

# On Decompositions of Ideals in Weak Crossed Product Algebras

Alexander Retakh  
New York University

Indiana University REU, Summer 1995

Professor Darrell Haile, advisor

**Abstract:** The first two chapters of this paper give a brief introduction into the subject of weak crossed product algebras. In Chapter 3 we present some new examples of weak 2-cocycles. The remaining chapters are dedicated to the consideration of the algebraic properties of weak crossed product algebras, mostly questions related to the decomposition of an algebra and its ideals.

## 1. Introduction: Classical Theory.

The main algebraic structure considered here, namely the crossed product algebras, can be understood with only the formal definition which is given in chapter 2. Nonetheless, it seems useful to justify the reasons for the consideration of this structure. In this we follow Herstein [He]; however, for the most part proofs are omitted.

DEFINITION 1.1. An algebra  $A$  is said to be *simple* if it contains no two-sided ideals aside from  $(0)$  and itself.

Simple algebras are, in a sense, the most primitive ones. Any other algebra can be factored and the study of the quotient algebra immediately contributes to our knowledge of the original algebra. To simple algebras, this method is inapplicable.

On the other hand, if an algebra nice enough (that is, Artinian) is factored by its radical, the quotient algebra is a direct sum of simple algebras. This demonstrates the importance of the study of simple algebras in the Artinian case.

We will now consider only simple algebras with the unit element  $\mathbf{1}$ . Let  $F$  be the base field. The subfield  $F\mathbf{1}$ , which we will identify with the field  $F$ , lies in the center of  $A$ . However, the converse does not necessarily hold.

DEFINITION 1.2. A simple algebra  $A$  over a field  $F$  is called a *central simple  $F$ -algebra* if its center consists entirely of  $F$ .

Therefore, central simple  $F$ -algebras are “more simple” than others with a unit element.

Central simple algebras are a fairly closed family, that is a tensor product of two is again a simple central algebra over the same field. A classical example of a central simple algebra is a matrix algebra over any field. Moreover, even matrices over a division algebra form a central simple algebra. However, this is all we’ve got up to isomorphism as the following demonstrates.

THEOREM 1.1. (Wedderburn) *Every central simple algebra  $A$  is isomorphic to a ring of all  $n \times n$  matrices over some division algebra  $D$ .*

It seems only natural to introduce the classification of central simple algebras such that two algebras belong to one class if and only if they may be viewed as the matrix rings over the same division algebra. This defines an equivalence relation. Furthermore, the tensor product respects classes, i.e. if  $A_1 \sim A_2$  and  $B_1 \sim B_2$ , then  $A_1 \otimes_F A_2 \sim B_1 \otimes_F B_2$ . One may define a binary operation on classes and, surprisingly, a group structure emerges with the class of matrix algebras over field  $F$  serving as the unit element. The inverse elements come along; we will not go into details here. The group is called the *Brauer group*,  $B(F)$ . It is abelian and torsion.

All would be well and covered with glory if the classification of division algebras were a simple task. Unfortunately, this is not the case and a slightly different approach in the study of central simple algebras must be employed. One may still try to use the Brauer group but to look for class representatives other than division algebras.

An important observation of a more philosophical nature argues that we should pay attention to maximal subfields of central simple algebras; after all, a field extension is a relatively well known object. The following statement paves the way for the further study of central simple algebras:

**THEOREM 1.3.** *In every equivalence class of central simple algebras there exists an algebra  $A$  with a maximal subfield  $K$  Galois over  $F$  such that  $[A : F] = [K : F]^2$ .*

Let  $G$  be the Galois group of  $K$  over  $F$ . A corollary of the *Noether-Skolem Theorem* states that for every element  $\sigma \in G$ , there is an invertible element  $x_\sigma$  of  $A$  such that  $k^\sigma = x_\sigma k x_\sigma^{-1}$  for every  $k \in K$ . Furthermore, the  $x_\sigma$  are linearly independent over  $K$  and, since the dimension of their linear span is  $n^2$  over  $F$ , it must be all of  $A$ . In short,  $A = \left\{ \sum_{\sigma \in G} k_\sigma x_\sigma \mid k_\sigma \in K \right\}$ .

It is a natural desire to study  $x_\sigma$  more closely. A simple computation reveals that  $(x_\sigma x_\tau)^{-1} x_{\sigma\tau} \in K^\times$ , in other words that  $x_\sigma x_\tau = f(\sigma, \tau) x_{\sigma\tau}$  where  $f(\sigma, \tau) \neq 0$ . We have obtained a function  $f : G \times G \rightarrow K^\times$ . Associativity of  $A$  translates in terms of  $f$  into the following property:

$$f^\sigma(\tau, \gamma) f(\sigma, \tau\gamma) = f(\sigma\tau, \gamma) f(\sigma, \tau). \quad (1.1)$$

It is easy to demonstrate that  $f(\text{id}, \sigma) = f^\sigma(\text{id}, \text{id})$  and that  $f(\text{id}, \text{id})^{-1} x_{\text{id}}$  is a unit element of  $A$ . In order to simplify the situation, we will allow only such functions  $f$  for which

$$f(\text{id}, \sigma) = f(\sigma, \text{id}) = 1. \quad (1.2)$$

**DEFINITION 1.3.** Let  $K$  be an extension of  $F$  with Galois group  $G$ . A function  $f : G \times G \rightarrow K^\times$  is called *2-cocycle* if it satisfies (1.1) and (1.2) for all  $\sigma, \tau, \gamma \in G$ .

Later it will become clear that even under the limitation (1.2), it is still possible to find in each class an algebra with  $f$  being a 2-cocycle. We may now formally define such algebras:

**DEFINITION 1.4.** Let  $K$  be an extension of  $F$  with Galois group  $G$ . Let  $f$  be a 2-cocycle. The algebra  $(K, G, f) = \left\{ \sum_{\sigma \in G} k_\sigma x_\sigma \mid k_\sigma \in K \right\}$  with component-wise addition and multiplication defined by

$$\begin{aligned} \text{(i)} \quad x_\sigma k &= k^\sigma x_\sigma && \text{for } k \in K, \\ \text{(ii)} \quad x_\sigma x_\tau &= f(\sigma, \tau) x_{\sigma\tau} && \text{for } \sigma, \tau \in G, \end{aligned}$$

is called the *crossed product* of  $K$  and  $G$  re  $f$ .

However, since formally the crossed product is a totally new structure, we need to establish its properties and, first of all, to show that it is indeed an algebra. The latter task is not extraordinarily difficult; as for the former, one may easily see that  $x_{\text{id}}$  acts as a unit element, that each  $x_\sigma$  is invertible, that the center of  $(K, G, f)$  is  $F$ , and that its dimension over  $F$  is  $[K : F]^2$ .

We will now demonstrate that  $(K, G, f)$  is simple. Let  $I \neq (0)$  be an ideal of  $(K, G, f)$  and let  $a = \sum_{\sigma \in G} k_{\sigma} x_{\sigma}$  be a non-zero element of  $I$  of shortest length. Multiplying by  $x_{\sigma}^{-1}$ , we may always achieve  $k_{\text{id}} \neq 0$ . For any  $l \in K$ ,  $la - al = \sum_{\sigma \in G} (l - l^{\sigma}) k_{\sigma} x_{\sigma}$  lies in  $I$ ; however, for  $\sigma = \text{id}$ ,  $l = l^{\sigma}$  and we get an element of shorter length. Therefore,  $k_{\sigma} = 0$  for all  $\sigma \neq \text{id}$  and  $a = k_{\text{id}} x_{\text{id}}$  which means that  $a$  is invertible. Hence  $I$  is all of  $(K, G, f)$ .

The reasonable wish now is to dig further into the crossed product algebras and, since we define them with respect to a basis, study what different bases give rise to the same algebras, i.e. study the isomorphisms.

Let the canonical basis of  $A = (K, G, f)$  be  $x_{\sigma}$ . It is clear that elements  $y_{\sigma} = \lambda_{\sigma} x_{\sigma}$ ,  $\lambda \in K^{\times}$  span  $A$ . Then,  $y_{\sigma} y_{\tau} = \lambda_{\sigma} x_{\sigma} \lambda_{\tau} x_{\tau} = \lambda_{\sigma} \lambda_{\tau}^{\sigma} f(\sigma, \tau) x_{\sigma\tau} = \lambda_{\sigma} \lambda_{\tau}^{\sigma} \lambda_{\sigma\tau}^{-1} f(\sigma, \tau) y_{\sigma\tau}$  and we get another 2-cocycle,

$$g(\sigma, \tau) = \lambda_{\sigma} \lambda_{\tau}^{\sigma} \lambda_{\sigma\tau}^{-1} f(\sigma, \tau). \quad (1.3)$$

We introduce another definition:

**DEFINITION 1.5.** Two cocycles  $f$  and  $g$  are said to be *equivalent* if (1.3) holds for some set of  $\lambda_{\sigma} \in K^{\times}$ .

One may also show that if  $(K, G, f)$  and  $(K, G, g)$  are isomorphic, then  $f \sim g$ . Had we allowed earlier cocycles to take any value of  $f(\sigma, \text{id})$ , it would be still possible to find an equivalent cocycle with  $f(\sigma, \text{id}) = 1$ , the  $\lambda_{\sigma}$  defined in this case by  $\lambda_{\sigma} = f^{\sigma}(\text{id}, \text{id})^{-1}$ .

We have demonstrated an important result:

**THEOREM 1.4.** *Let  $K$  be an extension of  $F$  with Galois group  $G$ . Let  $f$  be a 2-cocycle. Then the crossed product  $(K, G, f)$  is a central simple  $F$ -algebra. Furthermore, for every central simple  $F$ -algebra  $A$ , there exist  $K, G, f$  such that  $A \sim (K, G, f)$ .*

Equivalence classes of cocycles form a group  $H^2(G, K^{\times})$  with point-wise multiplication. A product of two cocycles  $f, g$  produces a crossed product algebra that is equivalent to the tensor product of the algebras arising from by  $f$  and  $g$ . Therefore, we can speak of a map  $H^2(G, K^{\times}) \rightarrow B(F)$  with exactly equivalent cocycles being mapped into one element of the Brauer group.

For further results on cocycles and central simple algebras, the reader is referred to [He].

## 2. Weak Crossed Product Algebras and Their Basic Properties.

The 2-cocycles discussed above were mappings  $G \times G \rightarrow K^{\times}$ . We allow them now to take value 0:

**DEFINITION 2.1.** Let  $K$  be an extension of  $F$  with Galois group  $G$ . A function  $f : G \times G \rightarrow K$  is called *weak 2-cocycle*<sup>†</sup> if it satisfies conditions (1.1) and (1.2) and for all  $\sigma, \tau, \gamma \in G$ .

The next step is to define weak crossed product algebras:

---

<sup>†</sup> Another name is *cosickle* and it well reflects the sick nature of these functions. However, the author views the term very ambiguous, for sickles that immediately spring to mind have long been in the realm of Agriculture and not Mathematics.

DEFINITION 2.2. Let  $K$  be an extension of  $F$  with Galois group  $G$ . Let  $f$  be a weak 2-cocycle. The algebra  $(K, G, f) = \{\sum_{\sigma \in G} k_{\sigma} x_{\sigma} \mid k_{\sigma} \in K\}$  with component-wise addition and multiplication defined by

$$\begin{aligned} \text{(i)} \quad x_{\sigma} k &= k^{\sigma} x_{\sigma} && \text{for } k \in K, \\ \text{(ii)} \quad x_{\sigma} x_{\tau} &= f(\sigma, \tau) x_{\sigma\tau} && \text{for } \sigma, \tau \in G, \end{aligned}$$

is called the *weak crossed product* of  $K$  and  $G$  re  $f$ .

For the sake of brevity, we will refer to weak 2-cocycles simply as cocycles. All algebras discussed below are weak crossed product algebras.

One may still try to find connections with the classical theory and search where  $f$  does not take value 0. Consider the set  $H$  of  $\sigma \in G$  such that  $f(\sigma, \tau) \neq 0$  for all  $\tau \in G$ . It follows from the equality

$$f^{\sigma_1}(\sigma_2, \tau) f(\sigma_1, \sigma_2 \tau) = f(\sigma_1 \sigma_2, \tau) f(\sigma_1, \sigma_2) \quad (2.1)$$

that if  $\sigma_1, \sigma_2 \in H$ , then  $\sigma_1 \sigma_2 \in H$ . Let  $\sigma_2 = \sigma_1^{-1}$ , then

$$f^{\sigma_1}(\sigma_1^{-1}, \tau) f(\sigma_1, \sigma_1^{-1} \tau) = f(\sigma_1 \sigma_1^{-1}, \tau) f(\sigma_1, \sigma_1^{-1}). \quad (2.2)$$

Since  $f^{\sigma_1}(\sigma_1^{-1}, \tau) \neq 0$ ,  $\sigma_1^{-1} \in H$ . Therefore,  $H$  is a group. From (2.2), it is easy to deduce that the necessary and sufficient condition for  $\sigma$  to belong to  $H$  is  $f(\sigma, \sigma^{-1}) \neq 0$ . In terms of algebra, this means that for all  $\sigma \in H$ ,  $x_{\sigma}$  is invertible which is yet another connection between  $H$  and the classical case. Moreover, if one is to consider a subgroup of  $G$  such that for every  $\sigma$  from this subgroup  $f(\tau, \sigma) \neq 0$  for every  $\tau \in G$ , one will eventually see that this group is nothing but  $H$ .

DEFINITION 2.3. The subgroup of  $G$ ,  $H = \{\sigma \mid f(\sigma, \sigma^{-1}) \neq 0\}$  is called the *inertial subgroup*.

We have just shown that for every  $\sigma \in H$  and every  $\tau \in G$ ,  $f(\sigma, \tau) \neq 0$  and  $f(\tau, \sigma) \neq 0$ . The algebra  $B = \bigoplus_{\sigma \in H} K x_{\sigma}$  is therefore a central simple  $K^H$ -algebra. Furthermore,  $J = \bigoplus_{\sigma \notin H} K x_{\sigma}$  is the Jacobson radical of  $A$ .

To study the algebra deeper, we would like to introduce the means of understanding how “far” an  $x_{\sigma}$  is from the simple component, in other words, how non-classical it is. Let us say that  $\sigma \leq \tau$  if there exists  $x_{\gamma}$  such that  $x_{\sigma} x_{\gamma} = x_{\tau}$ . Obviously,  $x_{\sigma} \leq x_{\tau}$  if and only if  $f(\sigma, \sigma^{-1} \tau) \neq 0$ . This gives a partial ordering on  $G$ . If  $\sigma \leq \tau$ , then for every  $h$  belonging to the inertial subgroup  $H$ ,

$$f^{\sigma}(\sigma^{-1} \tau, h) f(\sigma, \sigma^{-1} \tau h) = f(\tau, h) f(\sigma, \sigma^{-1} \tau)$$

and  $\sigma \leq \tau h$ . One may also demonstrate that  $\sigma h \leq \tau$ ; therefore, the constructed partial ordering is actually on the set of left cosets of  $G$ .

DEFINITION 2.4.  $\sigma H \leq \tau H$  if  $f(\sigma, \sigma^{-1} \tau) \neq 0$ .

THEOREM 2.1. *The partial ordering defined above is lower subtractive, that is, given  $\sigma H \leq \tau H$ , then  $\sigma H \leq \gamma H \leq \tau H$  if and only if  $\sigma^{-1} \gamma H \leq \sigma^{-1} \tau H$ .*

One may also introduce a partial ordering on right cosets:

DEFINITION 2.5.  $H\sigma \leq H\tau$  if  $f(\tau\sigma^{-1}, \sigma) \neq 0$ .

The lower subtractivity for the right cosets is formulated in the following way: given  $H\sigma \leq H\tau$ , then  $H\sigma \leq H\gamma \leq H\tau$  if and only if  $H\gamma\sigma^{-1} \leq H\tau\sigma^{-1}$ .

We will write  $\leq_l$  and  $\leq_r$  when both partial orderings are used in the discussion simultaneously.

Every partial ordering gives a rise to a graph, namely the elements of the set (in our case, the cosets) serve as a vertices. Two vertices  $a$  and  $b$  are connected by an edge if and only if one is greater or equal than the other and there exist no element  $c$  such that  $a \leq c \leq b$  and  $c \neq a$ ,  $c \neq b$ . Lower subtractivity in terms of graphs means that every part of a graph can be dragged down any number of vertices, so that it will coincide with the structure below.

The invertible cocycles form a group  $H^2(G, K^\times)$  under the equivalence defined in Chapter 1. All cocycles form a monoid  $M^2(G, K)$ , the elements of which we denote as  $[f]$ . The idempotent cocycles, that is cocycles taking only values 0 and 1, can not be equivalent to each other and thus uniquely correspond to the idempotent elements of  $M^2(G, K)$ . Let  $e$  be an idempotent cocycle. Consider cocycles assuming zero values where  $e$  assumes zeroes, or in more rigorous form, consider

$$M_e^2(G, K) = \{[f] \in M^2(G, K) \mid [f][e] = [f], \exists g [f][g] = [e]\}.$$

This is a group. Clearly, all cocycles such that their equivalence classes belong to one  $M_e^2$  have the same graph, thus there is exactly one graph corresponding to each  $M_e^2$ .

Moreover,  $M^2(G, K) = \bigsqcup_e M_e^2(G, K)$ . A homomorphism  $H^2(G, K) \rightarrow M_e^2(G, K)$  is given by  $[f] \mapsto [fe]$ . The restriction  $f|_{H \times H}$  is an invertible cocycle on  $H$ , and this provides us with a group homomorphism  $M_e^2(G, K) \rightarrow H^2(H, K^\times)$  given by  $[f] \mapsto [f|_{H \times H}]$ .

It was shown in [HLS] that the idempotents with the inertial subgroup  $H$  correspond one-to-one to the lower subtractive partial orderings on the left cosets  $G/H$ . Hence, the study of graphs, a structure reasonably simple to handle, gives information about  $M_e^2(G, K)$ , a rather complicated group. The most well-researched case is the case of a graph being a tree.

THEOREM 2.2. [H1] *If the graph of  $M_e^2(G, K)$  is a tree, then the homomorphism  $M_e^2(G, K) \rightarrow H^2(H, K^\times)$  described above is injective.*

Therefore, if  $H$  is trivial, there exists only one cocycle corresponding to any tree. Consider now the Waterhouse idempotent cocycle  $e_H$ :  $e_H(\sigma, \tau) \neq 0$  if and only if  $\sigma \in H$  or  $\tau \in H$ .

THEOREM 2.3. [H2] *If the graph of  $M_e^2(G, K)$  is a tree, then  $M_e^2(G, K)$  is isomorphic to  $M_{e_H}^2(G, K)$ .*

This fact makes possible to study  $M_e^2(G, K)$  for any tree, since  $M_{e_H}^2(G, K)$  is fairly simple to analyze, its graph being a tree with all leaves directly above the node.

We have stated above that for every cocycle, there exists a lower subtractive graph. However, the number of cocycles grows enormously as  $G$  becomes larger and sometimes

even the study of graphs does not furnish the desired information. One may try to construct examples and counterexamples by the means of constructing a lower subtractive graph and then looking for a cocycle corresponding to it. It is not known whether or not one necessarily succeeds.

CONJECTURE. *Given a lower subtractive graph, it is always possible to find a group such that there exists a cocycle on this group corresponding to the given graph.*

The stronger statement suggests that it is always possible to find a group and a cocycle such that the inertial subgroup is trivial. The weaker statement argues that it is always possible to find a group and a cocycle such that a subgraph of its graph is the given one.

### 3. Some Examples: Cyclic Groups and Cycles.

As we have said above, the most interesting situation emerges when the graph of a cocycle is not a tree. Moreover, since we are interested mostly in the differences between the classic and the weak cases, it would be reasonable to consider specially the finite fields. Their Brauer groups are trivial, yet there are a plenty of weak crossed product algebras in the finite case. Since the only possible Galois extensions of a finite field are the cyclic ones, some attention should be paid to the cyclic groups.

For the rest of this chapter, we will confine ourselves to the case of a trivial inertial subgroup. This enables us to reach direct conclusions about the cocycle by the consideration of the corresponding graph.

Consider a cyclic group  $C_n$  of order  $n$  generated by  $\sigma$ .

Our target is to have an example of a non-tree graph for  $C_n$ . However, every lower-subtractive graph with 3 vertices is a tree, so we consider  $n \geq 4$ . The immediate suggestion would be to have just one cycle with  $\sigma^0 = \text{id}$  at the bottom and some  $\sigma^m$  at the top. The intermediate elements, certainly, may be positioned in any fashion, yet the lower subtractivity should be obeyed. The simplest picture arises when the elements follow each other in the natural order:

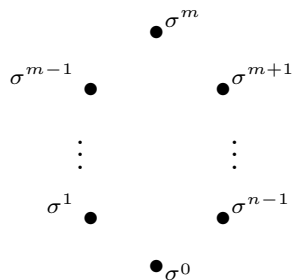


FIG. 3.1.

What other possibilities are there?

Assume that directly above  $\sigma^0$ , there are vertices  $\sigma^k$  and  $\sigma^l$  and  $\sigma^m$  is at the top:

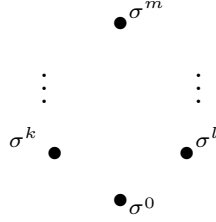


FIG. 3.2.

From lower subtractivity, directly above  $\sigma^k$ , there can be only  $\sigma^{k+l}$  or  $\sigma^{2k}$ ; above  $\sigma^l$ , only  $\sigma^{k+l}$  or  $\sigma^{2l}$ . If  $n = 4$ , then it is possible that  $\sigma^{k+l}$  is directly above both  $\sigma^k$  and  $\sigma^l$ :



FIG. 3.3.

Note that even though the graphs above correspond to two different sets of cocycles, they are similar, for an automorphism on  $C_4$  that exchange  $\sigma$  and  $\sigma^3$ , turns one case into the other.

However, for  $n > 4$  the presence of  $\sigma^{k+l}$  in both branches is impossible. By branch, we mean one of the paths from  $\sigma^0$  to  $\sigma^m$ . Hence, without loss of generality, we may assume that one of the two cases takes place:

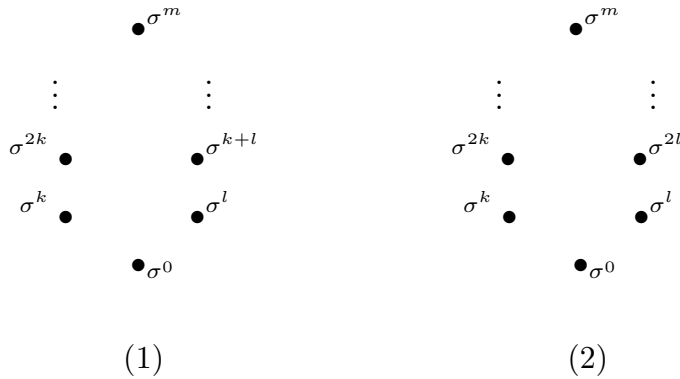


FIG. 3.4.

Owing to lower subtractivity, the branches should grow up homogeneously, i.e. above  $\sigma^{2k}$  only  $\sigma^{3k}$ ,  $\sigma^{4k}$ , etc. can be; and above  $\sigma^{k+l}$  only  $\sigma^{2k+l}$ ,  $\sigma^{3k+l}$ , etc.

Consider the case corresponding to the graph (1) in Figure 3.4. Obviously,  $m \equiv rk \pmod{n}$  and  $m \equiv sk + l \pmod{n}$  for some  $r, s$ , thus

$$k \equiv (r - s)k \pmod{n}.$$

We have constructed the graph in such a way that all elements above  $\sigma^l$  should fit between  $\sigma^k$  and  $\sigma^m$ , hence  $r \geq s$ . However, if the equality holds, then  $\sigma^l = \text{id}$ . Therefore,  $r > s$  but then  $r > r - s > 0$  and  $\sigma^{(r-s)k} = \sigma^l$  must be located between  $\sigma^k$  and  $\sigma^m$ . The contradiction demonstrates that case (1) is impossible if  $n > 4$ .

Consider now the graph (2). Since  $\sigma$  is one of the vertices, it is a power of either  $\sigma^k$  or  $\sigma^l$ , thus either  $\sigma^k$  or  $\sigma^l$  is a generator of  $C_n$ . We might rename the group elements, so that whichever of  $\sigma^k$  or  $\sigma^l$  is a generator, it becomes a new  $\sigma$ . The new  $\sigma^{n-1}$  can not be above the new  $\sigma$ , otherwise all elements will be lined up above the new  $\sigma$ , thus  $\sigma^{n-1}$  belongs to the other branch and the lowest element there (formerly  $\sigma^k$  or  $\sigma^l$ ) is also a generator. Having two generators, we may choose one with the longer branch and, if needed, rename it  $\sigma$ . The graph will become the following:

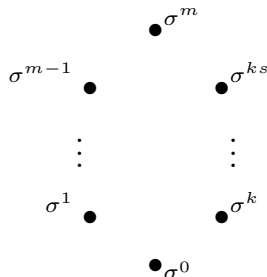


FIG. 3.5.

Obviously  $m < n - 1$ . We chose  $k$  so that  $2l \geq n$ . However, in this case if  $m \leq ik \pmod{n}$  for some  $i$ , then  $ik \leq k \pmod{n}$ . The best way to understand the previous statement is to draw a circle with all numbers from 0 to  $n - 1$  on it in a natural order, and look at this picture for a few moments. The statement itself suggests that because  $\sigma^{n-1}$  is somewhere in the graph,  $k$  must be equal to  $n - 1$ . Therefore, up to a group automorphism, for  $n > 4$  the only possible graph consisting of only one cycle is the one presented in Figure 3.1.

It is easy to see where the cocycle corresponding to this graph takes zero and non-zero values.

	$\sigma^0$	$\sigma$	$\dots\dots$	$\sigma^{m-1}$	$\sigma^m$	$\sigma^{m+1}$	$\dots\dots$	$\sigma^{n-1}$
$\sigma^0$	1	1	$\dots\dots$	1	1	1	$\dots\dots$	1
$\sigma$	1	*	$\dots\dots$	*	0	0	$\dots\dots$	0
$\vdots$	$\vdots$	$\vdots$	$\ddots$	0	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\sigma^{m-1}$	1	*	0	$\dots$	0	0	$\dots\dots$	0
$\sigma^m$	1	0	$\dots\dots$	0	0	0	$\dots\dots$	0
$\sigma^{m+1}$	1	0	$\dots\dots$	0	0	0	$\dots$ 0	*
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	0	$\ddots$	$\vdots$
$\sigma^{n-1}$	1	0	$\dots\dots$	0	0	*	$\dots\dots$	*

From the cocycle condition (1.1),

$$f^{\sigma^{i-1}}(\sigma, \sigma^j) f(\sigma^{i-1}, \sigma^{j+1}) = f(\sigma^i, \sigma^j) f(\sigma, \sigma^i)$$

and it is easy to prove by induction that in the upper triangle all entries depend on the values of  $f(\sigma, \sigma^i)$  which in their turn are independent. The last statement is also correct for the lower triangle and the entries  $f(\sigma^{n-1}, \sigma^i)$ . Hence, the dimension of the space of cocycles is  $n - 2$ .

However, our goal is to find the algebras corresponding to the graph in Figure 3.1, i.e. the order of the corresponding  $M_e^2$ , the group of the classes of equivalent cocycles. Recall that the set  $\{\lambda_{\sigma^i} x_{\sigma^i}\}$  spans the same algebra as the canonical basis  $\{x_{\sigma^i}\}$ .

So, let  $\{x_{\sigma^i}\}$  be the standard basis of  $(K, G, f)$ . We introduce new basis  $\{y_{\sigma^i}\}$ :

$$\begin{aligned}
y_\sigma &= kx_\sigma \\
y_{\sigma^{n-1}} &= k'x_{\sigma^{n-1}} \\
y_{\sigma^i} &= \begin{cases} (y_\sigma)^i, & 1 < i \leq m \\ (y_{\sigma^{n-1}})^{n-i}, & m < i < n-1 \end{cases}
\end{aligned}$$

The new cocycle  $f_\theta$  will take the following shape:

	$\sigma^0$	$\sigma$	.....	$\sigma^{m-1}$	$\sigma^m$	$\sigma^{m+1}$	.....	$\sigma^{n-1}$
$\sigma^0$	1	1	.....	1	1	1	.....	1
$\sigma$	1	1	.....	1	0	0	.....	0
$\vdots$	$\vdots$	$\vdots$	$\ddots$	0	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\sigma^{m-1}$	1	1	0 ...	0	0	0	.....	0
$\sigma^m$	1	0	.....	0	0	0	.....	0
$\sigma^{m+1}$	1	0	.....	0	0	0	... 0	$\theta$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	1
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	0	$\ddots$	$\vdots$
$\sigma^{n-1}$	1	0	.....	0	0	$\theta$	1 ...	1

where  $(y_{\sigma^{n-1}})^{n-m} = \theta y_{\sigma^m}$ .

What  $f_\theta$  are equivalent to the idempotent cocycle? Using the notations for the change of basis above, we may calculate  $\theta$  when  $f$  is idempotent. From the following equalities:

$$y_{\sigma^m} = (y_\sigma)^m = (kx_\sigma)^m = k\sigma(k) \cdot \dots \cdot \sigma^{m-1}(k)x_{\sigma^m},$$

$$\theta y_{\sigma^m} = (y_{\sigma^{n-1}})^{n-m} = (k'x_{\sigma^{n-1}})^{n-m} = k'\sigma^{n-1}(k') \cdot \dots \cdot \sigma^{(n-1)(n-m-1)}(k')x_{\sigma^m}$$

by substituting  $l$  for  $\sigma^{m+1}(k')$ , we obtain

$$\theta = \frac{l\sigma(l) \cdot \dots \cdot \sigma^{n-m-1}(l)}{k\sigma(k) \cdot \dots \cdot \sigma^{m-1}(k)}. \quad (3.1)$$

From this,

$$M_2^e = K^\times / \left\{ \frac{l\sigma(l) \cdot \dots \cdot \sigma^{n-m-1}(l)}{k\sigma(k) \cdot \dots \cdot \sigma^{m-1}(k)} \mid k, l \in K^\times \right\}.$$

We can also calculate  $M_e^2$  for  $C_4$  in the special case depicted on Figure 3.3.

The general form of the cocycle is:

	$\sigma^0$	$\sigma$	$\sigma^2$	$\sigma^3$
$\sigma^0$	1	1	1	1
$\sigma$	1	0	*	0
$\sigma^2$	1	*	0	0
$\sigma^3$	1	0	0	0

Since our goal is to classify the equivalence classes, by the same argument as above, we may assume that  $f(\sigma, \sigma^2) = 1$ . If so, then the table obtains this form:

	$\sigma^0$	$\sigma$	$\sigma^2$	$\sigma^3$
$\sigma^0$	1	1	1	1
$\sigma$	1	0	1	0
$\sigma^2$	1	$\theta$	0	0
$\sigma^3$	1	0	0	0

Following the discussion of the general case, we see that it is possible to take new  $y_\sigma = kx_\sigma$  and  $y_{\sigma^2} = k'x_{\sigma^2}$ . Thus if the cocycle is equivalent to the idempotent one,

$$\begin{aligned} y_{\sigma^3} &= kx_\sigma k'x_{\sigma^2} = k\sigma(k')x_{\sigma^3} \\ \theta y_{\sigma^3} &= k'x_{\sigma^2} kx_\sigma = k'\sigma^2(k)x_{\sigma^3}. \end{aligned}$$

We see that

$$\theta = \frac{k'\sigma^2(k)}{k\sigma(k')} \quad (3.2)$$

and

$$M_e^2 = K^\times / \left\{ \frac{k'\sigma^2(k)}{k\sigma(k')} \mid k, k' \in K^\times \right\}.$$

For the graph in Figure 3.1, we are able to obtain the more precise result in the finite case.

We have already remarked that every Galois extension of a finite field is cyclic. Furthermore, if  $|F| = q$  and  $|K| = q^n$ , then for every  $k \in K$ ,  $\sigma^i(k) = k^{q^i}$ . The multiplicative group of a finite field is generated by a single element  $a$ ; therefore, if in the equation (3.1) we consider  $k = a^s$  and  $l = a^t$ , then

$$\begin{aligned} \theta &= \frac{a^t a^{tq} \cdot \dots \cdot a^{tq^{n-m-1}}}{a^s a^{sq} \cdot \dots \cdot a^{sq^{m-1}}} = \\ &= a^{t(1+q+\dots+q^{n-m-1}) - s(1+q+\dots+q^{m-1})}. \end{aligned}$$

Thus the lowest possible value of  $\theta$  is  $a^{\gcd(1+q+\dots+q^{n-m-1}, 1+q+\dots+q^{m-1})}$ .

We will show now that

$$\gcd(1+q+\dots+q^{n-m-1}, 1+q+\dots+q^{m-1}) = 1+q+\dots+q^{\gcd(n,m)-1}.$$

Indeed, in this case the first step of the Euclidean algorithm is

$$1+q+\dots+q^{n-m-1} = (1+q+\dots+q^{m-1})(q^r+\dots) + (1+q+\dots+q^{r-1}),$$

where  $r = n \bmod m$ . On the other hand, for  $n$  and  $m$ , the first step of the Euclidean algorithm is

$$n = m \cdot u + r.$$

It is easy to see that these coincidences — the power of the remainder in the first algorithm plus one being equal the remainder in the second — will continue to occur until

we will arrive at  $1 + q + \dots + q^{\gcd(n,m)-1}$  which divides both  $1 + q + \dots + q^{n-m-1}$  and  $1 + q + \dots + q^{m-1}$ . Thus it is the greater common divisor that we wanted to get.

Therefore, the final answer says that if  $f_\theta$  is equivalent to the idempotent cocycle  $e$ , then  $\theta$  is a power of  $a^{1+q+\dots+q^{\gcd(n,m)-1}}$  where  $a$  generates  $K^\times$ , the multiplicative group of  $K$ . Hence,

$$|M_e^2| = \frac{q^{\gcd(n,m)} - 1}{q - 1}.$$

Thus, if  $m$  and  $n$  are relatively prime, i.e. when  $\sigma^m$  is a generator of  $G$ ,  $M_e^2$  is trivial.

This shows that the order of  $M_e^2$  depends not only on the geometrical properties of the corresponding graph but also on the positioning of vertices in the graph.

Furthermore, it seems that the geometry of a graph is not very crucial at all.

Our other example concerns cocycles on the groups  $C_n \times C_m$ . Let  $\sigma$  be a generator of  $C_n$  and  $\tau$  a generator of  $C_m$ . Consider the following grid:

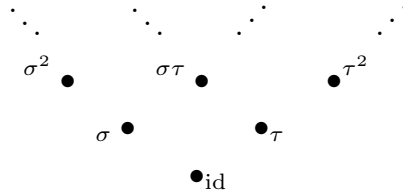


FIG. 3.6.

Unlike the previous example, it is more difficult to say what values the cocycle takes; however, we are still able to calculate the  $M_e^2$ . Indeed, whatever basis  $\{x_{\sigma^i\tau^j}\}$  and the corresponding cocycle are given, we may always construct another basis:

$$\begin{aligned} y_\sigma &= kx_\sigma \\ y_\tau &= k'x_\tau \\ y_{\sigma^i\tau^j} &= (y_\sigma)^i(y_\tau)^j. \end{aligned}$$

It is not difficult to observe that the new cocycle  $f_\theta$  depends solely on one parameter  $\theta = f(\tau, \sigma)$ . Moreover,  $\theta$  can take any non-zero value. The other values of  $f$  may be obtained by the use of associativity of the algebra and, since the cocycle condition (1.1) is equivalent to associativity, the cocycle condition will be preserved. Our only remaining task is to calculate what  $f_\theta$  are equivalent to the idempotent cocycle.

From the formulas for  $\{y_{\sigma^i\tau^j}\}$ , we see that

$$\begin{aligned} y_{\sigma\tau} &= kx_\sigma k'x_\tau = k\sigma(k')x_{\sigma\tau}, \\ \theta y_{\sigma\tau} &= k'x_\sigma kx_\tau = k'\tau(k)x_{\sigma\tau}. \end{aligned}$$

From this,

$$\theta = \frac{k'\tau(k)}{k\sigma(k')}. \quad (3.2)$$

and

$$M_e^2 = K^\times / \left\{ \frac{k'\tau(k)}{k\sigma(k')} \mid k, k' \in K^\times \right\}.$$

Note that  $k/\tau(k)$  has norm 1 over  $K^{C_m}$  and  $k'/\sigma(k')$  has norm 1 over  $K^{C_n}$ . Furthermore, by the *Hilbert Theorem 90*, the elements with norm 1 over  $K^{C_m}$  and  $K^{C_n}$  have precisely these forms, hence,  $M_e^2$  is a factor of  $K^\times$  by the product of the groups of elements of norm 1 in the extensions  $K/K^{C_m}$  and  $K/K^{C_n}$ .

Once again, we can find the order of  $M_e^2$  when  $F$  is finite. Note that  $m$  and  $n$  must be relatively prime in this case.

As previously, let  $a$  be a generator of  $K^\times$ ,  $k = a^s$  and  $k' = a^t$ . Let  $\gamma$  be a generator of  $C_n \times C_m$ , then obviously  $\sigma = \gamma^m$  and  $\tau = \gamma^n$ . We have the following equation for  $\theta$ :

$$\theta = a^{s(q^n-1)-r(q^m-1)}.$$

The lowest power of  $a$  that may be expressed in such a form is  $a^{\gcd(q^n-1, q^m-1)}$ . Clearly,  $\gcd(q^n-1, q^m-1) = (q-1) \cdot \gcd(1+q+\dots+q^{n-1}, 1+q+\dots+q^{m-1})$ . It follows from the calculations of the gcd in the cyclic case that the value of the latter expression is simply  $q-1$ ; therefore,

$$|M_e^2| = q-1.$$

Recall that it is possible to obtain the same result for the example discussed first. We see now that, whereas the absence of cycles in the graph influences  $M_e^2$ , the presence of those may lead to any possible result. Nonetheless, the graphs still remains a rather useful machinery which we will heavily employ below.

#### 4. Two-Sided Ideals.

In the remaining chapters, we will discuss the algebraic properties of the weak crossed product algebras.

One of the most important differences between the classical and the weak cases is the existence of two-sided ideals inside weak crossed product algebras. Naturally, these objects require attention. We will start by proving an important structural theorem.

**THEOREM 4.1.** [H1] *If  $I$  is a two-sided ideal, then  $I = \bigoplus_{x_\sigma \in I} Kx_\sigma$ .*

**PROOF.** Obviously,  $\bigoplus_{x_\sigma \in I} Kx_\sigma \subseteq I$ . Consider  $a \in I - \bigoplus_{x_\sigma \in I} Kx_\sigma$  of the shortest length. If in the standard decomposition of  $a$  some  $x_\sigma \in I$  has a non-zero coefficient  $k$ , then  $a - kx_\sigma$  is of a shorter length. Thus, if  $a = \sum_\tau k_\tau x_\tau$ , then  $x_\tau \notin I$ .

Take any  $x_\gamma$  such that in the standard decomposition of  $a$ ,  $x_\gamma$  has a non-zero coefficient. For any  $l \in K$ ,  $al = \sum_\tau k_\tau l^\tau x_\tau \in I$  and  $l^\gamma a = \sum_\tau k_\tau l^\gamma x_\tau \in I$ ; therefore,  $al - l^\gamma a \in I$  and has a shorter length. Hence,  $al = l^\gamma a$  and  $l^\tau = l^\gamma$  for every  $l \in K$ . This situation is possible only if  $a = k_\gamma x_\gamma$  but then, since  $k_\gamma \neq 0$ ,  $x_\gamma$  belongs to  $I$ . The contradiction proves the statement. ■

Let us now consider the ideals  $I_\sigma$  generated by a single  $x_\sigma$ . All other two-sided ideals are their sums (though, not necessarily direct). The ultimate goal is to understand what  $x_\tau$  belong to  $I_\sigma$ .

Assume  $x_\sigma \in I$ , then for any  $\tau$  above  $\sigma$  in the left graph,  $x_\sigma x_{\sigma^{-1}\tau} \in I$ , thus  $x_\tau \in I$ . This is also true for every  $\tau$  above  $\sigma$  in the right graph. This non-formal observation suggests a path for the examination of the structure of  $I_\sigma$ . First we need to define ‘‘above’’ rigorously.

DEFINITION 4.1. For any subset  $S$  of the group  $G$ ,

$$L(S) = \{\beta \mid \exists \alpha \in S \quad \alpha H \leq_l \beta H\},$$

$$R(S) = \{\beta \mid \exists \alpha \in S \quad H\alpha \leq_r H\beta\}.$$

It is easy to see that  $L(L(S)) = L(S)$  and  $R(R(S)) = R(S)$ . Also,  $L(S \cup T) = L(S) \cup L(T)$  and  $R(S \cup T) = R(S) \cup R(T)$ .

Furthermore, as we have noticed above, for every  $\tau$  that belongs to  $L(\{\sigma\})$  or  $R(\{\sigma\})$ ,  $x_\tau \in I$  for any two-sided ideal  $I$  that includes  $x_\sigma$ . In particular, for every  $\tau \in L(R(\{\sigma\}))$ ,  $x_\tau \in I_\sigma$ . The same is true for every  $\tau \in R(L(\{\sigma\}))$ .

THEOREM 4.2. [W] For every two-sided ideal  $I_\sigma$  generated by a single element  $x_\sigma$ ,  $I_\sigma = \bigoplus_{\tau \in L(R(\{\sigma\}))} Kx_\tau$ .

PROOF. By Theorem 4.1 and by the statement of the previous paragraph, we need to prove only that every  $x_\tau \in I_\sigma$  belongs to  $R(L(\{\sigma\}))$ .

Consider  $x_\tau \in I_\sigma$ . By definition,  $I_\sigma = Ax_\sigma A$ ; therefore,  $x_\tau = ax_\sigma b$  where  $a, b \in A$ . Among the elements with non-zero coefficients in the standard decomposition of  $a$ , there is at least one  $x_\gamma$ , such that  $x_\gamma x_\sigma \neq 0$  and in the standard decomposition of  $b$ ,  $x_{\sigma^{-1}\gamma^{-1}\tau}$  has a non-zero coefficient. Furthermore, in order for  $x_\tau$  to come from the product  $ax_\sigma b$ ,  $f(\sigma\gamma, \sigma^{-1}\gamma^{-1}\tau) \neq 0$ . Since  $f(\gamma, \sigma) = f(\gamma\sigma \cdot \sigma^{-1}, \sigma)$  and we chose  $\gamma$  such that  $f(\gamma, \sigma) \neq 0$ ,  $H\sigma \leq_r H\gamma\sigma$  and  $\gamma\sigma H \leq_l \tau$ . In other words,  $\tau \in L(R(\{\sigma\}))$ . ■

In the similar manner we could have shown that  $\tau \in R(L(\{\sigma\}))$ , hence  $L(R(\{\sigma\})) = R(L(\{\sigma\}))$ .

COROLLARY. For any set  $S$ ,  $R(L(S)) = L(R(S))$ .

For every  $\sigma$ ,  $I_\sigma$  includes  $x_{h_1\sigma h_2}$  where  $h_1, h_2 \in H$ . These elements and their combinations are the only possible elements of  $I_\sigma$  if and only if there are no vertices above  $\sigma$  in both left and right graph.

DEFINITION 4.2. An element  $x_\sigma$  is said to be *l-maximal* if  $L(\{\sigma\}) = \sigma H$ . An element  $x_\sigma$  is said to be *r-maximal* if  $R(\{\sigma\}) = H\sigma$ . An element is said to be *bimaximal* if it is both l-maximal and r-maximal.

Therefore, for every bimaximal  $x_\sigma$ ,  $I_\sigma = \bigoplus_{\tau \in H\sigma H} Kx_\tau$  is minimal. Not surprisingly, the converse is also true. To prove it, we need a small lemma.

LEMMA 4.1. If  $x_\sigma$  is l-maximal and  $H\sigma \leq_r H\tau$ , then  $x_\tau$  is l-maximal.

PROOF. Since  $x_\sigma$  is l-maximal, for every  $\gamma \notin H$ ,  $f(\sigma, \gamma) = f(\sigma, \sigma^{-1} \cdot \sigma\gamma) = 0$ . From the cocycle condition (1.1),

$$f^{\tau\sigma^{-1}}(\sigma, \gamma)f(\tau\sigma^{-1}, \sigma\gamma) = f(\tau, \gamma)f(\tau\sigma^{-1}, \sigma),$$

it follows that  $f(\tau, \gamma) = 0$ . Hence  $x_\tau$  is maximal. ■

Obviously, if  $x_\sigma$  is r-maximal and  $\sigma H \leq_l \tau H$ , then  $x_\tau$  is r-maximal.

**THEOREM 4.3.** *A two-sided ideal  $I$  is minimal if and only if it is generated by a bimaximal element.*

PROOF. We have demonstrated that for a bimaximal  $x_\sigma$ ,  $I_\sigma$  is minimal.

Consider now an arbitrary two-sided ideal  $I$ . By Theorem 4.1,  $I \supseteq I_\tau$  for some  $\tau \in G$ . We can always find an l-maximal  $x_\gamma$  such that  $\tau H \leq_l \gamma H$ , hence  $I_\gamma \subseteq I_\tau$ .

There exists an r-maximal  $x_\sigma$  such that  $H\gamma \leq_r H\sigma$ . Furthermore,  $x_\sigma$  is l-maximal according to Lemma 4.1, thus  $I_\sigma \subseteq I$  for some bimaximal  $x_\sigma$ . ■

**COROLLARY.** [W] *The intersection of all two-sided ideals is bigger than (0) if and only if for all bimaximal elements  $x_\sigma$ ,  $\sigma$  belongs to the same double coset.*

PROOF. We may reformulate the statement: There exists exactly one minimal ideal if and only if for all bimaximal elements  $x_\sigma$ ,  $\sigma$  belongs to the same double coset.

Indeed, if there exists only one minimal ideal, then for every two bimaximal  $x_{\sigma_1}$  and  $x_{\sigma_2}$ ,  $\sigma_2 \in L(R(\{\sigma_1\}))$ . Hence,  $\sigma_2 \in L(H\sigma_1)$ , thus  $\sigma_2 \in H\sigma_1H$ .

The reversed argument demonstrates sufficiency. ■

This result shows that not only weak crossed product algebras have two-sided ideals, even the intersection of those is not necessarily (0).

It was stated above that for every set  $S$ ,  $R(L(S)) = L(R(S))$ . Moreover, for every  $\sigma$ , the elements that are above it in both left and right graphs are precisely those that are contained in  $R(L(S))$ . Indeed,

$$\begin{aligned} R(R(L(S))) &= R(L(S)), \\ L(R(L(S))) &= L(L(R(S))) = L(R(S)) = R(L(S)), \end{aligned}$$

and the rest is clear.

**DEFINITION 4.3.** For any subset  $S$  of the group  $G$ ,

$$D(S) = R(L(S)).$$

If  $x_\sigma \in I$  for some two-sided ideal  $I$  and  $\tau \in D(\{\sigma\})$ , then  $x_\tau \in I$ . Moreover, we may say now that  $x_\tau$  belongs to  $I_\sigma$  if and only if  $\tau \in D(\{\sigma\})$ . After a few remarks, we will be able to make the similar statement for all two-sided ideals.

Although the left and the right graphs demonstrate  $D(S)$  rather well, one may try to find better graphical means of presentation, for instance, to use one and not two pictures. The following notion was introduced by Krashen [K].

DEFINITION 4.4. The *digraph* is an oriented graph with the set of vertices  $G$ . Two vertices  $\sigma$  and  $\tau$  are connected by the edge  $(\sigma, \tau)$  if either  $\sigma H \leq_l \tau H$  or  $H\sigma \leq_r H\tau$ .

From the discussion above, it becomes clear that if there exists a path between two vertices  $\sigma, \tau$  of the digraph, it consists of either one edge (when  $\tau \in R(\{\sigma\})$  or  $\tau \in L(\{\sigma\})$ ) or two edges.

For every two-sided ideal  $I$ , we define the subdigraph corresponding to  $I$ . It is a subgraph of the digraph that consists of all vertices  $\sigma$  such that  $x_\sigma \in I$  and all edges between such  $\sigma$ . Obviously, every subdigraph is closed, i.e. there is no edge coming from it. Clearly, if a closed subgraph of a digraph contains the set  $S$ , then it contains  $D(S)$ . Furthermore, every closed subgraph of a digraph defines a two-sided ideal, namely if  $x_{\gamma_i}$  are the vertices in the closed subgraph,  $I = \bigoplus_{\gamma_i} Kx_{\gamma_i}$  is an ideal.

We may also define connectivity of a subdigraph. The subdigraph is called connected if for every two vertices  $\sigma, \tau$  in it, there exists either a path from  $\sigma$  to  $\tau$  or a path from  $\tau$  to  $\sigma$ .

THEOREM 4.4. [K] *A two-sided ideal  $I$  is indecomposable if and only if its subdigraph is connected.*

PROOF. Indeed, assume that  $I$  is decomposable, i.e.  $I = R_1 \oplus R_2$  or some non-empty two-side ideals  $R_1$  and  $R_2$ . Then the subdigraphs of  $R_i$  make up the subdigraph of  $I$  and, since the subdigraphs of  $R_i$  are closed and do not overlap, the subdigraph of  $I$  is not connected.

Assume now that the subdigraph of  $I$  is not connected. Each connected component is closed, for no edge can lead from a vertex in this component to a vertex into another component or to a vertex outside the subdigraph of  $I$ . Hence,  $I$  is a direct sum of the ideals generated by the elements of each component. ■

The notion of a digraph does help to analyze the structure of two-sided ideals. However, it merely reflects the concept of  $D(S)$  and as such does not directly arise from the structure of  $G$ , whereas both right and left ideals certainly do. It would be better to have a graphic representation of  $D(S)$  more closely connected to the Galois group; so far no progress has been made in this direction.

## 5. One-Sided Ideals.

For the sake of brevity, in this chapter we will consider only right ideals. All facts presented below are true for the left ideals and the proofs can be easily modified.

Unfortunately, one-sided ideals are not as easy to handle as the two-sided ones. Whereas in the previous chapter we could understand the structure of the ideals as described in Theorems 4.1 and 4.2, the one-sided case is more complicated. There exists no classification theorems; however, we can provide analogous but weaker statements.

DEFINITION 5.1. An element  $x_\sigma$  is said to be *involved* in the set  $S \subset A$  if there exists an element  $a \in S$  such that  $x_\sigma$  has a non-zero coefficient in the standard decomposition of  $a$ .

We denote involvement by  $x_\sigma \tilde{\in} S$ .

**THEOREM 5.1.** *If  $x_\sigma$  is involved in the right ideal  $I$ , then for every  $\tau \in L(\{\sigma\})$ ,  $x_\tau$  is involved in  $I$ .*

**PROOF.** Since  $\tau \in L(\{\sigma\})$ ,  $f(\sigma, \sigma^{-1}\tau) \neq 0$ . Therefore, if  $x_\sigma$  has a non-zero coefficient in the standard decomposition of  $a \in I$ , the coefficient of  $x_\tau$  in the standard decomposition of  $ax_{\sigma^{-1}\tau}$  is non-zero too.  $I$  is a right ideal, thus  $ax_{\sigma^{-1}\tau} \in I$  and  $x_\tau \in I$ . ■

We will now confine ourselves to the case of a trivial inertial subgroup. This will ease the situation quite a bit. If one is interested in the general case, all statements would be true if  $B$  is substituted for  $K$  and instead of an element, a whole coset is considered.

It is time to move on to the consideration of minimal right ideals. Let  $\{\sigma_i\}$  be l-maximal elements of  $G$ . Consider the ideal  $aA$  generated by  $a = \sum_i k_i x_{\sigma_i}$ . For every  $\tau \neq \text{id}$ ,  $ax_\tau = 0$ , thus  $aA = aK$  and, since every  $\sigma$  is an automorphism of  $K$ , this ideal is minimal. Furthermore, every minimal ideal is of this very form.

**THEOREM 5.2.** *In an algebra produced by a cocycle with a trivial inertial subgroup, every minimal right ideal is of the form  $(\sum_i k_i x_{\sigma_i})K$  for some set of l-maximal elements  $\sigma_i$ .*

**PROOF.** We have already demonstrated above that every ideal of such a form is minimal.

Consider now an arbitrary right ideal  $I$ . It certainly involves some l-maximal elements. Consider all elements of  $I$ , in the standard decomposition of which at least one l-maximal element has a non-zero coefficient. Let  $a$  be such an element of the shortest length. Assume that in the standard decomposition of  $a$  some non-l-maximal  $x_\tau$  has a non-zero coefficient. If  $\sigma$  is an l-maximal vertex above  $\tau$ , then  $ax_{\sigma^{-1}\tau}$  involves an l-maximal element. However, its length is shorter than the length of  $a$  and we arrive at a contradiction.

Hence,  $a$  involves only l-maximal elements and  $I$  has a subideal  $aK$ . ■

Following the discussion of two-sided ideals, we will try now to understand how the one-sided ideals decompose. In this, we will again limit ourselves to the case of a cocycle with a trivial inertial subgroup.

We need to introduce a natural notion of level.

**DEFINITION 5.2.** The *level* of a vertex  $\sigma$  above a vertex  $\tau$ ,  $\text{lev}_\tau(\sigma)$ , is the maximal number of vertices between  $\sigma$  and  $\tau$ . If  $\sigma \not\leq \tau$ , then  $\text{lev}_\tau(\sigma)$  is not defined. The level of  $\sigma$  above a set of vertices  $S$ ,  $\text{lev}_S(\sigma)$ , is the maximal level of  $\sigma$  above all vertices in  $S$ .

The level is transitive, i.e.  $\text{lev}_\sigma(\gamma) = \text{lev}_\sigma(\tau) + \text{lev}_\tau(\gamma)$  if  $\sigma \leq \tau \leq \gamma$ . Furthermore, there is a correlation between the level and the multiplication in the algebra. If  $x_\sigma x_\tau \neq 0$ , we can define the level of the vertex corresponding to the product. However, if the product equals zero, there is no such possibility — a rather sad limitation of Definition 5.2. However, we can expand it in quite an awkward fashion, namely the level of 0 above any element of  $G$  is considered to be  $\infty$ ; even though, 0 is not a group element.

**LEMMA 5.1.** *For every  $\sigma, \tau$ , and  $\gamma$ , the level of the vertex corresponding to the product  $x_\gamma x_{\sigma^{-1}\tau}$  above  $\gamma$ , is greater or equal to  $\text{lev}_\sigma(\tau)$ .*

**PROOF.** If  $x_\gamma x_{\sigma^{-1}\tau} = 0$ , then the statement is obvious.

Assume now that  $x_\gamma x_{\sigma^{-1}\tau} \neq 0$ . Then  $\gamma \leq \gamma\sigma^{-1}\tau$ , and we need to demonstrate that  $\text{lev}_\gamma(\gamma\sigma^{-1}\tau) \geq \text{lev}_\sigma(\tau)$ .

Let  $\text{lev}_\sigma(\tau) = n$ . This means that there are  $n$  vertices between  $\sigma$  and  $\tau$ , namely  $\sigma = \alpha_0 \leq \alpha_1 \leq \dots \leq \alpha_n = \tau$ . Obviously,

$$x_\tau x_{\sigma^{-1}\tau} = x_{\alpha_0} x_{\alpha_0^{-1}\alpha_n} = x_{\alpha_0} x_{\alpha_0^{-1}\alpha_1} \cdots x_{\alpha_{n-1}^{-1}\alpha_n}.$$

Hence,  $x_{\sigma^{-1}\tau} = x_{\alpha_0} x_{\alpha_0^{-1}\alpha_1} \cdots x_{\alpha_{n-1}^{-1}\alpha_n}$ . Therefore,

$$x_\gamma x_{\sigma^{-1}\tau} = x_\gamma x_{\alpha_0} x_{\alpha_0^{-1}\alpha_1} \cdots x_{\alpha_{n-1}^{-1}\alpha_n}.$$

Every multiplication raises the product at least one vertex up, thus the total lift is not less than  $n$  vertices. ■

The next result follows from one stated in [K]; however, the proof is entirely different. The methods used below seem to be of a more general nature.

**THEOREM 5.3.** *In an algebra produced by a cocycle with a trivial inertial subgroup, a right ideal  $I$  generated by one element  $x_\sigma$  is indecomposable.*

**PROOF.** Since  $I$  is generated by  $x_\sigma$ ,  $I = x_\sigma A$  and all elements  $x_\gamma$  involved in it belong to  $L(\{\sigma\})$ . Moreover, every element involved in  $I$  has a level greater or equal than 1 above  $\sigma$ .

Assume now that  $I$  decomposes into the direct sum of two right ideals  $I = R_1 \oplus R_2$ . In this case  $x_\sigma = r_1 + r_2$ , where  $r_i \in R_i$ . Without loss of generality, we may assume that  $x_\sigma$  has a non-zero coefficient in the standard decomposition of  $r_1$ . Consider the set  $S = \{r_1 x_{\sigma^{-1}\gamma} \mid x_\gamma \in I\}$ . It is clear that  $S$  spans  $R_1$ . Furthermore,  $S$  forms a basis of  $R_1$ :

To prove this, we need to show that all elements of  $S$  are linearly independent. Assume the contrary and consider

$$\Omega = \sum_{x_\gamma \in I} k_\gamma r_1 x_{\gamma^{-1}\sigma}.$$

Our assumption is that  $\Omega = 0$  and by induction we will show that all  $k_\gamma$  must be 0 under this condition.

In the standard decomposition of  $\Omega$ ,  $x_\sigma$  may appear only once, namely from the summand  $r_1 x_{\sigma^{-1}\sigma}$ , therefore the coefficient of this summand in  $\Omega$  is 0. Let now some  $x_\tau$  be on the  $n$ -th level above  $\sigma$ . We assume that for every  $x_\gamma$  with  $\text{lev}_\sigma(\gamma) < n$ ,  $k_\gamma = 0$ . What coefficient can  $x_\tau$  have in the standard decomposition of  $\Omega$ ? Obviously,  $x_\tau$  comes from  $r_1 x_{\sigma^{-1}\tau}$ . Let it also appear from some  $r_1 x_{\sigma^{-1}\gamma}$ . If  $\text{lev}_\sigma(\gamma) > n$  then it is impossible, for all elements in the standard decomposition of  $r_1 x_{\sigma^{-1}\gamma}$  have level greater than  $n$  above  $\sigma$ . If  $\text{lev}_\sigma(\gamma) = n$ , then  $x_\sigma x_{\sigma^{-1}\gamma} = f(\sigma, \sigma^{-1}\gamma) x_\tau$  and  $x_\gamma = x_\tau$ . Therefore, the coefficient of  $x_\tau$  in the standard decomposition of  $\Omega$  is  $k_\tau$ , thus  $k_\tau = 0$ .

Hence, all elements of  $S$  are linearly independent and  $\dim R_1 = |S| = \dim I$ . Thus,  $I = R_1$  and  $R_2 = 0$ . ■

Consider now an ideal  $I$  generated by two elements  $x_{\sigma_1}$  and  $x_{\sigma_2}$ . It is clear that  $I = x_{\sigma_1} A + x_{\sigma_2} A$ . When  $L(\{\sigma_1\}) \cap L(\{\sigma_2\}) = \emptyset$ , the sum is direct. In case when the intersection is not empty, one would like to see indecomposable ideals. Unfortunately, as it is, this is not true.



element that involves  $x_{\sigma_1}$ , hence by subtraction, we can always have in  $R_1$  two elements, one of which of all  $x_{\sigma_i}$  involves only  $x_{\sigma_1}$ , the other only  $x_{\sigma_2}$ . Let them be  $a_1 = x_{\sigma_1} + \Omega_1$  and  $a_2 = x_{\sigma_2} + \Omega_2$  respectively.

Consider now the following set

$$S = \left\{ a_1 x_{\sigma_1^{-1}\gamma} \mid \sigma_1 \leq \gamma \text{ and } \sigma_2 \not\leq \gamma \right\} \cup \\ \left\{ a_1 x_{\sigma_1^{-1}\gamma} \mid \sigma_1 \leq \gamma, \sigma_2 \leq \gamma \text{ and } \text{lev}_{\sigma_1}(\gamma) \geq \text{lev}_{\sigma_2}(\gamma) \right\} \cup \\ \left\{ a_2 x_{\sigma_2^{-1}\gamma} \mid \sigma_2 \leq \gamma, \sigma_1 \leq \gamma \text{ and } \text{lev}_{\sigma_2}(\gamma) > \text{lev}_{\sigma_1}(\gamma) \right\} \cup \\ \left\{ a_2 x_{\sigma_2^{-1}\gamma} \mid \sigma_2 \leq \gamma \text{ and } \sigma_1 \not\leq \gamma \right\}.$$

It is clear that every  $x_\gamma$  involved in  $I$  is mentioned above.

All elements of  $S$  belong to  $R_1$ . Furthermore, they are linearly independent. Indeed, consider  $\sum_{s \in S} l_s s = 0$ . Our goal is to show that under this condition all  $l_s$  equal 0. As in the proof of Theorem 5.3, we will use induction by the level of  $\gamma$ 's.

By Lemma 5.1,  $x_{\sigma_1}$  comes into the sum only from the summand  $a_1 x_{\sigma_1^{-1}\sigma_1}$ ; the same for  $x_{\sigma_2}$ . Consider now  $\tau$  such that  $\text{lev}_{\{\sigma_1, \sigma_2\}}(\tau) = n$ . We assume that for any  $\gamma$  with  $\text{lev}_{\{\sigma_1, \sigma_2\}}(\gamma) < n$ , the corresponding  $l_s$  is 0. Where does  $x_\tau$  come from in the sum? Certainly, not from some summand in  $\Omega_i x_{\sigma_i^{-1}\gamma}$ , for the level of  $\gamma$  is at least  $n$ , thus the level of every summand in  $\Omega_i x_{\sigma_i^{-1}\gamma}$  is greater than  $n$ . Hence,  $x_\tau$  can only possibly come from the summand  $x_{\sigma_i} x_{\sigma_i^{-1}\gamma}$  which is impossible. Therefore,  $x_\tau$  comes only from one and only one  $s$ , thus in the sum, the coefficient of this  $s$  is 0.

This demonstrates the linear independence of  $S$ . Since  $\dim R_1 \geq |S|$  and  $|S| = \dim I$ , we conclude that  $R_1$  is all of  $I$  and  $I$  is indecomposable.

The immediate conclusion is that in the standard decomposition of every element of  $R_i$ ,  $x_{\sigma_i}$  must have either both zero or non-zero coefficients. It follows that if we write an element of  $R_i$  in the form  $x_{\sigma_1} k_1 + x_{\sigma_2} k_2 + \Omega$ , then for all elements of  $R_i$ ,  $k_1$ 's are proportional and  $k_2$ 's are proportional.

This gives at least some idea of the nature of the direct summands in the decomposition of an ideal generated by two elements if such is possible. However, so far no further progress has been made in understanding the decomposition of right ideals.

## 6. Decomposing the Algebra.

We now turn our attention to the decomposition of the algebra and closely related questions. We will work only with idempotent cocycles.

It is clear that  $A$  can not be decomposed into the sum of two-sided ideals, for in this case one of the summands will involve, thus include,  $x_{\text{id}}$ . However, the decomposition of  $A$  into the sum of one-sided ideals is more interesting. We will now view  $A$  as a right module over itself.

It follows from Theorem 5.3 that if the inertial subgroup is trivial,  $A$  is indecomposable.

Consider now the general case. We remind the reader that the direct summands of the algebra are called *principal indecomposable* ideals. It appears that there is an easy way to describe them. For this, we need to introduce new terminology.

DEFINITION 6.1. Two idempotents  $e_1, e_2$  are said to be *orthogonal* if  $e_1e_2 = e_2e_1 = 0$ . An idempotent  $e$  is called *primitive* if it is impossible to express  $e$  as a sum of two orthogonal idempotents.

It is clear that for any idempotent  $e$ ,  $eA$  is a right ideal.

THEOREM 6.1. [CR] *A right ideal  $I$  of  $A$  is principal indecomposable if and only if  $I = eA$  for some primitive idempotent  $e$  in  $A$ .*

The quotient ideal  $eA/eJ$  sits inside the central simple component of  $A$ . The following fact makes it possible to classify all principal indecomposable ideals of  $A$ .

THEOREM 6.2. [CR] *There is a one-to-one correspondence between classes of isomorphic principal indecomposable ideals and classes of isomorphic irreducible right  $A$ -modules, given by the mapping  $\{eA\} \rightarrow \{eA/eJ\}$ .*

However, there is only one class of irreducible submodules of  $B$ , namely if  $B = M_n(D)$ , where  $D$  is a division algebra, then every irreducible submodule is isomorphic to  $D^n$  and may be seen as a set of matrices with zero entries in all but one column. Therefore, all principal indecomposable ideals are isomorphic to each other. We will now attempt to construct one such ideal.

THEOREM 6.3. *If the algebra  $A$  is produced by an idempotent cocycle and if the characteristic of  $F$  does not divide  $|H|$ , an ideal  $eA$  for  $e = \frac{1}{|H|} \sum_{h \in H} x_h$  is principal indecomposable.*

PROOF. We will first show that  $e$  is an idempotent. Indeed,

$$\begin{aligned} e^2 &= \frac{1}{|H|^2} \sum_{h_1 \in H} x_{h_1} \sum_{h_2 \in H} x_{h_2} = \\ &= \frac{1}{|H|^2} \sum_{h_1, h_2 \in H} x_{h_1} x_{h_2} = \\ &= \frac{1}{|H|^2} \sum_{h \in H} \sum_{h' \in H} x_{h'} x_{h'^{-1}h} = \\ &= \frac{1}{|H|^2} \sum_{h \in H} |H| x_h = \frac{1}{|H|} \sum_{h \in H} x_h = e. \end{aligned}$$

Assume now that  $e = e_1 + e_2$  for some orthogonal  $e_1$  and  $e_2$ . Let  $e_1 = \Omega_1 + \Omega_2$  where  $\Omega_1 \in B$  and  $\Omega_2 \in J$ . Without loss of generality, we may assume that  $\Omega_1 \neq 0$ . It is clear that  $e\Omega_2$  can not involve elements of  $H$ ; therefore, since  $ee_1 = e_1$  and  $e\Omega_1 \in B$ ,  $e\Omega_1 = \Omega_1$  and  $e\Omega_2 = \Omega_2$ . Let  $\Omega_1 = \sum_{h \in H} hk_h$ , then

$$\begin{aligned} e\Omega_1 &= \frac{1}{|H|} \sum_{h_1, h_2 \in H} x_{h_1} x_{h_2} k_{h_2} = \\ &= \frac{1}{|H|} \sum_{h \in H} \left( x_h \sum_{h' \in H} k_{h'} \right) = \Omega_1. \end{aligned}$$

Hence, for every  $h$ ,  $\frac{1}{|H|} \sum_{h' \in H} k_{h'} = k_h$ . From this, it follows plainly that all  $k_h$  are equal and  $\Omega_1 = em$  for some  $m \in K$ . Without loss of generality, we may assume  $m \neq 0$ .

We may rewrite now  $e_1, e_2$  in the form  $e_1 = em + \Omega_2, e_2 = e(1 - m) + \Omega_2$ .

Since  $e_1$  is an idempotent,  $e_1^2 = e_1$  or, in more explicit form,  $e_1^2 = (em)^2 + em\Omega_2 + \Omega_2em + \Omega_2^2 = em + \Omega_2$ . However, no multiple of  $\Omega_2$  can involve an element of  $H$ , thus  $(em)^2 = em$ .

Taking the square of  $e_2$ , we see that  $(e(1 - m))^2 = e(1 - m)$  for the reasons stated above. In more explicit form,

$$\begin{aligned} e(1 - m)e(1 - m) &= e - em - eme + (em)^2 = \\ &= e - em - eme + em = e - eme = e(1 - m). \end{aligned}$$

Therefore,  $em = eme$ . On the other hand,  $em = emem$  and  $em \neq 0$  (otherwise  $e$  would be 0). Hence,  $eme = emem$  and  $m = 1$ .

We conclude that if  $e$  is not primitive,  $e_2 \in J$ . Hence,  $e_2$  is nilpotent which is impossible; therefore  $e$  is primitive and by Theorem 6.1,  $eA$  is principal indecomposable. ■

The set of elements  $ex_\tau$  includes a basis of  $eA$ . If  $\tau_1$  and  $\tau_2$  belong to the same right coset, then  $ex_{\tau_1} = ex_{\tau_2}$ . It follows that the set  $S$  of  $ex_\tau$  with each  $\tau$  belonging to a different right coset, also includes a basis. On the other hand, this set is linearly independent.

Indeed, assume linear dependence, that is, assume that  $\sum l_\tau ex_\tau = 0$ . The element  $x_\tau$  appears in the product  $ex_\tau$ . If it also comes from some  $ex_\gamma$ , then  $x_h x_\gamma = x_\tau$  for some  $h \in H$ , thus  $h\gamma = \tau$ . But this is precisely the condition for  $\tau$  and  $\gamma$  being in the same right coset. Therefore, since we postulated that there can be no such  $x_\gamma$  in the sum,  $S$  is a basis of  $eA$ .

Knowing the precise structure of a principal indecomposable ideal of  $A$ , we may use it in search of projective ideals.

DEFINITION 6.2. A right ideal  $I$  is called *projective* if every exact sequence of right  $A$ -modules

$$0 \longrightarrow M \longrightarrow N \longrightarrow I \longrightarrow 0 \tag{6.1}$$

splits.

THEOREM 6.4. [CR] *An ideal  $I$  is projective if and only if it is direct sum of principal indecomposable ideals.*

Hence, every projective ideal of  $A$  is isomorphic to a sum of the copies of  $eA$ ,  $e$  as in the proof of Theorem 6.3. Obviously, the algebra  $A$  itself is projective. What about its most interesting part, the radical?

THEOREM 6.5. *The radical  $J$  is not projective.*

PROOF. We will prove a stronger statement: no subideal of  $J$  is isomorphic to a principal indecomposable ideal.

Assume that such is not the case and that for some  $I \in J$  there exists an isomorphism  $\phi : eA \rightarrow I$ ,  $e$  a primitive idempotent. Then  $I$  is generated by  $\phi(e)$  and its basis is formed by  $\phi(ex_\tau) = \phi(e)x_\tau$ . Consider  $x_\sigma$  with  $\sigma$  r-maximal. Since  $\phi(e) \in J$ ,  $\phi(e)x_\sigma = 0$  while  $ex_\sigma \neq 0$ . The contradiction proves the desired statement. ■

Our proof has an obvious corollary: no subideal of the radical is projective. We know at least one ideal that is projective, namely the principal indecomposable ideal itself.

We introduce another concept which is similar to the notion of projective ideals.

DEFINITION 6.3. A right ideal  $I$  is called *injective* if every exact sequence of right  $A$ -modules

$$0 \longrightarrow I \longrightarrow N \longrightarrow M \longrightarrow 0 \quad (6.2)$$

splits.

Unlike the projective case, not every weak crossed product algebra is injective. To find those that are injective, we require the following fact.

THEOREM 6.6. [CR] *An algebra  $A$  is injective over itself if and only if for every minimal right ideal its dual ideal is minimal, and if for every minimal left ideal its dual ideal is minimal.*

We will again consider only the case of a trivial inertial group. One may show that the conclusion of the next theorem is also true in the general case if, instead of one element, one considers a coset.

THEOREM 6.7. *An algebra  $A$  produced by a cocycle with a trivial inertial subgroup is injective over itself if and only if has exactly one l-maximal and one r-maximal element.*

PROOF. According to Theorem 5.2, every minimal right ideal  $I$  has the form

$$\left( \sum_i k_i x_{\sigma_i} \right) K$$

for some l-maximal  $x_{\sigma_i}$ .

The dual ideal  $I'$  is the set of homomorphisms from  $I$  to  $A$ . It is clear that every such homomorphism  $\phi$  is defined by the image of  $a = \sum_i k_i x_{\sigma_i}$ . Furthermore, since for every  $x \in J$ ,

$$\phi(a)x = \phi(ax) = 0,$$

$\phi(a)$  must be a sum of l-maximal elements with some non-zero coefficients.

Since we require  $I'$  to be minimal, there must be only one l-maximal element. Moreover, the same line of argument may be applied to the left ideals and it will show that there must be only one r-maximal element. Therefore, we have established the existence of exactly one l-maximal element and one r-maximal element when  $A$  is injective.

On the other hand, when there is exactly one l-maximal, by Lemma 4.1 it must be also r-maximal, hence in this case the dual ideal of a minimal right ideal is automatically minimal. The same is true for a minimal left ideal when there is exactly one r-maximal element. ■

The argument in the last paragraph of the proof shows that we may rewrite the statement of the last theorem: An algebra produced by a cocycle with a trivial inertial subgroup is injective if and only if there exists only one bimaximal element and no other l- and r-maximal elements.

COROLLARY. *If algebra  $A$  is injective, it has only one minimal right ideal.*

PROOF. Indeed, we know that every minimal right ideal is of the form  $kx_\sigma K$  where  $x_\sigma$  is the bimaximal element but for every  $k_1, k_2 \in K$ ,  $k_1x_\sigma = k_2x_\sigma(k_1k_2^{-1})^{\sigma^{-1}}$ . Hence there exists only one such ideal. ■

COROLLARY. [K] *If algebra  $A$  is injective, then all its ideals are indecomposable.*

However, so far the case of injective algebras is the only one in which the one-sided ideals can be classified to some extent. The most interesting part of the algebra is that makes it non-simple, namely the radical  $J$ . As we have seen in the last two chapters, the structure of the radical in the general case is still a mystery.

### Acknowledgments.

I want to thank the National Science Foundation for providing the funds for the Summer REU program at Indiana University. I thank all students and professors who participated in this program for helpful discussions. My special thanks go to Professor Darrell Haile who introduced me to the subject of crossed product algebras and guided my research.

### BIBLIOGRAPHY

- [CR] C. CURTIS, I. REINER, “Representation Theory of Finite Groups and Associative Algebras,” John Wiley and Sons, New York, N.Y., 1962.
- [H1] D. HAILE, On crossed product algebras arising from weak cocycles, *J. Algebra* **74** (1982), 270-279.
- [H2] D. HAILE, Brauer monoid of a field, *J. Algebra* **81** (1983), 521-539.
- [He] I. HERSTEIN. “Noncommutative Algebra,” Carus Mathematical Monograph No.15, Mathematical Association of America, Washington, D.C., 1968.
- [HLS] D. HAILE, R. LARSON, AND M. SWEEDLER, A new invariant of  $\mathbf{C}$  over  $\mathbf{R}$ : Almost invertible cohomology theory and the classification of idempotent cohomology classes and algebras by partially ordered sets with a Galois group action, *Amer. J. Math.* **105** (1983), 689-814.
- [K] D. KRASHEN, Things to tell your friends about generalized crossed product algebras: Indecomposable ideals and automorphisms, in “REU Student Reports,” Indiana University, Bloomington, Ind., 1993.
- [LN] R. LIDL AND H. NIEDERREITER, “Introduction to Finite Fields and Their Applications,” Cambridge University Press, Cambridge, 1986.
- [W] K. WALD, On cosickles, in “REU Student Reports,” Indiana University, Bloomington, Ind., 1991.