Group Extensions and $H^2(G; A)$

Kyle Mickelson

April 29th, 2024

Contents

1 Introduction

Let G be a group and let A be a G-module. After reviewing some basic definitions and facts regarding group extensions, we tackle one of the main results of this paper, which is to make a concrete connection between the 2-cocycles of $Z^2(G, A)$ and the so-called factor sets associated to group extensions of G by A. Such factor sets arise in the definition of multiplication in such group extensions, in particular when different coset representatives are chosen.

The premier result will of course be a characterization of the second cohomology group of G with coefficients in A, the group $H^2(G, A)$. We shall use the results of this paper to showcase a bijection between equivalence classes of group extensions of G by A and the cohomology classes of $H^2(G, A)$.

$$\{\text{Extensions of } G \text{ by } A\}/\sim\ \cong H^2(G, A)$$

This bijection takes an extension E of G by A into the cohomology class of a normalized factor set f for E associated to any normalized section $\mu : G \to E$, and takes a cohomology class c in $H^2(G, A)$ to the extensions E_f constructed in Proposition 7 for any normalized 2-cocycle f in c. Moreover, under this bijection, split extensions of G by A correspond to the trivial cohomology class. We follow quite closely the exposition of [DF04], and use [Wei94] as a reference.

In general, it is a difficult task to compute cohomology groups, in particular second cohomology groups. Using the above characterization, we shall see how to translate this problem into an entirely group-theoretic one. For instance, we shall employ this point of view to show that $H^2(Z_2, \mathbb{Z}/4\mathbb{Z}) \cong Z_2$ and $H^2(Z_2, V_4) \cong V_4$ with little to no loss of sweat or blood or tears. Here V_4 denotes the Klein 4-group, $V_4 \cong Z_2 \times Z_2$.

Following this, we attempt to showcase, almost entirely without proof, how this characterization lends itself quite naturally to the study of so-called crossed product algebras and Brauer groups. Chief among such theory, we state and explore the consequences of the following isomorphism of groups:

$$\mathrm{Br}(K/k) \cong H^2(G, K^\times)$$

where $\mathrm{Br}(K/k)$ denotes the relative Brauer group, the group of similarity classes of central simple k-algebras which are split by K. Proofs and further information on the topic of crossed product algebras, Brauer groups, and more general applications to modern number theory may be found in [GS17].

We shall then use some of this theory to compute, again relatively painlessly, that $H^2(\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q), \mathbb{F}_{q^d}^\times) = 0$, and consequently that $\mathrm{Br}(\mathbb{F}_q) = 0$. As a consequence of this fact, we will have shown that every finite division algebra is a field.

2 Group Extensions, Factor Sets, and $H^2(G, A)$

2.1 Group Extensions

We begin by recalling that the notion of exactness of a sequence can be applied just as well to sequences of groups. In particular, given some short exact sequence of groups

$$1 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 1$$

we have $\mathrm{im}(\iota) = \ker(\pi)$, as well as that ι is injective and π is surjective. As such, we may apply the first isomorphism theorem to $\iota : A \to B$ to obtain $A \cong \mathrm{im}(\iota)$, as well as to $\pi : B \to C$ and obtain $B/\ker(\pi) \cong \mathrm{im}(\pi)$. Since $\ker(\pi) = \mathrm{im}(\iota) \cong A$, and $\mathrm{im}(\pi) \cong C$, we have in sum that

$$B/A \cong C.$$

We would like to analyze scenarios like the above further, and so we give a name to the special occasion in which we have a short exact sequence of groups.

Definition. Let G and A be groups. Then an *extension of G by A* is a short exact sequence $1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$.

From now on we shall identify A directly as a subgroup of the group E. We now present an example of a group extension. In particular, we present an example showcasing that, in general, there exist many different extensions of G by A.

Example 1. Consider $V_4 \cong Z_2 \times Z_2$, the Klein 4-group, and Z_2, the cyclic group of order 2. Both the dihedral group of order 8, $D_8 = \langle r, s \mid r^4 = s^2 = 1,\ rs = sr^{-1} \rangle$, and the quaternion group, $Q_8 = \langle x, y \mid x^4 = 1, x^2 = y^2, y^{-1}xy = x^{-1} \rangle$, are extensions of Z_2 by V_4. To see this, consider the following sequences:

$$1 \to Z_2 \xrightarrow{\iota} D_8 \xrightarrow{\varphi} V_4 \to 1$$

and

$$1 \to Z_2 \xrightarrow{\iota} Q_8 \xrightarrow{\varphi} V_4 \to 1$$

where ι in both cases denotes inclusion into the center, and π is projection onto $G/Z(G)$.

Definition. If $1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$ is an extension of G by A, then a *section of* π is a set-map $\mu : G \to E$ such that $\pi \circ \mu = \mathrm{id}_G$.

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r, "\iota"] & E \arrow[r, "\pi"] & G \arrow[r] \arrow[l, bend left, "\mu"] & 1 \end{tikzcd}$$

If, in addition, it is the case that $\mu(1) = 0$, that is, the identity element of G lifts to the identity of E under μ, then we call μ a *normalized section of* π.

In the special case when the section μ is a group homomorphism, we call μ a *splitting homomorphism.*

We now emphasize a particular type of extension of G by A which will feature heavily in our eventual connection of group extensions to cohomology groups of G with coefficients in A.

Definition. An extension $1 \to A \xrightarrow{\psi} E \xrightarrow{\varphi} G \to 1$ of G by A is called a *split extension* if there exists a subgroup complement to $\psi(A)$ in E. In this case, up to isomorphism, $E = A \rtimes G$.

We make a quick characterization of split extensions now, in terms of splitting homomorphisms defined above.

Proposition 1. *Let $1 \to A \xrightarrow{\psi} E \xrightarrow{\varphi} G \to 1$ be an extension of G by A. Then E is a split extension if and only if there exists a splitting homomorphism $\mu : G \to E$ such that $\varphi \circ \mu = id_G$.*

Proof. The proof is immediate from the definitions provided above. Given $\mu : G \to E$ a splitting homomorphism, define $G' = \mu(G) \subseteq E$, and if G' is given then define $\mu = \varphi^{-1}$. ■

We now give some examples of split and non-split extensions.

Example 2. The group D_8 is a split extension of Z_2 by Z_4; we have a short exact sequence

$$1 \to Z_4 \xrightarrow{\iota} D_8 \xrightarrow{\pi} Z_2 \to 1$$

where we take $Z_4 \cong \langle r \rangle$ and $Z_2 \cong \langle s \rangle$. Here ι is the inclusion map and π takes $r^a s^b$ to $\overline{s}^b$, projection onto the quotient $D_8/\langle r \rangle \cong Z_2$. Here we can see that $D_8 \cong \langle r \rangle \rtimes \langle s \rangle$, or also that $D_8 \cong Z_4 \rtimes Z_2$.

Example 3. The group Q_8 is not a split extension of Z_2 by Z_4. We do have a short exact sequence

$$1 \to Z_4 \xrightarrow{\iota} Q_8 \xrightarrow{\pi} Z_2 \to 1$$

where $Z_4 \cong \langle i \rangle$ has quotient isomorphic to Z_2. Note that no cyclic subgroup of Q_8 of order 4 has a complement in Q_8, hence the extension cannot be split.

One of the reasons we are interested in studying such extensions of groups is the following: given any such extension, we have an associated action of the rightmost group on the leftmost; in the notation above, we can obtain an action of G on A, which suffices to make A a G-module.

Two lemmas will be all that is necessary to acquire the action of G on A; two lemmas to make A into a G-module, which is our current goal.

Lemma 1. *Let $1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$ be an extension of groups, where A is an abelian group, and suppose that $\mu : G \to E$ is a section of π. Then for every $g \in G$, the map*

$$\psi_g : A \to A$$

$$a \mapsto \mu(g) a \mu(g)$$

which is conjugation by $\mu(g)$, is independent of the choice of lifting $\mu(g)$ of the element $g \in G$.

Proof. Suppose that $\mu' : G \to E$ is another section of π, so that $\pi \circ \mu' = \mathrm{id}_G$. Then, since π is a group homomorphism, we have

$$\pi(\mu'(g)\mu(g)^{-1}) = \pi(\mu'(g))\pi(\mu(g))^{-1} = gg^{-1} = 1_G$$

In particular, $\mu'(g)\mu(g)^{-1} \in \ker(\pi) = A$, so we may let $b = \mu'(g)\mu(g)^{-1}$ be some element of A. Thus $\mu'(g) = \mu(g)b$. Now we find

$$\mu'(g)a\mu'(g)^{-1} = \mu(g)(bab^{-1})\mu(g)^{-1} = \mu(g)a\mu(g)^{-1}$$

where $bab^{-1} = abb^{-1} = a$ since both $a, b \in A$, and by assumption A is abelian. ∎

Lemma 2. *Let $1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$ be an extension of groups, and suppose that $\mu : G \to E$ is a section of π. Then the map*

$$\Psi : G \to Aut(A)$$

$$g \longmapsto \psi_g$$

where for each $g \in G$, the map $\psi_g : A \to A$ is conjugation by $\mu(g)$ as in Lemma 1, is a group homomorphism.

Proof. It is clear that since $A \trianglelefteq E$, as $A = \ker(\pi)$, we have $\mu(g)a\mu(g)^{-1} \in A$ for all $g \in G$ and $a \in A$; that is, we have $\psi_g(a) \in A$ always. Since conjugation is an automorphism, we have $\psi_g \in \mathrm{Aut}(A)$. Now let $g, h \in G$ and $a \in A$ be arbitrary. Then

$$\begin{aligned}(\psi_g \circ \psi_h)(a) &= \psi_g(\mu(h)a\mu(h)^{-1}) \\ &= \mu(g)\mu(h)a\mu(h)^{-1}\mu(g)^{-1} \\ &= \mu(gh)a\mu(gh)^{-1} \\ &= \psi_{gh}(a)\end{aligned}$$

Note that the third line above follows from the second since $\mu(g)+\mu(h)$ and $\mu(gh)$ both are lifts of $gh \in G$, and Lemma 1 gives independence to the choice of lifting, granting the equality. ∎

Proposition 2. *If we have $0 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$ an extension of G by A, and $\mu : G \to E$ is a section of π, then A is a G-module with the action $g \cdot a$ of G on A given by $g \cdot a = \mu(g)a\mu(g)^{-1}$, equivalently $g \cdot a = \psi_g(a)$, for all $g \in G$ and $a \in A$.*

Proof. For A to be a G-module we need only refer to Lemma 2 which gives a group homomorphism of G into the group of automorphisms of A. ∎

Our next result will be to show that equivalent extensions of G by A define the same G-module structure on A. To do this, we briefly recall the notion of an equivalence between two extensions.

Definition. If $0 \to A \xrightarrow{\iota_1} E_1 \xrightarrow{\pi_1} G \to 1$ and $0 \to A \xrightarrow{\iota_2} E_2 \xrightarrow{\pi_2} G \to 1$ are two extensions of G by A, then we say the extensions are *equivalent* if there exists a group homomorphism $\beta : E_1 \to E_2$ such that the following diagram commutes

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\iota_1"] \arrow[d, equal] & E_1 \arrow[r, "\pi_1"] \arrow[d, "\beta"] & G \arrow[r] \arrow[d, equal] & 1 \\
0 \arrow[r] & A \arrow[r, "\iota_2"] & E_2 \arrow[r, "\pi_2"] & G \arrow[r] & 1
\end{tikzcd}$$

Note the requirement that $\beta : E_1 \to E_2$ only be a group homomorphism, not necessarily an isomorphism. This is because any such β making the diagram commute is necessarily an isomorphism by a quick application of the Short Five Lemma.

In a case such as the above, we simply say that β is an equivalence between the extensions. A quick (if tedious) check shows that the notion of equivalence of extensions of G by A is, in fact, an equivalence relation, being reflexive, symmetric, and transitive in the obvious ways.

We now make the assertion that equivalent extensions of G by A induce the same G-module structure on A.

Proposition 3. *Suppose $0 \to A \xrightarrow{\iota_1} E_1 \xrightarrow{\pi_1} G \to 1$ and $0 \to A \xrightarrow{\iota_2} E_2 \xrightarrow{\pi_2} G \to 1$ are two equivalent extensions of G by A. Then the two G-module structures on A induced via Proposition 2 coincide.*

Proof. Let $\beta : E_1 \to E_2$ be the group homomorphism making two extensions equivalent. Let e_g be any element of E_1 which maps to g under π_1, i.e., $\pi_1(e_g) = g$. We know that E_1 induces an action of G on A, and this action is conjugation which sends a to $e_g a e_g^{-1}$. Now let $e'_g = \beta(e_g)$. Since the diagram making E_1 and E_2 equivalent commutes, $\pi_2(e'_g) = g$ must hold. In other words, the induced action of G on A by E_2 takes a to $e'_g a e'_g$. Since β is a homomorphism, in fact an isomorphism, we have

$$\beta(e_g a e_g^{-1}) = \beta(e_g)\beta(a)\beta(e_g)^{-1} = e'_g a e'^{-1}_g$$

And now equality of the two actions is immediate from the commutativity of the diagram. ■

Now that we have either learned or reviewed some basis properties about group extensioons, we proceed to the next section, where we develop the notion of a factor set associated to an extension, and then we shall go on to connect this current discussion to $H^2(G, A)$, which is our goal.

2.2 Factor Sets

Now we aim to connect group extensions of G by A to 2-cocycles in $Z^2(G, A)$. To do this, we introduce so-called factor sets associated to extensions E of G by A with respect to a choice of section $\mu : G \to E$.

We present a more general definition, which shall serve only to facilitate our upcoming development of factor sets.

Definition. Let A be a subgroup of the group E. Then a *right transversal of* A, or a *complete system of coset representatives of* A, is a subset $X \subseteq E$ consisting of exactly one element from each right coset of A in E. That is, each $g \in X$ corresponds to a distinct coset Ag in E. For convenience, we assume that $0 \in X$ and that $x = 0$ corresponds to A, the coset consisting of just A in E.

It is clear how given an extension E of G by A we can construct right transversals for A, as we have that A is a subgroup of E by our running convention. We now show that right transversals for A are in bijection with sections associated to the extension E.

Proposition 4. *Let* $0 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$ *be an extension of* G *by* A. *Then right transversals of* A *in* E *correspond bijectively with sections of* π.

Proof. Let $X \subseteq E$ be a right transversal of A. Given any $g \in G$ the surjectivity of π implies that there exists some $e_g \in E$ such that $\pi(e_g) = g$. Construct a map $\mu : G \to E$ by $\mu(g) = e_g$ for each $g \in G$. We have $\pi \circ \mu = \mathrm{id}_G$ in the obvious way.

Conversely, given a section of π, say $\mu : G \to E$, we claim that $\mathrm{im}(\mu)$ is a right transversal of A. For any coset Ae in E/A, we know that $\pi(e) \in G$. We write $\pi(e) = g$. Now we have $\pi(e\mu(g)^{-1}) = 1_G$, hence $e\mu(g)^{-1} \in \ker(\pi) = A$, which means that $Ae = A\mu(g)$. In particular, every coset of A in E has a representative in $\mathrm{im}(\mu)$. Now we must prove that $\mathrm{im}(\mu)$ does not contain two elements which lie in the same coset. Assume this was the case, with $A\mu(g) = A\mu(h)$. Then there is $a \in A$ with $\mu(g)a = \mu(h)$, which since

$$\pi(\mu(g)a) = \pi(\mu(g))\pi(a) = g1_G = g$$

and $\pi(\mu(h)) = h$, necessitates $g = h$, meaning that indeed no two elements of $\mathrm{im}(\mu)$ lie in the same coset of A in E. ■

Now suppose we have an extension of G by A given as

$$0 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$$

If $\mu : G \to E$ is a section of π, not necessarily a splitting homomorphism, then the image of π gives us a transversal of A by Proposition 4, which we call X. Now, since

$$E = \coprod_{e \in X} Ae,$$

i.e., we may view E as the disjoint union of cosets of A in E, we can actually express each $e \in E$ uniquely as $e = a\mu(g)$ for some $a \in A$ and $g \in G$, owing to the fact that each $\mu(g)$ lies in a distinct coset $A\mu(g)$ of A in E.

Now let $g, h \in G$ be arbitrary. Since $\mu(gh)$ and $\mu(g)\mu(h)$ represent the same coset of A in E (apply π to $\mu(g)\mu(h)\mu(gh)^{-1}$ to show that it lies in the kernel of π, and hence in A), we know that

$$\mu(g)\mu(h) = a\mu(gh)$$

for some $a \in A$. We decorate this a somewhat, relating it back to g and h, writing $a = f(g, h)$. We attach a name to this situation, and then we shall relate it to cohomology.

Definition. If $0 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$ is an extension of G by A with $\mu : G \to E$ a section of π, then a *factor set* is a function $f : G \times G \to A$ such that for all $g, h \in G$

$$\mu(g)\mu(h) = f(g,h)\mu(gh)$$

If, in addition, a factor set f associated to the section μ of the extension E satisfies $f(g,1) = 0 = f(1,g)$, then we call f a *normalized factor set.*

It is at once clear that a factor set depends (quite heavily) upon the choice of section of π.

Note that in the case where a section of π above is a splitting homomorphism, then necessarily $f(g,h) = 0$ for all $g, h \in G$ since $\mu(g)\mu(h) = \mu(gh)$ must hold. Hence the factor set in the case where we have a split extension is identically 0.

Now we make the connection between group extensions of G by A and $Z^2(G,A)$. We shall show that the factor sets associated to an extension E of G by A with a choice of section μ are 2-cocycles.

Lemma 3. *Let $1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$ be an extension of G by A and let $\mu : G \to E$ be any section of π. Any factor set f for the extension E associated to μ is a 2-cocycle.*

Proof. We denote by $g \cdot a$ conjugation by $\mu(g)$ in E. We begin by recalling that the operation in E may be written as

$$\begin{aligned}(a\mu(g))(b\mu(h)) &= (a\mu(g))(b\mu(g)^{-1}\mu(g)\mu(h)) \\ &= (a + \mu(g)b\mu(g)^{-1})\mu(g)\mu(h) \\ &= (a + g \cdot b)(\mu(g)\mu(h)) \\ &= (a + g \cdot b + f(g,h))\mu(gh)\end{aligned}$$

for every $a, b \in A$ and $g, h \in G$, where we have used the fact that $\mu(g)\mu(h) = f(g,h)\mu(gh)$ from the factor set f. Recall also that we have an associative law in E for this binary operation above; we find via computation that

$$[\mu(g)\mu(h)]\mu(k) = (f(g,h) + f(gh,k))\mu(ghk)$$

$$\mu(g)[\mu(h)\mu(k)] = (g \cdot f(h,k) + f(g,hk))\mu(ghk)$$

However by the associative law, these two values must be the same for all $g, h, k \in G$. In other words, we have that

$$f(g,h) + f(gh,k) = g \cdot f(h,k) + f(g,hk)$$

for all $g, h, k \in G$, which makes f, by definition, a 2-cocycle, $f \in Z^2(G,A)$. ∎

In the next section, we cover the main theorem of this paper.

2.3 A Characterization of $H^2(G, A)$

In this section we work towards proving a correspondence between the equivalence classes of group extensions of G by A and the second cohomology group of G with coefficients in A.

We preface the discussion by recalling several definitions which will feature heavily in our forthcoming developments. Specifically, we recall the notion of a 2-cocycle and a 2-coboundary associated to the second cohomology group of some group G with coefficients in some G-module A.

Definition. Let G be a group and let A be a G-module, and denote the action of G on A by $g \cdot a$ for all $g \in G$ and $a \in A$. We call a function $f : G \times G \to A$ a 2-*cocycle* if it satisfies the identity

$$f(g,h) + f(gh,k) = g \cdot f(h,k) + f(g,hk)$$

for all $g, h, k \in G$. Equivalently, if we have a collection $\{a_{g,h}\}_{g,h \in G}$ of elements of A which satisfies $a_{g,h} + a_{gh,k} = g \cdot a_{h,k} + a_{g,hk}$ for all $g, h, k \in G$, then we call the function f which sends (g, h) to $a_{g,h}$ a 2-cocycle.

Definition. Let G be a group and let A be a G-module. We say that a 2-cochain f is a 2-*coboundary* if there exists a function $f_1 : G \to A$ such that

$$f(g,h) = g \cdot f_1(h) - f_1(gh) + f_1(g)$$

for all $g, h \in G$. In other words, we have that f is the image of the 1-cochain f_1 under the differential d_1.

Armed with the above definitions, We proceed by first exhibiting precisely how, given an extension E of G by A, we have a well-defined cohomology class in $H^2(G, A)$.

Proposition 5. *Let G be a group and A a G-module. For each group extension $1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$ of G by A there is a corresponding well-defined cohomology class in $H^2(G, A)$.*

Proof. From Lemma 3 we know that the factor set associated to any section of the extension E is an element in $Z^2(G, A)$. Hence, to prove the desired result, it suffices to show that factor sets associated to the extension E corresponding to different choices of sections give 2-cocycles in $Z^2(G, A)$ that differ by a 2-coboundary in $B^2(G, A)$.

To this end, suppose μ' is another section of π and let f' be its associated factor set. We know immediately that $\mu(g)$ and $\mu'(g)$ lie in the same coset Ag of E by definition of a section. In this way, $\mu'(g) = a\mu(g)$ for some specific $a \in A$; in particular, we may construct a function $f_1 : G \to A$ such that $\mu'(g) = f_1(g)\mu(g)$ for all $g \in G$. Now observe that, by definition of a factor set, we have

$$\begin{aligned} \mu'(g)\mu'(h) &= f'(g,h)\mu'(gh) \\ &= f'(g,h)(f_1(gh)\mu(gh)) \\ &= (f'(g,h) + f_1(gh))\mu(gh) \end{aligned}$$

where we have used that $\mu'(gh) = f_1(gh)\mu(gh)$ from above. However note that we may compute the above value in a different way, for instance by first using the map f_1 above:

$$\begin{aligned}\mu'(g)\mu'(h) &= (f_1(g)\mu(g))(f_1(h)\mu(h)) \\ &= (f_1(g) + g \cdot f_1 + f(g,h))\mu(gh)\end{aligned}$$

where the second line follows from the binary operation in E seen in the proof of Lemma 3. The two values derived above must equal one another, and hence we require

$$(f'(g,h) + f_1(gh))\mu(gh) = (f_1(g) + g \cdot f_1(h) + f(g,h))\mu(gh)$$

Appyling the inverse of $\mu(gh)$ in E to the right of both sides above yields

$$f'(g,h) + f_1(gh) = f_1(g) + g \cdot f_1(h) + f(g,h)$$

We may rearrange the above equation to obtain

$$f(g,h)' = f(g,h) + g \cdot f_1(g) - f_1(gh) + f_1(g)$$

Now define a function $f'' : G \times G \to A$ by $f''(g,h) = g \cdot f_1(h) - f_1(gh) + f_1(g)$ for all $g,h \in G$. By definition, f'' is a 2-coboundary, and in particular we have from our above work that

$$f'(g,h) = f(g,h) + f''(g,h)$$

for all $g,h \in G$, so that indeed f and f' differ by a 2-coboundary, which is precisely what we desired to prove. ■

Using the above proposition, we can actually quite easily determine which extensions of G by A correspond to the trivial cohomology class in $H^2(G,A)$.

Corollary 1. *Let G be a group and let A be a G-module. Then split extensions $1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$ of G by A correspond to the trivial class in $H^2(G,A)$.*

Proof. If $1 \to A \to E \to G \to 1$ is a split extension of G by A, then there exists a splitting homomorphism $\mu : G \to E$, which is in particular a section of π since it is also a set-map, Any factor set f associated to μ must then satisfy

$$\mu(g)\mu(h) = f(g,h)\mu(gh)$$

for all $g,h \in G$, however since $\mu(g)\mu(h) = \mu(gh)$ since μ is a group homomorphism, it follows that $f(g,h) = 0$ in A for all $g,h \in G$. Hence from Proposition 5 we know f corresponds to the trivial class in $H^2(G,A)$, as $f = 0$ is a 2-coboundary. ■

Since we are interested in exhibiting a bijection between the equivalence classes of extensions of G by A with $H^2(G,A)$, we must now check that equivalent extensions do indeed define the same cohomology class obtained via Proposition 5. To this end, we have the following proposition.

Proposition 6. *Let G be a group and let A be a G-module. Then equivalent extensions of G by A correspond to the same cohomology class in $H^2(G,A)$.*

Proof. Let $1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$ and $1 \to A \xrightarrow{\iota'} E' \xrightarrow{\pi'} G \to 1$ be two extensions of G by A, and assume β is an equivalence between them. That is, we have a commuting diagram

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\iota"] \arrow[d, "\mathrm{id}"] & E \arrow[r, "\pi"] \arrow[d, "\beta"] & G \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\
0 \arrow[r] & A \arrow[r, "\iota'"] & E' \arrow[r, "\pi'"] & G \arrow[r] & 1
\end{tikzcd}$$

Take a section $\mu : G \to E$ of π. Let $\mu' = \beta \circ \mu$. We claim that μ' is a section of π'; to see this, note that commutativity gives $\pi = \pi' \circ \beta$, and so

$$(\pi' \circ \mu')(g) = \pi'(\beta(\mu(g))) = (\pi' \circ \beta)(\mu(g)) = \pi(\mu(g)) = (\pi \circ \mu)(g) = g$$

where the final equality follows by the assumption that μ is a section of π. Now we may apply the homomorphism $\beta : E \to E'$ to the defining equation for a factor set f associated to μ to obtain

$$\beta(\mu(g))\beta(\mu(h)) = \beta(f(g,h))\beta(\mu(gh))$$

Once more by the commutativity of the diagram, $\beta|_A = \mathrm{id}_A$, i.e., β restricts to the identity on A, hence $\beta(f(g,h)) = f(g,h)$. Now we use our new section μ' of π' to write

$$\mu'(g)\mu'(h) = f(g,h)\mu'(gh)$$

and hence we have shown that the factor set for E' associated to μ' is precisely the same as the factor set for E associated to μ, proving the proposition. ■

We have now successfully showcased one side of our desired bijection. We now proceed with exhibiting how a cohomology class in $H^2(G,A)$ defines an equivlance class of extensions of G by A. Before doing so, however, we make the following definition, which shall serve to simplify several upcoming proofs.

Definition. Let G be a group and let A be a G-module. Then a 2-cocycle f such that $f(g,1) = 0 = f(1,g)$ for all $g \in G$ is called a *normalized 2-cocycle.*

The reason we have defined such 2-cocycles is that, as we will now show, any class of 2-cocycles in $H^2(G,A)$ has a representative given by a normalized 2-cocycle.

Lemma 4. *Let G be a group and let A be a G-module. Then any 2-cocycle f lies in the same cohomology class as a normalized 2-cocycle.*

Proof. Let $f : G \times G \to A$ be our 2-cocycle. Consider the function $f_1 : G \to A$ defined by $f_1(g) = f(1,1)$ for all $g \in G$, i.e., f_1 is the constant function on G with value $f(1,1) \in A$. Then $d_1 f_1$ is a 2-coboundary since it lies in the image of the differential d_1. As such, and hence $f - d_1 f_1$ is a 2-cocycle in the same cohomology class as f.

We claim that $f - d_1 f_1$ is a normalized 2-cocycle. The fact that it is a 2-cocycle is clear. Observe that for all $g \in G$ we have

$$\begin{aligned}(f - d_1 f_1)(g,1) &= f(g,1) - d_1 f_1(g,1) \\ &= f(g,1) - (g \cdot f_1(1) - f_1(g) + f_1(g)) \\ &= f(g,1) - g \cdot f_1(1) \\ &= f(g,1) - g \cdot f(1,1) \\ &= 0\end{aligned}$$

where the final line follows from the 2-cocycle condition for f, as we have

$$f(g,1) + f(g,1) = g \cdot f(1,1) + f(g,1)$$

and so subtracting yields $f(g,1) = g \cdot f(1,1)$. An entirely analagous computation shows that $(f - d_1 f_1)(1,g) = 0$ as well, which gives that $f - d_1 f_1$ is indeed normalized. Since f and $f - d_1 f_1$ lie in the same cohomology class in $H^2(G,A)$, we have proved the lemma. ∎

Equipped with the above lemma, we proceed with our development. We shall construct a class of extensions of G by A directly using only a normalized 2-cocycle, which without loss of generality, represents a specific cohomology class in $H^2(G,A)$.

Proposition 7. *Let G be a group and A a G-module. Then each cohomology class in $H^2(G,A)$ corresponds to an extension E_f of G by A with associated factor set f in the given class of $H^2(G,A)$.*

Proof. From Lemma 4 we may assume that any cohomology class in $H^2(G,A)$ is represented by a normalized 2-cocycle f. Let $E_f = A \times G$. Define a binary operation on E_f by

$$(a,g)(b,h) = (a + g \cdot b + f(g,h), gh)$$

for all $a, b \in A$ and $g, h \in G$, where $g \cdot b$ denotes the action of G on A. We prove that E_f equipped with this binary operation is a group. For associativity, note

$$\begin{aligned}(a,g)[(b,h)(c,k)] &= (a,g)(b + h \cdot c + f(h,k), hk) \\ &= (a + g \cdot (b + h \cdot c + f(h,k)) + f(g,hk), ghk) \\ &= (a + g \cdot b + g \cdot (h \cdot c) + g \cdot f(h,k) + f(g,hk), ghk) \\ &= (a + g \cdot b + gh \cdot c + f(g,h) + f(gh,k), ghk) \\ &= [(a,g)(b,h)](c,k)\end{aligned}$$

holds, where we have used the fact that f has the 2-cocycle condition to make the substitution $g \cdot f(h,k) + f(g,hk) = f(g,h) + f(gh,k)$. For an identity element, we take $(0,1)$. Note

$$(a,g)(0,1) = (a + g \cdot 0 + f(g,1), g1) = (a + 0 + 0, g) = (a,g)$$

since $f(g,1) = 0$ as f is normalized. A similar computation yields that $(0,1)(a,g) = (a,g)$, and so indeed $(0,1)$ is an identity. Lastly, we check inverses. Given $(a,g) \in E_f$, we claim that

$$(a,g)^{-1} = (-g^{-1} \cdot a - f(g^{-1}, g), g^{-1})$$

is an inverse. We may observe that

$$\begin{aligned}(a,g)(-g^{-1} \cdot a - f(g^{-1}, g), g^{-1}) &= (a + g \cdot (-g^{-1} \cdot a - f(g^{-1}, g)) + f(g, g^{-1}), gg^{-1}) \\ &= (a - (gg^{-1}) \cdot a - g \cdot f(g^{-1}, g) + f(g, g^{-1}), 1) \\ &= (a - a - g \cdot f(g^{-1}, g) + f(g, g^{-1}), 1) \\ &= (0,1)\end{aligned}$$

where we have used that $f(g, g^{-1}) + f(1, g) = g \cdot f(g^{-1}, g) + f(1, g)$ the 2-cocycle condition for f, obtaining $f(g, g^{-1}) = g \cdot f(g^{-1}, g)$. An entirely analagous computation yields that

$$(-g^{-1} \cdot a - f(g^{-1}, g), g^{-1}) = (0,1)$$

and hence we conclude that E_f is closed under inverses; hence a group with this operation.

Now we proceed. We claim that $A^* = \{(a,1) \mid a \in A\}$ is a subgroup of E_f. Observe that $(0,1) \in A^*$ and hence $A^* \neq \varnothing$. Also we have

$$\begin{aligned}(a,1)(b,1)^{-1} &= (a,1)(-1^{-1} \cdot b - f(1^{-1}, 1), 1^{-1}) \\ &= (a,1)(-b - f(1,1), 1) \\ &= (a + 1 \cdot (-b - f(1,1)) + f(1,1), 1) \\ &= (a - b, 1)\end{aligned}$$

and $(a - b, 1) \in A^*$ since $a - b \in A$. It is also clear now how $\iota^* : A \to A^*$ sending a to $(a,1)$ is an isomorphism of groups, i.e., $A \cong A^*$. Furthermore, we have that $\pi^* : E_f \to G$ defined by $\pi^*(a,g) = g$ is a surjective group homomorphism with kernel A^*. In particular, we have that $E_f / A^* \cong G$. Therefore the sequence

$$1 \to A \xrightarrow{\iota^*} E_f \xrightarrow{\pi^*} G \to 1$$

is an extension of G by A. However we need to ensure that this extension gives rise to an action of G on A which is compatible with the original action, which gave rise to our initial normalized factor set f. It is easy to see that

$$(0,g)(a,1)(0,g)^{-1} = (g \cdot a, 1)$$

for all $g \in G$ and $a \in A$, and so this is compatible. Consider the map $\mu : G \to E_f$ defined by $\mu(g) = (0,g)$ for all $g \in G$. It is at once clear that μ is a normalized section of π^*. We also have

$$\begin{aligned}\mu(g)\mu(h) &= (0,g)(0,h)\\ &= (0+g\cdot 0+f(g,h),gh)\\ &= (f(g,h),gh)\\ &= (f(g,h)+1\cdot 0+f(1,gh),gh)\\ &= (f(g,h),1)(0,gh)\\ &= (f(g,h),1)\mu(gh)\end{aligned}$$

which follows since $f(1,gh)=0$ since f is normalized. In particular, the factor set f is that corresponding to μ. Hence the proposition is proved. ■

Again, since we are deriving a bijection between $H^2(G,A)$ and the equivalence classes of extensions of G by A, we need to ensure that each extension E_f as constructed in Proposition 7 are all equivalent. That is, we must show that E_f depends only on the cohomology class of f in $H^2(G,A)$.

Proposition 8. *Let G be a group and A a G-module. Then the equivalence class of the extension E_f as constructed in Proposition 7 depends only on the cohomology class of f in $H^2(G,A)$.*

Proof. Suppose f' is another normalized 2-cocycle in the same cohomology class as f in $H^2(G,A)$, and let $E_{f'}$ be the corresponding extension obtained via Proposition 7. Let d_1f_1 be the 2-coboundary by which f and f' differ, where $f_1 : G\to A$ is some 1-cochain. We then have

$$f(g,h)-f'(g,h)=g\cdot f_1(h)-f_1(gh)+f_1(g)$$

for all $g,h\in G$. Taking $g=h=1$ gives that

$$1\cdot f_1(1)-f_1(1)+f_1(1)=f_1(1)$$

and since $f(1,1)-f'(1,1)=0$ since both f and f' are normalized, we get $f_1(1)=0$.

Now construct a map $\beta : E_f\to E_{f'}$ defined by $\beta((a,g))=(a+f_1(g),g)$ for all $(a,g)\in E_f$. We may observe that

$$\begin{aligned}\beta((a,g)(b,h)) &= \beta((a+g\cdot b+f(g,h),gh))\\ &= (a+g\cdot b+f(g,h)+f_1(gh),gh)\\ &= (a+f_1(g)+g\cdot(b+f_1(h))+f'(g,h),gh)\\ &= (a+f_1(g),g)(b+f_1(h),h)\\ &= \beta((a,g))\beta((b,h))\end{aligned}$$

so that β is a group homomorphism. We can easily see that $\beta|_A=\mathrm{id}_A$, as $\beta((a,1))=(a+f_1(1),1)=(a,1)$, and furthermore that β takes $(0,g)$ to g, and restricts to the identity on G when restricted to the second component of (a,g). In particular, by definition, β is an equivalence between the extensions E_f and $E_{f'}$ of G by A, proving the proposition. ■

We are now in a position to prove our main theorem. Having done all of the heavy-lifting above, the proof will merely be an assembly of propositions and lemmas.

Theorem 5. *Let G be a group and A a G-module. Then there is a bijection*

$$\frac{\{\text{Extensions of } G \text{ by } A\}}{\sim} \longleftrightarrow H^2(G,A)$$

between the equivalence classes of extensions E of G by A and the cohomology classes in $H^2(G,A)$. This bijection takes an extension E into the cohomology class of a normalized factor set f for E associated to any normalized section $\mu : G \to E$, and takes a cohomology class c in $H^2(G,A)$ to the extensions E_f constructed in Proposition 7 for any normalized 2-cocycle f in c.

Moreover, under this bijection, split extensions of G by A correspond to the trivial cohomology class.

Proof. Given an extension E of G by A, Proposition 5 provides us with a corresponding well-defined cohomology class c in $H^2(G,A)$ when presented with a normalized section μ and associated normalized factor set f. Any extension E' equivalent to E corresponds to c also via Proposition 6. Conversely, with c in $H^2(G,A)$, we have an extension $E_{f'}$ with factor set f' by Proposition 7, and this extension depends only on c by Proposition 8. Since f also lies in c, f and f' give an equivalence between E and E_f, proving the theorem. ■

There is immense power in this characterization of $H^2(G,A)$ which we have just developed. An easy corollary follows, which we now state.

Corollary 2. *Every extension of G by the abelian group A splits if and only if $H^2(G,A) = 0$.*

Proof. Since all split extensions of G by A are equivalent, and every extension of G by A splits, there is one equivalence class of extensions of G by A, which by Theorem 5 corresponds only to the trivial cohomology class in $H^2(G,A)$, giving that $H^2(G,A)$ is trivial. ■

In the following example, we show how cohomological information can be used to obtain facts regarding the number of inequivalent extensions of a particular G by A.

Example 4. Let $G = Z_2$ and $A = \mathbb{Z}/2\mathbb{Z}$, so that G acts trivially on A. From the cohomology of finite cyclic groups, we know that $H^2(G,A) = A^G/NA = \mathbb{Z}/2\mathbb{Z}$. Hence by Theorem 5 there are two inequivalent extensions of G by A; these are

$$1 \to A \xrightarrow{\iota} Z_4 \xrightarrow{\pi} G \to 1$$

$$1 \to A \xrightarrow{\iota'} V_4 \xrightarrow{\pi'} G \to 1$$

where ι and ι' are inclusions and π and π' are projections. One can easily find that the extension V_4 of G by A is split, and so this extension corresponds to the trivial class in $H^2(G,A)$.

In the next example, we neglect the cohomology of finite cyclic groups to show how the same information may be obtained simply by group-theoretic means.

Example 5. Let $G = Z_2$ and $A = \mathbb{Z}/4\mathbb{Z}$, and let G act trivially on A. We show that $|H^2(G, A)| = 2$.

Recall that $f : G \times G \to A$ is a 2-coboundary if it is a 2-cocycle with the additional requirement that there exists $f_1 : G \to A$ such that

$$f(g, h) = g \cdot f_1(h) - f_1(gh) + f_1(g)$$

In our case, G acts trivially on A, so $g \cdot f_1(h) = f_1(h)$. Since $G = \langle g \rangle$ we have possible values for any 2-coboundary given by:

$$f(1, 1) = f_1(1) - f_1(1) + f_1(1) = f_1(1)$$

$$f(g, 1) = f_1(1) - f_1(g) + f_1(g) = f_1(1)$$

$$f(1, g) = f_1(g) - f_1(g) + f_1(1) = f_1(1)$$

$$f(g, g) = f_1(g) - f_1(1) + f_1(g) = 2f_1(g) - f_1(1)$$

Clearly we have four options for $f_1(1)$ corresponding to the four elements of A. To determine $f(g, g)$, it then suffices to choose a value for $f_1(g)$. Note that choosing $f_1(g) = 1$ or $f_1(g) = 3$ gives $f(g, g) = 2 - f_1(1)$ and $f(g, g) = 6 - f_1(1)$. respectively, which are the same since $6 \equiv 2 \pmod 4$. Also choosing $f_1(g) = 0$ or $f_1(g) = 2$ gives $f(g, g) = 0 - f_1(1) = f_1(1)$ and $f(g, g) = 4 - f_1(1) = f_1(1)$, respectively, since $0 \equiv 4 \pmod 4$. In particular, we have two options for the value of $f_1(1)$. Combining all this together, we have $4 \cdot 2 = 8$ options for 2-coboundaries. Hence $|B^2(G, A)| = 2^3$.

Furthermore, any 2-cocycle $f : G \times G \to A$ must satisfy

$$f(g, h) + f(gh, k) = g \cdot f(h, k) + f(g, hk)$$

for all $g, h, k \in G$. Since G acts trivially on A in our case, we have $g \cdot f(h, k) = f(h, k)$. There are four possible values for each 2-cocycle, $f(1, 1)$, $f(1, g)$, $f(g, 1)$, and $f(g, g)$. We can see that

$$f(1, 1) + f(1, g) = f(1, g) + f(1, g)$$

gives $f(1, 1) = f(1, g)$, while

$$f(g, g) + f(1, g) = f(g, g) + f(g, 1)$$

gives $f(1, g) = f(g, 1)$. Hence there are four options for $f(1, 1) = f(1, g) = f(g, 1)$ corresponding to the four elements of A, and four options for $f(g, g)$. In particular, this means that $|Z^2(G, A)| \leq 4 \cdot 4 = 2^4$.

From the above, we have $|H^2(G, A)| \leq 2$. To prove that $|H^2(G, A)| = 2$, we exhibit two inequivalent extensions of G by A. Note that Example 2 shows that D_8 is a non-split extension of Z_2 by Z_4. Example 3 shows that Q_8 is a split extension of Z_2 by Z_4. It follows that these two extensions of G by A are non-equivalent, and hence correspond to distinct cohomology classes in $H^2(G, A)$. Thus $|H^2(G, A)| \geq 2$, and combined with our above work we get $|H^2(G, A)| = 2$.

The above example shows how the main theorem can be used practically in group theoretic applications. In a similar manner, many second cohomology groups for groups and G-modules of suitably small order may be computed quite painlessly, which is always nice.

2.4 Crossed Product Algebras and the Brauer Group

Before embarking upon our next development, we recall (and make) some definitions. Suppose k is a field. Recall that a k-algebra B is a ring containing the field k in its center, and that the identity of B is the identity of k.

Definition. A k-algebra A is called *simple* if A contains no non-trivial, proper two-sided ideals. A *central simple k-algebra* A is a simple k-algebra whose center is k, i.e., $Z(A) = k$.

Example 6. Perhaps the simplest example of a central simple k-algebra is the ring $M_n(k)$ of $n \times n$ matrices with entries in k. It can easily be checked that $M_n(k)$ is simple, and moreover that $Z(M_n(k)) \cong k$ by equating scalar matrices (those with some constant on the diagonal) with elements of k.

We now construct another class of central simple algebras. Suppose K/k is a finite Galois extension of fields with Galois group $G = \mathrm{Gal}(K/k)$. We shall use normalized 2-cocycles in $Z^2(G, K^\times)$ to build central simple k-algebras. We shall use the secondary definition of a 2-cocycle which we stated in the previous section, namely by viewing 2-cocycles as a collection of elements indexed by elements of G.

To this end, suppose $f = \{a_{\sigma,\tau}\}_{\sigma,\tau\in G}$ is a normalized 2-cocycle in $Z^2(G, K^\times)$. Denote by B_f the K-vector space with K-basis $\{u_\sigma \mid \sigma \in G\}$. We have:

$$B_f = \{\sum_{\sigma\in G} \alpha_\sigma u_\sigma \mid \alpha_\sigma \in K\}$$

We would like to place a multiplication on B_f above, so as to make B_f a ring. We define:

$$u_\sigma \alpha = \sigma(\alpha) u_\sigma$$
$$u_\sigma u_\tau = a_{\sigma,\tau} u_{\sigma\tau}$$

for all $\alpha \in K$ and $\sigma, \tau \in G$. The second equation above should remind readers of the definition of a factor set, and this is no coincidence. We would now like to show that this multiplication defined above is associative.

$$\begin{aligned}(u_\sigma u_\tau)u_\rho &= a_{\sigma,\tau} u_{\sigma\tau} u_\rho \\ &= a_{\sigma,\tau} a_{\sigma\tau,\rho} u_{\sigma\tau\rho}\end{aligned}$$

While also

$$\begin{aligned}u_\sigma(u_\tau u_\rho) &= u_\sigma a_{\tau,\rho} u_{\tau\rho} \\ &= \sigma(a_{\tau,\rho}) u_\sigma u_{\tau\rho} \\ &= \sigma(a_{\tau,\rho}) a_{\sigma,\tau\rho} u_{\sigma\tau\rho}\end{aligned}$$

Now we refer to the 2-cocycle property of $f = \{a_{\sigma,\tau}\}_{\sigma,\tau\in G}$, which states that

$$a_{\sigma,\tau}a_{\sigma\tau,\rho} = \sigma(a_{\tau,\rho}a_{\sigma,\tau\rho}$$

when rewritten in multiplicative form. In particular, the above shows that

$$(u_\sigma u_\tau)u_\rho = a_{\sigma,\tau}a_{\sigma\tau,\rho}u_{\sigma\tau\rho} = \sigma(a_{\tau,\rho})a_{\sigma,\tau\rho}u_{\sigma\tau\rho} = u_\sigma(u_\tau u_\rho)$$

and hence that the multiplication we have defined on B_f is indeed associative.

Since the 2-cocycle $f = \{a_{\sigma,\tau}\}_{\sigma,\tau\in G}$ is normalized, we have $a_{\sigma,1} = 1 = a_{1,\sigma}$ for all $\sigma \in G$, and hence that

$$u_\sigma u_1 = a_{\sigma,1}u_\sigma = u_\sigma = a_{1,\sigma}u_\sigma = u_1 u_\sigma$$

Thus u_1 is the identity element for multiplication in B_f. We now embed K in B_f as follows:

$$\iota : K \to B_f$$

$$\alpha \longmapsto \alpha u_1$$

is clearly seen to suffice. Hence we may view B_f as a k-algebra containing the overfield K with dimension n^2 over k, if we let $n = |G| = [K : k]$. We claim, in fact, that B_f is a central simple k-algebra.

Proposition 9. *The k-algebra B_f with K-vector space basis $\{u_\sigma \mid \sigma \in G\}$ with multiplication and identity defined above is a central simple k-algebra.*

Proof. We showed above that B_f is a k-algebra. Thus to prove the proposition we need to show that B_f is simple and that $Z(B_f) = k$.

Suppose $x = \sum_{\sigma\in G} \alpha_\sigma u_\sigma$ lies in the center of B_f. Then, in particular, $x\beta = \beta x$ for all $\beta \in K \subseteq B_f$, and hence $\sigma(\beta) = \beta$ if we have $\alpha_\sigma \neq 0$. However we know that for each $\sigma \in G$ there exists some $\beta \in K$ for which $\sigma(\beta) \neq \beta$, i.e., at least one element of the overfield K is not fixed by an automorphism in the Galois group. In particular, we have that $\alpha_\sigma = 0$ for all $\sigma \neq 1$ in G, and hence $x = \alpha_1 u_1$ must hold. But we also have that $xu_\tau = u_\tau x$ for all $\tau \in G$ since x commutes with all elements of B_f, and hence $\tau(\alpha_1) = \alpha_1$ for all $\tau \in G$, i.e., $\alpha_1 \in k$. Hence $x = \alpha_1 u_1 \in k$, to which $Z(B_f) \subseteq k$. The reverse inclusion is clear, giving $Z(B_f) = k$.

Now suppose I is a non-zero ideal of B_f. We may choose an element $x \in I$ with minimal non-zero terms, say m non-zero terms. Now let

$$x = \sum_{i=1}^{m} \alpha_{\sigma_i} u_{\sigma_i}$$

If it is the case that $m > 1$ then there exists an element $\beta \in K^\times$ with $\sigma_m(\beta) \neq \sigma_{m-1}(\beta)$.

Then

$$\begin{aligned}
x - \sigma_m(\beta)x\beta^{-1} &= \sum_{i=1}^{m} \alpha_{\sigma_i}u_{\sigma_i} - \sum_{i=1}^{n} \sigma_m(\beta)\alpha_{\sigma_i}u_{\sigma_i}\beta^{-1} \\
&= \sum_{i=1}^{m} \alpha_{\sigma_i}u_{\sigma_i} - \sum_{i=1}^{m} \sigma_m(\beta)\alpha_{\sigma_i}\sigma_i(\beta)^{-1}u_{\sigma_i} \\
&= \sum_{i=1}^{n} (\alpha_{\sigma_i} - \sigma_m(\beta)\alpha_{\sigma_i}\sigma_i(\beta)^{-1})u_{\sigma_i}
\end{aligned}$$

is an element of I by closure under left and right multiplication (since I is a 2-sided ideal) and by closure under addition. In particular, analyzing the $m-1$th coefficient, we have:

$$\alpha_{\sigma_{m-1}} - \sigma_m(\beta)\alpha_{\sigma_i}\sigma_{m-1}(\beta)^{-1} = (1 - \sigma_m(\beta)\sigma_{m-1}(\beta)^{-1})\alpha_{\sigma_{m-1}}$$

Note that the above is a non-zero element, and so the element $x - \sigma_m(\beta)x\beta^{-1}$ would have fewer non-zero terms than x, and still lie inside of I, which is a contradiction. Hence $m = 1$ is required, and so $x = \alpha u_\sigma$ for some $\alpha \in K$ and $\sigma \in G$. In fact, this element is a unit, with inverse given by $\sigma^{-1}(\alpha^{-1})u_{\sigma^{-1}}$, which implies that $I = B_f$. Hence B_f has no non-trivial proper 2-sided ideals, as desired. ■

We give such central simple k-algebras B_f associated to a factor set f in $Z^2(G, K^\times)$ with respect to a finite Galois extension of fields K/k a name.

Definition. The central simple k-algebra B_f constructed above is called the *crossed product k-algebra* for the factor set $f = \{a_{\sigma,\tau}\}_{\sigma,\tau\in G}$.

Historically, such crossed product algebras were the impetus for the development of abstract cohomology as we know it today. Now we connect this discussion to $H^2(G, K^\times)$, and develop theory which is crucial in modern number theory.

Proposition 10. *Every cohomology class c in $H^2(G, K^\times)$ defines an isomorphism class of central simple k-algebras, which is the isomorphism class of any crossed product k-algebra B_f for a normalized 2-cocycle f representing the class c.*

Proof. Suppse $f' = \{a'_{\sigma,tau}\}_{\sigma,\tau\in G}$ is another normalized 2-cocycle in the same cohomology class c in $H^2(G, K^\times)$ as $f = \{a_{\sigma,\tau}\}_{\sigma,\tau\in G}$. Then there are elements $b_\sigma \in K^\times$ for which

$$a'_{\sigma,\tau} = a_{\sigma,\tau}(\sigma(b_\tau)b_{\sigma\tau}^{-1}b_\sigma)$$

which is simply the multiplicative form of the 2-coboundary condition (recall that these normalized 2-cocycles f and f' must differ by a 2-coboundary). If we let $B_{f'}$ denote the crossed product k-algebra with K-basis $\{u'_\sigma \mid \sigma \in G\}$, then the map

$$\varphi : B_{f'} \to B_f$$

$$u'_\sigma \longmapsto b_\sigma u_\sigma$$

satisfies

$$\begin{aligned}\varphi(u'_\sigma u'_\tau) &= \varphi(a'_{\sigma,\tau}u'_{\sigma\tau})\\ &= a'_{\sigma,\tau}b_{\sigma\tau}u_{\sigma\tau}\\ &= b_\sigma\sigma(b_\tau)u_\sigma u_\tau\\ &= (b_\sigma u_\sigma)(b_\tau u_\tau)\\ &= \varphi(u'_\sigma)\varphi(u'_\tau)\end{aligned}$$

and hence φ is clearly seen to be a K-vector space homomorphism. In fact, φ is an isomorphism, which is easily seen, and hence $B_{f'} \cong B_f$. ■

In fact, we can push the above line of inquiry even further. We shall now show that the trivial cohomology class in $H^2(G, K^\times)$ corresponds to a the isomorphism class of crossed product k-algebras which are isomorphic to some matrix algebra $M_n(k)$, where $n = [K : k]$.

Proposition 11. *Let K/k be a finite Galois extension of fields, let $G = Gal(K/k)$, and let $n = [K : k]$. Then the crossed product k-algebra corresponding to the trivial cohomology class in $H^2(G, K^\times)$ is isomorphic (as a k-algebra) to the matrix k-algebra $M_n(k)$.*

Proof. For any $\alpha \in K$ we know that α defines a k-linear operator of K, which is simply multiplication by α. Similarly, every automorphism $\sigma \in G$ defines a k-linear transformation T_σ of K, and both T_α and T_σ may be viewed as elements of $M_n(k)$ upon fixing a k-basis for K over k.

Let B_0 denote the crossed product k-algebra for the trivial factor set $f' = \{a_{\sigma,\tau}\}_{\sigma,\tau\in G}$, where $\alpha_{\sigma,\tau} = 1$ for all $\sigma, \tau \in G$. Consider the map

$$\varphi : B_0 \to M_n(k)$$

$$\varphi(\alpha u_\sigma) = T_\alpha T_\sigma$$

Since $T_{a\alpha} = aT_\alpha$ for all $a \in k$, it is clear that φ is a k-linear transformation. Now, if we let $\beta \in K$, we can see that

$$T_\sigma T_\alpha(\beta) = T_\sigma(\alpha\beta) = \sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = T_{\sigma(\alpha)}T_\sigma(\beta)$$

and hence $T_\sigma T_\alpha = T_{\sigma(\alpha)}T_\sigma$ are equal on K. In particular, since $u_\sigma u_\tau = u_{\sigma\tau}$, we have

$$\begin{aligned}\varphi((\alpha u_\sigma)(\beta u_\tau)) &= \varphi(\alpha\sigma(\beta)u_{\sigma\tau})\\ &= T_{\alpha\sigma(\beta)}T_{\sigma\tau}\\ &= T_\alpha T_{\sigma(\beta)}T_\sigma T_\tau\\ &= T_\alpha T_\sigma T_\beta T_\tau\\ &= \varphi(\alpha u_\sigma)\varphi(\beta u_\tau)\end{aligned}$$

and hence φ is also a homomorphism of k-algebras from B_0 to $M_n(k)$. Since B_0 is a simple k-algebra by Proposition 9, and $\ker(\varphi)$ is an ideal of B_0, we have φ is injective. Now, by dimension considerations, φ is an isomorphism, for B_0 and $M_n(k)$ both have dimension n^2 over k. Hence the proposition is proved. ■

We now come to a point in our development where we must introduce, without proof, several results from the theory of simple algebras. In particular, these results will aid us in connecting the above theory to that of the Brauer group. We begin by introducing a few definitions.

Definition. Let A be a central simple k-algebra which is finite dimensional over k. If B is a simple k-algebra and $k \subseteq B \subseteq A$ then the *centralizer* B^c of B in A is the set of elements of A that commute with all elements of B.

Definition. Let A be a central simple k-algebra which is finite dimensional over k. Suppose B is a simple k-algebra and $k \subseteq B \subseteq A$. Then the *opposite algebra* B^{opp} is the set B with opposite multiplication. That is, the product $b_1 b_2$ in B^{opp} is given by $b_2 b_1$ in B.

The results are as follows:

Theorem 6. *Let A be a central simple k-algebra which is finite dimensional over k. Suppose B is a simple k-algebra and $k \subseteq B \subseteq A$. Then both B^c and B^{opp} are simple k-algebras and:*
(1) $(\dim_k(B^c))(\dim_k(B^{\text{opp}})) = \dim_k(A)$.
(2) $A \otimes_k B^{\text{opp}} \cong M_r(B^c)$ *as k-algebras, where* $r = \dim_k(B)$.
(3) $B \otimes_k B^c \cong A$ *if B is a central simple k-algebra.*

Theorem 7. *Let A be a central simple k-algebra which is finite dimensional over k. If A' is an Artinian (that is, satisfies the descending chain condition on left ideals) simple k-algebra, then $A \otimes_k A'$ is an Artinian simple k-algebra with center $(A')^c$.*

Theorem 8. *Let A be a central simple k-algebra which is finite dimensional over k. Then $A \cong M_r(D)$ for some division ring D whose center is k and some $r \geq 1$. Moreover, the division ring D and the integer r are uniquely determined by A.*

Full proofs for the theorems stated above may be found in [Pie82], alongside the bulk of simple algebra theory.

Definition. Two central simple k-algebras A and B are *similar* if $A \cong M_r(D)$ and $B \cong M_s(D)$ for the same division ring D, but with possibly different integers r and s.

Proposition 12. *The similarity classes of central simple k-algebras is a group under the binary operation $[A][B] = [A \otimes_k B]$ for any two central simple k-algebras A and B.*

Proof. Let $[A]$ denote the similarity class of the central simple k-algebra A. By Theorem 7, if A and B are central simple k-algebras then $A \otimes_k B$ is again a central simple k-algebra. This is because both A and B are Artinian, for instance they are simple k-algebras, and the centralizer of B is equal to k. Thus we may define a multiplication on similarity classes as in the proposition statement, where $[A][B] = [A \otimes_k B]$.

We see that the class $[k]$ is an identity for this multiplication by properties of the tensor product, as $A \otimes_k k \cong k \otimes_k A \cong A$, and hence $[A][k] = [k][A] = [A]$. Note that

$$[A]([B][C]) = [A][B \otimes_k C] = [A \otimes (B \otimes_k C)] = [(A \otimes_k B) \otimes_k C] = ([A][B])[C]$$

by the associativity of the tensor product; in particular multiplication is associative. Lastly, for inverses, note that by Theorem 7(2) we have

$$A \otimes_k A^{\mathrm{opp}} \cong M_n(A^c) = M_n(k)$$

since the centralizer of A in A is clearly k. Since $k \cong M_1(k)$ trivially holds, we have that $[A \otimes_k A^{\mathrm{opp}}] = [k]$, and hence $[A][A^{\mathrm{opp}}] = [k]$, so that $[A^{\mathrm{opp}}]$ is an inverse for $[A]$ under this multiplication. ■

Definition. The group of similarity classes of central simple k-algebras with multiplication $[A][B] = [A \otimes_k B]$ is called the *Brauer group* of k and is denoted $\mathrm{Br}(k)$.

To introduce the next object, we require the following definition.

Definition. If A is a central simple k-algebra then a field K containing k is said to *split* A if $A \otimes_k K \cong M_n(K)$ for some $n \geq 1$.

Let A be a central simple k-algebra. Equipped with the above definition, we can see that if K is any extension field of k, then by Theorem 7 the k-algebra $A \otimes_k K$ is a central simple K-algebra. Now the map

$$\mathrm{Br}(k) \to \mathrm{Br}(K)$$

$$[A] \longmapsto [A \otimes_k K]$$

is a well-defined group homomorphism. It is clear that the kernel of this homomorphism consists of the similarity classes of central simple k-algebras A such that $A \otimes_k K \cong M_n(K)$ for some $n \geq 1$. In other words, the kernel consists of those central simple k-algebras which are split by K.

The fact that the similarity classes of central simple k-algebras split by K is a kernel allows us to consider it with the same group structure as the Brauer group $\mathrm{Br}(k)$. We attach a name to this special subgroup:

Definition. If K/k is a field extension then we define the *relative Brauer group*, denoted by $\mathrm{Br}(K/k)$, to be the group of similarity classes of central simple k-algebras that are split by K.

We now state, without direct proof, several theorems which summarize some major results in the area of crossed product algebras and Brauer groups, especially with respect to cohomological connections.

Theorem 9. *Suppose K/k is a finite Galois extension with $[K : k] = n$, and let $G = Gal(K/k)$. Then*

(1) The central simple k-algebra A with $\dim_k(A) = n^2$ is split by K if and only if $A \otimes_k K \cong M_n(K)$ if and only if A is isomorphic to a crossed product algebra B_f, where f is a factor set associated with a normalized 2-cocycle representing a cohomology class in $Z^2(G, K^\times)$.

(2) There is a bijection

$$\{k\text{-}CSAs\ A\ with\ A\otimes_k K\cong M_n(K)\}\ /\ \cong_k\ \longleftrightarrow H^2(G,K^\times)$$

between the k-isomorphism classes of central simple k-algebras A with $A\otimes_k K\cong M_n(K)$ and cohomology classes in $H^2(G,K^\times)$. Under the bijection, the cohomology class c containing the normalized 2-cocycle f corresponds to the isomorphism class of the crossed product k-algebra B_f.

Moreover, the trivial cohomology class corresponds to the central simple k-algebras which are isomorphic to $M_n(k)$.

(3) Every central simpple k-algebra of finite dimension over k and split by K is similar to one of dimension n^2 split by K. The bijection in (2) above also establishes a bijection

$$Br(K/k)\cong H^2(G,K^\times)$$

which is actually a group isomorphism.

(4) There is a bijection between the collection of k-isomorphism classes of central simple division k-algebras and $H^2(G,K^\times)$.

Full proofs of the theorems above may be found in [GS17]. We illustrate merely a small fraction of the immense power inherent in the above results by giving a proof that every finite division ring is a field.

Example 7. Let $\mathbb{F}_q$ be a finite field. Before we can prove the result, we need to show that $H^2(\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q),\mathbb{F}^\times_{q^d})=0$. Let $G=\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)=\langle\sigma_q\rangle$, where σ_q is the Frobenius automorphism. Let also $N=1+\sigma_q+\cdots+\sigma_q^{d-1}$ be the norm map.

From the cohomology of finite cyclic groups, we know that

$$H^1(G,\mathbb{F}^\times_{q^d}) =_N (\mathbb{F}^\times_{q^d})/(\sigma_q-1)\mathbb{F}^\times_{q^d}$$

Hilbert's Theorem 90 asserts that $H^1(G,\mathbb{F}^\times_{q^d})=0$, which follows since $\mathbb{F}_{q^d}/\mathbb{F}_q$ is a finite Galois extension with cyclic Galois group G. In particular, we have ${}_N(\mathbb{F}^\times_{q^d})=(\sigma_q-1)\mathbb{F}^\times_{q^d}$. From the first isomorphism theorem we have the following:

$$(\sigma_q-1)\mathbb{F}^\times_{q^d}\cong\mathbb{F}^\times_{q^d}/\ker(\sigma_q-1)$$

Moreover, since $\ker(\sigma_q-1)=\mathbb{F}^\times_q$ we require

$$|(\sigma_q-1)\mathbb{F}^\times_{q^d}|=\frac{|\mathbb{F}^\times_{q^d}|}{|\mathbb{F}^\times_q|}=\frac{q^d-1}{q-1}$$

Thus $|{}_N(\mathbb{F}^\times_{q^d})|=(q^d-1)/(q-1)$. Now, we consider the norm map $N:\mathbb{F}^\times_{q^d}\to\mathbb{F}^\times_q$, and observe that $\ker(N) =_N (\mathbb{F}^\times_{q^d})$; hence the first isomorphism theorem may be employed once more to yield $\mathbb{F}_{q^d}^\times / \ker(N) \cong N(\mathbb{F}_{q^d}^\times)$. In particular, we require that

$$|N(\mathbb{F}_{q^d}^\times)| = \frac{q^d - 1}{(q^d-1)/(q-1)} = q - 1$$

However since $N(\mathbb{F}_{q^d}^\times) \subseteq \mathbb{F}_q$ by construction, the above forces $\mathbb{F}_q = N(\mathbb{F}_{q^d}^\times)$, and hence we know that the norm map is surjective.

From the cohomology of finite cyclic groups once again, we have the following:

$$H^n(G, \mathbb{F}_{q^d}^\times) = \left\{ \begin{array}{ll} (\mathbb{F}_{q^d}^\times)^G / N(\mathbb{F}_{q^d}^\times), & \text{if } n \text{ is even, } n \geq 2 \\ \\ {}_N(\mathbb{F}_{q^d}^\times)/(\sigma_q - 1)\mathbb{F}_{q^d}^\times, & \text{if } n \text{ is odd, } n \geq 1 \end{array} \right\}$$

Hilbert's Theorem 90 actually also gives us that $H^n(G, \mathbb{F}_{q^d}^\times) = 0$ for all odd $n \geq 1$. The surjectivity of the norm map, combined with the fact that $(\mathbb{F}_{q^d}^\times)^G = \mathbb{F}_q^\times$, which holds since G is the Galois group of $\mathbb{F}_{q^d}/\mathbb{F}_q$, yields that $H^n(G, \mathbb{F}_{q^d}^\times) = 0$ for all even $n \geq 2$. In particular, we have shown that $H^n(G, \mathbb{F}_{q^d}^\times) = 0$ for all $n \geq 1$.

Now, the above result combined with Theorem 9 means $\text{Br}(\mathbb{F}_{q^d}/\mathbb{F}_q) = 0$, and hence that $\text{Br}(\mathbb{F}_q) = 0$. As a consequence, every finite division ring is a field. To see this, let D be a finite division algebra, then D is a central simple $Z(D)$-algebra, and since $Z(D)$ is a finite field, $\text{Br}(Z(D)) = 0$ and hence $Z(D)$ is split by D, meaning $D \cong M_n(Z(D))$. But for $n > 1$ $M_n(Z(D))$ would not be a divison algebra (simply find a zero divisor). Hence $n = 1$ and so $D \cong M_1(Z(D)) \cong Z(D)$ is a field.

References

[DF04] David Steven Dummit and Richard M Foote. *Abstract algebra*, volume 3. Wiley Hoboken, 2004.

[GS17] Philippe Gille and Tamás Szamuely. *Central simple algebras and Galois cohomology*, volume 165. Cambridge University Press, 2017.

[Pie82] Richard S. Pierce. *Associative Algebras.* Springer, 1982.

[Wei94] Charles A Weibel. *An introduction to homological algebra.* Number 38. Cambridge University Press, 1994.