1963

Galois completely primary rings

Donovan Forest Sanderson
Iowa State University

SANDERSON, Donovan Forest, 1935–
GALOIS COMPLETELY PRIMARY RINGS.

Iowa State University of Science and Technology
Ph.D., 1963
Mathematics

GALOIS COMPLETELY PRIMARY RINGS

by

Donovan Forest Sanderson

A Dissertation Submitted to the

Graduate Faculty in Partial Fulfillment of

The Requirements for the Degree of

DOCTOR OF PHILOSOPHY

Major Subject: Mathematics

Approved:

Signature was redacted for privacy.

In Charge of Major Work

Signature was redacted for privacy.

Head of Major Department

Signature was redacted for privacy.

Dean of Graduate College

Iowa State University
Of Science and Technology
Ames, Iowa

1963

TABLE OF CONTENTS

		Page
I.	INTRODUCTION	1
II.	GALOIS VECTOR SPACES	3
III.	COMPLETELY PRIMARY RINGS	6
IV.	LEFT-GALOIS RINGS	9
V.	GRADED RINGS	13
VI.	DIAGONAL RINGS	17
VII.	GENERALITIES	22
VIII.	BIBLIOGRAPHY	25
IX.	ACKNOWLEDGMENT	26
X.	APPENDIX	27

I. INTRODUCTION

A two-sided space over a division ring is said to be left-Galois if there is a left basis, $\{u\}$, such that $u\Delta \subset \Delta u$ for all $u \in \{u\}$. This concept was initiated by Dieudonne (2) and Hochschild (3) and was revised and extended by Jacobson (4) in order to explore the Galois theory of division and semi-simple rings. We shall use the concept for somewhat different, although related, purposes.

If A is a completely primary ring with maximal ideal N and quotient division ring Δ , then it is classically well known that the quotients, N^j/N^{j+1}, of the Loewy series are two sided vector spaces. If each of these spaces is left-Galois, we say A is left-Galois. This paper is devoted to the study of such rings.

In chapter II, we introduce left-Galois space and explore some of their basic properties. We study general completely primary rings in chapter III and relate the elements in the quotients, N^j/N^{j+1}, to the elements in N. Our basic result, in this chapter, is that every element in N can be represented uniquely in the form $\Sigma\theta(\delta_\alpha)u_\alpha$, where θ is a section, $\delta_\alpha \in \Delta$, and the u_α's are fixed representatives of the bases for each of the quotient spaces.

Chapter IV is devoted to proving that a basis of N^j/N^{j+1} can be determined by the symbolic products of a basis for N/N^2, if A is left-Galois. We then prove that A is left-Galois if and only if the space N/N^2 is left-Galois.

In chapter V, we explore the structure of cleft graded left-Galois rings and prove that if G is a semi-group of isomorphisms of Δ , then there is a cleft left-Galois ring which realizes G.

We explore the right regular representation of diagonal rings in chapter VI. A cleft ring is diagonal if the matrices representing Δ are all diagonal. We prove that A is diagonal if and only if N is a left-Galois vector space.

In chapter VII, we study some possible generalizations of the foregoing theory.

II. GALOIS VECTOR SPACES

In all of the following material, let Δ designate a division ring. A two-sided vector space over Δ may have a left basis which is not a right basis. Hence, there may be an element u such that $u\Delta \not\subset \Delta u$. An element u in a two-sided space will be called <u>left-Galois</u> if $u\Delta \subset \Delta u$. A two-sided space is <u>left-Galois</u> if it has a left basis consisting of left-Galois elements. Such a left basis will be said to be a left-Galois basis.

We shall ordinarily shorten "left-Galois" to "Galois" in cases where there can be no confusion.

The following material is essentially contained in the book by Jacobson (4, pages 142-144).

Let u be a Galois element in a vector space. For every $\delta \in \Delta$, $u\delta \in \Delta u$. Thus, there is a $\delta_1 \in \Delta$ such that $\delta_1 u = u\delta$. Define the mapping $\sigma: \Delta \longrightarrow \Delta$ by $\sigma(\delta) = \delta_1$ if and only if $u\delta = \delta_1 u$. It is clear that σ is well defined and the distributive and mixed associative laws guarantee us that it is a (ring) homomorphism. Since Δ is a division ring, σ is an isomorphism. This mapping is said to be <u>associated</u> with u, and conversely.

We say two isomorphisms, σ_1 and σ_2, of Δ into itself are equivalent if there is an inner automorphism, θ, of Δ such that $\sigma_1 = \theta\sigma_2$. If σ_1 is equivalent to σ_2, we write $\sigma_1 \sim \sigma_2$.

For a given Galois vector space, define the following:

$$V_\sigma = \{v \in V \mid \sigma(\delta)\, v = v\,\delta\text{ , for every } \delta \in \Delta\,.\}\,,$$

$\bar{V}_{(\sigma)} = \{ v \in \bar{V} \mid \theta(\delta) v = v \delta$, for every $\delta \in \Delta$, where $\theta \sim \sigma$. $\}$.

Let Δ_σ be the subring of Δ composed of elements which commute elementwise with the image of σ. It is clear that Δ_σ is a division ring and, if σ is an automorphism, it is the center of Δ .

Proposition 1. If the isomorphism σ is associated with the Galois element u and if $\theta \sim \sigma$, then there is a $v \in \Delta u$ associated with θ . Conversely, every element in Δu is Galois and is associated with an isomorphism equivalent to σ.

Proof. Assume $v = \delta_1 u$ for some $\delta_1 \in \Delta$. Then $(\delta_1 u) \delta = \theta(\delta)(\delta_1 u) = (\theta(\delta)\delta_1) u$. But $(\delta_1 u) \delta = \delta_1 (u \delta) = \delta_1 (\sigma(\delta) u) = (\delta_1 \sigma(\delta)) u$ and thus $\theta(\delta) = \delta_1 \sigma(\delta) \delta_1^{-1}$. All of the arguments may be reversed to complete the proof.

Proposition 2. V_σ is a left vector space over Δ_σ.

Proof. Suppose that $\delta_1 \in \Delta_\sigma$ and $v \in V_\sigma$. Then $(\delta_1 v) \delta = \delta_1 (v \delta) = \delta_1 (\sigma(\delta) v) = (\delta_1 \sigma(\delta)) v = (\sigma(\delta) \delta_1) v = \sigma(\delta)(\delta_1 v)$ for every $\delta \in \Delta$.

Proposition 3. $V_{(\sigma)}$ is a two-sided vector space over Δ .

Proof. Closure under multiplication on the left follows from proposition 1, and closure on the right follows from this.

Theorem 4. Let V be a Galois space over Δ and let $\{(\sigma)\}$ be the set of equivalence classes of isomorphisms associated with a particular Galois basis of V. Let $\{\sigma\}$ be a set of representatives, one and only one from each of the equivalence classes, of these isomorphisms. Then

(1.) $V_{(\sigma)} \cong \Delta \otimes_{\Delta_\sigma} V_\sigma$, $\sigma \in (\sigma)$ and

(2.) $V \cong \sum_{\sigma} V_{(\sigma)}$.

Proof. See Jacobson's book (4, page 144).

Corollary 5. $V_{(\sigma)}$ has a left basis $\{u_\alpha\}$ which satisfies the property that u_α is associated with σ, for every α.

Proof. V_σ certainly has such a basis. The result now follows from equation 1.

Proposition 6. Let u be a Galois element in a vector space associated with the isomorphism σ. Then σ is an automorphism if and only if $\Delta u = u \Delta$.

Proof. If $\Delta u = u \Delta$, then the mapping θ, defined by $\theta(\delta) = \delta_1$ if and only if $\delta u = u \delta_1$, is clearly an isomorphism and is the inverse of σ.

Conversely, if σ is an automorphism of Δ , then, if $\delta \in \Delta$, there is a $\delta_1 \in \Delta$ such that $\sigma(\delta_1) = \delta$. Hence, $\delta u = \sigma(\delta_1) u = u \delta_1$ and $u \Delta \supset \Delta u$.

III. COMPLETELY PRIMARY RINGS

A completely primary ring is a ring with a unique maximal ideal such that the ring modulo the maximal ideal is a division ring. We shall customarily denote the ring by A, the maximal ideal by N, and the quotient division ring by Δ. Let us also denote the canonical map from A to Δ by π.

Lemma 1. If a and b are two representatives of δ Δ, that is, if a and $b \in \pi^{-1}(\delta)$, then $a - b \in N$.

Proof. N is clearly the kernel of π and $\pi(a-b) = \pi(a) - \pi(b) = \delta - \delta = 0$.

Define, as usual, N^j to be the product of N with itself j times. We shall assume that N^j properly contains N^{j+1} for each j. We shall also have occasion to denote A by N^o.

If $a \in A$, and if $a \neq 0$, then there is a unique j such that $a \in N^j - N^{j+1}$. This j will be called the degree of a and will be designated by deg(a). Zero has no degree.

Let us note that if $a \in A$ and if $\pi(a) \neq 0$, then a has an inverse. If not, we would contradict the uniqueness of N.

Lemma 2. If $a \in A$, if $\pi(a) \neq 0$, if $n \in N$, and if $\deg(n) = j$, then $\deg(an) = \deg(na) = j$.

Proof. If $n \in N^j$, then $a\,n \in N^j$ and if $a\,n \in N^i$, then $a^{-1}\,a\,n = n \in N^i$.

Lemma 3. If n_1 and $n_2 \in N$, then $\deg(n_1n_2) \geq (\deg(n_1)) + (\deg(n_2))$.

Proof. Suppose $\deg(n_1) = i$ and $\deg(n_2) = j$. Since $N^iN^j \subset N^{i+j}$, $n_1n_2 \in N^{i+j}$ and hence $\deg(n_1n_2) \geq i + j$.

Denote the canonical mapping from N^j to N^j/N^{j+1} by π_j. Note that this implies $\pi = \pi_0$.

Proposition 4. Suppose $\delta \in \Delta$, a and b are representatives of δ in A, n_1 and $n_2 \in N^j$, and $\pi_j(n_1) = \pi_j(n_2)$. Then $\pi_j(an_1) = \pi_j(bn_2)$.

Proof. Since $\pi_j(n_1) = \pi_j(n_2)$, $n_1 - n_2 \in N^{j+1}$. Hence, $a(n_1 - n_2) = a n_1 - a n_2 \in N^{j+1}$. Since $a - b \in N$, by lemma 1, $(a - b) n_2 = a n_2 - b n_2 \in N^{j+1}$. Thus, $a n_1 - a n_2 + a n_2 - b n_2 = a n_1 - b n_2 \in N^{j+1}$.

A similar result will be valid, if the products are commuted.

Now, if $\bar{n} \in N^j/N^{j+1}$, there is an $n \in N^j$ such that $\pi_j(n) = \bar{n}$. Let a be any representative of δ in A. Define $\delta \bar{n}$ to be equal to $\pi_j(a n)$. The above proposition guarantees us that this product is well defined. It is easily verified that N^j/N^{j+1} is a left vector space over Δ by using the properties of A. We may, similarly, make N^j/N^{j+1} into a right vector space over Δ. The associativity of A implies that this is a two-sided vector space structure.

A section is a (group) homomorphism from Δ into A which is a right inverse for π.

Theorem 5. Assume that N is nilpotent. Let $\{\bar{u}_{\alpha i}\}$, $\alpha \in \mathfrak{A}_i$, be a left basis for N^i/N^{i+1} and let $u_{\alpha i}$ be a representative of $\bar{u}_{\alpha i}$ in N^i for each α and i. Let θ be a section. Then every element in A can be uniquely expressed in the form

$$\theta(\delta_o) + \sum_i \sum_\alpha \theta(\delta_{\alpha i}) u_{\alpha i}\text{, where } \delta_o \text{ and } \delta_{\alpha i} \text{ are in } \Delta .$$

Proof. Let $a \in A$ and suppose deg(a) = j. Then $\pi_j(a) = \sum_\alpha \delta_{\alpha j} \bar{u}_{\alpha j}$. Hence, $a - \sum_\alpha \theta(\delta_{\alpha j}) u_{\alpha j} \in N^{j+1}$. Suppose deg(a -

$\sum_{\alpha} \theta\ (\delta_{\alpha j})\ u_{\alpha j}) = k > j$. Then $\pi_k\ (a - \sum_{\alpha} \theta\ (\delta_{\alpha j})\ u_{\alpha j}) = \Sigma\ \delta_{\alpha k}\ \overline{u}_{\alpha k}$. Thus, $a - (\sum_{\alpha} \theta\ (\delta_{\alpha j})\ u_{\alpha j} + \Sigma\ \theta\ (\delta_{\alpha k})\ u_{\alpha k}) \in N^{k+1}$. Let us now proceed recursively and suppose that $a - (\sum_{j} \sum_{\alpha} \theta\ (\delta_{\alpha j})\ u_{\alpha j}) \in N^{n+1}$. We may now repeat the process above and lengthen our sum. Eventually, however, since N is nilpotent, we must arrive at zero and thus, have the equality described in the theorem.

Now suppose $\sum_{j} \sum_{\alpha} \theta\ (\overline{\delta}_{\alpha j})\ u_{\alpha j}$ is any second representation. Then $\sum_{j} \sum_{\alpha} \theta\ (\delta_{\alpha j} - \overline{\delta}_{\alpha j})\ u_{\alpha j} = 0$. Let k be the smallest j occurring in this sum. Then $\pi_k\ (\sum_{j} \sum_{\alpha} \theta\ (\delta_{\alpha j} - \overline{\delta}_{\alpha j})\ u_{\alpha j}) = \sum_{\alpha} (\delta_{\alpha k} - \overline{\delta}_{\alpha k})\ \overline{u}_{\alpha k} = 0$. This implies $\delta_{\alpha k} = \overline{\delta}_{\alpha k}$. The proof is completed easily by using induction.

A completely primary ring is <u>cleft</u> if and only if there is a section which is a ring homomorphism and hence, a ring isomorphism. We shall commonly identify Δ with its image under such a section. Note that in theorem 5, if θ is a ring isomorphism, the representatives form a basis for A over the image of Δ.

Corollary 6. If A is cleft and if N is nilpotent, then for each $j = 0, 1, \ldots, [N^j : \Delta]_L = \sum_{i \geq j} [N^i/N^{i+1} : \Delta]_L$.

A similar result clearly holds for the right dimensions.

We shall suppose, in the remainder of this paper, that a section always exists.

IV. LEFT-GALOIS RINGS

A completely primary ring is said to be left-Galois over its quotient division ring if and only if each of the vector spaces N^j/N^{j+1} are left-Galois.

Proposition 1. If $u \in N^i/N^{i+1}$, $v \in N^j/N^{j+1}$, $\bar{u}$ and $\bar{v}$ are representatives of u and v in A respectively, $\bar{u}\,\bar{v}$ has degree $i + j$, and if u and v are Galois, then the image of $\bar{u}\,\bar{v}$ in N^{i+j}/N^{i+j+1} is also Galois. Further, if σ is associated with u and if θ is associated with v, then $\sigma\,\theta$ is associated with the image of $\bar{u}\,\bar{v}$.

Proof. Assume that μ is a section and let $\delta \in \Delta$ be arbitrary. Then, since $\sigma(\delta)\,u - u\delta = 0$, $\mu(\sigma(\delta))\,\bar{u} - \bar{u}\,\mu(\delta) \in N^{i+1}$. Similarly, $\mu(\theta(\delta))\,\bar{v} - \bar{v}\,\mu(\delta) \in N^{j+1}$. Thus, $\bar{u}\,\mu(\theta(\delta))\,\bar{v} - \overline{uv}\,\mu(\delta) \in N^{i+j+1}$ and $\mu(\sigma\,\theta(\delta))\,\bar{u}\,\bar{v} - \bar{u}\,\mu(\theta(\delta))\,\bar{v} \in N^{i+j+1}$ by lemma 3 of the previous chapter, and hence, $\bar{u}\,\mu(\theta(\delta))\,\bar{v} - \bar{u}\,\bar{v}\,\mu(\delta) + \mu(\sigma\,\theta(\delta))\,\bar{u}\,\bar{v} - \bar{u}\,\mu(\theta(\delta))\,\bar{v} = \mu(\sigma\,\theta(\delta))\,\bar{u}\,\bar{v} - \bar{u}\,\bar{v}\,\mu(\delta) \in N^{i+j+1}$. Let w be the image of $\bar{u}\,\bar{v}$ in N^{i+j}. We then have $\sigma\,\theta(\delta)\,w - w\,\delta = 0$ as was to be proved.

Proposition 2. Let $\{u_\alpha\}$ be a fixed left-Galois basis for N/N^2 and for each α, let $\bar{u}_\alpha$ be a given representative of u_α. Define $\overline{U^r}$ to be the set of products, r at a time, of the $\bar{u}_\alpha$'s. Further, let U^r be the image of $\overline{U^r}$ in N^r/N^{r+1}. Then U^r contains a set of left generators for N^r/N^{r+1} over Δ .

Proof. Let θ be a particular section. Then, by theorem 5 of the preceeding chapter, every element in N is congruent, modulo N^2, to an element of the form $\sum_\alpha \theta(\delta_\alpha)\,\bar{u}_\alpha$. By the definition of N^r, every element in N^r is the sum of products, r at a time, of elements in N. Hence, it is congruent, modulo N^{r+1}, to a sum of products, r at a time, of elements of the form of the above sum. By the previous proposition, we may permute the $\theta(\delta_\alpha)$'s and the $\bar{u}_\beta$'s appropriately, modulo N^{r+1}, to arrive at a representation of the form

$$\sum_i \left(\prod_j^r \theta(\delta_{ij}) \prod_j^r \bar{u}_{\alpha(i,j)}\right) ,$$

where each $\bar{u}_{\alpha(i,j)}$ is equal to $\bar{u}_\alpha$ for some α. We note that $w_i = \prod_j^r \bar{u}_{\alpha(i,j)} \in \overline{U^r}$ for each i.

Since π_r is multiplicative for each r, every element in N^r/N^{r+1} may be written in the form $\sum_i \delta_i \pi_r (w_i)$, where $\delta_i = \pi_r (\prod_j \theta(\delta_{ij}))$. Notice that $\pi_r (w_i) \in U^r$.

Corollary 3. A completely primary ring which has a section is left-Galois if and only if N/N^2 is left-Galois.

Proof. If our ring is left-Galois, the definition implies that N/N^2 is left-Galois.

Conversely, by proposition 2, the set U^r is a set of generators for N^r/N^{r+1} and hence, it contains a basis. Proposition 1 implies U^r consists of Galois elements and thus, the basis is Galois.

Let $u \in N^i/N^{i+1}$ and $v \in N^j/N^{j+1}$. By the symbol u v, the symbolic product of u and v, we shall mean the image of the product of a representative of u and a representative of v in N^{i+j}/N^{i+j+1}. In the remainder of the paper, we shall suppose we are dealing with the actual product unless we state otherwise. As we have seen, this product is independent of the particular representatives. Note that the Δ operations on N^i/N^{i+1} are, in fact, symbolic products.

Let V_α^r be the subspace of N^r/N^{r+1} associated with an isomorphism α, as discussed in chapter II.

Proposition 4. If $u \in V_\alpha^i$ and $v \in V_\theta^j$, then u v (symbolic product) $\in V_{\alpha\theta}^{i+j}$.

This is nothing more than a restatement of proposition 1.

Suppose $u \in V_\alpha^i$, $v \in V_\theta^j$, and u v (symbolic product) $\neq 0$. If $\delta \in \Delta_\alpha$ and $\delta_1 \in \Delta_\theta$, then $\delta u \in V_\alpha^i$ and $\delta_1 v \in V_\theta^j$, by lemma 2 of the previous chapter and proposition 2 of chapter II. Hence, by the previous proposition, $\delta u \delta_1 v$ (symbolic product) $= \delta \alpha (\delta_1) u v$ (symbolic product) $\in V_{\alpha\theta}^{i+j}$ and is non-zero. Let $\bar{\delta} \in \Delta$. Then $\delta \alpha (\delta_1) u v \bar{\delta}$ (symbolic product) $= \alpha \theta (\bar{\delta}) \delta \alpha (\delta_1) u v$ (symbolic product). But $\delta \alpha (\delta_1) u v \delta$ (symbolic product) $= \delta \alpha(\delta_1) \alpha \theta (\bar{\delta}) u v$ (symbolic product). Thus, $\delta \alpha (\delta_1) \in \Delta_{\alpha\theta}$. Clearly, $\Delta_\alpha \subset \Delta_{\alpha\theta}$ and we have proved

Proposition 5. If $V_\alpha^i V_\theta^j \neq \{0\}$, then $\alpha (\Delta_\theta) \subset \Delta_{\alpha\theta}$.

As we have noted previously, if α is an automorphism, then Δ_α is the center of Δ.

Corollary 6. If α and θ are automorphisms and if $V_\alpha^i V_\theta^j \neq \{0\}$, then the center of Δ is stable under α.

The above proposition might be considered to be the initial steps toward relating our theory to the Galois theory of division rings. This will not be pursued further here.

We say a semi-group of isomorphisms, G (A), of Δ is <u>associated</u> with A if and only if (i) G (A) contains a set of generators H such that if $\alpha \in$ H, then there is a j for which $V_\alpha^j \neq \{0\}$, and (ii) if $V_\alpha^k \neq \{0\}$ for some k, then $\alpha \in$ G (A). It is clear that G (A) is necessarily unique.

Note that, by proposition 1 of chapter II, if an isomorphism is in G (A), so are all isomorphisms equivalent to it.

An isomorphism, σ , is realized in A, if there is a k such that $V_\sigma^k \neq \{0\}$. A semi-group of isomorphisms is realized in A, if it has a collection of generators, each of which is realized in A.

Proposition 7. Let $\sigma \in G$ (A) and suppose $V_\sigma^j \neq \{0\}$. Then there exist $\sigma_1, \sigma_2, \ldots, \sigma_j \in G$ (A) such that $V^1 \sigma_i \neq \{0\}$, for each i, and $\sigma = \sigma_1 \sigma_2 \ldots \sigma_j$.

Proof. By propositions 1 and 2, a Galois basis for N^j/N^{j+1} can be found in the set of symbolic products, j at a time, of Galois elements in N/N^2. Proposition 1 allows us to conclude the proof.

Corollary 8. The isomorphisms associated with N/N^2 form a generating set for G (A) .

Corollary 9. If the isomorphisms associated with N/N^2 are all automorphisms, then G (A) consists entirely of automorphisms.

V. GRADED RINGS

Assume, in this chapter, A is cleft.

Define, for each $j \geq 1$, $M^j = \{ n \in N \mid \deg(n) = j \} \cup \{ 0 \}$. In general, M^j is not a subspace of N, since even if n_1 and $n_2 \in M^j$, it is not necessarily true that $n_1 - n_2$ must be.

A ring is <u>generalized graded</u> if and only if M^j is a subspace of N for every j. It is <u>graded</u> if and only if $M^j M^k \subset M^{j+k}$, for each j and k, and it is generalized graded.

Proposition 1. If A is generalized graded, then $M^j \cong N^j/N^{j+1}$ as two sided vector spaces.

Proof. Certainly $M^j \subset N^j$ and every element in N^j/N^{j+1} is an image of an element in M^j. Also, $M^j \cap N^{j+1} = \{ 0 \}$. Hence, π_j is an epimorphism and a monomorphism and is, thus, an isomorphism.

Corollary 2. If A is graded, then the symbolic product corresponds to the actual product.

Suppose A is an arbitrary (possibly uncleft) completely primary ring. Define $F(A) = \Delta \oplus \sum_j \oplus N^j/N^{j+1}$ and define the product on F (A) to be the symbolic product. F (A) is easily seen to be a completely primary cleft graded ring with quotient ring Δ, if N is nilpotent.

Proposition 3. If A is Galois, so is F (A).

Proposition 4. A is graded if and only if A is isomorphic (as a ring) to F (A).

Proof. This follows immediately from proposition 1 and the definition of F (A).

Assume A is left-Galois and graded. In the previous section, we have determined the vector space structure of A in terms of the spaces N^j/N^{j+1}. Theorem 4 of chapter II allows us to express the structure in terms of the V_σ^j's.

Define $G^j = \{ \sigma \in G(A) \mid V_\sigma^j \neq \{0\} \}$ and let H^j be a subset of G^j which contains one, and only one, representative of an equivalence class in G^j.

Proposition 5. In the case described above, $A \cong \Delta \oplus \sum_j \sum_\sigma V^j_{(\sigma)} \cong \Delta \oplus \sum_j \sum_\sigma \Delta \otimes_{\Delta_\sigma} V_\sigma^j$, $\sigma \in H^j$, as two-sided vector spaces.

Proof. This follows immediately from theorem 4 of chapter II and the results of the foregoing section.

Denote the center of Δ by C.

Corollary 6. In the case described above, if G^1 consists of automorphisms, then $A \cong \Delta \otimes_C (\Delta \oplus \sum_j \sum_\sigma V_\sigma)$, $\sigma \in H^j$, as vector spaces.

The product is somewhat more difficult to determine. However, we may prove the following result.

Proposition 7. If $V_\sigma^j \neq \{0\}$, then $V_\sigma^j = \sum_{\sigma(1)\ldots\sigma(j)=\sigma} \Delta_\sigma V^1_{\sigma(1)} \cdots V^1_{\sigma(j)}$.

Proof. If $v \in V_\sigma^j$, then, according to propositions 1 and 2 of chapter IV, there exist Galois elements, $\{u_{kl}\}$, in M^1 such that $v = \sum_k \delta_k \prod_1^j u_{kl}$, where $\delta_k \in \Delta$. We may suppose, without loss of generality, the products $\prod_1^j u_{kl}$ are linearly independent.

Let σ be associated with v and let σ_k be associated with $\prod_1^j u_{kl}$. Then, if $\delta \in \Delta$, $\sigma(\delta)\, v = v\, \delta = \sum_k \delta_k \prod_1^j u_{kl}\, \delta = \sum_k \delta_k\, \sigma_k(\delta) \prod_1^j u_{kl} = \sigma(\delta) \sum_k \delta_k \prod_1^j u_{kl} = \sum_k \sigma(\delta)\, \delta_k \prod_1^j u_{kl}$. Thus, $\delta_k\, \sigma_k(\delta) = \sigma(\delta)\, \delta_k$, and $\sigma \sim \sigma_k$ for all k. However, proposition 1 of chapter II allows us to revise the u_{ki}'s so that $\sigma_k = \sigma$. This forces $\delta_k \in \Delta_\sigma$.

The reverse inclusion is obvious.

We note that for an arbitrary completely primary ring A, the above result is valid for F (A).

We shall now explore the product further in a special case. Suppose A is cleft and graded and suppose that if $V^j_\sigma \neq \{0\}$, then $[V^j_\sigma : \Delta]_L = 1$. Assume also that any isomorphism of Δ is realized in at most one M^j. Let $\{u_\sigma\}$ be a basis for N as a left space over Δ subject to the following conditions:

(1.) $\{u_\sigma\}$ is the union of left bases for the M^j's;

(2.) The isomorphism σ is associated with u_σ;

(3.) If σ (i) and θ (j) are associated with basis elements, for i = 1, 2, ..., r and j = 1, 2, ..., s, and if $\prod_i \sigma(i) \sim \prod_j \theta(j)$, then $\prod_i \sigma(i) = \prod_j \theta(j)$.

Under these conditions, in view of the preceeding material, the product of two basis elements has the form $u_\sigma u_\theta = \delta_{\sigma,\theta} u_{\sigma\theta}$, where $\delta_{\sigma,\theta}$ $\Delta_{\sigma\theta}$.

Since we are dealing only with associative rings, we must have $u_\lambda (u_\sigma u_\theta) = (u_\lambda u_\sigma) u_\theta$, for all λ, σ, and θ. But $u_\lambda (u_\sigma u_\theta) = u_\lambda (\delta_{\sigma,\theta} u_{\sigma\theta}) = \lambda(\delta_{\sigma,\theta}) u_\lambda u_{\sigma\theta} = \lambda(\delta_{\sigma,\theta}) \delta_{\lambda,\sigma\theta} u_{\lambda\sigma\theta}$ and $(u_\lambda u_\sigma) u_\theta = \delta_{\lambda,\sigma} u_{\lambda\sigma} u_\theta = \delta_{\lambda,\sigma} \delta_{\lambda\sigma,\theta} u_{\lambda\sigma\theta}$. Hence, we have the following proposition.

Proposition 8. If, under the conditions described above, $u_{\lambda\sigma\theta} \neq 0$, then

(4.) $\lambda(\delta_{\sigma,\theta}) \delta_{\lambda,\sigma\theta} = \delta_{\lambda,\sigma} \delta_{\lambda\sigma,\theta}$.

Equation 4 will be recognized to be the factor set identity in the theory of crossed products as described by, for instance, Albert (1, page 67). Actually, our theory may be considered to be a part of a generalized theory of such products. See the next chapter for a more general form of these identities.

Note that, in view of proposition 7, the third condition may always be satisfied in this case.

We are now in the position to be able to give an existence theorem.

Let G be a semi-group of isomorphisms of Δ. We shall suppose G is closed under equivalence. Let $\overline{G}$ be a set of generators of G and define $H \subset \overline{G}$ to be a set containing one, and only one, representative from each equivalence class in $\overline{G}$.

Let N be defined to be the left vector space with basis $\{u_\sigma \mid \sigma \in H\}$. Define a right Δ structure on N by letting $u_\sigma \delta = \sigma(\delta) u_\sigma$, for all $\sigma \in H$ and all $\delta \in \Delta$. Define the multiplication on N to be trivial, and let A be the direct sum of the rings Δ and N. Now, $(1 + \sum_\sigma \delta_\sigma u_\sigma)(1 - \Sigma \delta_\sigma u_\sigma) = 1 + \sum_\sigma \delta_\sigma u_\sigma - \sum_\sigma \delta_\sigma u_\sigma - \sum_\sigma \sum_\theta \delta_\sigma \sigma(\delta_\theta) u_\sigma u_\theta = 1$. Hence, A is a completely primary cleft ring with unique maximal ideal N and quotient ring Δ. Since $N^2 = \{0\}$, by the definition of N, A is left-Galois. We have the following theorem.

Theorem 9. If G is a semi-group of isomorphisms which is closed under equivalence, then there is a completely primary ring A such that $G = G(A)$.

Corollary 10. If G is a semi-group of isomorphisms, then G is realized by some completely primary ring.

Proof. Imbed G in its closure under equivalence.

VI. DIAGONAL RINGS

In this chapter, we shall assume our ring is cleft.

In general, an element may fail to be Galois in N even though its image in the appropriate quotient space is Galois. A is said to be diagonal if and only if A is Galois and there exists, for each j, a Galois basis for N^j/N^{j+1} which has a set of representatives, each of which is Galois.

Proposition 1. If N is nilpotent and if A is diagonal, then N is a Galois space over Δ .

Proof. Let $\{u_\alpha\}$ be the set of representatives discussed above. By theorem 5 of chapter III, this set is a left basis for N. Since each of the u_α's is Galois, so is the basis.

Proposition 2. If N is Galois as a Δ vector space, then N/N^2, and hence, A, is Galois.

Proof. The image of the Galois basis of N in N/N^2 certainly consists of Galois elements and generates N/N^2.

Corollary 3. If N is nilpotent, then A is diagonal if and only if N is Galois.

We list one sufficient condition for A to be diagonal. See the book by Jacobson (4, page 174) for a proof.

Proposition 4. If Δ is Galois, as a division ring, over the sub-division ring Γ and if N is Galois over Γ, then N is Galois over Δ.

We, of course, have the following:

Proposition 5. If A is graded, then A is diagonal.

Let A be a cleft completely primary diagonal ring with nilpotent maximal ideal. Suppose also that $[N : \Delta]_L < \infty$. Any algebra which contains a division ring and is finite dimensional over that ring may be associated with an isomorphic ring of matrices via the right regular representation. In this section, we shall study this construction in our context.

By the previous material, to determine the product in A, we need only partition the isomorphisms associated with N/N^2 into equivalence classes, take one, and only one, representative, σ, from each equivalence class and thus, determine V_σ^1, select a Galois basis $\{u_{\sigma_\alpha}\}$ for each V_σ^1 as a left basis over Δ_σ, and determine the products $\delta\, V_{\sigma\alpha}$ and $V_{\sigma\alpha} V_{\theta\beta}$ for all σ, θ, α, β, and for all $\delta \in \Delta$, where $V_{\sigma\alpha}$ is a particular representative of $u_{\sigma\alpha}$. The remainder of the product will follow from these by simple applications of the associative law, the distributive law, the Galois commutative law, and various of the preceeding results.

In particular, once we have chosen the bases $\{u_{\sigma_\alpha}\}$ for each σ, by our assumptions, we may choose the representatives $V_{\sigma\alpha}$ so they are Galois in N. The products of these elements form a set of generators for N, and hence, a left basis. This basis is clearly Galois.

Before we define our matrices, let us introduce some notation. Let G^k (A) be the subset of G (A) which is realized in N^k/N^{k+1}. Order the equivalence classes in G^i (A) as (σ_{ij}), j = 1, 2, ..., m (i), i = 1, 2, ..., m, where m is the degree of nilpotency of N. Let $s_{ij} = [V_{\sigma ij}^i : \Delta]_L$ and define $r_i = \sum_j s_{ij}$. Suppose $n = \sum_i r_i$.

Let $\{u_\alpha \mid s_{ij-1} < \alpha \leq s_{ij}\}$ be the representatives of the Galois basis of $V_{\sigma_{ij}}^i$ as selected above. We shall have occasion to say σ_α is associated with u_α with the realization that $\sigma_\alpha = \sigma_{ij}$ if $s_{ij-1} < \alpha \leq s_{ij}$.

By the assumptions above, we have the following equations.

(1.) $u_\alpha \delta = \sigma_\alpha (\delta) u_\alpha$, for each α and for $\delta \in \Delta$.

(2.) $u_\alpha u_\beta = \sum_\alpha \delta_{\alpha\beta\gamma} u_\gamma$, for all α and β . Note that equation 1 may be written in the form $u_\alpha \delta = \sum_\beta \delta_{\alpha\beta} u_\beta$, with $\delta_{\alpha\beta} = 0$ if $\alpha \neq \beta$, and $\delta_{\alpha\alpha} = \sigma_\alpha (\delta)$.

For each $\delta \in \Delta$, designate the matrix $(\delta_{\alpha\beta})$ by $\overline{\delta}$ and for each β , let $(\delta_{\alpha\beta\gamma})$ be denoted by U_β . It is clear the set of these matrices generate a ring isomorphic to A. Let us explore them in greater detail.

Proposition 6. For each $\delta \in \Delta$, $\overline{\delta}$ is a diagonal matrix.

This is the motivation for defining diagonal rings. In fact, we may prove the following result.

Proposition 7. If, in the right regular representation of a completely primary cleft algebra over Δ , the representation of Δ is diagonal for some basis, then A is diagonal.

Proof. If the representation is diagonal, then a form of equation 1 is valid for this basis.

Proposition 8. For fixed α and β , $\delta_{\alpha\beta\gamma} \in \Delta_{\sigma_\alpha \sigma_\beta}$ and $\sigma_\alpha \sigma_\beta = \sigma_\gamma$, for all γ, if $\delta_{\alpha\beta\gamma} \neq 0$.

Proof. $\sum_\gamma \sigma_\alpha \sigma_\beta (\delta_{\alpha\beta\gamma}) u_\gamma = \sigma_\alpha \sigma_\beta (\delta) u_\alpha u_\beta = u_\alpha u_\beta \delta =$ $\sum_\gamma \delta_{\alpha\beta\gamma} u_\gamma \delta = \sum_\gamma \delta_{\alpha\beta\gamma} \sigma_\gamma (\delta) u_\gamma$. Hence, $\sigma_\alpha \sigma_\beta (\delta) \delta_{\alpha\beta\gamma} = \delta_{\alpha\beta\gamma} \sigma_\gamma (\delta)$, and $\sigma_\alpha \sigma_\beta \sim \sigma_\gamma$ or $\delta_{\alpha\beta\gamma} = 0$. By our hypothesis, $\sigma_\alpha \sigma_\beta \sim \sigma_\gamma$ implies $\sigma_\alpha \sigma_\beta = \sigma_\gamma$.

Corollary 9. If $\sigma_\alpha \sigma_\beta \neq \sigma_\gamma$, then $\delta_{\alpha\beta\gamma} = 0$.

A is associative, so $u_\alpha (u_\beta u_\gamma) = (u_\alpha u_\beta) u_\gamma$. But $u_\alpha (u_\beta u_\gamma) =$

$u_\alpha (\sum_\lambda \delta_{\beta\gamma\lambda} u_\lambda) = \sum_\lambda \sigma_\alpha (\delta_{\beta\gamma\lambda}) u_\alpha u_\lambda = \sum_\lambda \sigma_\alpha (\delta_{\beta\gamma\lambda}) \sum_\mu \delta_{\alpha\lambda\mu} u_\mu =$

$\sum_\mu (\sum_\lambda \sigma_\alpha (\delta_{\beta\gamma\lambda}) \delta_{\alpha\lambda\mu}) u_\mu$, and $(u_\alpha u_\beta) u_\gamma = \sum_\lambda \delta_{\alpha\beta_\lambda} u_\lambda u_\gamma = \sum_\mu (\sum_\lambda \delta_{\alpha\beta\lambda} \delta_{\lambda\gamma\mu}) u_\mu$.

Proposition 10. For every α, β, γ, and μ,

(3.) $\sum_\lambda \sigma_\alpha (\delta_{\beta\gamma\lambda}) \delta_{\alpha\lambda\mu} = \sum_\lambda \delta_{\alpha\beta\lambda} \delta_{\lambda\gamma\mu}$.

This equation will be recognized to be the promised generalization of equation 4 of chapter V.

Proposition 11. If $\alpha > r_i$, $\beta > r_j$, and $\gamma \leq r_{i+j+1}$, then $\delta_{\alpha\beta\gamma} = 0$.

Proof. Suppose $u_\alpha \in N^{i+1}$ and $u_\beta \in N^{j+1}$. Then $u_\alpha u_\beta \in N^{i+k+2}$.

Let us consider the form of the matrices in another way. Suppose $r_{i-1} < \alpha \leq r_i$.

$$U_\alpha = \left(\begin{array}{c} \underbrace{00\ldots010\ldots0}_{1+2} \\ \underbrace{\qquad\qquad\qquad}_{1 + \sum_{j \leq i} r_j} A^\alpha \end{array} \right)$$

, where $A^\alpha = (A^\alpha_{r_k r_l})$,

$1 \leq k \leq m-i$, $i + 1 \leq l \leq m$, and $A^\alpha_{r_k r_l} = (0)$ if $l - k < 0$. These inequalities express the diagonal nature of the matrices as discussed in proposition 11.

$A^\alpha_{r_k r_l} = (B^\alpha_{s_{kp} s_{lq}})$, where $B^\alpha_{s_{kp} s_{lq}}$ is an $s_{kp} \times s_{lq}$ matrix of elements of Δ which satisfies the following properties.

(4.) If $s_{lq-1} < \alpha \leq s_{lq}$, δ is an entry in $B^\alpha_{s_{kp} s_{lq}}$ only if $\delta \in \Delta_{\sigma_\alpha}$. This is a second expression for proposition 8.

(5.) $B^\alpha_{s_{kp} s_{lq}} = (0)$, if $\sigma_\beta \neq \sigma_\gamma \sigma_\gamma$, where $s_{lq-1} < \beta \leq s_{lq}$ and

$s_{k_{p-1}} < \gamma \leq s_{k_p}$. This property is a restatement of corollary 9.

Of course, the entries are also subject to equation 3.

To see this actually characterizes such rings, suppose we have a ring of matrices generated over the diagonal representation of Δ by matrices of the form of the U_α's. The entries in the first row guarantee the independence of the U_α's and properties 4 and 5 guarantee the Galois character of the ring.

VII. GENERALITIES

In this chapter, we shall indicate some of the difficulties one encounters in attempting to generalize the methods of the previous chapters and in further determining the structure of an arbitrary left-Galois ring.

Suppose A is cleft and N is nilpotent, but suppose A is not diagonal. We may still write equations 1 and 2 of the previous chapter, although in a slightly revised form.

(1.) $u_\alpha \delta = \sum_\beta \delta_{\alpha\beta} u_\beta$.

(2.) $u_\alpha u_\beta = \sum_\gamma \delta_{\alpha\beta\gamma} u_\gamma$.

The first difficulty arises when we attempt to determine the $\delta_{\alpha\beta}$'s and the $\delta_{\alpha\beta\gamma}$'s. The method of proof of proposition 8 of the preceeding chapter is no longer applicable.

Let us consider the matrix representation of $\delta \in \Delta$ in such a ring. It is easily verified that $\overline{\delta} = (\theta_{\alpha\beta}(\delta))$, where the $\theta_{\alpha\beta}$'s satisfy:

(3.) $\theta_{\alpha\beta}$ is a (group) homomorphism of Δ into Δ;

(4.) $\theta_{\alpha\alpha}$ is a ring homomorphism;

(5.) $\theta_{\alpha\beta} = 0$, if $\alpha > \beta$; and

(6.) For all δ_1 and δ_2 in Δ , $\theta_{\alpha\beta}(\delta_1 \delta_2) = \sum_\gamma \theta_{\alpha\gamma}(\delta_1)\, \theta_{\alpha\beta}(\delta_2)$.

Such a set of mappings might be called generalized derivations. See the book by Jacobson (4, pages 170 and 171) for a discussion.

It would still seem to be possible to construct and determine the structure of the matrix representation of such a ring. However, there are immediate notational difficulties. How many subscripts are admissible before confusion reigns? Thus, other methods would seem to be necessary for an adequate exploration.

In a more general case, where A is possibly uncleft even though a section exists, two immediate difficulties arise. Δ is no longer a subring of A and hence, we must work with coefficients in an additive abelian group which is the image of Δ under a section. Thus, we would be considering an additive group with an additive group of operators!

In general, if σ is a section and if u is the representative of a Galois element which is associated with θ , we have $\sigma(\theta(\delta))u - u\sigma(\delta) \neq 0$.

Let us define some functions and indicate their interrelationship.

If $\delta \in \Delta$, θ is a section, and if u is a representative of a Galois element associated with σ , $v(\theta, u, \delta) = \theta(\sigma(\delta))u - u\theta(\delta)$.

If $\delta \in \Delta$, and if θ and σ are two sections, $w(\theta, \sigma, \delta) = \theta(\delta) - \sigma(\delta)$.

If θ is a section and if δ_1 and δ_2 are in Δ , $y(\theta, \delta_1, \delta_2) = \theta(\delta_1 \delta_2) - \theta(\delta_1)\theta(\delta_2)$.

Note that $v(\theta, u, -)$ and $w(\theta, \sigma, -)$ are group homomorphisms from Δ into N. $y(\theta, -, -)$ is a biadditive map from $\Delta \times \Delta$ to N.

$$\begin{aligned} v(\theta, u, \delta) &= \theta(\sigma(\delta))u - u\theta(\delta) \\ &= \pi(\sigma(\delta))u + w(\theta, \pi, \sigma(\delta))u \\ &\quad + u\pi(\theta) + u\,w(\theta, \pi, \delta). \end{aligned}$$

$$\begin{aligned} y(\theta, \delta_1\delta_2, \delta_3) &- y(\theta, \delta_1, \delta_2\delta_3) \\ &= \theta(\delta_1\delta_2\delta_3) - \theta(\delta_1\delta_2)\theta(\delta_3) - \theta(\delta_1\delta_2\delta_3) \\ &\quad + \theta(\delta_1)\theta(\delta_2\delta_3) \\ &= \theta(\delta_1)\theta(\delta_2\delta_3) - \theta(\delta_1\delta_2)\theta(\delta_3) \end{aligned}$$

$$= \theta(\delta_1)\, y(\theta, \delta_2, \delta_3) - y(\theta, \delta_1, \delta_2)\, \theta(\delta_3)$$

$$\begin{aligned} w(\theta, \pi, \delta_1 \delta_2) &= \theta(\delta_1 \delta_2) - \pi(\delta_1 \delta_2) \\ &= \theta(\delta_1)\, \theta(\delta_2) + y(\theta, \delta_1, \delta_2) \\ &\quad - \pi(\delta_1)\, \pi(\delta_2) - y(\pi, \delta_1, \delta_2) \\ &= \theta(\delta_1)\, w(\theta, \pi, \delta_2) + w(\theta, \pi, \delta_1)\, \pi(\delta_2) \\ &\quad + y(\theta, \delta_1, \delta_2) - y(\pi, \delta_1, \delta_2). \end{aligned}$$

Hence, we have the equations:

(7.) $v(\theta, u, \delta) - v(\pi, u, \delta) = w(\theta, \pi, \sigma(\delta))\, u - u_\sigma\, w(\theta, \pi, \delta);$

(8.) $\theta(\delta_1)\, y(\theta, \delta_2, \delta_3) - y(\theta, \delta_1 \delta_2, \delta_3) + y(\theta, \delta_1, \delta_2 \delta_3)$
$- y(\theta, \delta_1, \delta_2)\, \theta(\delta_3) = 0;$

(9.) $\theta(\delta_1)\, w(\theta, \pi, \delta_2) - w(\theta, \pi, \delta_1 \delta_2) + w(\theta, \pi, \delta_1)\, \pi(\delta_2)$
$= y(\pi, \delta_1, \delta_2) - y(\theta, \delta_1, \delta_2).$

These equations indicate the relationship of this theory to the cohomology theory of algebras. Unfortunately, the author's knowledge of this area is very limited. Thus, results will have to await further preparation and study.

If no sections exist, then other problems arise. Note however, if A and Δ are algebras over a field, then a section always exists.

VIII. BIBLIOGRAPHY

1. Albert, A. Adrian. Structure of algebras. American Mathematical Society Colloquium Publications 24. 1939.

2. Dieudonne, Jean. La theorie de Galois des anneaux simples et semi-simples. Commentarii Mathematici Helvetici 21: 154-184. 1948.

3. Hochschild, G. Double vector spaces over division rings. American Journal of Mathematics 71: 443-460. 1949.

4. Jacobson, Nathan. Structure of rings. American Mathematical Society Colloquium Publications 37. 1956.

IX. ACKNOWLEDGMENT

I wish to thank Professor Bernard Vinograde for his patient encouragement and counsel.

X. APPENDIX

The Loewy series of a completely primary ring with maximal ideal N is the series of ideals $N \supset N^2 \supset N^3 \supset \cdots$.

An element, u, in a two-sided vector space over a division ring, Δ , is left-Galois if $u\,\Delta \subset \Delta\, u$. A two-sided vector space is left-Galois if it has a left basis of left-Galois elements.

$V_\sigma = \{ v \in V \mid \sigma(\delta)\, v = v\,\delta$, for every $\delta \in \Delta$. $\}$.

$V_{(\sigma)} = \{ v \in V \mid$ There is a $\tau \sim \sigma$ such that $\tau(\delta)\, v = v\delta$, for all $\delta \in \Delta$. $\}$.

$\Delta_\sigma = \{ \delta \in \Delta \mid \delta\, \delta_1 = \delta_1\, \delta$, for all $\delta_1 \in \sigma(\Delta)$. $\}$.

For each j = 0, 1, 2, ... , π_j is the canonical mapping from N^j to N^j/N^{j+1}. π_0 is usually denoted by π.

If we assume N^r properly contains N^{r+1}, if $N^r \neq \{0\}$, for each r, each element, n, in N is associated with an integer j such that $n \in N^j - N^{j+1}$. This integer is the degree of n.

A section is a (group) homomorphism from Δ into A which is a right inverse for π. A ring is cleft if it has a section which is a ring homomorphism.

A completely primary ring is left-Galois if each of the spaces N^j/N^{j+1} are left-Galois.

A cleft ring is generalized graded if for each j, $M^j = \{ n \in N \mid \deg(n) = j \} \cup \{0\}$ is a two-sided vector space. It is graded if it is generalized graded and for each j and k, $M^j M^k \subset M^{j+k}$.

A completely primary ring is diagonal if and only if it is cleft and the maximal ideal is left-Galois over the quotient division ring.