{G}$ of the subgroup $\mathfrak{J}$ of all inner automorphisms of $\mathfrak{K}$, and $\mathfrak{C}$ is the center of $\mathfrak{K}$. The completion $\mathfrak{G}\mathfrak{J}$ of $\mathfrak{G}$ is evidently $\mathfrak{G}$ so that $q=(\mathfrak{G}:\mathfrak{J}\cap\mathfrak{G})$. Thus $\mathfrak{J}\cap\mathfrak{G}$ has order $d=[\mathfrak{F}':\mathfrak{C}]$. If the inner automorphisms effected by regular elements $x_1, \cdots, x_d$ constitute $\mathfrak{J}\cap\mathfrak{G}$, then it is clear that $x_1, \cdots, x_d$ is an independent $\mathfrak{C}$-basis of $\mathfrak{F}'$. By the criterion of [6, Hilfssatz 1], the equation $(\mathfrak{G}:\mathfrak{J}\cap\mathfrak{G})[\mathfrak{F}':\mathfrak{C}]=n$ implies that the elements $g_1, \cdots, g_n$ of $\mathfrak{G}$ are right linearly independent over $\mathfrak{K}^r$. Kasch's arguments in the proof of [6, Satz 7, pp. 457–458] may be transferred step-by-step to the present case. These we summarize as follows:

(X) Since $[\mathfrak{E}:\mathfrak{K}^r]=n$ by [6, Hilfssatz 5], $\mathfrak{E}=\mathfrak{G}(\mathfrak{K}^r)$, and $g_1, \cdots, g_n$ is an independent right $\mathfrak{K}^r$-basis of $\mathfrak{E}$; also $\mathfrak{E}=\mathfrak{K}g_1+\cdots+\mathfrak{K}g_n$.

(Y) If $w_1, \cdots, w_n$ is an independent right $\mathfrak{F}$-basis of $\mathfrak{K}$, then $\mathfrak{E}=\sum_{i=1}^{n} w_i^r(\mathfrak{F}^r g_1+\cdots+\mathfrak{F}^r g_n)$.

(Z) Since $[\mathfrak{E}:\mathfrak{F}^r]=n^2$, and since $\mathfrak{G}(\mathfrak{F}^r)=\mathfrak{F}^r g_1+\cdots+\mathfrak{F}^r g_n$ $(=g_1\mathfrak{F}^r+\cdots+g_n\mathfrak{F}^r)$ has dimension n over $\mathfrak{F}^r$, then $w_1^r, \cdots, w_n^r$ must be an independent right $\mathfrak{G}(\mathfrak{F}^r)$-basis of $\mathfrak{E}$ as desired.

Theorem 1 and its corollary are now applicable to the simple ex-

---

[9] *Added in proof*: This fact, in the case K itself is a division ring, has been obtained independently by Onerada and Tominaga, *On strictly Galois extensions of degree* p^e *over a division ring of characteristic* p, Math. J. Okayama University vol. 7 (1957) pp. 77–81.

tensions $\mathfrak{K}/\mathfrak{F}$ of Theorem 2. In Theorem 1, the assumption that $\mathfrak{H}$ be normal in $\mathfrak{G}$ implies that every automorphism of $\mathfrak{G}$ maps Δ onto itself. Then, as was noted in Lemma 2, $\Delta/\mathfrak{F}$ is $\mathfrak{P}$-Galois.

Although it is immediate, it perhaps should be noted that the assumption on the simplicity of $\mathfrak{F}'$ in Theorem 2 is automatically satisfied when $\mathfrak{K}$ is a division ring. The same is true whenever $\mathfrak{G}$ is an outer group of automorphisms. In this latter case, as was noted in the remarks preceding Theorem 2, $\mathfrak{G}$ is then the Galois group $\mathfrak{G}(\mathfrak{K}/\mathfrak{F})$.

5. **Completely basic extensions.** Let $\mathfrak{K}$ and $\mathfrak{F}$ be division rings, such that $\mathfrak{K}/\mathfrak{F}$ is $\mathfrak{G}$-Galois where $\mathfrak{G}=\mathfrak{G}(\mathfrak{K}/\mathfrak{F})$ is a finite group of outer automorphisms. If Δ is any intermediate division ring, $\mathfrak{H}=\mathfrak{G}(\mathfrak{K}/\Delta)$ is also outer. Both extensions $\mathfrak{K}/\mathfrak{F}$ and $\mathfrak{K}/\Delta$ possess normal bases. Let $P_1, P_2, \cdots, P_q$ be right coset representatives of $\mathfrak{G}$ relative to $\mathfrak{H}$, so that for $u\in\mathfrak{K}$, $T_{\mathfrak{G}}(u)=v^{P_1}+\cdots+v^{P_q}$, where $v=T_{\mathfrak{H}}(u)\in\Delta$. Now suppose $\mathfrak{K}$ has prime characteristic p, and $(\mathfrak{K}:\mathfrak{F})=p^e$. If u is a normal basis element of $\mathfrak{K}/\mathfrak{F}$, $T_{\mathfrak{G}}(u)\neq 0$, so that $v\neq 0$. Thus by the corollary to Theorem 1, u is a normal basis element of $\mathfrak{K}/\Delta$ also. Employing terminology used in [3] we shall say that an outer Galois extension $\mathfrak{K}/\mathfrak{F}$ possessing a normal basis is *completely basic* if every normal basis element of $\mathfrak{K}/\mathfrak{F}$ is also a normal basis element of $\mathfrak{K}/\Delta$, where Δ is any intermediate ring for which $\mathfrak{K}/\Delta$ possesses a normal basis. Completely basic field extensions were studied in [3] where it was shown that every Kummer field extension is completely basic. Until now the only known examples of completely basic extensions were Abelian field extensions. The above example not only permits us to assert the existence of completely basic extensions which are not fields but it also establishes the existence of completely basic field extensions which are not Abelian. This latter statement is a consequence of the fact that normal (or Galois) field extensions of degree p^e over a field of prime characteristic p need not have an Abelian Galois group.

References

1. A. S. Amitsur, *Non-commutative cyclic fields*, Duke Math. J. vol. 21 (1954) pp. 87–106.

2. H. Cartan, *Théorie de Galois pour les corps non-commutatifs*, Ann. École Norm. Sup. vol. 64 (1947) pp. 59–77.

3. C. C. Faith, *Extensions of normal bases and completely basic fields*, Trans. Amer. Math. Soc. vol. 85 (1957) pp. 406–427.

4. ———, *Normal extensions in which every element with nonzero trace is a normal basis element*, Bull. Amer. Math. Soc. vol. 63 (1957) pp. 95–96.

5. N. Jacobson, *Structure of rings*, Amer. Math. Soc. Colloquium Publications, vol. 37, 1956.

6. F. Kasch, *Über den Endomorphismring eines Vektoraumes und den Satz von der Normal basis*, Math. Ann. vol. 126 (1953) pp. 447–463.

7. T. Nakayama, *Normal basis of a quasi-field*, Proc. Imp. Acad. Tokyo vol. 16 (1940) pp. 532–536.

8. ———, *Galois theory of simple rings*, Trans. Amer. Math. Soc. vol. 73 (1952) pp. 276–292.

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

THE PENNSYLVANIA STATE UNIVERSITY

REMARK ON AUTOMORPHISMS OF GROUPS

MAURICE AUSLANDER

Let G be a group with center C. Let α be an automorphism of G and n an integer such that α^n is an inner automorphism. Thus there is a g in G such that $\alpha^n(x) = gxg^{-1}$ for all x in G. Applying α to both sides of this equation we have that $\alpha^n(\alpha(x)) = \alpha(g)\alpha(x)\alpha(g)^{-1}$ for all x in G. Since every element in G can be written as $\alpha(x)$ for some x in G, it follows that g and $\alpha(g)$ induce the same inner automorphism of G. Thus $g^{-1}\alpha(g) = c$ where c is in C. Now if y is in C, then $(gy)^{-1}\alpha(gy) = g^{-1}y^{-1}gc\alpha(y) = cy^{-1}\alpha(y)$. Thus as x runs through all x in G which induce the inner automorphism α^n, the elements of the form $x^{-1}\alpha(x)$ run through the entire coset cC_α in C/C_α, where C_α is the subgroup of C consisting of all elements of the form $y^{-1}\alpha(y)$ (y in C). This element of C/C_α depends on n and will be denoted by $o(\alpha, n)$.

THEOREM. *If all the fixed points of α are in the center of G, then $\alpha^{n^2} = 1$. Further $\alpha^n = 1$ if and only if $o(\alpha, n) = (1)$.*

PROOF. Let g in G induce the inner automorphism α^n. Then by the previous remarks we have that $g^{-1}\alpha(g) = c$ where c is in C. Thus the abelian subgroup of G generated by C and g is stable under α. Since $\alpha^n(g) = g$, it follows that $\prod_{i=0}^{n-1} \alpha^i(g)$ is a fixed point of α and is thus in C. On the other hand, since $\alpha(g) = gc$, we have that $\prod_{i=0}^{n-1} \alpha^i(g) = g^n d$ for some d in C. Therefore g^n is in C which means that $\alpha^{n^2} = 1$.

It is clear that if $\alpha^n = 1$, then $o(\alpha, n) = (1)$. Suppose $o(\alpha, n) = (1)$. Then by our introductory remarks, we can choose a g in G such that g induces the inner automorphism α^n and $g^{-1}\alpha(g) = 1$. Thus g is a fixed point of α. Consequently g is in the center of G, which means that $\alpha^n = 1$.

Received by the editors September 17, 1957.