DeMeyer, F. R.
Osaka J. Math.
2 (1965), 117-127

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 ($\Gamma=\Lambda^G$).

Let $\Delta(\Lambda:G)$ be the crossed product of Λ and G with trivial factor set. That is

$$\Delta(\Lambda:G)=\Sigma_{\sigma\in G}\Lambda U_\sigma \qquad \text{such that}$$
$$x_1U_\sigma x_2U_\tau = x_1\sigma(x_2)U_{\sigma\tau} \qquad x_1,\, x_2\ \Lambda\,;\ \sigma,\, \tau\in G\,.$$

This work was done while the author held a National Science Foundation Cooperative Fellowship.

View Λ as a right Γ module and define

$$j : \Delta(\Lambda : G) \to \mathrm{Him}_\Gamma(\Lambda, \Lambda) \quad \text{by}$$
$$j(aU_\sigma)x = a\sigma(x) \qquad a, x \in \Lambda ; \sigma \in G .$$

Theorem 1. *The following are equivalent*:

A. Λ *is finitely generated projective as a right* Γ *module and* $j : \Delta(\Lambda : G) \to \mathrm{Hom}_\Gamma(\Lambda, \Lambda)$ *is an isomorphism.*

B. There exists $x_1, \cdots, x_n ; y_1, \cdots, y_n \in \Lambda$ *such that*

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

Following Auslander and Goldman, Kanzaki called Λ a Galois extension of Γ 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 Λ a Galois extension of Γ 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 $f_i \in \mathrm{Hom}_\Gamma(\Lambda, \Gamma)$ by $f_i(x) = \Sigma_{\sigma \in G} \sigma(y_i x)$ $x \in \Lambda$, $\sigma \in G$. For any $x \in \Lambda$

$$\Sigma_{i=1}^n x_i f_i(x) = \Sigma_{i,\sigma} x_i \sigma(y_i) \sigma(x) = x .$$

Thus by the Dual Basis lemma, Λ is finitely generated and projective as a right Γ module.

Now we show $j : \Delta(\Lambda : G) \to \mathrm{Hom}_\Gamma(\Lambda, \Lambda)$ is an isomorphism. Let U_τ be a Basis element in $\Delta(\Lambda : G)$. Then

$$\begin{aligned} \Sigma_{i=1}^n j(U_\tau)[x_i] \cdot (\Sigma_\sigma U_\sigma) y_i &= \Sigma_{i,\sigma} \tau(x_i) \sigma(y_i) U_\sigma \\ &= \Sigma_\sigma \tau(\Sigma_i x_i \tau^{-1} \sigma(y_i)) U_\sigma = U_\tau . \end{aligned}$$

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

$$U = \Sigma_{i=1}^n j(U)[x_i] \cdot (\Sigma_\sigma U_\sigma) y_i .$$

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 $h \in \mathrm{Hom}_\Gamma(\Lambda, \Lambda)$ and let

$$U = \Sigma_{i=1}^n \Sigma_{\sigma \in G} h(x_i) U_\sigma y_i , \qquad U \in \Delta(\Lambda : G)$$

for any $x \in \Lambda$,
$$\begin{aligned} j(U)[x] &= \Sigma_{i=1}^n \Sigma_{\sigma \in G} h(x_i) \sigma(y_i x_i) \\ &= h(\Sigma_{i=1}^n \Sigma_{\sigma \in G} x_i \sigma(y_i x)) \qquad (\Sigma_\sigma \sigma(y_i x) \in \Gamma) \\ &= h(\Sigma_{i=1}^n x_i f_i(x)) = h(x) . \end{aligned}$$

Thus j is an isomorphism.

To prove the converse, we first show that

$$(*) \qquad \mathrm{Hom}_\Gamma(\Lambda, \Gamma) = j(t\cdot\Lambda) \qquad \text{where} \quad t = \Sigma_{\sigma\in G} U_\sigma .$$

Pick $a\in\Lambda$, $j(ta)[x]=\Sigma_{\sigma\in G}\sigma(ax)\in\Gamma$. So $j(ta)\in\mathrm{Hom}_\Gamma(\Lambda, \Gamma)$. Suppose $f=j(y)\in\mathrm{Hom}_\Gamma(\Lambda, \Gamma)$, $y\in\Delta(\Lambda:G)$. If $y=\Sigma_\sigma a_\sigma U_\sigma$, then for all $x\in\Lambda$, $\Sigma_\sigma a_\sigma\sigma(x)\in\Gamma$ so $\rho(\Sigma_\sigma a_\sigma\sigma(x))=\Sigma_\sigma a_\sigma\sigma(x)$ for all $\rho\in G$. Thus $\Sigma_{\tau\in G}\rho(a_{\rho^{-1}\tau})\tau(x)$ $=\Sigma_{\tau\in G}a_\tau\tau(x)$, $(\tau=\rho\sigma)$ but j is an isomorphism so $\rho(a_{\rho^{-1}\tau})=a_\tau$ so $a_\sigma=\sigma(a)$, thus $y=\Sigma_\sigma\sigma(a)U_\sigma=\tau\cdot a_1$. 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 $U=\Sigma_{i=1}^n x_i t y_i\in\Delta(\Lambda:G)$. Then $j(U)[x]=\Sigma_{\sigma\in G}\Sigma_{i=1}^n x_i\sigma(y_i x)=\Sigma_{i=1}^n x_i f_i(x)$ $=x$. j is an isomorphism so $U=\Sigma_{i=1}^n x_i t y_i=1$. Thus $\Sigma_{i=1}^n x_i U_\sigma y_i=\begin{cases}1 & \sigma=1\\ 0 & \sigma\neq 1\end{cases}$ so since j is an isomorphism, $\Sigma_{i=1}^n x_i\sigma(y_i)=\begin{cases}1 & \sigma=1\\ 0 & \sigma\neq 1\end{cases}$ 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 Λ 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 Λ is a Galois extension of $\Lambda^G=\Gamma$ and there exists a* 1–1 *correspondence between the K-separable subalgebras Ω of Λ containing Γ and the K-separable subalgebras A of C given by*

$$A \to A\cdot\Gamma$$
$$\mathfrak{Z}(\Omega) \leftarrow \Omega$$

Proof. Λ is a Galois extension of Γ by B of theorem 1 and by the hypothesis that C is Galois over K.

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

$$\begin{aligned}\Gamma &= K\cdot\Gamma\\ &= \{\Sigma_\sigma\sigma(x)\,|\,x\in C\}\cdot\Gamma\\ &= \{\Sigma_\sigma\sigma(xt)\,|\,x\in C,\ t\in\Gamma\}\subseteq\Gamma\,, \quad (\Lambda^G=\Gamma)\,.\end{aligned}$$

Thus $\Gamma=\{\Sigma_\sigma\sigma(x)\,|\,x\in\Lambda\}$ and there exists $f\in\mathrm{Hom}_\Gamma(\Lambda,\Gamma)$ $(f=\Sigma_{\sigma\in G}\sigma)$ and there exists an $a\in\Lambda$ so that $f(a)=1$. Thus Γ is a direct summand of Λ as a Λ–Γ module.

We now show Γ is separable over K by showing Γ 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 Λ is separable over K. Since Γ is a direct summand of Λ and the hypothesis insure that Λ is projective over K (Λ 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, Λ is projective as both a left and right Γ module. (Λ is $\Gamma-\Gamma$ projective.) So $\Lambda\otimes_K\Lambda^0$ is projective as a $\Gamma\otimes_K\Gamma^0$ module. Hence Λ and thus Γ 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 Γ 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 Γ (denoted $\mathfrak{Z}(\Gamma)$) is K, for if $x\in\mathfrak{Z}(\Gamma)$ then $x\in\mathfrak{Z}(\Lambda)$, ($\Lambda=h(\Gamma\otimes_K C)$) 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 Ω be a K-separable subalgebra of Δ containing Γ. Let A be a K-separable subalgebra of C. Define

$$\psi:\Omega\to\mathfrak{Z}(\Omega)$$
$$(\gamma: A\to h(\Gamma\otimes_K)) \qquad (\text{notice } \Gamma\otimes_K A\subseteq\Gamma\otimes_K C)$$

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

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

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

$$\Omega\simeq\gamma\psi(\Omega)\otimes_{\mathfrak{Z}(\Omega)}\Omega' \qquad \text{and}$$

thus Ω' is contained in the centralizer in Λ of Γ. But then $\Omega'\leq C$. Thus $\Omega'=\mathfrak{Z}(\Omega)$ 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 Λ containing Γ and the subgroups H of G.*

If Ω is a K-separable subalgebra of Λ containing Γ then there exists a subgroup H of G so that $\Omega=\Lambda^H$.

Moreover for all subgroups H of G, Λ is Galois over Λ^H and if H is a normal subgroup of G then Λ^H in Galois over Γ 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 $H\leftrightarrow C^H$. By lemma 2 there is a one-one correspondence between the K-separable subalgebras of C and the K-separable subalgebras of Λ containing Γ by

$$A \to h(\Gamma\otimes_K A),$$

Combining these two facts, we have the one-one correspondence, thus every K-separable subalgebra Ω of Λ containing Γ is of the form Λ^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 Λ over Λ^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 Λ be a faithful K-algebra and G a finite group represented as ring automorphisms of Λ so that $\Lambda^G=K$. Then all the elements in G are K-algebra automorphisms of Λ. As before, Λ 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 Λ is a Galois K-algebra with group G. If $C=$ Center of Λ contains no idempotents except 0 and 1 then $C=\Lambda^H$ where $H=\{\sigma\in G\mid \sigma(x)=x$ 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 Λ is a Calois K-algebra then*

$$\Lambda = \Lambda e_1\oplus\cdots\oplus Ae_n \qquad (e_i \textit{ minimal central idempotents})$$

and Λe_i is a Galois extension of K with group $J_i=\{\sigma\in G\mid\sigma(e_i)=e_i\}$. Moreover $\mathfrak{Z}(\Lambda e_i)=Ce_i=\Lambda e_i^{H_i}$ where H_i is a normal subgroup of J_i.

Proof. C is finitely generated projective and separable over K since Λ is finitely generated projective and separable over K. By theorem (7) of [8] since K has no idempotents but 0 and 1

$$C = \oplus\Sigma Ce_i \qquad e_i \text{ minimal idempotents in } C.$$

thus
$$\Lambda = \oplus\Sigma\Lambda e_i \qquad e_i \text{ minimal central idempotents in } \Lambda.$$

Let $J_i = \{\sigma\in G \mid \sigma(e_i)=e_i\}$. 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] Λe_i is a Galois extension of K with group J_i. $Ce_i = \mathfrak{Z}(\Lambda e_i)$. Let $H_i = \{\sigma\in J_i \mid \sigma(x)=x$ for all $x\in Ce_i\}$. Then by Lemma 3 H_i is a normal subgroup of J_i and $\Lambda e_i^{H_i} = Ce_i$. 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 Λ over K with group G so that $\mathfrak{Z}(\Lambda)=K$. 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 Λ is a central separable K-algebra and σ is an algebra automorphism of Λ of finite order n such that no element in $P(K)$ has order dividing n then σ is an inner automorphism of Λ, 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 Λ is a central Galois K-algebra, then Λ is separable over K, theorem (1) of [6]. Assume the elements of the Galois group G are inner on Λ. 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_σ for each $\sigma\in G$ and define $a(\,,)$ mapping $G\times G$ to $U(K)=$Units of K by

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

From the associative law in Λ,

$$a(\sigma\tau,\rho)a(\sigma,\tau) = a(\sigma,\tau\rho)a(\tau,\rho)$$

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

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

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

$$\Lambda = KG_a, \qquad a(\,,)\in Z^2(G, U(K)).$$

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

$$\begin{aligned}&\eta \in {}_{\text{skew}}(G\otimes G,\ U(K)) = \\ &\{\gamma \in \operatorname{Hom}(G\otimes G,\ U(K)) \mid = \gamma(\sigma, \sigma) = 1 \\ &\text{for all } \sigma \in G\}\,.\end{aligned}$$

Moreover since $\Lambda^G = K$, $\eta(\sigma, G) = 1$ implies $\sigma = e$. That is η 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 Λ is a central Galois extension of K with Abelian group G, and if all the automorphisms of G are inner on Λ, then there exists a primitive n^{th} root of 1 in K where n is the exponent of G.*

Proof. $\operatorname{Hom}_{\text{skew}}(G\otimes G,\ U(K)) \neq \emptyset$.

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

$$H_i^\perp = H_1 \oplus \cdots \oplus H_{i-1} \oplus H_{i+1} \cdots \oplus H_n\,.$$

In [6] we showed

Theorem 8. *If Λ is a central Galois extension of K with Abelian group G and all the automorphisms of G are inner on Λ then $\Lambda = \Lambda_1 \otimes_K \Lambda_2 \otimes_K \cdots \otimes_K \Lambda_n$ where Λ_i is a central Galois extension of K with group H_i and $\Lambda_i = \Lambda^{H_i^\perp}$.*

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

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 $\mathfrak{p}$ of K*

$$(K_\phi \otimes_K S_1) \otimes_{K_\phi} (K_\phi \otimes_K S_2) \simeq K_\phi \otimes_K S \quad by$$
$$\psi_\phi(s_{1\phi}(\otimes s_{2\phi}) = s_{1\phi} s_{2\phi} \quad then$$
$$S \simeq S_1 \otimes_K S_2 \quad by \quad \phi(s_1 \otimes s_2) = s_1 s_2 .$$

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

$$0 \to K \to \mathfrak{Z}(S_i) \to \mathfrak{Z}(S_i)/K \to 0 \qquad \text{gives}$$
$$0 \to K_\phi \to K_\phi \otimes_K \mathfrak{Z}(S_i) \to K_\phi \otimes_K \mathfrak{Z}(S_i) | K \to 0$$

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

By theorem 3.3 of (2), $S \simeq S \otimes_K S^{S_1}$, $(S^{S_1} =$

$$\{x \in S \mid ax = xa \quad \text{for all } a \in S\}),$$

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

Let $x \in S^{S_1}$, then as above for every prime ideal ϕ of K we obtain the exact sequence

$$0 \to K_\phi \otimes_K Kx \to K_\phi \otimes_K (Kx + S_2) \to K_\phi \otimes_K (Kx + S_2)/S_2 \to 0$$

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

Dually $S_2 \subseteq S^{S_1}$. Again by theorems 3.5 and 3.3 of (2) $S \simeq S \otimes_K S_2$ by $\psi(S_1 \times S_2) = S_1 S_2$.

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

Proof. Let ϕ be any prime ideal of K, then $K_\phi \otimes_K \Lambda$ is a central Galois extension of K_ϕ with group G. Since K_ϕ is local, all automorphisms of G are inner on $K_\phi \otimes_K S$, thus $K_\phi \otimes_K S \simeq (K_\phi \otimes_K S)^{H_1} \otimes_K \phi (K_\phi \otimes_K S)^{H_1}$ via $\psi_\phi(s_\phi \otimes s_{2\phi}) = s_1 \phi s_2 \phi$. Thus the hypothesis of lemma 9 are satisfied and $S \simeq S^{H_1} \otimes_K S^{H_i^\perp}$. 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 Λ be a (non necesearily central) Galois extension* *of the commutative ring K with cyclic group G. Then Λ is commutative.*

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

We may thus assume K is local. By lemma 5, $\Lambda=\Lambda e_1 \oplus \cdots \otimes \Lambda e_n$, e_i minimal central idempotents in Λ and each Λe_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

$$\mathfrak{Z}(\Lambda)e_i = \mathfrak{Z}(\Lambda e_i) = \Lambda e_i^{H_i} \qquad (H_i \text{ cyclic.})$$

Now Λe_i is a central Galois extension of $\mathfrak{Z}(\Lambda e_i)$ with group H_i. Let μ be a maximal ideal in $\mathfrak{Z}(\Lambda e_i)$, then $\mathfrak{Z}(\Lambda e_i)/\mu$ is a field and by theorem (2) of [6], $\mathfrak{Z}(\Lambda e_i)/\mu \otimes_{\mathfrak{Z}(\Lambda e_i)} \Lambda e_i$ is a Galois extension of $\mathfrak{Z}(\Lambda e_i)/\mu$ 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 $\mathrm{Hom}_{\mathrm{skew}}(H_i, U(K))=\emptyset$ we must have $H_i=\{e\}$ so $\Lambda e_i=\mathfrak{Z}(\Lambda e_i)$ and Λ is commutative.

Section III

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

Proposition 12. *Let Λ, K, G be as above. Then $\Lambda=KG_a$ $a(\ ,\ )\in Z^2(G, U(K))$ and $KG_a=\{\Sigma_\sigma \alpha_\sigma U_\sigma \mid \alpha_\sigma \in K\}$. 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 $(1\otimes x^0-x^0\otimes 1)\varepsilon=0$ for all $x\in\Lambda$.

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

$$l(\varepsilon) = \Sigma_\tau\Sigma_\sigma \eta(\tau, \sigma)V_\tau \qquad \text{where} \quad \tau(V_\sigma)=U_{\sigma\eta}a(\sigma, \tau)\,,$$

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

$$(*) \qquad x\Sigma_\sigma\cdot\eta(\sigma, \tau) = \Sigma_\sigma\eta(\sigma, \tau)\tau(x)$$

thus $(x-\tau(x))\Sigma_\sigma\eta(\sigma,\tau)=0$, for all $x\in\Lambda$. Since $\Delta(\Lambda:G)\simeq\mathrm{Hom}_K(\Lambda,\Lambda)$ by theorem 1, A;

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

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

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

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

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* $\{\sigma(x)\mid\sigma\in G\}$ *are a set of free generators of* Λ *as a* K *module.*

Proof. $\Lambda=KG_a=\oplus\Sigma KU_\sigma$ with the $U_\sigma U_\tau=U_{\sigma\tau}a(\sigma,\tau)$ and $a(\ ,\ )\in Z^2(G, U(K))$, and $\eta(\sigma,\tau)=a(\sigma,\tau)/a(\tau,\sigma)$. Let $x=\Sigma_{\sigma\in G}U_\sigma$.

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

$$\Sigma_{\tau\in G}\alpha_\tau\eta(\gamma,\tau)=\begin{cases}1 & \text{if } \gamma=\sigma\\ 0 & \text{if } \gamma\neq\sigma.\end{cases}$$

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

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

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

2. $\{\sigma(x)\sigma\{\in G$ are linearly independent. Assume $\Sigma_{\tau\in G}\alpha_\tau\tau(x)=0$. Then $\Sigma_{\sigma\in G}\Sigma_{\tau\in G}\alpha_\tau\eta(\sigma,\tau)U_\sigma=0$ so $\Sigma_\tau\alpha_\tau\eta(\sigma,\tau)=0$ for all σ. By the non-singularity of η, the characters $\eta(\ ,\tau)$ are linearly independent over K. Thus $\alpha_\tau=0$ for all τ. 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

[1] E. Artin, Geometric Algebra, Interscience Tracts in Pure and Applied Mathematics, Vol. 3, Interscience Publishers, Inc., 1957.

[2] M. Auslander and O. Goldman, *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc. **97** (1960), 367–409.

[3] H. Cartan and S. Eilenberg, Homological Algebra, Princeton, Princeton University Press, 1956.

[4] S. U. Chase, D. K. Harrison, A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc. No. 52, (1965).

[5] C. W. Curtis and Irving Reiner, Representation Theory of Finite Groups and Associative Algebras, Interscience Publishers, 1962.

[6] F. R. DeMeyer, *Galois theory in algebras over commutative rings*, Illinois J. Math. (to appear)

[7] D. K. Harrison, *Abelian extensions of arbitrary fields*, Trans. Amer. Math. Soc. **106** (1963), 230–235.

[8] D. K. Harrison, *Abelian extensions of commutative rings*, Trans. Amer. Math. Soc. (1965).

[9] D. K. Harrison, *Finite and infinite primes fo·· rings and fields*, Trans. Amer. Math. Soc. (1965).

[10] T. Kanzaki, *On commutor rings and Galois theory of separable algebras*, Osaka J. Math. **1** (1964), 103–115.

[11] A. Rosenberg and D. Zelinsky, *Automorphisms of separable algebras*, Pacific J. Math. **11** (1957), 1109–1118.

[12] S. Williamson, *Crossed products and hereditary orders*, Nagoya Math. J. **23** (1963), 103–120.