SOME NOTES ON THE GENERAL GALOIS THEORY OF RINGS

F. R. DeMEYER

(Received January 25, 1965)

Introduction

In [2] M. Auslander and O. Goldman introduced the notion of a Galois extension of commutative rings. Further work by D. K. Harrison [9] indicates that the notion of a Galois extension will have significant applications in the general theory of rings. T. Kanzaki, in this journal, proved a “Fundamental Theorem of Galois Theory” for an outer Galois extension of a central separable algebra over a commutative ring. We generalize, complete, and give a new shorter proof of this result. The inspiration for the improvements in Kanzaki’s result came from a paper by S. U. Chase, D. K. Harrison and A. Rosenberg [4].

This author in [6] began the study of ‘Galois algebras’. These are not necessarily commutative Galois (in the sense of [2]) extensions of a commutative ring. Here we continue that study by extending some of the results in [4] and by proving a generalized normal basis type theorem in this setting. This paper forms a portion of the author’s Doctoral Dissertation at the University of Oregon. The author is indebted to D. K. Harrison for his advice and encouragement.

Section 0

Throughout Λ will denote a K algebra, C will denote the center of Λ (\(C=\mathfrak{Z}(\Lambda)\)). G will denote a finite group represented as ring automorphisms of Λ and Γ the subring of all elements of Λ left invariant by all the automorphisms in G (Γ=\(\Lambda^G\)).

Let Δ(Λ : G) be the crossed product of Λ and G with trivial factor set. That is

\[
\Delta(\Lambda : G) = \Sigma_{\sigma \in G}\Lambda U_{\sigma} \quad \text{such that}
\]

\[
x_1 U_{\sigma} x_2 U_{\tau} = x_1 \sigma(x_2) U_{\sigma \tau} \quad x_1, x_2 \Lambda ; \sigma, \tau \in G.
\]

This work was done while the author held a National Science Foundation Cooperative Fellowship.
View $\Lambda$ as a right $\Gamma$ module and define

$$j: \Delta(\Lambda : G) \to \text{Hom}_r(\Lambda, \Lambda)$$

by

$$j(aU_\sigma)x = a\sigma(x) \quad a, x \in \Lambda; \sigma \in G.$$

**Theorem 1.** The following are equivalent:

- $A$. $\Lambda$ is finitely generated projective as a right $\Gamma$ module and $j: \Delta(\Lambda : G) \to \text{Hom}_r(\Lambda, \Lambda)$ is an isomorphism.
- $B$. There exists $x_1, \ldots, x_n; y_1, \ldots, y_n \in \Lambda$ such that

$$\Sigma_i x_i \sigma(y_i) = \begin{cases} 1 & \sigma = e \\ 0 & \sigma \neq e \end{cases} \quad \text{for every } \sigma \in G.$$

Following Auslander and Goldman, Kanzaki called $\Lambda$ a Galois extension of $\Gamma$ in case $A$ held. Condition $B$ was discovered for commutative rings by S. U. Chase, D. K. Harrison and A. Rosenberg in [4]. We call $\Lambda$ a Galois extension of $\Gamma$ with group $G$ if either $A$ or $B$ holds.

Our proof of theorem 1 parallels the proof given for theorem (1.3) of [4]. First we prove that $B$ implies $A$.

Define $f_i \in \text{Hom}_r(\Lambda, \Gamma)$ by $f_i(x) = \Sigma_{\sigma \in G} \sigma(y_i x)$ $x \in \Lambda, \sigma \in G$. For any $x \in \Lambda$

$$\Sigma_i x_i f_i(x) = \Sigma_i x_i \sigma(y_i) \sigma(x) = x.$$ 

Thus by the Dual Basis lemma, $\Lambda$ is finitely generated and projective as a right $\Gamma$ module.

Now we show $j: \Delta(\Lambda : G) \to \text{Hom}_r(\Lambda, \Lambda)$ is an isomorphism. Let $U_\sigma$ be a Basis element in $\Delta(\Lambda : G)$. Then

$$\Sigma_i x_i f_i(U_\sigma) = \Sigma_i x_i \sigma(y_i) U_\sigma = \Sigma_i x_i \sigma(y_i) U_\sigma = U_\tau.$$

Hence by linearity, for all $U \in \Delta(\Lambda : G)$

$$U = \Sigma_i x_i f_i(U_\sigma) = \Sigma_i x_i \sigma(y_i) U_\sigma = U_\tau.$$

Thus if $j(U)[x] = 0$ for all $x \in \Lambda$, then $U = 0$ so $j$ is a monomorphism.

To prove $j$ is onto let $h \in \text{Hom}_r(\Lambda, \Lambda)$ and let

$$U = \Sigma_i x_i h(x_i) U_\sigma y_i, \quad U \in \Delta(\Lambda : G)$$

for any $x \in \Lambda$, $j(U)[x] = \Sigma_i x_i h(x_i) \sigma(y_i x_i)$

$$= h(\Sigma_i x_i \sigma(y_i x_i)) = h(\Sigma_i x_i f_i(x)) = h(x).$$

Thus $j$ is an isomorphism.

To prove the converse, we first show that
\[(*) \quad \text{Hom}_\Gamma(A, \Gamma) = j(t \cdot \Lambda) \quad \text{where} \quad t = \sum_{\sigma \in G} U_\sigma.\]

Pick \(a \in \Lambda\), \(j(ta)[x] = \sum_{\sigma \in G} \sigma(ax) \in \Gamma\). So \(j(ta) \in \text{Hom}_\Gamma(A, \Gamma)\). Suppose \(f = j(y) \in \text{Hom}_\Gamma(A, \Gamma)\), \(y \in \Delta(\Lambda : G)\). If \(y = \sum a_\sigma U_\sigma\), then for all \(x \in \Lambda\), \(\sum a_\sigma \sigma(x) \in \Gamma\) so \(\rho(\sum a_\sigma \sigma(x)) = \sum a_\sigma \sigma(x) \) for all \(\rho \in G\). Thus \(\sum_{\rho \in G} \rho(a_\rho^{-1}) \tau(x) = \sum_{\rho \in G} a_\rho \tau(x)\), \((\tau = \rho \circ \sigma)\) but \(j\) is an isomorphism so \(\rho(a_\rho^{-1}) = a_\sigma\), so \(a_\sigma = \sigma(a)\), thus \(y = \sum \sigma(a) U_\sigma = \tau \cdot a\). This proves \((*)\).

Now we want to find \(x_1 \cdots x_n; y_1 \cdots y_n \in \Lambda\) satisfying \(B\). Let \(x_1 \cdots x_n, f_1 \cdots f_n\) be given by the Dual Basis Lemma. By \((*)\) there exists \(y_1 \cdots y_n \in \Lambda\) so that

\[f_i(x) = j(ty_i)x.\]

Let \(U = \sum_{i \leq n} x_i y_i \in \Delta(\Lambda : G)\). Then \(j(U)[x] = \sum_{\sigma \in G} x_i y_i = x\). \(j\) is an isomorphism so \(U = \sum_{i \leq n} x_i y_i = 1\). Thus \(\sum_{i \leq n} x_i y_i = \left\{ \begin{array}{ll} 1 & \sigma = 1 \\ 0 & \sigma = 1 \end{array} \right\}\) so since \(j\) is an isomorphism, \(\sum_{i \leq n} \sigma(y_i) = \left\{ \begin{array}{ll} 1 & \sigma = 1 \\ 0 & \sigma = 1 \end{array} \right\}\) and this completes the proof.

**Section I**

In this section we prove a sharper version of Kanzaki's result. All notation is as it was in section 0.

**Lemma 2.** Let \(\Lambda\) be separable over \(C\), and assume \(G\) induces a group of automorphisms of \(C\) isomorphic to \(G\) and that \(C\) is a Galois extension of \(C^G = K\). Then \(\Lambda\) is a Galois extension of \(\Lambda^G = \Gamma\) and there exists a 1–1 correspondence between the \(K\)-separable subalgebras \(\Omega\) of \(\Lambda\) containing \(\Gamma\) and the \(K\)-separable subalgebras \(A\) of \(C\) given by

\[A \rightarrow A \cdot \Gamma\]

\[\mathfrak{B}(\Omega) \leftarrow \Omega\]

**Proof.** \(\Lambda\) is a Galois extension of \(\Gamma\) by \(B\) of theorem 1 and by the hypothesis that \(C\) is Galois over \(K\).

By theorem \((A.3)\) of [2], \(K = \{\sigma \in G|x \in C\}\) so

\[\Gamma = K \cdot \Gamma\]

\[= \{\sigma \sigma(x)|x \in C\} \cdot \Gamma\]

\[= \{\sigma \sigma(x)|x \in C, t \in \Gamma\} \subseteq \Gamma, \quad (\Lambda^G = \Gamma).\]

Thus \(\Gamma = \{\sigma \sigma(x)|x \in \Lambda\}\) and there exists \(f \in \text{Hom}_\Gamma(A, \Gamma)\) \((f = \sum_{\sigma \in G} \sigma)\) and there exists an \(a \in \Lambda\) so that \(f(a) = 1\). Thus \(\Gamma\) is a direct summand of \(\Lambda\) as a \(\Lambda \cdot \Gamma\) module.

We now show \(\Gamma\) is separable over \(K\) by showing \(\Gamma\) is a projective
\( \Gamma \otimes_K \Gamma^0 \) module. \( \Lambda \oplus \Lambda' \cong \Lambda \otimes_K \Lambda^0 \) as \( \Lambda \otimes_K \Lambda^0 \) modules since \( \Lambda \) is separable over \( K \). Since \( \Gamma \) is a direct summand of \( \Lambda \) and the hypothesis insure that \( \Lambda \) is projective over \( K \) (\( \Lambda \) is finitely generated projective over \( C \) and \( C \) is finitely generated projective over \( K \)) the sequence \( 0 \to \Gamma \otimes_K \Gamma^0 \to \Lambda \otimes_K \Lambda^0 \) is exact. Thus \( \Lambda \oplus \Lambda' \cong \Lambda \otimes_K \Lambda^0 \) as \( \Gamma \otimes_K \Gamma^0 \) modules. By the symmetry of condition \( B \) of theorem 1, \( \Lambda \) is projective as both a left and right \( \Gamma \) module. (\( \Lambda \) is \( \Gamma - \Gamma \) projective.) So \( \Lambda \otimes_K \Lambda^0 \) is projective as a \( \Gamma \otimes_K \Gamma^0 \) module. Hence \( \Lambda \) and thus \( \Gamma \) is projective over \( \Gamma \otimes_K \Gamma^0 \).

Now define a homomorphism \( h: \Gamma \otimes_K C \to \Lambda \) by \( h(t \otimes c) = t \cdot c ; t \in \Gamma, c \in C \). Since \( C \) is Galois over \( K \), by theorem (1.7) of [4] or a glance at \( B \) of theorem 1, one sees that \( \Gamma \otimes_K C \) is Galois of \( \Gamma \) with the same group \( G \). (\( \sigma(t \otimes c) = t \otimes \sigma c \)). By lemma (1) of [6] or by a computation using \( B \) of theorem 1, \( h \) is an isomorphism.

Thus the center of \( \Gamma \) (denoted \( \mathcal{Z}(\Gamma) \)) is \( K \), for if \( x \in \mathcal{Z}(\Gamma) \) then \( x \in \mathcal{Z}(\Lambda) \), \( (\Lambda = h(\Gamma \otimes_K C)) \) so \( x \in C \). But \( x \in \Gamma \) implies \( x \in C^G \) so \( x \in K \).

Now we prove the 1-1 correspondence of the lemma. Let \( \Omega \) be a \( K \)-separable subalgebra of \( \Delta \) containing \( \Gamma \). Let \( A \) be a \( K \)-separable subalgebra of \( C \). Define

\[
\psi: \Omega \to \mathcal{Z}(\Omega) \\
(\gamma : A \to h(\Gamma \otimes_K)) \\
(\text{notice } \Gamma \otimes_K A \subseteq \Gamma \otimes_K C)
\]

If \( x \in \mathcal{Z}(\Omega) \) then \( x \) belongs to centralizer in \( \Lambda \) of \( \Gamma \) so \( x \in \mathcal{Z}(\Lambda) \) and \( \mathcal{Z}(\Omega) \subseteq C \). \( \mathcal{Z}(\Omega) \) is separable over \( K \) by theorem (3.3) of [2] thus \( \psi \) is well defined.

Since \( \Gamma \) is a central separable \( K \)-algebra, \( A \otimes_K \Gamma \) is a central separable \( A \) algebra (theorem (1.6) of [2]) thus \( h(\Gamma \otimes_K \Gamma) \) is a separable \( K \)-algebra, central over \( A \) and containing \( \Gamma \). Thus \( \gamma \) is well defined and \( \psi \gamma(A) = A \) for all \( K \)-separable subalgebras \( A \) of \( C \).

Now \( \gamma \psi(\Omega) = h(\mathcal{Z}(\Omega) \otimes_K \Gamma) \subseteq \mathcal{Z}(\Omega) \) and \( \gamma \psi(\Omega) \) is a central separable over \( \mathcal{Z}(\Omega) \). If \( \Omega \neq \gamma \psi(\Omega) \) then by theorems 3.3 and 3.5 of [2] there exist a central separable \( \mathcal{Z}(\Omega) \) algebra \( \Omega' \) such that

\[
\Omega = \gamma \psi(\Omega) \otimes \mathcal{Z}(\Omega) \Omega' \quad \text{and}
\]

thus \( \Omega' \) is contained in the centralizer in \( \Lambda \) of \( \Gamma \). But then \( \Omega' \subseteq C \). Thus \( \Omega = \mathcal{Z}(\Omega) \) and \( \gamma \psi(\Omega) = \Omega \). This proves the lemma.

Here is the generalization of Kanzaki's result:

**Theorem 3.** With the notation and hypotheses of lemma 2, assume \( C \) has no idempotents except 0 and 1. Then there is a one-one correspondence between the \( K \)-separable subalgebras of \( \Lambda \) containing \( \Gamma \) and the subgroups \( H \) of \( G \).
If \( \Omega \) is a \( K \)-separable subalgebra of \( \Lambda \) containing \( \Gamma \) then there exists a subgroup \( H \) of \( G \) so that \( \Omega = \Lambda^H \).

Moreover for all subgroups \( H \) of \( G \), \( \Lambda \) is Galois over \( \Lambda^H \) and if \( H \) is a normal subgroup of \( G \) then \( \Lambda^H \) in Galois over \( \Gamma \) with group \( G/H \).

Proof. By theorem (2.3) of [4] there is a one-one correspondence between the \( K \)-separable subalgebras of \( C \) and the subgroups of \( G \) given by \( H \mapsto C^H \). By lemma 2 there is a one-one correspondence between the \( K \)-separable subalgebras of \( C \) and the \( K \)-separable subalgebras of \( \Lambda \) containing \( \Gamma \) by

\[
\Lambda \rightarrow h(\Gamma \otimes_K A),
\]

Combining these two facts, we have the one-one correspondence, thus every \( K \)-separable subalgebra \( \Omega \) of \( \Lambda \) containing \( \Gamma \) is of the form \( \Lambda^H \) for some subgroup \( H \) of \( G \).

If \( H \) is a subgroup of \( G \) then by theorem (2.2) of [4] \( C \) is a Galois extension of \( C^H \) with group \( H \). The same elements which satisfy \( B \) of theorem 1 for \( C \) over \( C^H \) satisfy \( B \) of theorem 1 for \( \Lambda \) over \( \Lambda^H \). The same theorem in [4] and the same reasoning apply when \( H \) is a normal subgroup of \( G \). This completes the proof.

Section II

Now we expand our point of view. Let \( \Lambda \) be a faithful \( K \)-algebra and \( G \) a finite group represented as ring automorphisms of \( \Lambda \) so that \( \Lambda^G = K \). Then all the elements in \( G \) are \( K \)-algebra automorphisms of \( \Lambda \). As before, \( \Lambda \) is Galois over \( K \) or a Galois \( K \)-algebra in case either \( A \) or \( B \) of theorem 1 hold. In [6] the author showed:

**Lemma 4.** Assume \( \Lambda \) is a Galois \( K \)-algebra with group \( G \). If \( C = \text{Center of } \Lambda \) contains no idempotents except 0 and 1 then \( C = \Lambda^H \) where \( H = \{ \sigma \in G | \sigma(x) = x \text{ for all } x \in C \} \) and \( H \) is a normal subgroup of \( G \) so that \( C \) is a Galois extension of \( K \) with group \( G/H \).

Proof. See theorem (1) of [6].

We now prove a lemma which allows us to extend the range of application of Lemma 4.

**Lemma 5.** If \( K \) contains no idempotents except 0 and 1 and \( \Lambda \) is a Galois \( K \)-algebra then

\[
\Lambda = \Lambda e_1 \oplus \cdots \oplus \Lambda e_n \quad (e_i \text{ minimal central idempotents})
\]

and \( \Lambda e_i \) is a Galois extension of \( K \) with group \( J_i = \{ \sigma \in G | \sigma(e_i) = e_i \} \). Moreover \( \mathcal{O}(\Lambda e_i) = C e_i = \Lambda e_i^{H_i} \) where \( H_i \) is a normal subgroup of \( J_i \).
Proof. \( C \) is finitely generated projective and separable over \( K \) since \( \Lambda \) is finitely generated projective and separable over \( K \). By theorem (7) of [8] since \( K \) has no idempotents but 0 and 1

\[
C = \bigoplus \Sigma C e_i \quad e_i \text{ minimal idempotents in } C.
\]

thus

\[
\Lambda = \bigoplus \Sigma \Lambda e_i \quad e_i \text{ minimal central idempotents in } \Lambda.
\]

Let \( J_i = \{ \sigma \in G | \sigma(e_i) = e_i \} \). By the minimality of \( e_i \), \( \sigma(e_i) \cdot e_i = \begin{cases} 0 & \sigma \notin J_i \\ e_i & \sigma \in J_i \end{cases} \) so by theorem (7) of [8] \( \Lambda e_i \) is a Galois extension of \( K \) with group \( J_i \). \( C e_i = \mathbb{Z}(\Lambda e_i) \). Let \( H_i = \{ \sigma \in J_i | \sigma(x) = x \text{ for all } x \in C e_i \} \). Then by Lemma 3 \( H_i \) is a normal subgroup of \( J_i \) and \( \Lambda e_i^{H_i} = C e_i \). This completes the proof.

We note that if \( K \) has no idempotents except 0 and 1 this lemma reduces the study of Galois \( K \)-algebras to those already considered in Section 1 and to the study of central Galois algebras, i.e., Galois algebras \( \Lambda \) over \( K \) with group \( G \) so that \( \mathbb{Z}(\Lambda) = K \). We now give the structure of a broad class of central Galois algebras.

The class group “\( P(K) \)” of a commutative ring \( K \) was defined by A. Rosenberg and D. Zelinsky in [11] and they showed

1. If \( \Lambda \) is a central separable \( K \)-algebra and \( \sigma \) is an algebra automorphism of \( \Lambda \) of finite order \( n \) such that no element in \( P(K) \) has order dividing \( n \) then \( \sigma \) is an inner automorphism of \( \Lambda \), i.e., there exists a \( U_\sigma \in \Lambda \) such that \( \sigma(x) = U_\sigma x U_\sigma^{-1} \) for all \( x \in \Lambda \).

2. If \( K \) is a field, Principal Ideal Domain or local ring, then \( P(K) = 0 \).

If \( \Lambda \) is a central Galois \( K \)-algebra, then \( \Lambda \) is separable over \( K \), theorem (1) of [6]. Assume the elements of the Galois group \( G \) are inner on \( \Lambda \). Then for each \( \sigma \in G \) there is a \( U_\sigma \in \Lambda \) so that \( \sigma(x) = U_\sigma x U_\sigma^{-1} \) for all \( x \in \Lambda \). Pick a \( U_\sigma \) for each \( \sigma \in G \) and define \( a(\cdot, \cdot) \) mapping \( G \times G \) to \( U(K) = \text{Units of } K \) by

\[
a(\sigma, \tau) = U_\sigma U_\tau U_{\sigma \tau}^{-1}
\]

From the associative law in \( \Lambda \),

\[
a(\sigma \tau, \rho) a(\sigma, \tau) = a(\sigma, \tau \rho) a(\tau, \rho)
\]

for all \( \sigma, \tau, \rho \in G \). Thus \( a(\cdot, \cdot) \) is a 2-cocycle of \( G \) \( a(\cdot, \cdot) \in Z^2(G, U(K)) \).

A twisted group algebra \( KG_\sigma \) is a free \( K \) module with basis \( \{ U_\sigma \} \) \( \sigma \in G \) and multiplication given by \( U_\sigma U_\tau = U_{\sigma \tau} a(\sigma, \tau), a(\cdot, \cdot) \in Z^2(G, U(K)) \).

**Theorem 6.** If \( \Lambda \) is a central Galois extension of \( K \) with group \( G \), and if \( G \) is represented by inner automorphisms on \( \Lambda \) then

\[
\Lambda = KG_\sigma, \quad a(\cdot, \cdot) \in Z^2(G, U(K)).
\]
Proof. This is theorem 2 of [6].

This result gives a very clear picture of the central Galois algebras over \( K \) with Abelian group \( G \) if no element in \( P(K) \) has order dividing that of an element in \( G \).

Let \( \Lambda \) be a central Galois extension of \( K \) with Abelian group \( G \), and assume all the automorphisms in \( G \) are inner on \( \Lambda \). Then \( \Lambda = KG_a = \bigoplus \Sigma KU_a \) with \( U_aU_a^{-1} = U_a \sigma(\sigma, \tau), a \in \mathbb{Z}^2(G, U(K)) \). If \( \tau \in G \) then \( \tau(U_a) = U_aU_a^{-1} = U_a \sigma(\tau, \sigma)/a(\sigma, \tau) \). Let \( \eta : G \times G \to U(K) \) be defined by \( \eta(\sigma, \tau) = a(\sigma, \tau)/a(\tau, \sigma) \). One checks easily that

\[
\eta \in \text{skew}(G \otimes G, U(K)) = \{ \gamma \in \text{Hom}(G \otimes G, U(K)) \mid \gamma(\sigma, \sigma) = 1 \text{ for all } \sigma \in G \}.
\]

Moreover since \( \Lambda^G = K \), \( \eta(\sigma, G) = 1 \) implies \( \sigma = e \). That is \( \eta \) is a non-singular skew inner product on \( G \).

In [6] a classification of central Galois extensions with Abelian groups was obtained employing this information. Here we extend one of the basic results in [6] and obtain some additional information about Galois extensions with Abelian groups. We notice at once

**Corollary 7.** If \( \Lambda \) is a central Galois extension of \( K \) with Abelian group \( G \), and if all the automorphisms of \( G \) are inner on \( \Lambda \), then there exists a primitive \( n^{th} \) root of 1 in \( K \) where \( n \) is the exponent of \( G \).

**Proof.** \( \text{Hom}_{\text{skew}}(G \otimes G, U(K)) \neq 0 \).

If \( G \) is an Abelian group and \( G = H_1 \oplus \cdots H_n \) is its decomposition into sylow \( p \)-subgroups, let

\[
H_i^+ = H_1 \oplus \cdots \oplus H_{i-1} \oplus H_{i+1} \cdots \oplus H_n.
\]

In [6] we showed

**Theorem 8.** If \( \Lambda \) is a central Galois extension of \( K \) with Abelian group \( G \) and all the automorphisms of \( G \) are inner on \( \Lambda \) then \( \Lambda = \Lambda_1 \otimes K \Lambda_2 \otimes K \cdots \otimes K \Lambda_n \) where \( \Lambda_i \) is a central Galois extension of \( K \) with group \( H_i \) and \( \Lambda_i = \Lambda_{i,1}^{H_i} \).

By means of the next lemma we will remove the restriction in theorem 8 that all the automorphisms in \( G \) be inner on \( \Lambda \).

**Lemma 9.** Let \( S \) be a central separable algebra over a commutative ring \( K \). Let \( S_i(i=1,2) \) be separable subalgebras, finitely generated and projective over \( K \). Assume that for every prime ideal \( \phi \) of \( K \)
(K_8 \otimes K S_i) \otimes_{K_8} (K_8 \otimes K S_j) = K_8 \otimes K S_i \otimes_{K_8} (K_8 \otimes K S_j) \simeq K_8 \otimes K S_i
\psi_\phi(s_{1\phi} \otimes s_{2\phi}) = s_{1\phi} s_{2\phi}

then
S = S_i \otimes_{K_8} S_j
by \phi(s_i \otimes s_j) = s_i s_j.

Proof. By theorem 3.5 of (2) and the fact that the S_i are finitely generated and projective, the K_8 \otimes K S_i are central separable subalgebras of K_8 \otimes K S, and the centralizer of K_8 \otimes S_i in K_8 \otimes S is K_8 \otimes S_j (i \neq j). The exact sequence

0 \to K \to \mathfrak{I}(S_i) \to \mathfrak{I}(S_i)/K \to 0
0 \to K_8 \to K_8 \otimes K \mathfrak{I}(S_i) \to K_8 \otimes K \mathfrak{I}(S_i)/K \to 0

\mathfrak{I}(S_i) is finitely generated over K since S_i is finitely generated projective and separable over K so since K_8 \otimes \mathfrak{I}(S_i)/K = 0 for all prime ideals \phi of K, \mathfrak{I}(S_i) = K.

By theorem 3.3 of (2), S = S \otimes_K S^s_i, (S^s_i = \{x \in S | ax = xa \ for \ all \ a \in S\}),

via the map \psi(s \otimes t) = st.

Let x \in S^s_i, then as above for every prime ideal \phi of K we obtain the exact sequence

0 \to K_8 \otimes_K K x \to K_8 \otimes_K (K x + S_2) \to K_8 \otimes_K (K x + S_2)/S_2 \to 0

and by theorem 3.5 of (2) together with the hypotheses, K_8 \otimes (x + S_2)/S_2 = 0; thus x \in S_2.

Dually S_2 \subseteq S^s_i. Again by theorems 3.5 and 3.3 of (2) S = S \otimes_K S_2
by \psi(s_1 \otimes s_2) = s_1 s_2.

Theorem 10. If \Lambda is a central Galois extension of K with Abelian group G then \Lambda = \Lambda_1 \otimes_K \cdots \otimes_K \Lambda_n where \Lambda_i is a central Galois extension of K with group H_i and \Lambda_i \simeq \Lambda_i^{H_i} (the H_i as before are the sylow p-components of G).

Proof. Let \phi be any prime ideal of K, then K_8 \otimes_K \Lambda is a central Galois extension of K_8 with group G. Since K_8 is local, all automorphisms of G are inner on K_8 \otimes_K S, thus K_8 \otimes_K S = (K_8 \otimes_K S)^H \otimes_K \phi(K_8 \otimes_K S)^H, via \psi_\phi(s_1 \otimes s_2) = s_1 \phi s_2 \phi. Thus the hypothesis of lemma 9 are satisfied and S \simeq S^{H_1} \otimes_K S^{H_1}. By induction on the number of sylow p-components of G, the theorem follows.

We now obtain the following amusing result first observed in the situation where K is a field by D. K. Harrison.

Theorem 11. Let \Lambda be a (non necessarily central) Galois extension
of the commutative ring \( K \) with cyclic group \( G \). Then \( \Lambda \) is commutative.

Proof. First observe that if for every prime ideal \( \phi \) of \( K, K_\phi \otimes_K \Lambda \) is commutative, then \( \Lambda \) is commutative. A quick way of seeing this is observing that the \( K \) submodule \( E = \{ xy - yx \mid x, y \in \Lambda \} \) of \( \Lambda \) is finitely generated over \( K \). Since \( K_\phi \otimes_K E = 0 \) for each prime ideal \( \phi \), \( E = 0 \) and \( \Lambda \) is commutative.

We may thus assume \( K \) is local. By lemma 5, \( \Lambda = \Lambda e_1 \oplus \cdots \oplus \Lambda e_n, e_i \) minimal central idempotents in \( \Lambda \) and each \( \Lambda e_i \) is a Galois extension of \( K \) with group \( J_i, J_i \) a subgroup of \( G \) and thus also cyclic.

Continuing to apply the results of lemma 5, there exists a normal subgroup \( H_i \) of \( J_i \) so that

\[
\mathfrak{N}(\Lambda)e_i = \mathfrak{N}(\Lambda e_i) = \Lambda e_i^{H_i} \quad (H_i \text{ cyclic.})
\]

Now \( \Lambda e_i \) is a central Galois extension of \( \mathfrak{N}(\Lambda e_i) \) with group \( H_i \). Let \( \mu \) be a maximal ideal in \( \mathfrak{N}(\Lambda e_i) \), then \( \mathfrak{N}(\Lambda e_i) / \mu \) is a field and by theorem (2) of [6], \( \mathfrak{N}(\Lambda e_i) / \mu \otimes \mathfrak{N}(\Lambda e_i) \Lambda e_i \) is a Galois extension of \( \mathfrak{N}(\Lambda e_i) / \mu \) with cyclic group \( H_i \). By Harrison's result for fields, or by theorem 2 plus the fact that if \( H_i \) is cyclic, then \( \text{Hom}_{skew}(H_i, U(K)) = 0 \) we must have \( H_i = \{ e \} \) so \( \Lambda e_i = \mathfrak{N}(\Lambda e_i) \) and \( \Lambda \) is commutative.

Section III

In this section we deal exclusively with central Galois extensions \( \Lambda \) of a commutative ring \( K \) whose group \( G \) is Abelian, and such that all the automorphisms in \( G \) are inner on \( \Lambda \). The principal purpose of the section is to prove the Normal Basis Theom in this setting.

Proposition 12. Let \( \Lambda, K, G \) be as above. Then \( \Lambda = KG, a(, \in Z^*(G, U(K)) \) and \( KG_a = \{ \Sigma_\sigma a_\sigma U_\sigma \mid a_\sigma \in K \} \). Then set \( \{ U_\sigma^{-1}/[G:1], U_\sigma \} \) satisfy "B" of theorem 1.

Proof. By lemma (1) of [6] together with theorem 6, \( \varepsilon = \Sigma_\sigma U_\sigma^{-1}/[G:1] \otimes U_\sigma^0 \) is an idempotent in \( \Lambda \otimes_K \Lambda^0 \) such that \( (1 \otimes x - x \otimes 1)\varepsilon = 0 \) for all \( x \in \Lambda \).

Since \( \Lambda \) is a Galois extension of \( K, \Lambda \otimes_K \Lambda^0 \cong \oplus \Sigma_\sigma \Lambda V_\sigma \) as \( K \) modules under \( l(s \otimes t) = \Sigma_\sigma s_\sigma(t)V_\sigma \) (theorem (1.3) of [4])

\[
l(\varepsilon) = \Sigma_\sigma \Sigma_\sigma \gamma(\tau, \sigma)V_\tau \quad \text{where} \quad \tau(V_\sigma) = U_\sigma a(\sigma, \tau),
\]

\( \gamma \in \text{Hom}_{skew}(G \otimes G, U(K)) \) since \( (1 \otimes x - x \otimes 1)\varepsilon = 0 \). We have for all \( x \in \Lambda \) and \( \tau \in G \).

(\* ) \[ x \Sigma_\sigma \gamma(\sigma, \tau) = \Sigma_\sigma \gamma(\sigma, \tau) \tau(x) \]
thus \((x-\pi(x))\sum_\sigma \eta(\sigma, \tau) = 0\), for all \(x \in \Lambda\). Since \(\Delta(\Lambda : G) = \text{Hom}_K(\Lambda, \Lambda)\) by theorem 1, \(A\):

\[
[\sum_\sigma \eta(\sigma, \tau) \cdot 1 - \sum_\sigma \eta(\sigma, \tau) \cdot \tau] x = 0 \quad \text{for all } x,
\]

so \(\sum_\sigma \eta(\sigma, \tau) = \begin{cases} [G : 1] & \tau = 1 \\ 0 & \tau \neq 1 \end{cases}\) which proves the proposition.

Using the same argument as above, one can show in the case where \(G\) is an arbitrary finite group that \(\{U^{-1}_\pi/[G : 1], U_\pi\}\) forms a set satisfying \(B\) of theorem 1 if and only if

\[
\sum_{\sigma \in G} \sigma(U_\pi) = \begin{cases} [G : 1] & \tau = \pi \\ 0 & \tau \neq \pi \end{cases} \quad \text{for all } \pi \in G.
\]

Finally we have the normal basis theorem in this setting.

**Theorem 13.** With the same hypothesis as in Proposition 12, there exists an \(x \in \Lambda\) such that \(\{\sigma(x) | \sigma \in G\}\) are a set of free generators of \(\Lambda\) as a \(K\) module.

Proof. \(\Lambda = KG = \bigoplus \Sigma KU_\sigma\) with the \(U_\sigma U_\pi = U_\pi a(\sigma, \tau)\) and \(a(,) \in Z^2 (G, U(K))\), and \(\eta(\sigma, \tau) = a(\sigma, \tau)/a(\tau, \sigma)\). Let \(x = \sum_{\sigma \in G} U_\sigma\).

1. \(\{\sigma(x)\} \sigma \in G\) generates \(\Lambda\). Since for each \(\tau \in G\), \(\tau(x) = \sum_{\sigma \in G} \eta(\sigma, \tau) U_\sigma\) it will suffice to show that for all \(\tau \in G\) there is \(\alpha(\in K\) and \(\tau \in G\) so that

\[
\sum_{\sigma \in G} \alpha(\eta(\gamma, \tau) = \begin{cases} 1 & \gamma = \sigma \\ 0 & \gamma \neq \sigma \end{cases}.
\]

By Proposition 12, \(\sum_\gamma \eta(\gamma, \tau) = \begin{cases} 1 & \gamma \neq \pm 1 \\ 0 & \gamma \neq \pm 1 \end{cases}\) for all \(\gamma \in G\). Thus

\[
\sum_{\gamma \in G} \eta(\sigma^{-1}, \tau) \eta(\gamma, \tau) = \sum_{\gamma \in G} \eta(\sigma^{-1} \gamma, \tau) = \begin{cases} [G : 1] & \gamma = \sigma \\ 0 & \gamma \neq \sigma \end{cases}
\]

so we just let \(\alpha(\tau) = \eta(\sigma^{-1}, \tau)/[G : 1]\).

2. \(\{\sigma(x)\} \sigma \in G\) are linearly independent. Assume \(\sum_{\sigma \in G} \alpha(\tau) = 0\). Then \(\sum_{\sigma \in G} \sum_{\tau \in G} \alpha(\tau) U_\sigma = 0\) so \(\sum_{\sigma} \alpha(\sigma, \tau) = 0\) for all \(\sigma\). By the nonsingularity of \(\eta\), the characters \(\eta(\sigma, \tau)\) are linearly independent over \(K\). Thus \(\alpha(\tau) = 0\) for all \(\tau\). This proves the theorem.

Employing theorem (4.2) of [4] together with this result, one may obtain several generalized normal basis type theorems.

University of Oregon
Bibliography


