

ROOTED LOWER SUBTRACTIVE ORDERS, WEAK COCYCLES AND ALGEBRAS

DAVID M. ETLINGER

ABSTRACT. We describe a class of partial orders called rooted lower subtractive orders. We then discuss a class of F -central algebras from cohomology theory, characterize them in terms of associated partial orders, and show how to relate some properties of the two.

1. INTRODUCTION

We will begin by discussing a specific type of partial order on a set of cosets G/H called a rooted, lower subtractive order. We will describe some properties of this order, and give an algorithm to generate orders of this type, given G/H . We will then discuss a class of algebras, motivated by cohomology theory, arising from consideration of Galois field extensions and their Galois groups. We will then show how these algebras are characterized by rooted, lower subtractive orders. Finally, we give several examples of how certain properties of the orders imply properties of the algebras. This is useful, because the properties of the orders are easy to see graphically, whereas the corresponding properties of the algebras might be quite difficult to work with.

2. ROOTED LOWER SUBTRACTIVE GRAPHS

Definition 2.1. A relation \leq on a set S , denoted (S, \leq) is called a *partial order* if it satisfies the following two conditions:

- (1) $s \leq t$ and $t \leq s$ implies $s = t$
- (2) $r \leq s$ and $s \leq t$ implies $r \leq t$

Given a group G and a subgroup H , not necessarily normal in G , we can form the set of left cosets of H in G : $G/H \equiv \{gH | g \in G\}$. We can then define various partial orders on this set. These orders can be represented as graphs in the following way: if $\sigma H \leq \tau H$, we place σH below τH and draw a line connecting them:

$$\begin{array}{c} \tau H \\ | \\ \sigma H \end{array}$$

Definition 2.2. A partial order \leq on G/H is called *rooted lower subtractive* if

- (1) $H \leq gH \forall g \in G$
- (2) Given $\alpha H \leq \gamma H$, we have

$$\alpha H \leq \beta H \leq \gamma H \iff \alpha^{-1}\beta H \leq \alpha^{-1}\gamma H.$$

Definition 2.3. Given a partial order $(G/H, \leq)$, and $\sigma \in G$, define $V_\sigma \equiv \{\tau H \mid \sigma H \leq \tau H\}$. Define $\varphi_\sigma : V_\sigma \rightarrow G/H$ by $\varphi_\sigma(\tau H) = \sigma^{-1}\tau H$. We say φ_σ is *closed* if $(\varphi_\sigma[V_\sigma], \leq|_{\varphi_\sigma[V_\sigma]})$ is a subpartial ordering (that is, for $\alpha H, \beta H \in V_\sigma$, we have $\alpha H \leq \beta H \iff \varphi_\sigma(\alpha H) \leq \varphi_\sigma(\beta H)$). We say $\varphi_\sigma[V_\sigma] \subseteq G/H$ is *complete* if, for $\sigma^{-1}\alpha H, \sigma^{-1}\beta H \in \varphi_\sigma[V_\sigma]$, we have $\sigma^{-1}\alpha H \leq \gamma H \leq \sigma^{-1}\beta H \iff \gamma H \in \varphi_\sigma[V_\sigma]$.

Theorem 2.4. Let $(G/H, \leq)$ be a partial order, and assume it is rooted ($H \leq \sigma H \forall \sigma \in G$). Then the following are equivalent:

- (1) $(G/H, \leq)$ is lower subtractive
- (2) For all $\sigma \in G$, φ_σ is a one-to-one, closed map, and $\varphi_\sigma[V_\sigma]$ is complete.

Proof. First assume that $(G/H, \leq)$ is lower subtractive. Let $\alpha H, \beta H \in V_\sigma$. Suppose $\varphi_\sigma(\alpha H) = \varphi_\sigma(\beta H) = \gamma H$. Then $\gamma H = \sigma^{-1}\alpha H = \sigma^{-1}\beta H$. By lower subtractivity, $\sigma H \leq \alpha H \leq \beta H$ and $\sigma H \leq \beta H \leq \alpha H$, so $\alpha H = \beta H$, showing φ_σ is one-to-one.

Now let $\alpha H, \beta H \in V_\sigma$. By lower subtractivity, we have

$$\sigma H \leq \alpha H \leq \beta H \iff \sigma^{-1}\alpha H \leq \sigma^{-1}\beta H,$$

so φ_σ is closed.

Finally, let $\sigma^{-1}\alpha H, \sigma^{-1}\beta H \in \varphi_\sigma[V_\sigma]$, $\lambda H \in G/H$, and assume

$$\sigma^{-1}\alpha H \leq \lambda H \leq \sigma^{-1}\beta H.$$

By lower subtractivity,

$$(\sigma^{-1}\alpha)^{-1}\lambda H \leq (\sigma^{-1}\alpha)^{-1}(\sigma^{-1}\beta)H,$$

or $\alpha^{-1}\sigma\lambda H \leq \alpha^{-1}\beta H$. Since φ_σ is closed,

$$\sigma^{-1}\alpha H \leq \sigma^{-1}\beta H \iff \alpha H \leq \beta H.$$

Lower subtractivity then shows $\alpha H \leq \sigma\lambda H \leq \beta H$. Thus $\lambda H = \sigma^{-1}(\sigma\lambda)H$, and $\sigma H \leq \alpha H \leq \sigma\lambda H$ shows $\sigma H \leq \sigma\lambda H$. Hence $\lambda H \in \varphi_\sigma[V_\sigma]$, proving completeness.

Now assume φ_σ is one-to-one, closed, and $\varphi_\sigma[V_\sigma]$ is complete, for all $\sigma \in G$. Let $\sigma H \leq \gamma H$. First assume $\sigma H \leq \tau H \leq \gamma H$. Then $\sigma H, \tau H, \gamma H \in V_\sigma$, so

$$H, \sigma^{-1}\tau H, \sigma^{-1}\gamma H \in \varphi_\sigma[V_\sigma].$$

By closure, $\sigma^{-1}\tau H \leq \sigma^{-1}\gamma H$, showing one direction of lower subtractivity. Now assume $\sigma^{-1}\tau H \leq \sigma^{-1}\gamma H$. Since $(G/H, \leq)$ is rooted, we have

$$H \leq \sigma^{-1}\tau H \leq \sigma^{-1}\gamma H.$$

Since $\sigma H, \gamma H \in V_\sigma$, we have $H, \sigma^{-1}\gamma H \in \varphi_\sigma[V_\sigma]$, and so by completeness, $\sigma^{-1}\tau H \in \varphi_\sigma[V_\sigma]$, or $\tau H \in V_\sigma$, or $\sigma H \leq \tau H$. Closure tells us that $\tau H \leq \gamma H$, so $\sigma H \leq \tau H \leq \gamma H$, and we have proved lower subtractivity. \square

Let $(G/H, \leq)$ be a partial order. By *height-1* elements, we mean those elements σH such that $H \neq \sigma H$ and $H \leq \alpha H \leq \sigma H$ implies $\alpha H = H$ or $\alpha H = \sigma H$ (the notion of height will be made more precise later). Then we state the following without proof (the argument is an induction argument).

Theorem 2.5. *Let $(G/H, \leq)$ be a partial order, and assume it is rooted ($H \leq \sigma H \forall \sigma \in G$). Then the following are equivalent:*

- (1) $(G/H, \leq)$ is lower subtractive
- (2) For all $\sigma \in G$ such that σH is height-1, φ_σ is a one-to-one, closed map, and $\varphi_\sigma[V_\sigma]$ is complete.

We now prove a lemma that is used in the next section.

Lemma 2.6. *Let $(G/H, \leq)$ be rooted, lower subtractive. Let σH be height-1. Then, for any $h \in H$, $h\sigma H$ is also a height-1 element.*

Proof. We cannot have $h\sigma H = H$, as that would imply $\sigma H = h^{-1}H = H$. Assume $H = hH \leq \alpha H \leq h\sigma H$. By lower subtractivity, that means $h^{-1}\alpha H \leq \sigma H$, so $h^{-1}\alpha H = H$ or $h^{-1}\alpha H = \sigma H$. If $h^{-1}\alpha H = H$ then $\alpha H = hH = H$. If $h^{-1}\alpha H = \sigma H$ then $\alpha H = h\sigma H$. Hence $h\sigma H$ is height-1. \square

3. THE STANDARD ALGORITHM

We now describe an algorithm to construct rooted lower subtractive orders on G/H . The algorithm is called the *Standard Algorithm*, and orders produced by it are called *standard orders* or *standard graphs*. The algorithm was first developed for trivial H by Abdulla Aljouiee in his thesis; we present here a generalization to nontrivial H .

- (1) Let G be a group, H a subgroup, and consider G/H .

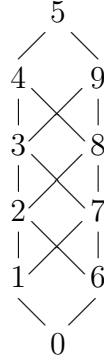
- (2) Let $\{s_1, \dots, s_k\}$ generate G/H in the sense that any $\alpha H \in G/H$ can be written as $s_{i_1} \dots s_{i_m} H$. Note that this does not have to be a minimal generating set.
- (3) For all $h \in H$ and each s_i , add the relation $H \leq hs_i H$. For notational simplicity, we refer to these elements as the height-1 elements $\{\sigma_1 H, \dots, \sigma_n H\}$.
- (4) For each height-1 element $\sigma_i H$, add the relations

$$\sigma_i H \leq \sigma_i \sigma_1 H, \dots, \sigma_i H \leq \sigma_i \sigma_n H$$

unless $\sigma_i \sigma_j H$ is another height-1 element or H itself. We refer to these new elements as the height-2 elements.

- (5) Continue in this manner, adding above each height- n element the elements formed by multiplying by each of the height-1 elements, unless the element to be added is already on the graph at height n or less.
- (6) Stop when every element of G/H has been placed in the order.

The following is an example of a rooted lower subtractive graph produced by the Standard Algorithm. The group is $G = \mathbb{Z}_{10}$ with trivial subgroup $H = \{0\}$, and generators 1 and 6:



We will not further discuss orders in terms of their graphs, but it is often helpful to visualize the orders in this way to aid intuition.

Definition 3.1. Let $(G/H, \leq)$ be a rooted, lower subtractive partial order. If $\sigma H \leq \tau H$, a *maximal chain* (or *maximal path*) is a chain

$$\sigma H = \sigma_0 H \leq \sigma_1 H \leq \dots \leq \sigma_n H = \tau H$$

such that, if $\sigma_i H \leq \alpha H \leq \sigma_{i+1} H$, we have $\sigma_i H = \alpha H$ or $\sigma_{i+1} H = \alpha H$. A partial order is called *catenary* if, for all $\sigma H \leq \tau H$, the length of any two maximal chains from σH to τH is the same. Given a catenary order, we define the *height* of an element to be the length of a maximal

path from H to σH , which we denote by $\ell(\sigma H)$.¹ We define the height of the order (or the height of the graph) to be the maximum of the heights of all the elements.

Theorem 3.2. *Any standard order is catenary.*

Proof. Let $\sigma H \leq \tau H$ in a standard order, and let

$$\sigma H \leq \sigma_1 H \leq \dots \leq \sigma_n H \leq \tau H$$

and

$$\sigma H \leq \sigma^1 H \leq \dots \leq \sigma^m H \leq \tau H$$

(where the superscripts denote an index, not exponentiation) be two maximal chains. Assume $n < m$. Then in the step of the algorithm that operates on $\sigma^m H$, τH will already be in the order at a lower level, and hence the relation $\sigma^m H \leq \tau H$ will not be added, contradicting our hypothesis. Hence we must have $n = m$. Since this was for arbitrary elements, the order is catenary. \square

Definition 3.3. In the standard order, define a *minimal representation* of σH to be $s_1 \dots s_n H$, where $\sigma H = s_1 \dots s_n H$, the s_i are all height-1 elements, and there is no smaller n such that σH can be written in this way. We call n the length of the minimal representation.

Lemma 3.4. *In the standard order, $\ell(\sigma H)$ is the length of a minimal representation of σH .*

Proof. The lemma is clear for $\ell(\sigma H) = 1$. So assume $\ell(\sigma H) \geq 2$. Suppose one minimal representation of σH is $\sigma H = s_1 \dots s_n H$. We must have $s_1 H \leq s_1 s_2 H$: the only way this cannot happen is if $s_1 s_2 H$ is a height-1 element, but that would allow for a shorter minimal representation of σH ($s_1 s_2 H \neq H$, as if it did, we would have $s_1 s_2 = h \in H$. Lemma 2.6 then shows that $s_1 s_2 s_3 H = h s_3 H$ is also a height-1 coset, allowing for a shorter minimal representation). Also, it is clear from the algorithm that $s_1 s_2 H$ sits directly above $s_1 H$. Similar arguments show that $s_1 \dots s_i H \leq s_1 \dots s_{i+1} H$, and there are no intervening elements. Hence we have constructed a maximal chain of length n from H to σH , so $\ell(\sigma H) = n$. \square

Lemma 3.5. *In the standard order,*

$$gH \leq gg'H \iff \ell(gH) + \ell(g'H) = \ell(gg'H).$$

¹The length of a chain is determined by counting the number of relations, not the number of elements. So $\sigma H \leq \tau H \leq \gamma H$ is a chain of length two.

Proof. Suppose first that $gH \leq gg'H$. Since $H \leq gH \leq gg'H$, there must be a maximal path from H to $gg'H$ that contains gH . Hence

$$\ell(gg'H) = \ell(gH) + (\text{length of a maximal path from } gH \text{ to } gg'H).$$

So we must show that

$$\ell(g'H) = (\text{length of a maximal path from } gH \text{ to } gg'H).$$

Let

$$gH = gg_0H \leq gg_1H \leq \dots \leq gg_nH = gg'H$$

be a maximal chain. By Theorem 2.4, φ_g is one-to-one and closed, and $\varphi_g[V_g]$ is complete. Closure tells us that

$$H = g_0H \leq g_1H \leq \dots \leq g_nH = g'H.$$

Suppose $g_iH \leq \alpha H \leq g_{i+1}H$. Then completeness tells us that $\alpha H \in \varphi_g[V_g]$, and closure then tells us that $gg_iH \leq g\alpha H \leq gg_{i+1}H$. By the maximality hypothesis, that implies that either $g\alpha H = gg_iH$ or $g\alpha H = gg_{i+1}H$. Therefore, either $\alpha H = g_iH$ or $\alpha H = g_{i+1}H$. Hence

$$H = g_0H \leq \dots \leq g_nH = g'H$$

is a maximal chain. Therefore,

$$\ell(g'H) = (\text{length of a maximal path from } gH \text{ to } gg'H),$$

and we have proved this direction.

Now assume $\ell(gH) + \ell(g'H) = \ell(gg'H)$. Let the minimal representations be $gH = s_1 \dots s_n H$ and $g'H = t_1 \dots t_m H$. We have $g = s_1 \dots s_n h$ and $g' = t_1 \dots t_m h'$, so one representation of $gg'H$ is $s_1 \dots s_n h t_1 \dots t_m h' H$. The h' can be discarded. Since $t_1 H$ is a height-1 element, Lemma 2.6 says $h t_1 H$ is too, and we can write $h t_1 H = \sigma_1 H$, so $h t_1 = \sigma_1 h''$. Continuing this process, we can write $gg'H = s_1 \dots s_n \sigma_1 \dots \sigma_m H$. Now, suppose that $gH \not\leq gg'H$; that is, suppose

$$s_1 \dots s_n \sigma_1 \dots \sigma_k H \not\leq s_1 \dots s_n \sigma_1 \dots \sigma_{k+1} H$$

for some k between 0 and $m-1$. Let this be the largest k such that this holds. By the definition of the standard algorithm, the only reason this can happen is if $s_1 \dots s_n \sigma_1 \dots \sigma_{k+1} H$ already exists at a lower level of the graph. Then

$$\ell(gg'H) \leq \ell(s_1 \dots s_n \sigma_1 \dots \sigma_{k+1} H) + (m - (k + 1)).$$

We have $1 \leq k + 1 \leq m$, so $0 \leq m - (k + 1) \leq m - 1$. Also,

$$\begin{aligned} \ell(s_1 \dots s_n \sigma_1 \dots \sigma_{k+1} H) &\leq \ell(gH) + k \\ &< \ell(gH) + (k + 1). \end{aligned}$$

Hence

$$\begin{aligned}\ell(gg'H) &< (\ell(gH) + (k+1)) + (m - (k+1)) \\ &= \ell(gH) + m.\end{aligned}$$

Lemma 3.4 shows that $\ell(g'H) = m$, so we have $\ell(gg'H) < \ell(gH) + \ell(g'H)$, contradicting our hypothesis. So we must have

$$s_1 \dots s_n \sigma_1 \dots \sigma_k H \leq s_1 \dots s_n \sigma_1 \dots \sigma_{k+1} H \quad \forall 0 \leq k \leq m-1,$$

which shows that $gH \leq gg'H$. \square

Corollary 3.6. *Let $(G/H, \leq)$ be rooted lower subtractive and catenary. Then $gH \leq gg'H$ implies $\ell(gH) + \ell(g'H) = \ell(gg'H)$.*

Proof. Inspection of the proof of this direction in Lemma 3.5 shows that only properties of catenary graphs, and not any further properties of the standard graph, were used. \square

Corollary 3.7. *Let $(G/H, \leq)$ be rooted lower subtractive and catenary. Then $\ell(\sigma H) = \ell(h\sigma H)$ for all $h \in H$.*

Proof. We have $hH = H \leq h\sigma H$. Hence by Corollary 3.6,

$$\begin{aligned}\ell(hH) + \ell(\sigma H) &= 0 + \ell(\sigma H) \\ &= \ell(\sigma H) \\ &= \ell(h\sigma H).\end{aligned} \quad \square$$

Theorem 3.8. *The standard algorithm always constructs a partial order that is rooted, lower subtractive.*

Proof. The algorithm will clearly generate a partial order that is rooted, as everything is above H . Also, every element of G/H will be added, as every element is generated by the height-1 elements. So we only need to show lower subtractivity. Let $gH \leq g\alpha\beta H$, so $\ell(gH) + \ell(\alpha\beta H) = \ell(g\alpha\beta H)$ by Lemma 3.5. First assume $gH \leq g\alpha H \leq g\alpha\beta H$. This tells us that $\ell(gH) + \ell(\alpha H) = \ell(g\alpha H)$ and $\ell(g\alpha H) + \ell(\beta H) = \ell(g\alpha\beta H)$, so

$$\begin{aligned}\ell(\alpha H) + \ell(\beta H) &= \ell(g\alpha H) - \ell(gH) + \ell(g\alpha\beta H) - \ell(g\alpha H) \\ &= \ell(g\alpha\beta H) - \ell(gH) \\ &= \ell(gH) + \ell(\alpha\beta H) - \ell(gH) \\ &= \ell(\alpha\beta H),\end{aligned}$$

so $\alpha H \leq \alpha\beta H$. Now assume that $\alpha H \leq \alpha\beta H$, or $\ell(\alpha H) + \ell(\beta H) = \ell(\alpha\beta H)$. Suppose that $gH \not\leq g\alpha H$. By Lemma 3.4, it is clear that this

can only happen if $\ell(gH) + \ell(\alpha H) > \ell(g\alpha H)$. Then we have

$$\begin{aligned}\ell(gH) + \ell(\alpha H) &= \ell(g\alpha\beta H) - \ell(\alpha\beta H) + \ell(\alpha\beta H) - \ell(\beta H) \\ &= \ell(g\alpha\beta H) - \ell(\beta H),\end{aligned}$$

which implies that $\ell(g\alpha\beta H) - \ell(\beta H) > \ell(g\alpha H)$, or $\ell(g\alpha H) + \ell(\beta H) < \ell(g\alpha\beta H)$. This can never happen, so we must have $gH \leq g\alpha H$, or $\ell(gH) + \ell(\alpha H) = \ell(g\alpha H)$. Similarly, assume $g\alpha H \not\leq g\alpha\beta H$, or $\ell(g\alpha H) + \ell(\beta H) > \ell(g\alpha\beta H)$. This gives

$$\ell(gH) + \ell(\alpha H) + \ell(\alpha\beta H) - \ell(\alpha H) > \ell(g\alpha\beta H),$$

or $\ell(gH) + \ell(\alpha\beta H) > \ell(g\alpha\beta H)$, contradicting our hypothesis. Hence $g\alpha H \leq g\alpha\beta H$, proving lower subtractivity. \square

4. COCYCLES AND ALGEBRAS

Definition 4.1. In the discussion that follows, let K be a field extension of F that is Galois of finite degree, with Galois group G . A function $f : G \times G \rightarrow K$ is called a *cocycle* if

- (1) $f(1, \sigma) = f(\sigma, 1) = 1 \ \forall \sigma \in G$
- (2) $f^\sigma(\tau, \gamma)f(\sigma, \tau\gamma) = f(\sigma, \tau)f(\sigma\tau, \gamma) \ \forall \sigma, \tau, \gamma \in G$.

The cocycle is called *weak* if the image contains the value 0, otherwise it is called a *strong* cocycle, or simply a cocycle.

We can build a ring from this as follows: for each $\sigma \in G$, let x_σ be an indeterminate. Define

$$A_f \equiv \bigoplus_{\sigma \in G} Kx_\sigma.$$

The addition operation is the natural one:

$$\sum_{\sigma \in G} k_\sigma x_\sigma + \sum_{\sigma \in G} l_\sigma x_\sigma = \sum_{\sigma \in G} (k_\sigma + l_\sigma) x_\sigma.$$

Multiplication is defined by the following two rules:

- (1) $x_\sigma k = k^\sigma x_\sigma \ \forall k \in K, \ \sigma \in G$
- (2) $x_\sigma x_\tau = f(\sigma, \tau) x_{\sigma\tau}$

This is in fact a ring, as the next theorem shows. It contains an isomorphic copy of K given by mapping $k \in K$ to kx_1 .

Definition 4.2. A ring A of finite dimension over a field F such that $F \subseteq Z(A)$ (where $Z(A) \equiv \{z \in A \mid za = az \ \forall a \in A\}$ is called the *center*) is called an *F-algebra*. An *F-algebra* A is called *F-central* if $F = Z(A)$. A ring is called *simple* if the only two-sided ideals are $\{0\}$ and the whole ring.

Theorem 4.3. *A_f is an F -central algebra, called the crossed product algebra. If the cocycle is strong, A_f is simple.*

Proof. It is an abelian group because the addition operation is inherited from the field K . The multiplicative identity is x_1 :

$$\begin{aligned} \left(\sum_{\sigma \in G} a_\sigma x_\sigma \right) x_1 &= \sum_{\sigma \in G} a_\sigma f(\sigma, 1) x_{\sigma 1} \\ &= \sum_{\sigma \in G} a_\sigma x_\sigma, \end{aligned}$$

and similarly from the left. Associativity is a consequence of the definition of a cocycle. Let $a = \sum_{\alpha \in G} a_\alpha x_\alpha$, $b = \sum_{\beta \in G} b_\beta x_\beta$, $c = \sum_{\gamma \in G} c_\gamma x_\gamma$. We have

$$\begin{aligned} (ab)c &= \left(\sum_{\alpha} \sum_{\beta} a_\alpha b_\beta^\alpha f(\alpha, \beta) x_{\alpha\beta} \right) \sum_{\gamma} c_\gamma x_\gamma \\ &= \sum_{\alpha} \sum_{\beta} \sum_{\gamma} a_\alpha b_\beta^\alpha c_\gamma^{\alpha\beta} f(\alpha, \beta) f(\alpha\beta, \gamma) x_{\alpha\beta\gamma} \end{aligned}$$

and

$$\begin{aligned} a(bc) &= \sum_{\alpha} a_\alpha x_\alpha \left(\sum_{\beta} \sum_{\gamma} b_\beta c_\gamma^\beta f(\beta, \gamma) x_{\beta\gamma} \right) \\ &= \sum_{\alpha} \sum_{\beta} \sum_{\gamma} a_\alpha b_\beta^\alpha (c_\gamma^\beta)^\alpha f^\alpha(\beta, \gamma) f(\alpha, \beta\gamma) x_{\alpha\beta\gamma}. \end{aligned}$$

By the definition of a cocycle, these expressions are equal,² hence A_f is a ring. To see that $[A_f : F]$ is finite, we first note that $[K : F] = |G|$. We claim that $\{x_\sigma | \sigma \in G\}$ is a K -basis for A_f , as any element of A_f can be written $k_{\sigma_1} x_{\sigma_1} + \dots + k_{\sigma_n} x_{\sigma_n}$, where $n = |G|$. Hence $[A_f : F] = n^2$.

We show it is F -central by showing $F \subseteq Z(A_f)$ and $Z(A_f) \subseteq F$ (where F again means the isomorphic copy Fx_1). Let $f \in F$, and let

²Careful readers will note that $(c_\gamma^\beta)^\alpha = \alpha(\beta(c_\gamma)) = \alpha\beta(c_\gamma) = c_\gamma^{\alpha\beta}$, and not $c_\gamma^{\beta\alpha}$ as the notation suggests.

$a = \sum_{\sigma} a_{\sigma} x_{\sigma}$ be an element of A_f . We have

$$\begin{aligned} af &= \left(\sum_{\sigma} a_{\sigma} x_{\sigma} \right) f x_1 \\ &= \sum_{\sigma} a_{\sigma} f^{\sigma} x_{\sigma} \\ &= \sum_{\sigma} a_{\sigma} f x_{\sigma}, \end{aligned}$$

since f is fixed by G . We have also

$$\begin{aligned} fa &= f x_1 \sum_{\sigma} a_{\sigma} x_{\sigma} \\ &= \sum_{\sigma} a_{\sigma} f x_{\sigma}, \end{aligned}$$

and so $f \in Z(A_f)$. Conversely, let $a = \sum_{\sigma} a_{\sigma} x_{\sigma}$ be in A_f . If $a_{\sigma} \neq 0$ for some $\sigma \neq 1$, we can choose $c \in K$ such that $c^{\sigma} \neq c$. Then the coefficient of x_{σ} in $a(cx_1)$ is $a_{\sigma} c^{\sigma}$, but in $(cx_1)a$ it is $a_{\sigma} c$, hence $a \notin Z(A_f)$. So for an element to be in the center, it must be of the form kx_1 . If $k \notin F$, we can find some $\sigma \in G$ such that $k^{\sigma} \neq k$. Then $x_{\sigma}(kx_1) = k^{\sigma} x_{\sigma}$, but $(kx_1)x_{\sigma} = kx_{\sigma}$. Hence any element in the center must be of the form fx_1 for some $f \in F$. We have thus shown that $F = Z(A_f)$, and so A_f is F -central.

Finally, we show A_f is simple when the cocycle is strong. Define $\ell(j)$ for all $j \in A_f$ as the number of nonzero terms in the expansion $j = \sum_{\sigma} j_{\sigma} x_{\sigma}$. Let I be a nonzero ideal, and let $a = \sum_{\sigma} a_{\sigma} x_{\sigma} \in I$ be nonzero. If $a_1 = 0$, we can choose some $\tau \in G$ such that $a_{\tau} \neq 0$. Then

$$\begin{aligned} ax_{\tau^{-1}} &= \sum_{\sigma} a_{\sigma} x_{\sigma} x_{\tau^{-1}} \\ &= \sum_{\sigma} a_{\sigma} f(\sigma, \tau^{-1}) x_{\sigma\tau^{-1}} \\ &= \sum_{\sigma} b_{\sigma} x_{\sigma}, \end{aligned}$$

where $b_{\sigma\tau^{-1}} \equiv a_{\sigma} f(\sigma, \tau^{-1})$. Since $b_{\sigma\tau^{-1}} \neq 0$ if and only if $a_{\sigma} \neq 0$, we have $\ell(a) = \ell(b)$ and $b_1 \neq 0$. If $b = b_1 x_1$, note that $b_1^{-1}(b_1 x_1) \in I$, and hence $I = A_f$. Otherwise, choose $k \in K$ such that $k^{\tau} \neq k$ for at least one $b_{\tau} \neq 0$. We have $b(kx_1) = \sum_{\sigma} b_{\sigma} k^{\sigma} x_{\sigma}$ and $(kx_1)b = \sum_{\sigma} kb_{\sigma} x_{\sigma}$. They are not equal, as the coefficient of x_{τ} differs. However, they both have the same coefficient for x_1 . Hence $\ell(b(kx_1) - (kx_1)b) < \ell(b)$, $b(kx_1) - (kx_1)b \in I$, and $b(kx_1) - (kx_1)b \neq 0$. Thus given any element of

a nonzero ideal with length at least two, we can always find a nonzero element of smaller length, from which it is clear every nonzero ideal contains a unit and hence equals A_f . \square

In the classical case of strong cocycles, we have the following theorem due to Wedderburn, which we state here without proof.

Theorem 4.4. *Let F be any field, and A any algebra that is F -central simple. Then there exists an F -central division algebra D such that $A \cong M_n(D)$ ($n \times n$ matrices with elements from D) for some n , with D unique up to isomorphism and n unique.*

Hence in the strong cocycle case, our construction always gives an algebra that is matrices over a division ring. We can go the other direction, from central simple algebras to cocycles, in the following way. Let F be any field, A any F -central simple algebra. Theorem 4.4 shows that $A \cong M_n(D)$, for some uniquely determined F -central division algebra D . Fixing F , we define $A \sim B$ if and only if we have $A \cong M_n(D)$ and $B \cong M_m(D)$, for some n and m . This is in fact an equivalence relation. Then we have the following theorem, also stated without proof.

Theorem 4.5. *Suppose A is an F -central simple algebra. Then there exists another F -central simple algebra B such that:*

- (1) $A \sim B$
- (2) $F \subseteq K \subseteq B$, where K is a Galois field extension
- (3) $[K : F]^2 = [B : F]$
- (4) $C_B(K) = K$, where $C_B(K) = \{b \in B \mid bk = kb \ \forall k \in K\}$.

In this case, we claim without proof that B can be shown to arise from the cocycle construction described earlier. To summarize, we have shown that given a Galois field extension K/F and a strong cocycle f , we can construct an F -central simple algebra A_f . This algebra will be matrices over an F -central division ring. Conversely, given any F -central simple algebra A , we can find a Galois extension K/F and a strong cocycle f such that $A \sim A_f$.

5. WEAK COCYCLES

We now expand the class of algebras we are studying by allowing weak cocycles. In this case, our algebra will (in general) no longer be simple, but this loss of knowledge is compensated for by the fact that we can now build a rooted lower subtractive ordering from the weak cocycle, which will contain information about the algebra.

Theorem 5.1. *Given a Galois extension K of F , $[K : F]$ finite, and a weak cocycle $f : G \times G \rightarrow K$, let $H = \{\sigma \in G \mid f(\sigma, \sigma^{-1}) \neq 0\}$. The following are true:*

- (1) $H = \{\sigma \in G \mid x_\sigma \text{ is invertible in } A_f\}$
- (2) H is a subgroup of G
- (3) Define a relation \leq on G/H by $\sigma H \leq \tau H \iff f(\sigma, \sigma^{-1}\tau) \neq 0$. This is a well-defined relation, a partial order, and rooted, lower subtractive.
- (4) $\sigma H \leq \tau H \iff x_\sigma \mid_\ell x_\tau$ (i.e., $x_\tau = x_\sigma a$ for some $a \in A_f$)
- (5) $f(h, \sigma) \neq 0$ and $f(\sigma, h) \neq 0 \forall h \in H, \sigma \in G$

Proof. Assume $f(\sigma, \sigma^{-1}) \neq 0$. Then there is a $k \in K$ such that $k^\sigma = (f(\sigma, \sigma^{-1}))^{-1}$, and so $x_\sigma(kx_{\sigma^{-1}}) = f(\sigma, \sigma^{-1})k^\sigma x_{\sigma\sigma^{-1}} = x_1$. Conversely, if x_σ is invertible, the only form its inverse can take is $x_\sigma^{-1} = kx_{\sigma^{-1}}$, so $x_\sigma kx_{\sigma^{-1}} = f(\sigma, \sigma^{-1})k^\sigma x_{\sigma\sigma^{-1}} = x_1$, which implies $f(\sigma, \sigma^{-1}) \neq 0$, proving part 1.

The set H contains 1, as $x_1 x_1 = x_1$. If $\alpha \in H$, our construction of x_α^{-1} above shows that $\alpha^{-1} \in H$. Finally, let $\alpha, \beta \in H$. Then there exists x_α^{-1} and x_β^{-1} . Then $(x_\alpha x_\beta)(x_\beta^{-1} x_\alpha^{-1}) = x_1$, so $x_\alpha x_\beta = f(\alpha, \beta)x_{\alpha\beta} \neq 0$. Then there is a $k \in K$ such that $k^{\beta\alpha} = f(\alpha, \beta)$. So

$$\begin{aligned} x_{\alpha\beta}(kx_\beta^{-1}x_\alpha^{-1}) &= (f(\alpha, \beta))^{-1} k^{\beta\alpha} x_\alpha x_\beta x_\beta^{-1} x_\alpha^{-1} \\ &= x_1, \end{aligned}$$

showing that $\alpha\beta \in H$, proving part 2.

We now prove part 3, first showing the relation is well-defined. Suppose $\sigma H \leq \tau H$, and let $\sigma H = \sigma' H$, $\tau H = \tau' H$. We can write $\sigma' = \sigma h_\sigma$, $\tau' = \tau h_\tau$. We must show that

$$f(\sigma', \sigma'^{-1}\tau') = f(\sigma h_\sigma, h_\sigma^{-1}\sigma^{-1}\tau h_\tau) \neq 0.$$

By the cocycle condition, we have

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

We show each term on the right-hand side is nonzero, noting that $f^\sigma(\alpha, \beta) \neq 0 \iff f(\alpha, \beta) \neq 0$. Applying the cocycle definition to the first term, we get

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

Since $h_\sigma \in H$, $f(h_\sigma, h_\sigma^{-1}) \neq 0$, and $f(1, \sigma^{-1}\tau h_\tau) = 1$ by definition. Hence $f(h_\sigma, h_\sigma^{-1}\sigma^{-1}\tau h_\tau) \neq 0$. Turning to the second term, we have

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

By hypothesis, $f(\sigma, \sigma^{-1}\tau) \neq 0$. Using the cocycle definition,

$$f(\tau, h_\tau) f(\tau h_\tau, h_\tau^{-1}) = f^\tau(h_\tau, h_\tau^{-1}) f(\tau, h_\tau h_\tau^{-1}).$$

Since $h_\tau \in H$, $f(h_\tau, h_\tau^{-1}) \neq 0$, and $f(\tau, 1) = 1$, hence $f(\tau, h_\tau) \neq 0$, in turn showing $f(\sigma, \sigma^{-1}\tau h_\tau) \neq 0$, so $f(\sigma h_\sigma, h_\sigma^{-1}\sigma^{-1}\tau h_\tau) \neq 0$, proving the relation is well-defined.

We now show the relation is a partial order. Suppose first that $\sigma H \leq \tau H$ and $\tau H \leq \gamma H$, or $f(\sigma, \sigma^{-1}\tau) \neq 0$ and $f(\tau, \tau^{-1}\gamma) \neq 0$. By the cocycle definition,

$$f(\sigma, (\sigma^{-1}\tau)(\tau^{-1}\gamma)) f^\sigma(\sigma^{-1}\tau, \tau^{-1}\gamma) = f(\sigma, \sigma^{-1}\tau) f(\tau, \tau^{-1}\gamma) \neq 0,$$

hence $f(\sigma, \sigma^{-1}\gamma) \neq 0$ or $\sigma H \leq \gamma H$, showing transitivity. Now assume $\sigma H \leq \tau H$ and $\tau H \leq \sigma H$. By definition,

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

The right-hand side is nonzero by hypothesis, hence $f(\tau^{-1}\sigma, \sigma^{-1}\tau) \neq 0$, so $\tau^{-1}\sigma \in H$, or $\tau H = \sigma H$, proving antisymmetry. Hence the relation is a partial order.

We now show the partial order is rooted, lower subtractive. We have

$$H \leq \sigma H \iff f(1, \sigma) \neq 0.$$

Since the right-hand side is always true, the order is rooted. Now, let $\alpha H \leq \gamma H$. First assume $\alpha H \leq \beta H \leq \gamma H$. We have

$$f(\alpha, \alpha^{-1}\gamma) f^\alpha(\alpha^{-1}\beta, \beta^{-1}\gamma) = f(\alpha, \alpha^{-1}\beta) f(\beta, \beta^{-1}\gamma)$$

by the cocycle condition. The right-hand side is nonzero by hypothesis, so $f(\alpha^{-1}\beta, (\beta^{-1}\alpha)(\alpha^{-1}\gamma)) \neq 0$, or $\alpha^{-1}\beta H \leq \alpha^{-1}\gamma H$. Conversely, assume $\alpha^{-1}\beta H \leq \alpha^{-1}\gamma H$. We again have

$$f(\alpha, \alpha^{-1}\gamma) f^\alpha(\alpha^{-1}\beta, \beta^{-1}\gamma) = f(\alpha, \alpha^{-1}\beta) f(\beta, \beta^{-1}\gamma),$$

but now the hypotheses tell us that the left-hand side is nonzero. Hence the right-hand side is nonzero, giving $\alpha H \leq \beta H \leq \gamma H$. That proves lower-subtractivity.

We now prove part 4. Assume first that $\sigma H \leq \tau H$, or $f(\sigma, \sigma^{-1}\tau) \neq 0$. We have $x_\tau = x_\sigma(kx_{\sigma^{-1}\tau})$, where $k^\sigma = (f(\sigma, \sigma^{-1}\tau))^{-1}$. Conversely, assume $x_\sigma |_\ell x_\tau$. The only possibility is that $x_\tau = x_\sigma(kx_{\sigma^{-1}\tau})$, which shows that $f(\sigma, \sigma^{-1}\tau) \neq 0$, or $\sigma H \leq \tau H$.

Finally, we prove part 5. Let $h \in H$. We have

$$hH = H \leq h\sigma H \quad \forall \sigma \in G,$$

which by definition means $f(h, \sigma) \neq 0$. Also, $\sigma H \leq \sigma hH$, so $f(\sigma, h) \neq 0$. \square

Part 5 of Theorem 5.1 tells us that $f|_{H \times H}$ is a strong cocycle. Hence we can split A_f into two pieces, by defining

$$B_f \equiv \bigoplus_{\sigma \in H} Kx_\sigma \quad J_f \equiv \bigoplus_{\sigma \notin H} Kx_\sigma.$$

Then $A_f = B_f \oplus J_f$, and B_f is a central simple K^H -algebra (where K^H is the fixed field of H in K). This is called the Wedderburn principal splitting.

Theorem 5.2. *J_f is a two-sided ideal in A_f , and is nilpotent: $(J_f)^{k+1} = \{0\}$, where k is the height of the graph of $(G/H, \leq)$.*

Proof. It is clearly an additive group. Let $j = \sum_{\sigma \notin H} j_\sigma x_\sigma \in J_f$, and let $a = \sum_{\tau \in G} a_\tau x_\tau \in A_f$. We have

$$ja = \sum_{\sigma \notin H} \sum_{\tau} j_\sigma a_\tau^\sigma f(\sigma, \tau) x_{\sigma\tau}.$$

If $\sigma\tau \in H$, $f(\sigma\tau, \tau^{-1}\sigma^{-1}) \neq 0$. By definition,

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

Since $\sigma \notin H$, $f(\sigma, \sigma^{-1}) = 0$, so $f(\sigma, \tau) = 0$. Hence $ja \in J_f$. Similarly,

$$aj = \sum_{\tau} \sum_{\sigma \notin H} a_\tau j_\sigma^\tau f(\tau, \sigma) x_{\tau\sigma}.$$

If $\tau\sigma \in H$, then $f(\tau\sigma, \sigma^{-1}\tau^{-1}) \neq 0$. By the cocycle condition,

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

If $\tau \notin H$, then $f(\tau, \tau^{-1}) = 0$, so $f(\tau, \sigma) = 0$. If $\tau \in H$, then $f(\sigma, \sigma^{-1}\tau^{-1}) = 0$ as $\sigma H \not\leq \tau^{-1}H = H$, so $f(\tau, \sigma) = 0$. Hence $aj \in J_f$, proving that it is a two-sided ideal.

To show that it is nilpotent, we must show that $j_1 \dots j_{k+1} = 0$ for any such product ($j_1, \dots, j_{k+1} \in J_f$). Let $j_i = \sum_{\sigma_i \notin H} j_{i, \sigma_i} x_{\sigma_i}$. Then the product

$$\begin{aligned} j_1 \dots j_{k+1} &= \left(\sum_{\sigma_1 \notin H} j_{1, \sigma_1} x_{\sigma_1} \right) \dots \left(\sum_{\sigma_{k+1} \notin H} j_{k+1, \sigma_{k+1}} x_{\sigma_{k+1}} \right) \\ &= \sum_{\sigma_1 \notin H} \dots \sum_{\sigma_{k+1} \notin H} j_{1, \sigma_1} \dots j_{k+1, \sigma_{k+1}}^{\sigma_1 \dots \sigma_k} f(\sigma_1, \sigma_2) \dots f(\sigma_1 \dots \sigma_k, \sigma_{k+1}) x_{\sigma_1 \dots \sigma_{k+1}}. \end{aligned}$$

Suppose $f(\sigma_1, \sigma_2) \neq 0, \dots, f(\sigma_1 \dots \sigma_k, \sigma_{k+1}) \neq 0$. Then we have

$$\sigma_1 H \leq \sigma_1 \sigma_2 H \leq \dots \leq \sigma_1 \dots \sigma_k H \leq \sigma_1 \dots \sigma_{k+1} H.$$

None of these are degenerate (i.e., $\sigma_1 \dots \sigma_i H \neq \sigma_1 \dots \sigma_{i+1} H$), as that would mean $(\sigma_1 \dots \sigma_{i+1})^{-1} (\sigma_1 \dots \sigma_i) = \sigma_{i+1} \in H$. The minimal height that the chain can have occurs if $\sigma_1 H$ is a height-1 element, in which case the chain has height $k+1$, contradicting the definition of k . Hence at least one term is zero, and since this is the product of arbitrary elements in J_f , we have shown that it is nilpotent. \square

We state without proof the following theorem, which classifies the algebras we have constructed.

Theorem 5.3. *Let A_f be an algebra constructed from a weak cocycle and Galois field extension, as above. Then $A_f \cong M_n(D)$, where $D = S \oplus J(D)$. Here $J(D)$ is the radical of S (the largest nilpotent ideal in S), $D/J(D) \cong S$, and S is a division algebra.*

6. THE STRUCTURE OF COCYCLE CLASSES

In this section we describe some of the structure of the set of cocycles that can arise from a given Galois extension K . This material is not immediately pertinent to the results given in section 8, but it is a fundamental motivating factor for the objects we are studying.

We begin by determining when two strong cocycles give rise to isomorphic F -algebras. Let K/F be a Galois extension, with $\{x_\sigma | \sigma \in G\}$ and $\{y_\sigma | \sigma \in G\}$ two choices of K -bases giving rise to the same F -algebra,

$$A_f = \bigoplus_{\sigma \in G} Kx_\sigma = \bigoplus_{\sigma \in G} Ky_\sigma.$$

Let the cocycle associated with $\{x_\sigma\}$ be f , and that associated with $\{y_\sigma\}$ be g . In other words, $x_\sigma x_\tau = f(\sigma, \tau)x_{\sigma\tau}$ and $y_\sigma y_\tau = g(\sigma, \tau)y_{\sigma\tau}$. Consider $y_\sigma x_\sigma^{-1} = y_\sigma c x_{\sigma^{-1}}$, where $c^\sigma = (f(\sigma, \sigma^{-1}))^{-1}$. This must be an element of K^* , as none of the terms are 0, and it commutes with every element of K :

$$\begin{aligned} (c^\sigma y_\sigma x_{\sigma^{-1}}) k &= \left(k^{\sigma^{-1}}\right)^\sigma (c^\sigma y_\sigma x_{\sigma^{-1}}) \\ &= k (c^\sigma y_\sigma x_{\sigma^{-1}}) \quad \forall k \in K. \end{aligned}$$

Hence we can write $y_\sigma x_\sigma^{-1} = k_\sigma$, or $y_\sigma = k_\sigma x_\sigma$, for some $k_\sigma \in K^*$. We can use this as follows:

$$\begin{aligned} y_\sigma y_\tau &= g(\sigma, \tau) y_{\sigma\tau} \\ &= g(\sigma, \tau) k_{\sigma\tau} x_{\sigma\tau} \\ &= (k_\sigma x_\sigma) (k_\tau x_\tau) \\ &= k_\sigma k_\tau^\sigma f(\sigma, \tau) x_{\sigma\tau}, \end{aligned}$$

giving

$$g(\sigma, \tau) = \frac{k_\sigma k_\tau^\sigma}{k_{\sigma\tau}} f(\sigma, \tau).$$

Conversely, given a basis $\{x_\sigma\}$, we can choose a set $\{k_\sigma\}$, which will give another cocycle in the way outlined above. This motivates the following definition and theorem, which we do not further justify.

Definition 6.1. Two cocycles (possibly weak), $f : G \times G \rightarrow K$ and $g : G \times G \rightarrow K$, are called *cohomologous* or *equivalent* if there is a function $\alpha : G \rightarrow K^*$ such that

$$f(\sigma, \tau) = \frac{\alpha(\sigma)\alpha^\sigma(\tau)}{\alpha(\sigma\tau)} g(\sigma, \tau)$$

for all $\sigma, \tau \in G$. We denote this by $f \sim g$.

Theorem 6.2. *Given two algebras A_f and A_g and the corresponding strong cocycles f and g , we have $f \sim g \iff A_f \cong A_g$.*

The relation $f \sim g$ is in fact an equivalence relation; we denote equivalence classes by $[f]$. The set $H^2(G, K^*) \equiv \{[f] | f \text{ a cocycle}\}$ is a group.³ The identity element is the class $[\mathbf{1}]$ such that $\mathbf{1}(\sigma, \tau) = 1$ for all $\sigma, \tau \in G$. Multiplication is the natural one: $[f][g] = [fg]$, where $fg(\sigma, \tau) = f(\sigma, \tau)g(\sigma, \tau)$. Finally, if f is a cocycle, then its inverse is denoted f^{-1} , where $f^{-1}(\sigma, \tau) = (f(\sigma, \tau))^{-1}$. Then $[f][f^{-1}] = [\mathbf{1}]$. We leave further verification of these facts to the reader.

We now turn to the case of weak cocycles. We maintain the same definition of cohomologous. We have the following modification of theorem 6.2, stated without proof:

Theorem 6.3. *Given two algebras A_f and A_g and the corresponding weak cocycles f and g , we have $f \sim g \iff A_f \cong A_g$ over K ; that is, there is an isomorphism $\varphi : A_f \rightarrow A_g$ such that $\varphi(k) = k$ for all $k \in K$.*

Define $M^2(G, K) \equiv \{[f] | f \text{ a weak cocycle}\}$. This is no longer a group, as any cocycle that gives $f(\sigma, \tau) = 0$ for some $\sigma, \tau \in G$ cannot have an inverse. In fact, it is a monoid. We have $H^2(G, K^*) \subseteq M^2(G, K)$ is precisely the subgroup of invertible elements.

We can better understand $M^2(G, K)$ with the following general construct. For any monoid M , if $e \in M$ is idempotent ($e^2 = e$), we can form the set

$$M_e = \{f \in M | fe = f \text{ and } \exists g \in M \text{ such that } fg = e\}.$$

³The motivation for the notation $H^2(G, K^*)$ comes from cohomology theory and is outside the scope of this paper.

This is then a group with identity element e (it is not technically a subgroup of M , as it has a different identity, unless $e = 1$).

Now, given a weak cocycle f , define $e_f : G \times G \rightarrow \{0, 1\}$ by

$$e_f(\sigma, \tau) = \begin{cases} 1 & \text{if } f(\sigma, \tau) \neq 0, \\ 0 & \text{if } f(\sigma, \tau) = 0. \end{cases}$$

It is fairly straightforward to show that e_f is also a cocycle, and clearly $e_f^2 = e_f$. Also, we can define $g_f : G \times G \rightarrow K$ by

$$g_f(\sigma, \tau) = \begin{cases} (f(\sigma, \tau))^{-1} & \text{if } f(\sigma, \tau) \neq 0, \\ 0 & \text{if } f(\sigma, \tau) = 0. \end{cases}$$

It is also straightforward to show that g_f is a cocycle, and that $f e_f = f$, $f g_f = e_f$, and $g_f e_f = g_f$. So in the notation given above,

$$[f] \in M^2(G, K)_{[e_f]}.$$

Conversely, given $e : G \times G \rightarrow \{0, 1\}$ a cocyle, we can simplify our notation and let

$$\begin{aligned} M_e^2(G, K) &\equiv M^2(G, K)_{[e]} \\ &= \{[f] \in M^2(G, K) \mid e_f = e\}. \end{aligned}$$

Since each f will correspond to exactly one e_f , we have

$$M^2(G, K) = \coprod M_e^2(G, K);$$

that is, $M^2(G, K)$ is the disjoint union of groups.

In terms of the partial orders we have been considering, recall that we defined $(G/H, \leq)$ by $\sigma H \leq \tau H \iff f(\sigma, \sigma\tau) \neq 0$. Hence the partial order does not depend on f , but only on e_f . Conversely, if we start with a rooted lower subtractive order $(G/T, \leq)$, we can easily write down an e giving rise to this order by defining

$$e(\sigma, \tau) = \begin{cases} 1 & \sigma T \leq \sigma\tau T, \\ 0 & \sigma T \not\leq \sigma\tau T. \end{cases}$$

We see that the rooted lower subtractive partial orders on G/H , as H varies over all subgroups of G , are in one-to-one correspondence with the idempotent elements of $M^2(G, K)$.

7. EQUIVALENCE OF LEFT AND RIGHT COSETS

In this section, we briefly justify our use of left cosets by showing that there is a one-to-one correspondence between orders on left and right cosets. Most of this could have been done immediately after defining

rooted lower subtractivity, but a few of the proofs are made easier by later results.

Theorem 7.1. *Suppose $(G/H, \leq)$ is rooted, lower subtractive. Then $(H \setminus G, \leq_R)$, where $H\sigma \leq_R H\tau \iff \tau\sigma^{-1}H \leq \tau H$, is well-defined and is rooted, lower subtractive (making the necessary modifications to the definition of lower subtractivity to handle right cosets: if $H\sigma \leq_R H\tau$, then $H\sigma \leq_R H\gamma \leq_R H\tau \iff H\gamma\sigma^{-1} \leq_R H\tau\sigma^{-1}$).*

Proof. Suppose $H\sigma \leq_R H\tau$, or $\tau\sigma^{-1}H \leq \tau H$. Choosing arbitrary coset representatives, let $H\sigma = H\sigma'$ and $H\tau = H\tau'$. $\sigma' \in H\sigma \rightarrow \sigma' = h_\sigma\sigma$ for some h_σ . Similarly, $\tau' = h_\tau\tau$. Substituting gives

$$\begin{aligned} \tau'\sigma'^{-1}H \leq \tau'H &\iff h_\tau\tau\sigma^{-1}h_\sigma^{-1}H \leq h_\tau\tau H \\ &\iff h_\tau\tau\sigma^{-1}H \leq h_\tau\tau H. \end{aligned}$$

By lower subtractivity on the left,

$$\tau\sigma^{-1}H \leq \tau H \iff h_\tau H \leq h_\tau\tau\sigma^{-1}H \leq h_\tau\tau H,$$

so $H\sigma \leq_R H\tau \iff H\sigma' \leq_R H\tau'$, hence \leq_R is well-defined.

The right-hand relation is rooted, as $H \leq_R H\alpha \iff \alpha H \leq \alpha H$. Since this holds always, we have $H \leq_R H\alpha$ for all $\alpha \in G$.

Finally, we demonstrate lower subtractivity. Let $H\alpha \leq_R H\gamma$. Suppose first that $H\alpha \leq_R H\beta \leq_R H\gamma$. $H\alpha \leq_R H\gamma \iff \gamma\alpha^{-1}H \leq \gamma H$, and

$$H\alpha \leq_R H\beta \leq_R H\gamma \iff \beta\alpha^{-1}H \leq \beta H \text{ and } \gamma\beta^{-1}H \leq \gamma H.$$

By lower subtractivity,

$$\gamma\beta^{-1}H \leq \gamma\alpha^{-1}H \leq \gamma H \iff \beta\alpha^{-1}H \leq \beta H;$$

the right-hand side is true by hypothesis. So $\gamma\beta^{-1}H \leq \gamma\alpha^{-1}H$, or equivalently, $H\beta\alpha^{-1} \leq_R H\gamma\alpha^{-1}$, showing one direction of lower subtractivity.

Suppose now that $H\beta\alpha^{-1} \leq_R H\gamma\alpha^{-1}$, or $\gamma\beta^{-1}H \leq \gamma\alpha^{-1}H$. We know $\gamma\alpha^{-1}H \leq \gamma H$. So $\gamma\beta^{-1}H \leq \gamma\alpha^{-1}H \leq \gamma H$ gives us $\gamma\beta^{-1}H \leq \gamma H$ and, by lower subtractivity, $\beta\alpha^{-1}H \leq \beta H$. Combining these gives $H\alpha \leq_R H\beta \leq_R H\gamma$, showing the other direction of lower subtractivity. \square

Corollary 7.2. *There is a one-to-one correspondence between rooted lower subtractive orderings on left cosets and rooted lower subtractive orderings on right cosets.*

Proof. We have shown that every rooted lower subtractive ordering on left cosets generates a corresponding ordering on right cosets. We must show that every rooted lower subtractive ordering on right cosets

is generated by an ordering on left cosets. Given $(H \setminus G, \leq_R)$, define an ordering $(G/H, \leq)$ by $\sigma H \leq \tau H \iff H\sigma^{-1}\tau \leq_R H\tau$. This is a well-defined rooted lower subtractive ordering; the proofs are quite similar to those given above, so we omit them. Then this order on left cosets is seen to generate the corresponding order on right cosets as described in Theorem 7.1. Hence we have shown a one-to-one correspondence between rooted lower subtractive orders on left and right cosets. \square

Lemma 7.3. *Let H be the trivial subgroup. Given (G, \leq) as induced by Theorem 5.1, and (G, \leq_R) the associated right-hand order described in Theorem 7.1, define a new relation \preceq on G by $\sigma \preceq \tau$ if and only if there exists a chain $\sigma = \sigma_0 \leq \sigma_1 \leq_R \sigma_2 \leq \dots \leq_R \sigma_n = \tau$ where the \leq 's and \leq_R 's alternate (the chain may start and end with either \leq or \leq_R , so long as the alternating condition is maintained). Then the following conditions are equivalent:*

- (1) $\sigma \preceq \tau$
- (2) $A_f x_\tau A_f \subseteq A_f x_\sigma A_f$

Proof. Assume first that such a chain exists. We will use the chain given in the statement of the lemma; the other cases are similar. The first relation, $\sigma_0 \leq \sigma_1$, tells us by Theorem 5.1 that $x_{\sigma_1} = x_{\sigma_0}(k_{a_1}x_{a_1})$. The second relation tells us that $x_{\sigma_2} = (k_{a_2}x_{a_2})x_{\sigma_1} = k_{a_2}x_{a_2}x_{\sigma_0}k_{a_1}x_{a_1}$.⁴ Continuing in this way, it is clear that we can write

$$x_\tau = kx_{a_n} \dots x_{a_2}x_\sigma x_{a_1} \dots x_{a_{n-1}}.$$

Hence for any $\alpha x_\tau \beta \in A_f x_\tau A_f$, we can rewrite it as

$$\alpha kx_{a_n} \dots x_{a_2}x_\sigma x_{a_1} \dots x_{a_{n-1}}\beta \in A_f x_\sigma A_f,$$

and so $A_f x_\tau A_f \subseteq A_f x_\sigma A_f$.

Conversely, assume that $A_f x_\tau A_f \subseteq A_f x_\sigma A_f$. Then we can write $x_\tau = x_\alpha x_\sigma x_\beta$ (ignoring constants). Since $x_\sigma x_\beta |_R x_\tau$, $\sigma\beta \leq_R \tau$. Also, $\sigma \leq \sigma\beta \iff f(\sigma, \beta) \neq 0$, which we know is true as $x_\tau = x_\alpha f(\sigma, \beta)x_{\sigma\beta} \neq 0$. Hence we have $\sigma \leq \sigma\beta \leq_R \tau$, or $\sigma \preceq \tau$. \square

Theorem 7.4. *The relation \preceq defined above is a partial order.*

Proof. Suppose $\sigma \preceq \tau$ and $\tau \preceq \gamma$. By the lemma, $A_f x_\tau A_f \subseteq A_f x_\sigma A_f$ and $A_f x_\gamma A_f \subseteq A_f x_\tau A_f$, so $A_f x_\gamma A_f \subseteq A_f x_\sigma A_f$, or $\sigma \preceq \gamma$, showing transitivity.

Now suppose $\sigma \preceq \tau$ and $\tau \preceq \sigma$. By the lemma, $A_f x_\sigma A_f = A_f x_\tau A_f$. The only way this can happen is if $x_\sigma = x_\gamma x_\tau x_\delta$ and $x_\tau = x_\alpha x_\sigma x_\beta$

⁴The proof that $\sigma H \leq_R \tau H \iff x_\sigma |_R x_\tau$ is analogous to the proof of the statement for the left order.

(ignoring constants). Substituting again gives

$$x_\sigma = x_\gamma x_\alpha x_\sigma x_\beta x_\delta = x_{\gamma\alpha} x_\sigma x_{\beta\delta}.$$

Defining $\gamma\alpha \equiv a$, we must have

$$\begin{aligned} x_\sigma &= x_a x_\sigma x_{\sigma^{-1}a^{-1}\sigma} \\ &= f(a, \sigma) f(a\sigma, \sigma^{-1}a^{-1}\sigma) x_\sigma, \end{aligned}$$

which tells us that $a \leq a\sigma \leq \sigma$. By lower subtractivity, this implies $\sigma \leq a^{-1}\sigma$. We can continue this process, and since this is a finite group, we must get $\sigma \leq a^{-1}\sigma \leq a^{-2}\sigma \leq \dots \leq \sigma$. The only way this can happen is if $\sigma = a^{-1}\sigma$, implying $a = \gamma\alpha = 1$, or $\gamma = \alpha^{-1}$. We also have $f(\gamma, \alpha) \neq 0$, or $\gamma \leq \gamma\alpha = 1$, or $\gamma = \alpha = 1$. Similarly, $f(\beta, \delta) \neq 0$, or $\beta \leq \beta\delta = 1$, or $\beta = \delta = 1$. Hence $x_\sigma = x_1 x_\tau x_1$, or $\sigma = \tau$, proving antisymmetry. \square

8. CORRESPONDENCES BETWEEN PROPERTIES OF ORDERINGS AND ALGEBRAS

In this section, we describe several important properties of these algebras that can be shown to correspond with properties of the associated rooted, lower subtractive order. Often, it is easier to show that the order has some necessary property than to work directly with the algebra.

Definition 8.1. Let A be an F -algebra. We say A is *Frobenius* if there is a map $T : A \times A \rightarrow F$ with the following properties:

- (1) (Associativity) $T(ab, c) = T(a, bc)$
- (2) (Bilinearity) $T(a_1 + a_2, b) = T(a_1, b) + T(a_2, b)$ and $T(a, b_1 + b_2) = T(a, b_1) + T(a, b_2)$
- (3) (Nondegeneracy) $T(a, b) = 0 \forall a \in A$ implies $b = 0$, and $T(a, b) = 0 \forall b \in A$ implies $a = 0$

A canonical example of such a function is given by $T : M_n(F) \times M_n(F) \rightarrow F$ where $T(A, B) = \text{Tr}(AB)$; in other words, T is like a generalization of the trace function.

Definition 8.2. Let $(G/H, \leq)$ be a rooted, lower subtractive order. An element σH is called *maximal* if $\sigma H \leq \tau H$ implies $\sigma H = \tau H$. The order is called *Frobenius* if there exists a unique maximal element.

We state the following theorem without proof; it was first shown by Abdulla Aljouiee in his thesis.

Theorem 8.3. *Let A_f and the associated order $(G/H, \leq)$ be as in Theorem 5.1. Then A_f is Frobenius if and only if $(G/H, \leq)$ is Frobenius.*

We now turn to a different property.

Definition 8.4. A partial order $(G/H, \leq)$ is called a *lattice* if every pair of elements has a least upper bound; more precisely, if

- (1) For every pair of elements $\sigma H, \tau H$ there exists a λH such that $\sigma H \leq \lambda H$ and $\tau H \leq \lambda H$
- (2) Further, if $\sigma H \leq \delta H$ and $\tau H \leq \delta H$, then $\lambda H \leq \delta H$.

Lemma 8.5. *Let $(G/H, \leq)$ be the induced order described in Theorem 5.1. Then the following are equivalent:*

- (1) λH is the least upper bound for σH and τH
- (2) $x_\lambda A_f = x_\sigma A_f \cap x_\tau A_f$

Proof. Suppose first that λH is the least upper bound for σH and τH . By Theorem 5.1, we can write $x_\lambda = x_\sigma k x_{\sigma'}$ (where $k^\sigma = (f(\sigma, \sigma'))^{-1}$). Hence for any $x_\lambda a \in x_\lambda A_f$, we have $x_\lambda a = x_\sigma (k x_{\sigma'} a) \in x_\sigma A_f$, and so $x_\lambda A_f \subseteq x_\sigma A_f$. Similarly, $x_\lambda A_f \subseteq x_\tau A_f$, and so

$$x_\lambda A_f \subseteq x_\sigma A_f \cap x_\tau A_f.$$

We now show containment in the other direction. Let $x_\sigma a = x_\tau b \in x_\sigma A_f \cap x_\tau A_f$, or equivalently,

$$\begin{aligned} x_\sigma \sum_{\alpha} a_{\alpha} x_{\alpha} &= \sum_{\alpha} a_{\alpha}^{\sigma} f(\sigma, \alpha) x_{\sigma \alpha} \\ &= \sum_{\beta} b_{\beta}^{\tau} f(\tau, \beta) x_{\tau \beta} \\ &= x_{\tau} \sum_{\beta} b_{\beta} x_{\beta}. \end{aligned}$$

We want to write this as $\sum_{\gamma} c_{\gamma}^{\lambda} f(\lambda, \gamma) x_{\lambda \gamma} \in x_{\lambda} A_f$. If $\sigma \alpha = \tau \beta$ for fixed α, β , we can choose γ such that $\lambda \gamma = \sigma \alpha = \tau \beta$. The coefficients of $x_{\sigma \alpha}$ and $x_{\tau \beta}$ are equal by hypothesis, and we want to show we can make the coefficient of $x_{\lambda \gamma}$ match this value. When both coefficients are 0, we can simply take $c_{\gamma}^{\lambda} = 0$. When they are nonzero, we have $f(\sigma, \alpha) \neq 0$ and $f(\tau, \beta) \neq 0$, or $\sigma H \leq \sigma \alpha H$ and $\tau H \leq \tau \beta H$. By the least upper bound hypothesis, we then have $\lambda H \leq \lambda \gamma H$, or $f(\lambda, \gamma) \neq 0$. Hence the coefficient of $x_{\lambda \gamma}$ can be made to match, and we can write $x_{\sigma} a = x_{\tau} b = x_{\lambda} c$. This shows that $x_{\sigma} A_f \cap x_{\tau} A_f \subseteq x_{\lambda} A_f$, and thus $x_{\sigma} A_f \cap x_{\tau} A_f = x_{\lambda} A_f$.

Now assume that $x_{\lambda} A_f = x_{\sigma} A_f \cap x_{\tau} A_f$. We can write $x_{\lambda} = x_{\sigma} a$, so by Theorem 5.1, $\sigma H \leq \lambda H$. Similarly, $\tau H \leq \lambda H$. Now, suppose $\sigma H \leq \delta H$ and $\tau H \leq \delta H$. Again by Theorem 5.1, we can write $x_{\delta} = x_{\sigma} a' = x_{\tau} b'$. Then by hypothesis, we must be able to write $x_{\delta} = x_{\lambda} c'$,

which shows that $\lambda H \leq \delta H$. Hence λH is the least upper bound for σH and τH . \square

Corollary 8.6. *The order $(G/H, \leq)$ is a lattice if and only if, for every pair $\sigma, \tau \in G$, we have $x_\sigma A_f \cap x_\tau A_f = x_\lambda A_f$ for some $\lambda \in G$.*

Proof. Suppose the order is a lattice. Then for every pair $\sigma, \tau \in G$ there is a least upper bound λH for σH and τH . The lemma shows that $x_\sigma A_f \cap x_\tau A_f = x_\lambda A_f$. Conversely, if $x_\sigma A_f \cap x_\tau A_f = x_\lambda A_f$ for every $\sigma, \tau \in G$ and some $\lambda \in G$, then the lemma tells us that every pair $\sigma H, \tau H$ has a least upper bound, and hence the order is a lattice. \square

The right ideals of a ring, equipped with the intersection operation, will always form a lattice. In the case of a partial order $(G/H, \leq)$ that is a lattice, we see that the subset of ideals generated by a single element form a sublattice. These ideals are in one-to-one correspondence with the partial order relations as shown above. Hence in this case, all information contained in the ordering is contained also in the ideal structure.

We describe now a final algebraic property that can be studied through the partial ordering.

Definition 8.7. Given an algebra A and a commutative monoid M , we say the algebra is M -graded if it can be written as the direct sum $A = \bigoplus_{m \in M} V_m$ such that if $a \in V_n$ and $b \in V_m$ we have $ab \in V_{m+n}$. The elements of V_n are called the *homogeneous elements of degree n* .

Theorem 8.8. *Let $(G/H, \leq)$ be the order induced as in Theorem 5.1. If this partial order is catenary, then the algebra A_f is \mathbb{Z}_k -graded, where k is the height of the graph. The V_n 's are both left and right B_f -modules.*

Proof. Let $V_n \equiv \bigoplus_{\ell(\sigma H)=n} Kx_\sigma$ (i.e., the sum is taken over all $\sigma \in G$ such that $\ell(\sigma H) = n$). Then we can write $A_f = \bigoplus_{n=0}^k V_n$, as each x_σ will be in exactly one of the V_n . Given $x_\sigma \in V_n$ and $x_\tau \in V_m$, we have $x_\sigma x_\tau = f(\sigma, \tau)x_{\sigma\tau}$. If $\sigma H \leq \sigma\tau H$, then $f(\sigma, \tau) \neq 0$. By Lemma 3.5, $\ell(\sigma H) + \ell(\tau H) = \ell(\sigma\tau H)$, so $x_\sigma x_\tau \in V_{n+m}$. If $\sigma H \not\leq \sigma\tau H$, then $f(\sigma, \tau) = 0$ and so $x_\sigma x_\tau = 0$ (which is in every V_i).⁵ Distributivity ensures that the grade still holds for homogeneous elements $\sum_{\ell(\sigma H)=n} k_\sigma x_\sigma \in V_n$. Hence the algebra is graded.

Recall $B_f = \bigoplus_{\sigma \in H} Kx_\sigma$. We show V_n is a left and right B_f -module. Since the requirements of module multiplication are automatically satisfied by the ring multiplication, we need only show that $B_f V_n \subseteq V_n$ and

⁵Note that if $n + m > k$, we must have $f(\sigma, \tau) = 0$: otherwise, $\ell(\sigma\tau H) > k$, contradiction. Hence in this case, $x_\sigma x_\tau \in V_0$ and $x_\sigma x_\tau \in V_{n+m}$. It is a matter of preference whether to think of $n + m$ as 0 or $n + m \pmod k$.

$V_n B_f \subseteq V_n$. Let $x_h \in B_f$, $x_\alpha \in V_n$. It is clear that $\ell(\alpha h H) = \ell(\alpha H)$, and Corollary 3.7 shows that $\ell(h \alpha H) = \ell(\alpha H)$. Hence $x_{h\alpha}, x_{\alpha h} \in V_n$. It is clear that this still holds for sums. We have thus shown containment. \square

Corollary 8.9. *If $(G/H, \leq)$ arises from the Standard Algorithm, then then the associated algebra A_f is \mathbb{Z}_k -graded.*

Proof. Theorem 3.2 showed that standard orders are catenary, hence Theorem 8.8 applies. \square

9. CONCLUSION

We have established several important properties of rooted lower subtractive orders on G/H , including giving an algorithm to generate them. We then characterized, in some sense, all F -central simple algebras. We broadened the class of algebras we considered by dropping the requirement of simplicity, or equivalently, allowing weak cocycles. We then showed how these algebras give rise to rooted lower subtractive orders. Finally, we established several connections between the orders and algebraic properties.

There are several areas of possible future exploration. One is to give necessary and/or sufficient conditions for rooted lower subtractive graphs to have certain properties. For example, it is unknown under what conditions the Standard Algorithm will give graphs that are Frobenius or lattices. An open conjecture is that all catenary orders are suborders of standard orders. Also, we suspect that there is more information to be gained from the lattice condition. In terms of gradings, a little reflection will show that simply knowing an algebra is graded is not enough to show the graph is catenary. However, it would be satisfying to show that some class of grades gives information about the order. Finally, any additional connections between order properties and graph properties are desirable. One likely class of correspondences are those that yield additional information about an algebra's ideal structure, but others are also likely.

10. ACKNOWLEDGEMENTS

I would like to thank Dr. Darrell Haile and Dr. Carolyn Yackel for advising this REU project. Both were extremely well-prepared, clear in presentation and fun to work with. I would also like to thank Kevin Foster for assistance with the initial stages of this project, and Prof. Naomi Jochnowitz for giving me an excellent background in abstract algebra.

REFERENCES

1. **Darrell Haile**, *On Crossed Product Algebras Arising from Weak Cocycles*, J. Algebra **74** (1982), 270–279;
2. **Darrell Haile**, *The Brauer Monoid of a Field*, J. Algebra **91** (1983), 521–539;
3. **Darrell Haile, R. Larson and M. Sweedler**, *A New Invariant for \mathbb{C} over \mathbb{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;
4. **Darrell Haile**, *Weakly Azumaya Algebras*, J. Algebra **250** (2002), 134–177.