[Rose-Hulman Undergraduate Mathematics Journal](https://scholar.rose-hulman.edu/rhumj)

Volume 18
Issue 2

Article 6

The Brauer Group of a Field

Jonathan Aycock
University of North Carolina at Chapel Hill, jaycock@uoregon.edu

Rose-Hulman Undergraduate Mathematics Journal

The Brauer Group of a Field

J. Aycock[a]

Volume 18, No. 2, Fall 2017

Sponsored by

Rose-Hulman Institute of Technology
Department of Mathematics
Terre Haute, IN 47803
mathjournal@rose-hulman.edu
scholar.rose-hulman.edu/rhumj

[a]The University of North Carolina at Chapel Hill

Rose-Hulman Undergraduate Mathematics Journal
Volume 18, No. 2, Fall 2017

The Brauer Group of a Field

J. Aycock

Abstract. In this paper we discuss the Brauer group of a field and its connections with cohomology groups. Definitions involving central simple algebras lead to a discussion of splitting fields, which are the important step in the connection of the Brauer group with cohomology groups. Finally, once the connection between the Brauer group and cohomology groups is established, the paper finishes by calculating specific examples of cocycles associated to certain classes of central simple algebras.

1 Introduction

The Brauer group is an invariant that pops up in many areas of mathematics, including number theory, algebraic geometry, and representation theory. The general construction by way of Azumaya algebras does little to reveal why this might be. Through a little bit of work, one can see that it is related to certain cohomology groups. The ubiquitousness of cohomology in modern mathematics then does a better job explaining its significance. In the sections following, we explore this connection in the special case of the Brauer group of a field.

In Section 2, we define the Brauer group of a field through the introduction of central simple algebras, which are the Azumaya algebras in this case. In Section 3, we introduce Galois cohomology and construct an isomorphism between the Brauer group and a certain cohomology group. In Section 4, we perform calculations explicitly using this isomorphism. Section 5 explores inflation maps on cohomology and how they relate to some patterns we notice in the previous section. Finally, in Section 6, we make more calculations involving the group operation to illustrate that the isomorphism we constructed in Section 3 is an isomorphism of groups.

2 Central Simple Algebras and Splitting Fields

Elements of the Brauer group are equivalence classes of central simple algebras. As such, it is important to have an understanding of these algebras to understand the Brauer group. This section aims to lay the foundation for the rest of our discussion; this foundation starts with the definition of a CSA.

Definitions 2.1: Fix some field k.

1. An algebra over k is a ring A along with an embedding $\psi : k \hookrightarrow A$, where 1 in k maps to 1 in A. This embedding induces a scalar product that allows A to have a vector space structure over k. The image $\psi(k)$ is often denoted $k \cdot 1$, or simply k. We require $\psi(k)$ to commute with every element of the algebra, so that the "left scalar product" and a similarly defined "right scalar product" will be the same.

2. The center of an algebra A is the set $Z(A) = \{z \in A : az = za \quad \forall a \in A\}$. If this set is the subspace $k \cdot 1$, A is said to be central.

3. A (two-sided) ideal of an algebra is a (two-sided) ideal of the algebra viewed as a ring. Note that $(x \cdot 1)i = x \cdot i \in I$ for every $x \in k$, so it includes the stipulation of being closed under scalar multiplication. If the only ideals of A are $\{0\}$ and A, A is said to be simple.

4. An algebra is a central simple algebra if it is both central and simple. We will refer to central simple algebras as CSAs, a common abbreviation.

In addition to these definitions, it is useful to know when an algebra is finite-dimensional. An algebra is finite-dimensional when it is finite-dimensional as a vector space over k. All algebras will be assumed to be finite-dimensional unless stated otherwise.

Examples 2.2: Common examples of CSAs include:

1. The ring of $n \times n$ matrices $M_n(k)$ is a CSA over k for all $n > 0$. It is equipped with a scalar product operation that multiplies each entry by an element of k.

2. Central division algebras, meaning central algebras over k in which every nonzero element has a multiplicative inverse, are CSAs over k as well. The field k itself falls into this category.

3. The quaternion algebra $\left(\frac{a,b}{k}\right)$, generated by i and j with $i^2 = a, j^2 = b, ij = -ji$ is a central simple algebra over k. In fact, it is either a division algebra or it is isomorphic to $M_2(k)$. A discussion of these algebras and their properties is found in [Lam].

4. Cyclic algebras over k are also CSAs over k. They are constructed as follows: Let $K|k$ be a cyclic extension of degree m, and fix σ a generator of the galois group $\mathrm{Gal}(K|k)$. Then choose some $b \in k$. The cyclic algebra A is generated by K and a particular element y, subject to the relations $y^m = b$ and $\lambda y = y\sigma(\lambda)$ for every $\lambda \in K$.

Cyclic algebras are in fact a generalization of quaternion algebras. We can view the quaternion algebra $\left(\frac{a,b}{k}\right)$ as a cyclic algebra generated by $K = k(\sqrt{b})$ and i, with i playing the role of y. This follows because the generator (and only non-identity element) of $\mathrm{Gal}(k(\sqrt{b})|k)$ is the automorphism $g : x + y\sqrt{b} \mapsto x - y\sqrt{b}$.

Tensor products involving CSAs are of particular importance. The following lemma, in two parts, will prove useful for two separate but important statements: Lemma 2.4 and Proposition 2.6. It relates the tensor product to the properties of central simple algebras.

Lemma 2.3: Let k be a field. The symbol $\otimes$ always means tensor over k.

1. Let A and B both be algebras over k. Then $Z(A \otimes B) = Z(A) \otimes Z(B)$.

2. Let A be a CSA over k, and let B be a simple k-algebra. Then $A \otimes B$ is simple.

Proof.

1. The inclusion $\supset$ is obvious, leaving $\subset$ as a nontrivial part of the proof. We first do the case of pure tensors. Let $a \otimes b \in Z(A \otimes B)$ with $a, b \neq 0$. Since it commutes with every element of $A \otimes B$, it in particular commutes with every element of the form $a' \otimes 1$, so:

$$(a' \otimes 1)(a \otimes b) - (a \otimes b)(a' \otimes 1) = (a'a - aa') \otimes b = 0.$$

Since $b \neq 0$, this requires $a'a - aa'$ to be 0, which means a commutes with a' for all a', so $a \in Z(A)$. By a similar argument, $b \in Z(B)$.

This leads to the general case. Let $z = \sum_{i=1}^{r} a_i \otimes b_i \in Z(A \otimes B)$, and choose an expansion for z such that r is minimal. In particular, this means the a_i are linearly independent, and similarly for the b_i. Then pick $a' \in A$ and consider:

$$(a' \otimes 1)z - z(a' \otimes 1) = \sum_{i=1}^{r} (a'a_i - a_i a') \otimes b_i = 0.$$

Then for each j, this means:

$$\sum_{i \neq j} (a'a_i - a_i a') \otimes b_i = (a_j a' - a'a_j) \otimes b_j.$$

But the left hand side is in $A \otimes \mathit{span}(b_i)_{i \neq j}$ and the right hand side is in $A \otimes \mathit{span}(b_j)$, and since the b_i's are linearly independent, these sets only intersect at 0. That means $(a_j a' - a'a_j) \otimes b_j = 0$ for each j, which means each a_j is in $Z(A)$. Again, a similar argument shows each b_j is in $Z(B)$, so we must have $z \in Z(A) \otimes Z(B)$, as desired.

2. To show that $A \otimes B$ is simple, we take some nonzero ideal $I \subset A \otimes B$ and show it is all of $A \otimes B$, by "forcing" 1 to be an element of it as well. Let $z \in I \setminus \{0\}$, where

$$z = \sum_{i=1}^{r} a_i \otimes b_i,$$

and z is such that r is minimal among nonzero elements of I. Now, since A is simple, the ideal generated by a_1 in A is all of A – this means that there is an equation $ca_1 d = 1$ for some pair $c, d \in A$. Similarly, we have $c'b_1 d' = 1$ for some pair $c', d' \in B$. Then we set $z' = (c \otimes c')z(d \otimes d')$, and we know that $z' \in I$, and find that

$$z' = 1 \otimes 1 + \sum_{i=2}^{r} a'_i \otimes b'_i,$$

where $a'_i = ca_i d$ and $b'_i = c'b_i d'$. Then fix some $a_0 \in A$, and note

$$(a_0 \otimes 1)z' - z'(a_0 \otimes 1) = \sum_{i=2}^{r} (a_0 a'_i - a'_i a_0) \otimes b_i \in I.$$

Since r was minimal for an element of I, this element must be 0. Next fix $b_0 \in B$, noting

$$(1 \otimes b_0)z' - z'(1 \otimes b_0) = \sum_{i=2}^{r} a_i \otimes (b_0 b'_i - b' b_0).$$

Similarly, this must be zero. This means z' commutes with every tensor of the form $(a \otimes 1)$ and of the form $(1 \otimes b)$. It further commutes with every product of elements of that form, and sums of those elements. This means it commutes with all of $A \otimes B$. Then $z' \in Z(A \otimes B)$, which is equal to $Z(A) \otimes Z(B)$ by part 1. Then since $Z(A)$ is just the one-dimensional space $k \cdot 1$, we must have $r = 1$, so z' was just $1 \otimes 1$ to begin with. So every nonzero ideal contains $1 \otimes 1$, and is thus all of $A \otimes B$, so $A \otimes B$ is simple.

This lemma gives the following as an immediate corollary:

Corollary 2.4: If A and B are central simple algebras over k, then so is $A \otimes B$.

This leads to our definition of the Brauer group.

Definition 2.5: The Brauer group of a field k, $Br(k)$, is the group whose underlying set is the set of all CSAs over k with the equivalence relation $A \sim B$ if and only if $M_m(A) \cong M_n(B)$ for some choice of m and n. The equivalence class containing A is denoted $[A]$. The group operation is $[A] \cdot [B] = [A \otimes B]$.

What is defined above is certainly at least a monoid, and it will become a group if every element $[A] \in Br(k)$ has an inverse. Each element does have an inverse, with $[A]^{-1} = [A^{op}]$, the class of its opposite algebra, which is defined to have the same underlying set and additive structure, but $a^{(op)} \cdot b^{(op)} = (b \cdot a)^{(op)}$, where the superscript ${}^{(op)}$ denotes an element of the opposite algebra. We will not prove this here, as proofs are found both in [Lam] and in [GS].

The following statements lead to a final theorem on splitting fields which will be useful in our cohomological study of $Br(k)$.

Proposition 2.6: Let A be an algebra over k, and let $K|k$ be a finite field extension. Then A is central simple over k if and only if $A \otimes K$ is central simple over K.

Proof. For the backward implication, note that if I is an ideal in A, $I \otimes K$ is an ideal in $A \otimes K$, so if A is not simple, $A \otimes K$ is not simple. Also note that $Z(A) \otimes K$ is the center of $A \otimes K$ by part 1 of Lemma 2.3, so if $Z(A)$ is not just k, $Z(A \otimes K)$ will not just be $k \otimes K$, which is the embedding of K in $A \otimes K$. Thus if A is not central simple over k, $A \otimes K$ is not central simple over K. For the forward implication, Let A be a central simple algebra. Note again that $Z(A \otimes K)$ is $Z(A) \otimes K$, so since A is central, $Z(A \otimes K) = K$. By part 2 of Lemma 2.3, since A is central simple and K is simple, $A \otimes K$ is simple. Then if A is central simple over k, $A \otimes K$ is central simple over K.

Theorem 2.7: Wedderburn's Theorem. Every CSA over k is isomorphic to a matrix algebra $M_n(D)$ for some integer $n > 0$ and some central division algebra D over k. The isomorphism class of D and the integer n are both uniquely determined.

Unfortunately, the proof is quite involved, and uses machinery we will not use again. As such, anyone who wishes to learn about this fact will be redirected to section 2.1 in [GS]. However, the importance of this result necessitates its inclusion. An immediate corollary is that every element of $Br(k)$ can be represented by a unique central division algebra over k, which often leads to the claim that the Brauer group is a tool for classifying division algebras. This theorem is also used as the first reduction in the proof of the next lemma, concerning the case when k is algebraically closed.

Lemma 2.8: If k is algebraically closed, then any CSA over k is isomorphic to $M_n(k)$ for some choice of n.

Proof. By Theorem 2.7, it is sufficient to show that k is the only central division algebra over k. Assume D is a division algebra over k, and take $d \in D$. Since D has finite dimension over k, the elements $1, d, d^2, \ldots$ are linearly dependent over k. This means d satisfies some minimal polynomial $f \in k[x]$, which is irreducible over k. But since k is algebraically closed, the only irreducible polynomials are degree 1, which means $d \in k$. Thus $D \subset k$, so $D = k$, and k is the only (central) division algebra over k.

In Lemma 2.8, the implicit assumption that every algebra is finite dimensional is integral to the proof. This lemma and Proposition 2.6 together form the basis for the proof of the next theorem, which is very important in the next section. The theorem will be followed by the definition of $Br(K|k)$, a particular subgroup of $Br(k)$.

Theorem 2.9: Let k be a field, and A an algebra over k. Then A is a CSA if and only if there exists an integer $n > 0$ and a finite field extension $K|k$ such that $A \otimes K \cong M_n(K)$.

Proof. The reverse implication follows from Proposition 2.6, since $M_n(K)$ is central simple over K. Now for the forward direction, first fix $\overline{k}$ an algebraic closure of k. By Lemma 2.8, $A \otimes \overline{k} \cong M_n(\overline{k})$ for some choice of n. Though $\overline{k}|k$ may not be a finite extension, the existence of some field extension $\overline{k}|k$ such that $A \otimes \overline{k} \cong M_n(\overline{k}$ will help us in our search for our finite extension $K|k$ with $A \otimes K \otimes M_n(K)$.

For any finite field extension $K|k$, the inclusion map $K \hookrightarrow \overline{k}$ defines an inclusion $A \otimes K \hookrightarrow A \otimes \overline{k}$, and the union of these algebras $A \otimes K$ gives $A \otimes \overline{k}$ since $\overline{k}$ is an algebraic extension of k. Then the elements corresponding to the e_{ij} in $M_n(\overline{k})$ each have to be in one of the finite field extensions. For each pair i, j, let $K_{i,j}$ be a field extension for which $A \otimes K_{i,j}$ contains e_{ij} under the inclusion maps mentioned above, and let K^* be the compositum of all these fields, $K^* = K_{1,1}K_{1,2} \ldots K_{n,n}$. Then since each $K_{i,j}$ was finite, this

K^* will be finite as well, and $A \otimes K^*$ contains each $e_{i,j}$, so it is isomorphic to $M_n(K^*)$, proving the theorem.

The theorem states that every CSA has a "splitting field" among its finite extensions. There is further discussion in [GS] that implies that at least one of these finite splitting fields is Galois. Splitting fields are useful because of the following fact: $(A \otimes K) \otimes (B \otimes K) \cong (A \otimes B) \otimes K$, so if K splits A and B, then it splits $A \otimes B$. This leads to a definition of a kind of a "bonus" Brauer group, which is the basis for our discussion in the next section.

Definition 2.10: Let k be a field and K a Galois extension. The Brauer group of k relative to K is the subgroup of $Br(k)$ consisting of those CSAs split by K. It is denoted $Br(K|k)$.

Finally, since the k-dimension of any CSA A over k is the same as the K-dimension of $A \otimes K$ over K, we have that the dimension of a CSA over a field is always a square. We call the integer $\sqrt{dim_k(A)}$ the degree of A, and it is also the n in Theorem 2.9.

3 Galois Cohomology

This section begins with the definition of cohomology groups for a general projective resolution, and then defines the standard resolution, before using that to associate the elements of $Br(k)$ and $Br(K|k)$ to the elements of two of these groups. No calculations are done on these groups until the following section – this section simply sets the foundation for those that come after.

Definitions 3.1: Let G be a group.

1. A G-module is an abelian group A equipped with a G-action $G \times A \to A$, $(\sigma, a) \mapsto \sigma a$, satisfying $\sigma(\tau a) = (\sigma\tau)a$ and $\sigma(a + b) = \sigma a + \sigma b$. Equivalently, it is a module in the usual sense over the group ring $\mathbb{Z}[G]$.

2. A projective G-module is a G-module P such that, for every surjective map of G-modules $\alpha : A \to B$, the natural map $\mathrm{Hom}(P, A) \to \mathrm{Hom}(P, B)$ given by $\lambda \mapsto \alpha \circ \lambda$ is surjective. Free modules are always projective.

3. Given any G-module A, a projective resolution P_* of A is an exact sequence
$$\cdots \to P_3 \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} A \to 0,$$
With P_i projective for each i.

4. A chain complex M^* is a sequence of G-modules
$$M_0 \xrightarrow{c_0} M_1 \xrightarrow{c_1} M_2 \xrightarrow{c_2} \ldots,$$
Where $c_i \circ c_{i-1} = 0$ for all i. That is, $\mathrm{im}(c_{i-1}) \subset \ker(c_i)$ – if the sets are equal, the chain is called exact.

5. Given a chain complex M^* as above, the group $H^i(M^*)$ is defined to be the quotient $Ker(c_i)/Im(c_{i-1})$. If M^* is exact, these are trivial for all i.

Now we can connect definitions 3 and 4 above. Given a projective resolution P_* of some G-module X and another G-module A, there is an associated chain complex M^* with $M_i = \mathrm{Hom}_G(P_i, A)$, and $c_i : f \mapsto f \circ d_{i+1}$. This is a complex since $(c_{i+1} \circ c_i)(f) = f \circ d_{i-1} \circ d_i = f \circ 0 = 0$ is trivial. We can write this chain complex as $\mathrm{Hom}_G(P_*, A)$. The next definition uses this connection.

Definition 3.2: Fix some projective resolution P_* of $\mathbb{Z}$ as a trivial G-module. (That is, $\mathbb{Z}$ as an abelian group with $g \cdot n = n$ for all $n \in \mathbb{Z}$ and all $g \in G$.) Then the ith cohomology group of G with values in A is $H^i(\mathrm{Hom}_G(P_*, A))$, as defined above. It is denoted $H^i(G, A)$. These groups also have the following nice properties:

1. The zeroth cohomology group $H^0(G, A) = A^G$ is the subgroup consisting of elements of A fixed by G.

2. Any G-homomorphism $A \to B$ induces a homomorphism $H^i(G, A) \to H^i(G, B)$ for all i.

3. Given a short exact sequence of G-modules $0 \to A \to B \to C \to 0$, we have a long exact sequence

$$\cdots \to H^{i-1}(G, C) \to H^i(G, A) \to H^i(G, B) \to H^i(G, C) \to H^{i+1}(G, A) \to \ldots$$

   of Abelian groups, starting with $0 \to H^0(G, A)$.

Remark: It can be shown, using the properties of projective modules, that the groups $H^i(G, A)$ are well-defined. That is, that you get the same group regardless of the choice of resolution. This is discussed in [GS] in section 3.1. The properties 1-3 above are also discussed in that section.

Now, since the choice of resolution P_* does not change the groups, we can choose a specific resolution, and study cohomology groups induced this way. The resolution most often used is the standard resolution.

Definitions 3.3: These definitions culminate in the definition of the standard resolution.

1. Define the map $s_j^i : \mathbb{Z}[G^{i+1}] \to \mathbb{Z}[G^i]$ so that
$$s_j^i(g_0, g_1, \ldots, g_i) = (g_0, \ldots, g_{j-1}, g_{j+1}, \ldots, g_i).$$

2. Now define the map $d_i : \mathbb{Z}[G^{i+1}] \to \mathbb{Z}[G^i]$ in terms of the s_j^i:
$$d_i = \sum_{j=0}^{i} (-1)^j s_j^i.$$

3. Finally, the standard resolution is the resolution
$$\ldots \xrightarrow{d_2} \mathbb{Z}[G^2] \xrightarrow{d_1} \mathbb{Z}[G] \xrightarrow{d_0} \mathbb{Z} \to 0,$$
where the d_i are as above.

It's easy to check that the alterating signs force $d_{i+1} \circ d_i = 0$ for all i, which shows that $\mathrm{im}(d_{i+1}) \subset \ker(d_i)$. However to show that the standard resolution is exact, we need further that $\ker(d_i) = \mathrm{im}(d_{i+1})$, which is stronger. To show this, fix $g \in G$ define functions $h^i : \mathbb{Z}[G^{i+1}] \to \mathbb{Z}[G^{i+2}]$ so that $h^i(g_0, \ldots, g_i) = (g, g_0, \ldots, g_i)$. Check that
$$d_{i+1} \circ h^i + h^{i-1} \circ d_i = Id_{\mathbb{Z}[G^{i+1}]}.$$
Now take some element $x \in \mathbb{Z}[G^{i+1}]$ which is in the kernel of d_i. Then:
$$x = \mathrm{id}_{\mathbb{Z}[G^{i+1}]}(x) = (d_{i+1} \circ h^i + h^{i-1} \circ d_i)(x) = (d_{i+1} \circ h^i)(x) + (h^{i-1} \circ d_i)(x) = d_{i+1}(h^i(x)) + 0,$$
which shows that $x \in \mathrm{im}(d_{i+1})$, so $\ker(d_i) = \mathrm{im}(d_{i+1})$ for all i. Thus the standard resolution is in fact a resolution.

Using the standard resolution, we can calculate the cohomology groups explicitly, and find properties of the elements. First, we define objects closely related to the elements of $H^i(G, A)$, and then we explore their properties from there.

Definitions 3.4:

1. An i-cochain is a G-homomorphism from $\mathbb{Z}[G^{i+1}]$ to A, i.e., an element of $\mathrm{Hom}_G(P_i, A)$.

2. An i-cocycle is an element of $\ker(d_i)$.

3. An i-coboundary is an element of $\mathrm{im}(d_{i-1})$. Thus i-coboundaries are i-cocycles.

These are groups, with the group of coboundaries a (normal) subgroup of the group of cocycles. The group $H^i(G, A)$ is given as the factor group of the cocycles modulo coboundaries.

We now cover what are called "inhomogeneous cochains" in [GS], which recover the cocycle relation that will be generalized to the non-commutative case. The relation follows from a specific choice of basis for the elements of $\mathbb{Z}[G^{i+1}]$, and calculation of the differentials in the standard resolution on them. The relation that we wish to recover for 1-cocycles is

$$a_{\sigma\tau} = a_\sigma \sigma(a_\tau).$$

Definition 3.5: Let A be a G-module. In $\mathbb{Z}[G^{i+1}]$, consider the basis elements

$$[\sigma_1, \ldots, \sigma_i] = (1, \sigma_1, \sigma_1\sigma_2, \ldots, \sigma_1 \ldots \sigma_i)$$

as a free $\mathbb{Z}[G]$-module. Note that when we apply d_i to each of these, we get

$$d_i([\sigma_1, \ldots, \sigma_i]) = \sigma_1[\sigma_2, \ldots, \sigma_i] + \sum_{j=1}^{i} (-1)^j [\sigma_1, \ldots, \sigma_j\sigma_{j+1}, \ldots, \sigma_i] + (-1)^{i+1}[\sigma_1, \ldots, \sigma_{i-1}].$$

Since the set of these form a basis for $\mathbb{Z}[G^{i+1}]$, we can identify the i-cochains with maps $[\sigma_1, \ldots, \sigma_i] \mapsto a_{\sigma_1,\ldots,\sigma_i}$, and the induced map $\mathrm{Hom}_G(\mathbb{Z}[G^i], A) \to \mathrm{Hom}_G(\mathbb{Z}[G^{i+1}], A)$ is given by

$$d_i^* : a_{\sigma_1,\ldots,\sigma_{i-1}} \mapsto \sigma_1 a_{\sigma_2,\ldots,\sigma_i} + \sum_{j=1}^{i} (-1)^j a_{\sigma_1,\ldots,\sigma_j\sigma_{j+1},\ldots,\sigma_i} + (-1)^{i+1} a_{\sigma_1,\ldots,\sigma_{i-1}}.$$

These functions $a_{\sigma_1,\ldots,\sigma_i}$ are called inhomogeneous cochains.

Remarks: This relation holds for arbitrary i in the case where A is commutative, but for this paper the most important dimensions are $i = 2$ in the commutative case and $i = 1$ in the noncommutative case. For each dimension, the relation above gives the following for cocycles and coboundaries:

$i = 2$, A commutative: in the next sections, this case will be written multiplicatively, so we do this now as well. 2-cocycles are functions $a_{\sigma,\tau}$ satisfying

$$\sigma_1(a_{\sigma_2,\sigma_3}) \cdot a^{-1}_{\sigma_1\sigma_2,\sigma_3} \cdot a_{\sigma_1,\sigma_2\sigma_3} \cdot a^{-1}_{\sigma_1,\sigma_2} = 1,$$

with coboundaries satisfying

$$a_{\sigma_1,\sigma_2} = \sigma_1(b_{\sigma_2}) \cdot b^{-1}_{\sigma_1\sigma_2} \cdot b_{\sigma_1}$$

for some 1-cochain (not necessarily cocycle) b_σ. The *Abelian group* $H^2(G, A)$ is defined to be the subgroup of 2-cocycles modulo the subgroup of 2-coboundaries.

$i=1$, A not neccesarily commutative: this case is requires a little bit of messing around to get a nice relation in the noncommutative case. What the relation above actually says is this: a 1-cocycle with values in A is a 1-cochain a_σ satisfying

$$\sigma(a_\tau)\cdot a_{\sigma\tau}^{-1}\cdot a_\sigma = 1.$$

After multiplying on the left by a_σ, on the right by a_σ^{-1}, and finally on the right again by $a_{\sigma\tau}$, we recover the cocycle relation from before,

$$a_{\sigma\tau} = a_\sigma \cdot \sigma(a_\tau).$$

Now for the coboundaries we take a different approach from the case where A is commutative. Rather than defining the subgroup of coboundaries and taking the quotient group of cocycles modulo coboundaries, we define an equivalence relation on our set of cocycles that leaves the coboundaries equivalent to the identity. Our equivalence relation is as follows: If a_σ and b_σ are two cocycles, we say $a_\sigma \sim b_\sigma$ if and only if there is some element $c \in A$ such that $c^{-1}a_\sigma\sigma(c) = b_\sigma$ for all $\sigma \in G$. In this case $H^1(G, A)$ is defined to be the *pointed set* of equivalence classes of cocycles. The distinguished point is the class of coboundaries. Though it is not a group, we will still refer to $H^1(G, A)$ as a cohomology group in the case that A may not be commutative.

Now, after one more definition, we will finally get to the results of this section.

Definition 3.6: Let $K|k$ be a field extension, and let A and B be two algebras over k. The algebras A and B are said to be $K|k$-twisted forms if $A \otimes K \cong B \otimes K$.

The fact that twisted forms are important to us can be seen by reviewing Theorem 2.9. The theorem can be restated as follows: "a k-algebra A is central simple if and only if it is a $K|k$-twisted form of the algebra $M_n(k)$ for some finite extension K of k." Thus a classification of twisted forms would help us tremendously in classifying CSAs. Such a classification comes next.

Theorem 3.7: Let A be an algebra, let $G = \mathrm{Gal}(K|k)$, and define the action of G on $\mathrm{Aut}(A \otimes K)$ to be such that $\sigma(\phi) = (\mathrm{id}_A \otimes \sigma) \circ \phi \circ (\mathrm{id}_A \otimes \sigma^{-1})$. Then the set of isomorphism classes of $K|k$-twisted forms of A is isomorphic to $H^1(G, \mathrm{Aut}(A \otimes K))$.

Proof: We sketch the proof. We first associate to each twisted form a cocycle. To associate a cocycle to B, we first fix an isomophism $\phi : A \otimes K \to B \otimes K$. Then let the cocycle b_σ associated to B to be the map $\sigma \mapsto \phi^{-1}\sigma(\phi)$. We check:

$$b_\sigma\sigma(b_\tau) = (\phi^{-1}\sigma\phi\sigma^{-1})(\sigma\phi^{-1}\tau\phi\tau^{-1}\sigma^{-1}) = \phi^{-1}\sigma\tau(\phi) = b_{\sigma\tau},$$

so it is indeed a cocycle.

Now, to show that the class of the cocycle associated to B is unchanged by the choice of the isomorphism ϕ, we take another isomorphism $\psi : A \otimes K \to B \otimes K$. Note that

$$(\psi^{-1}\phi)^{-1}\left(\psi^{-1}\sigma(\psi)\right)\sigma(\psi^{-1}\phi) = \phi^{-1}\sigma(\phi),$$

so the class of the cocycles for B in $H^1(G, A)$ is unchanged by the choice of isomorphism $A \otimes K \to B \otimes K$.

Now by Theorem 2.9, we have that the set of $K|k$-twisted forms of $M_n(k)$ is exactly the set of CSAs over k split by K with degree n. We call this set $CSA_n(K|k)$, and since $\mathrm{Aut}(M_n(K)) \cong PGL_n(K)$ (by the Skolem-Noether theorem), we have now identified $CSA_n(K|k)$ with the cohomology group $H^1(\mathrm{Gal}(K|k), PGL_n(K))$. We want to go forward and identify the entire group $Br(K|k)$ with some cohomology group, rather than just those of a certain degree. To do this, we define $PGL_\infty(K)$ with each of these as a subgroup as follows: given two integers m and n, define the map $i_{m,n} : PGL_m(K) \to PGL_{mn}(K)$ to be the map that takes some $m \times m$ matrix M to the $mn \times mn$ block matrix with n copies of M along the diagonal. We define $PGL_\infty(K)$ to be the limit of $PGL_{1\cdot 2\cdot 3\cdot \dots \cdot n}(K)$ as $n \to \infty$, such that $PGL_m(K)$ is realized as a subgroup by the inclusion $i_{m,1\cdot 2\cdot \dots \cdot n}$ for every m. This way we can have $Br(K|k) \cong H^1(Gal(K|k), PGL_\infty(K))$.

Now we have a classification of the group $Br(K|k)$ in terms of cohomology, but unfortunately the *group* $Br(K|k)$ is being identified with the *pointed set* $H^1(\mathrm{Gal}(K|k), PGL_\infty(K))$. Even worse, the module $PGL_\infty(K)$ is intractable, so hoping to understand this pointed set is likely a lost cause. Fortunately, the group $PGL_\infty(K)$ is closely related to the group $GL_\infty(K)$, which behaves more nicely. Precisely what we mean when we say that is covered in the next theorem, which is known as "Hilbert's Theorem 90."

Theorem 3.8: $H^1(G, GL_n(K)) \cong \{0\}$.

Proof. The proof here uses a more general form of Theorem 3.7. In fact, the twisted forms of an algebra are not the only time when that theorem holds – for this proof we use the fact that it holds for vector spaces. However, for a vector space, the only invariant we need to find to find its isomorphism class is its dimension. Thus the twisted forms of a vector space V are just the vector spaces already isomorphic to V, so the set of isomorphism classes of $K|k$-twisted forms of V is the one element set $\{V\}$. The set $Aut(V)$ is also the set $GL(V)$, which is $GL_n(K)$ for a vector space V of dimension n over a field K. Thus the theorem tells us that the set of $K|k$-twisted forms of V is isomorphic to $H^1(G, GL_n(K))$. Then $H^1(G, GL_n(K))$ is a one element set, so it is isomorphic to $\{0\}$ for all K and n. The same argument also works for $GL_\infty(K)$.

The next theorem will only be stated; it is described both in Proposition 2.7.1 and in Proposition 4.4.1 in [GS]. It will serve a central purpose in the proof of Theorem 3.10.

Theorem 3.9: Let G be a group and $1 \to A \to B \to C \to 1$ be an exact sequence of G-modules, such that A is commutative and contained in the center of B. (B and C need not be commutative.) Then there is an exact sequence

$$1 \to A^G \to B^G \to C^G \to H^1(G, A) \to H^1(G, B) \to H^1(G, C) \xrightarrow{\partial} H^2(G, A).$$

Though we do not prove the preceding theorem, understanding the map labeled ∂ above is very important. We describe it here, as it is used in the calculations of nearly every proposition from here on. Given a 1-cocycle $c_\sigma : G \to C$, we construct a 2-cocycle $a_{\sigma,\tau} : G^2 \to A$ using the following process. For each element $c_\sigma \in C$, lift it to an element $b_\sigma \in B$. Then to each pair of elements σ, τ in G^2, associate the element $b^*_{\sigma,\tau} = b_\sigma \sigma(b_\tau) b_{\sigma\tau}^{-1} \in B$. Since c_σ was a cocycle, the projection of this element to C gives the identity in C. Then by the exactness of the sequence, there must be some element $a_{\sigma,\tau}$ that maps to $b^*_{\sigma,\tau}$. The map taking (σ, τ) to this $a_{\sigma,\tau}$ is the image of c_σ under ∂. It is crucial that choosing a different lift b_σ will give the same element $\partial(c_\sigma) = a_{\sigma,\tau} \in H^2(G, A)$; while the construction will yield a different cocycle, we find that it will be in the same class regardless of the choice of lift.

The final proposition for this section takes us back to the Brauer group by associating it to some cohomology groups. It uses Theorem 3.7 as a starting point, associating $Br(K|k)$ to $H^1(\mathrm{Gal}(K|k), PGL_\infty(K))$, and then uses Theorems 3.8 and 3.9 to show that it is also isomorphic to $H^2(\mathrm{Gal}(K|k), K^\times)$, which is easier to deal with.

Theorem 3.10: The objects $Br(K|k)$, $H^1(Gal(K|k), PGL_\infty(K))$, and $H^2(Gal(K|k), K^\times)$ are all isomorphic (as pointed sets).

Proof. A full proof of this is found in the reference [GS], and is not reproduced here. A sketch is as follows. The first two objects are isomorphic because of Theorem 3.7 and the remarks following it (regarding inclusion maps of $PGL_n(K)$ into $PGL_{mn}(K)$). For the second two groups, consider the exact sequence

$$1 \to K^\times \to GL_\infty(K) \to PGL_\infty(K) \to 1$$

and applying Theorem 3.9 to it, we get the smaller exact sequence

$$H^1(G, GL_\infty(K)) \to H^1(G, PGL_\infty(K)) \xrightarrow{\partial} H^2(G, K^\times).$$

Since the first group is trivial by Theorem 3.8, the map ∂ is injective. Then the surjectivity of this map is all that is in doubt, and is also established by a clever diagram chase.

4 Calculations of Cocycles in $Br(K|k)$

In this section we calculate the 2-cocycles associated to quaternion and cyclic algebras over a field for certain splitting fields. To do so, we use the explicit description of the set $H^1(\mathrm{Gal}(K|k), PGL_n(K))$ in terms of twisted forms of $M_n(K)$, and our map ∂ which induces the isomorphism $H^1(\mathrm{Gal}(K|k), PGL_n(K)) \xrightarrow{\sim} H^2(Gal(K|k), K^\times)$. Recall that the action of $\mathrm{Gal}(K|k)$ on $A \otimes K$ is $g \cdot (a \otimes \lambda) = a \otimes g(\lambda)$, where g is viewed as a map $K \to K$. Our general strategy for these computations is this: first, for an algebra A, we fix an isomorphism $\phi\colon A \otimes K \xrightarrow{\sim} M_n(K)$, and then we calculate using Theorem 3.7 what a 1-cocycle $c_\sigma \in H^1(\mathrm{Gal}(K|k), PGL_n(K))$ associated to A is. Then we calculate $\partial(c_\sigma)$. Recall that to do this, we choose a specific lift b_σ of c_σ. Then, using the action $\sigma \cdot \phi = \sigma \circ \phi \circ \sigma^{-1}$, we calculate the values $b_\sigma \sigma(b_\tau) b_{\sigma\tau}^{-1}$ for all $\sigma, \tau \in Gal(K|k)$. Finally, we see that these are scalar matrices, and thus obtained from the inclusion $K^\times \to GL_n(K)$. The cocycle $a_{\sigma,\tau}$ associated to our algebra associates to each pair of group elements σ and τ the scalar along the diagonal of this matrix $b_\sigma \sigma(b_\tau) b_{\sigma\tau}^{-1}$. This process will be used throughout this section, as well as the last two sections in which we find cocycles in slightly different cases.

Note: in this section and others, we employ a particular abuse of notation where the elements of $GL_m(K)$ are not distinguished from their images in $PGL_m(K)$. This does not cause any problems, especially as most of the calculations themselves occur in $GL_m(K)$.

Proposition 4.1: Let $A = \left(\frac{a,b}{k}\right)$, and let $K = k(\sqrt{b})$ be a splitting field for A. Further let $\mathrm{Gal}(K|k) = \{e, g\}$ where g is the non-identity element. Then the class $[A]$ in $Br(K|k)$ is given by the cocycle $a_{\sigma,\tau}$:

$$a_{\sigma,\tau} = \begin{cases} 1, & \sigma = e \text{ or } \tau = e \\ a, & \sigma = \tau = g \end{cases}.$$

Proof. To find the 2-cocycle associated to A, we first have to find the 1-cocycle associated to A. To find that, we first have to define an isomorphism $\phi : A \otimes K \to M_n(K)$. We use this one:

$$\phi : w + xi + yj + zk \mapsto w \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + x \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix} + y \begin{pmatrix} \sqrt{b} & 0 \\ 0 & -\sqrt{b} \end{pmatrix} + z \begin{pmatrix} 0 & -a\sqrt{b} \\ \sqrt{b} & 0 \end{pmatrix}$$

where w, x, y, z are all in K. We then find $\phi^{-1} g(\phi)$ on each basis element:

$$(\phi^{-1} g \phi g^{-1})(1) = 1, \quad (\phi^{-1} g \phi g^{-1})(i) = i,$$

$$(\phi^{-1} g \phi g^{-1})(j) = -j, \quad (\phi^{-1} g \phi g^{-1})(k) = -k$$

The initial idea then is to conjugate by i in A, which would be given by $\phi(i)$ in $PGL_2(K)$, as the automorphism group of $M_2(K)$. We can check:

$$\begin{pmatrix} 0 & 1 \\ a^{-1} & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ a^{-1} & 0 \end{pmatrix} \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ a^{-1} & 0 \end{pmatrix} \begin{pmatrix} \sqrt{b} & 0 \\ 0 & -\sqrt{b} \end{pmatrix} \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -\sqrt{b} & 0 \\ 0 & \sqrt{b} \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ a^{-1} & 0 \end{pmatrix} \begin{pmatrix} 0 & -a\sqrt{b} \\ \sqrt{b} & 0 \end{pmatrix} \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a\sqrt{b} \\ -\sqrt{b} & 0 \end{pmatrix}$$

which is exactly the automorphism we were looking for. Using the class of I_2 will obviously work for e, since $\phi^{-1}e(\phi)$ fixes everything, as does conjugation by the identity. The 1-cocycle is then determined, with $c_e = I_2, c_g = \phi(i) =: M$. The transfer to the 2-cocycle is then this: Take a lifting b_σ from c_σ to $GL_2(K)$. The one we use is to write them the same (here the abuse of notation mentioned above comes in handy!), and then we set $a_{\sigma,\tau}$ to be the element of K that maps to $b_\sigma \sigma(b_\tau) b_{\sigma\tau}^{-1}$. This gives

σ	τ	$b_\sigma \sigma(b_\tau) b_{\sigma\tau}^{-1}$	$\leftarrow$	$a_{\sigma,\tau}$
e	e	$I_2 I_2 I_2^{-1} = I_2$	$\leftarrow$	1
e	g	$I_2 M M^{-1} = I_2$	$\leftarrow$	1
g	e	$M I_2 M^{-1} = I_2$	$\leftarrow$	1
g	g	$M M I_2^{-1} = M^2$	$\leftarrow$	a

since $M^2 = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$. This proves the proposition.

This may seem a little odd, since it seems to forget completely about b. The next proposition does this again, and after we will try to explain why this happens.

Proposition 4.2: Let $K|k$ be a cyclic extension of degree m with galois group $G = \langle g \rangle$, and let A be the cyclic algebra over k generated by K and y with $y^m = a$. The 2-cocycle associated to $[A]$ in $Br(K|k)$ is given by the cocycle $a_{\sigma,\tau}$:

$$a_{g^p,g^q} = \begin{cases} 1, & p+q < m \\ a, & p+q \geq m \end{cases}$$

Proof. as above, we first have to go through the 1-cocycle, which requires a specific isomorphism. Our extension K is generated by some β, along with $g(\beta)$, $g^2(\beta)$, ... which leads us to this isomorphism $\phi : A \otimes K \to M_n(K)$ with

$$\phi(y \otimes 1) = \begin{pmatrix} 0 & \dots & 0 & a \\ 1 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & 0 \end{pmatrix}, \quad \phi(\beta \otimes 1) = \begin{pmatrix} \beta & 0 & \dots & 0 \\ 0 & g^{m-1}(\beta) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & g(\beta) \end{pmatrix}.$$

Again, a simple check reveals that $\phi(y)^{-1}\phi(\beta)\phi(y) = \phi(g(\beta))$, which is the only relation we have to check. (The rest follow from the fact that g is an automorphism.) This also shows where we're going with the 1-cocycle, but first a quick remark about the natural action of G on $A \otimes K$.

We say that A includes the elements of K, but it would be more appropriate to say that A contains a commutative subalgebra isomorphic to K. As such, the natural action of G on $A \otimes K$ fixes elements in $A \otimes k$. This means $g(\beta \otimes 1) = \beta \otimes 1$, while $g(1 \otimes \beta) = 1 \otimes g(\beta)$.

The 1-cocycle c_σ can be extrapolated from the value of c_g, since G is cyclic. Note:

$$\phi^{-1}(g(\phi(g^{-1}(\beta \otimes 1)))) = g(\beta) \otimes 1.$$

This means that the value of c_g should be $\phi(y \otimes 1)$, and $c_{g^p} = \phi(y \otimes 1)^p$. After lifting c_σ to b_σ, we get

$$b_{g^p} g^p(b_{g^q}) b_{g^{p+q}}^{-1} = \phi(y)^{p+q} \cdot b_{g^{p+q}}^{-1}.$$

If $p+q$ is less than m, then $b_{g^{p+q}}$ is just $\phi(y)^{-p-q}$, but if $p+q$ is m or more we have $b_{g^{p+q}} = \phi(y)^{-p-q+m}$. These two cases, along with the fact that $\phi(y)^m = aI$ give us our 2-cocycle $a_{\sigma,\tau}$ as described above,

$$a_{g^p,g^q} = \begin{cases} 1, & p+q < m \\ a, & p+q \geq m \end{cases}.$$

Remarks:

1. Proposition 4.2 reduces to proposition 4.1 in the case $m = 2$, since we can take $K = k(\sqrt{b})$, $\beta = \sqrt{b}$, $g(\beta) = -\beta = -\sqrt{b}$ and $y = i$. This is what we expect, since this is how we view quaternion algebras as cyclic algebras.

2. Here, we notice a peculiar property that we mentioned briefly before. When we find the cocycle associated to the algebra $\left(\frac{a,b}{k}\right)$, the cocycle only seems to mention a, and "forget" about b, because the only constant present in the cocycle is a. In the more general construction of Proposition 4.2, we seem to remember a, but lose β. To see why this happens, we have to think about what group we are working in: in each case, the fact that we are working in $Br(K|k)$ for various extensions K implicitly assumes that our algebra is split by K. In the quaternion algebra case, it means that our algebra is isomorphic to $\left(\frac{x,b}{k}\right)$ for some x, and the cocycle just gives us a particular value for x. We explore this further in next two propositions by giving cocycles for a quaternion algebra over different splitting fields. Patterns we see in these next calculations transition us into the next section.

Proposition 4.3: Let $A = \left(\frac{a,b}{k}\right)$, and let $K = k(\sqrt{a}, \sqrt{b})$ be a splitting field for A. We write the elements of the Galois group $G = Gal(K|k)$ as $\{e, g_a, g_b, g_{ab}\}$, where e is the identity on K and g_a fixes $k(\sqrt{a})$ while sending $\sqrt{b}$ and $\sqrt{ab}$ to their negatives. The other Galois elements g_b and g_{ab} are defined similarly. A 2-cocycle associated to A in $Br(K|k)$ is given in the following table, where σ is given by the column and τ is given by the row.

$\tau \backslash \sigma$	e	g_a	g_b	g_{ab}
e	1	1	1	1
g_a	1	a	-1	$-a$
g_b	1	1	b	b
g_{ab}	1	a	$-b$	$-ab$

Proof. Again, we first have to fix an isomorphism $\phi : A \otimes K \to M_2(K)$. Since $i \otimes 1$ and $j \otimes 1$ generate $A \otimes K$ as a K-algebra, we just specify their images:

$$\phi(i \otimes 1) = \begin{pmatrix} 0 & \sqrt{a} \\ \sqrt{a} & 0 \end{pmatrix}, \quad \phi(j \otimes 1) = \begin{pmatrix} \sqrt{b} & 0 \\ 0 & -\sqrt{b} \end{pmatrix}.$$

Now we find the 1-cocycle $c_\sigma : G \to PGL_2(K)$.

$$c_e = I, \quad c_{g_a} = \phi(i \otimes 1), \quad c_{g_b} = \phi(j \otimes 1), \quad c_{g_{ab}} = \phi(k \otimes 1).$$

We use I, M_a, M_b, and M_{ab} as shorthand for each of these respectively. For each, we compute $b_\sigma \sigma(b_\tau) b_{\sigma\tau}^{-1}$ for the lifting b_σ:

σ	τ	$b_\sigma \sigma(b_\tau) b_{\sigma\tau}^{-1}$	$\leftarrow$	$a_{\sigma,\tau}$
e	e	$Ie(I)I^{-1} = I$	$\leftarrow$	1
e	g_a	$Ie(M_a)M_a^{-1} = I$	$\leftarrow$	1
e	g_b	$Ie(M_b)M_b^{-1} = I$	$\leftarrow$	1
e	g_{ab}	$Ie(M_{ab})M_{ab}^{-1} = I$	$\leftarrow$	1
g_a	e	$M_a g_a(I)M_a^{-1} = I$	$\leftarrow$	1
g_a	g_a	$M_a g_a(M_a)I^{-1} = aI$	$\leftarrow$	a
g_a	g_b	$M_a g_a(M_b)M_{ab}^{-1} = -I$	$\leftarrow$	-1
g_a	g_{ab}	$M_a g_a(M_{ab})M_b^{-1} = -aI$	$\leftarrow$	$-a$
g_b	e	$M_b g_b(I)M_b^{-1} = I$	$\leftarrow$	1
g_b	g_a	$M_b g_b(M_a)M_{ab}^{-1} = I$	$\leftarrow$	1
g_b	g_b	$M_b g_b(M_b)I^{-1} = bI$	$\leftarrow$	b
g_b	g_{ab}	$M_b g_b(M_{ab})M_a^{-1} = bI$	$\leftarrow$	b
g_{ab}	e	$M_{ab} g_{ab}(I)M_{ab}^{-1} = I$	$\leftarrow$	1
g_{ab}	g_a	$M_{ab} g_{ab}(M_a)M_b^{-1} = aI$	$\leftarrow$	a
g_{ab}	g_b	$M_{ab} g_{ab}(M_b)M_a^{-1} = -bI$	$\leftarrow$	$-b$
g_{ab}	g_{ab}	$M_{ab} g_{ab}(M_{ab})I^{-1} = -abI$	$\leftarrow$	$-ab$

Many of these calculations follow from the fact that $M_{ab} = M_a M_b = -M_b M_a$. This fits with the table we started with, so we're done.

Proposition 4.4: Let A, K, and G be as above. Another cocycle associated to A in $Br(K|k)$ is given by this table:

$\tau \backslash \sigma$	e	g_a	g_b	g_{ab}
e	1	1	1	1
g_a	1	a	1	a
g_b	1	1	1	1
g_{ab}	1	a	1	a

Proof. Here we fix a new isomorphism, but we "forget" that $\sqrt{a}$ is an option. Define $\phi : A \otimes K \to M_2(K)$:

$$\phi(i \otimes 1) = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}, \quad \phi(j \otimes 1) = \begin{pmatrix} \sqrt{b} & 0 \\ 0 & -\sqrt{b} \end{pmatrix}.$$

This is exactly the same isomorphism we used for $K = k(\sqrt{b})$. As such, we will get a similar 1-cocycle:

$$c_e = c_{g_b} = I, \quad c_{g_a} = c_{g_{ab}} = \phi(i \otimes 1).$$

Again we use M as shorthand for $\phi(i \otimes 1)$. Recreating the calculations from the last proof:

σ	τ	$b_\sigma \sigma(b_\tau) b_{\sigma\tau}^{-1}$	$\leftarrow$	$a_{\sigma,\tau}$
e	e	$Ie(I)I^{-1} = I$	$\leftarrow$	1
e	g_a	$Ie(M)M^{-1} = I$	$\leftarrow$	1
e	g_b	$Ie(I)I^{-1} = I$	$\leftarrow$	1
e	g_{ab}	$Ie(M)M^{-1} = I$	$\leftarrow$	1
g_a	e	$Mg_a(I)M^{-1} = I$	$\leftarrow$	1
g_a	g_a	$Mg_a(M)I^{-1} = aI$	$\leftarrow$	a
g_a	g_b	$Mg_a(I)M^{-1} = I$	$\leftarrow$	1
g_a	g_{ab}	$Mg_a(M)I^{-1} = aI$	$\leftarrow$	a
g_b	e	$Ig_b(I)I^{-1} = I$	$\leftarrow$	1
g_b	g_a	$Ig_b(M)M^{-1} = I$	$\leftarrow$	1
g_b	g_b	$Ig_b(I)I^{-1} = I$	$\leftarrow$	1
g_b	g_{ab}	$Ig_b(M)M^{-1} = I$	$\leftarrow$	1
g_{ab}	e	$Mg_{ab}(I)M^{-1} = I$	$\leftarrow$	1
g_{ab}	g_a	$Mg_{ab}(M)I^{-1} = aI$	$\leftarrow$	a
g_{ab}	g_b	$Mg_{ab}(I)M^{-1} = I$	$\leftarrow$	1
g_{ab}	g_{ab}	$Mg_{ab}(M)I^{-1} = aI$	$\leftarrow$	a

which again agrees with our stated table.

Remark: The tables created above have a curious property. When you cover up certain rows and columns in the table for $\left(\frac{a,b}{k}\right)$ in $Br(k(\sqrt{a},\sqrt{b})|k)$, you get cocycles for the same algebra in the smaller Brauer group $Br(k(\sqrt{b})|k)$. For example, only looking at the rows and columns associated to e and g_a gives the table

$\tau\backslash\sigma$	e	g_a
e	1	1
g_a	1	a

while looking at the rows and columns for e and g_{ab} gives the table

$\tau\backslash\sigma$	e	g_{ab}
e	1	1
g_{ab}	1	$-ab$

The first is the table for $\left(\frac{a,b}{k}\right)$ in the smaller group, while the second is the table for $\left(\frac{-ab,b}{k}\right)$ as we constructed above. These two algebras are in fact isomorphic, since we can use k and j in the place of i and j in the first one and get the presentation as the second. This property is reason to believe that we can construct natural maps from the group $Br(K|k)$ to the group $Br(L|k)$ whenever $L|K|k$ is a tower of Galois field extensions, "inflating" the table in $Br(K|k)$ to a larger one in $Br(L|k)$. The next section talks about these maps, which exist for more arbitrary cohomology groups, called inflation maps.

5 Maps between $Br(K|k)$ and $Br(L|k)$

The property of the above table leads us to believe that, when we have a tower of extensions $L|K|k$, we should have a map between $Br(K|k)$ and $Br(L|k)$. This map is, in fact, a map that exists more generally between cohomology groups: inflation maps. As such, we have a slight detour into more group cohomology to define these inflation maps, before coming back to the focus of our paper, the Brauer groups. Before we define these maps, we first show that they will apply.

Remark Let $L|K|k$ be a tower of field extensions, so that L/K, L/k, and K/k are all Galois. The groups $\mathrm{Gal}(L|k)$, $\mathrm{Gal}(L|K)$, and $\mathrm{Gal}(K|k)$ fit into the following short exact sequence:

$$1 \to \mathrm{Gal}(L|K) \to \mathrm{Gal}(L|k) \to \mathrm{Gal}(K|k) \to 1.$$

This is a standard fact from Galois theory. The reason we mention this is that, if we take $G = \mathrm{Gal}(L|k)$ and $H = \mathrm{Gal}(L|K)$, the quotient group G/H is isomorphic to $\mathrm{Gal}(K|k)$. This is important, as we will see when we define inflation maps.

Proposition 5.1: If A is a G-module and H is a normal subgroup of G, then A^H, the set of elements of A fixed by H, is a G/H module.

Proof. We just have to show that A^H is stable under the action of G. To see this, take $g \in G, h \in H$, and $a \in A^H$, and considering

$$h(g(a)) = g(g^{-1}hg)(a) = g(h'(a)) = g(a)$$

shows that $g(a)$ is fixed by h for every $g \in G, h \in H$, and $a \in A^H$.

In particular, take $G = \mathrm{Gal}(L/k)$ and $H = \mathrm{Gal}(L/K)$ as above, and look at the G-module $L^\times$. The G/H module $(L^\times)^H$ is just $K^\times$ as a $\mathrm{Gal}(K/k)$-module in the natural way.

We would now like to construct the inflation maps. Given an i-cocycle $a_{\sigma_1,\ldots,\sigma_i}$ representing a class in $H^i(G/H, A^H)$, we would like to construct an i-cocycle $\inf(a_{\sigma_1,\ldots,\sigma_i})$ representing a class in $H^i(G, A)$. Concretely, the i-cocycle for G is a function $G^i \to A$, while the i-cocycle that we start with is a function $(G/H)^i \to A^H$. The natural thing to do is to set

$$\inf(a_{\sigma_1,\ldots,\sigma_i})_{g_1,\ldots,g_i} := a_{g_1H,\ldots,g_iH},$$

where gH denotes the equivalence class of g in G/H. The next proposition shows us that there are natural, well-defined maps $H^i(G/H, A^H) \to H^i(G, A)$, and tracing through with the standard resolution will give us that the map we define below is the map described above.

Proposition 5.2: Let H be a normal subgroup of a group G. There exist natural maps $\inf : H^i(G/H, A^H) \to H^i(G, A)$ for all i.

Proof. We construct these maps, by setting up the construction of the cohomology groups in Definition 3.2. Let P_* be a projective resolution of $\mathbb{Z}$ as a trivial G-module, and let Q_* be a projective resolution of $\mathbb{Z}$ as a trivial G/H-module. Using the projection $G \to G/H$, we can also view each Q_i as a G-module. By using the fact that the P_i are projective, this gives us natural maps α_i so that the diagram

$$\begin{array}{ccccccccc}
\ldots & \to & P_2 & \xrightarrow{p_2} & P_1 & \xrightarrow{p_1} & P_0 & \xrightarrow{p_0} & \mathbb{Z} & \to & 0 \\
 & & \downarrow \alpha_2 & & \downarrow \alpha_1 & & \downarrow \alpha_0 & & \downarrow Id_{\mathbb{Z}} & & \\
\ldots & \to & Q_2 & \xrightarrow{q_2} & Q_1 & \xrightarrow{q_1} & Q_0 & \xrightarrow{q_0} & \mathbb{Z} & \to & 0
\end{array}$$

of G-modules commutes. Each α_i induces a map $\mathrm{Hom}_G(Q_i, A^H) \to \mathrm{Hom}_G(P_i, A^H)$, which preserves the images and kernels of the boundary maps induced by the p_i and q_i. Further, since H fixes every element of A^H, $\mathrm{Hom}_{G/H}(Q_i, A^H) = \mathrm{Hom}_G(Q_i, A^H)$, which means these induce nice maps $\mathrm{Hom}_{G/H}(Q_i, A^H) \to \mathrm{Hom}_G(P_i, A^H)$. They then induce homomorphisms $H^i(G/H, A^H) \to H^i(G, A^H)$. We now use the inclusion map $A^H \to A$, gives us a natural homomorphism $H^i(G, A^H) \to H^i(G, A)$. Composing these two gives us the inflation maps

$$\inf : H^i(G/H, A^H) \to H^i(G, A)$$

for all i.

To see why these inflation maps are useful, we invoke the first remark in this section. If $L|K|k$ is a tower of Galois field extensions, we write $G = \mathrm{Gal}(L/k)$, $H = \mathrm{Gal}(L/K)$, and we get $G/H \cong \mathrm{Gal}(K|k)$. Now if we take $L^\times$ as our A, we have $K^\times$ as our A^H, and we get a natural map for $i = 2$ in particular,

$$\inf : H^2(\mathrm{Gal}(K|k), K^\times) \to H^2(\mathrm{Gal}(L|k), L^\times),$$

which is in fact a map $Br(K|k) \to Br(L|k)$, whose construction is the point of this section. To finish our discussion of inflation maps, we try to recover the cocycle for $\left(\frac{a,b}{k}\right)$ we found in Proposition 4.4 from the one we found in Proposition 4.1.

Construction 5.3: Take k a field, $K = k(\sqrt{b})$, and $L = k(\sqrt{a}, \sqrt{b})$. The Galois groups $G = \mathrm{Gal}(L|k)$ and $G/H = \mathrm{Gal}(K|k)$ (where $H = \mathrm{Gal}(L|K)$) will be denoted as in the previous section, with $G/H = \{e, g\}$ and $G = \{e, g_a, g_b, g_{ab}\}$. The projection map $G \to G/H$ takes e and g_b to e and takes g_a and g_{ab} to g. Then take the cocycle $a_{\sigma,\tau}$ for $\left(\frac{a,b}{k}\right)$ in $Br(K|k)$ as described in Proposition 4.1. We construct a cocycle $a'_{\sigma,\tau}$ for that algebra in $Br(L|k)$:

σ	τ	$a'_{\sigma,\tau}$
e	e	$a_{e,e} = 1$
e	g_a	$a_{e,g} = 1$
e	g_b	$a_{e,e} = 1$
e	g_{ab}	$a_{e,g} = 1$
g_a	e	$a_{g,e} = 1$
g_a	g_a	$a_{g,g} = a$
g_a	g_b	$a_{g,e} = 1$
g_a	g_{ab}	$a_{g,g} = a$
g_b	e	$a_{e,e} = 1$
g_b	g_a	$a_{e,g} = 1$
g_b	g_b	$a_{e,e} = 1$
g_b	g_{ab}	$a_{e,g} = 1$
g_{ab}	e	$a_{g,e} = 1$
g_{ab}	g_a	$a_{g,g} = a$
g_{ab}	g_b	$a_{g,e} = 1$
g_{ab}	g_{ab}	$a_{g,g} = a$

which fits into the table we constructed in proposition 4.4:

$\tau \backslash \sigma$	e	g_a	g_b	g_{ab}
e	1	1	1	1
g_a	1	a	1	a
g_b	1	1	1	1
g_{ab}	1	a	1	a

Remark: Finally, we mention that $Br(k)$ itself is identified with $Br(k_{sep}|k)$ for some separable closure k_{sep} of k. This means that if we let G be the Galois group $\mathrm{Gal}(k_{sep}|k)$, we have $Br(k) \cong H^2(G, k_{sep}^{\times})$. Further, since k_{sep} is a Galois extension of k, if we have a specific presentation of G, we can use inflation maps as above to find cocycles for algebras in $Br(k)$ once we have a cocycle in $Br(K|k)$, so that working in the smaller groups $Br(K|k)$ gives us all the information we need to work in the absolute Brauer group $Br(k)$.

6 Cocycles for tensor products

Remember that all the work we did in Section 3 only established that the group $Br(K|k)$ and the group $H^2(\mathrm{Gal}(K|k), K^{\times})$ are isomorphic as pointed sets. Here, we present some evidence that they are in fact isomorphic as groups, although we still fall short of proving it. In this section we calculate the cocycles associated to certain tensor products of quaternion algebras and cyclic algebras. First, we calculate the cocycle associated to a tensor product of two quaternion algebras split by the same quadratic extension, and then we use this result to find a presentation of the tensor products of two quaternion algebras split by the same quadratic extension. Finally, we calculate the cocycle associated to a tensor product of two cyclic algebras, and observe what algebra this means that tensor product should be isomorphic to.

First, however, we require the Kronecker product of matrices, to create an isomorphism from $M_m(K) \otimes M_n(K)$ to $M_{mn}(K)$. This isomorphism is very simple; if $\{e_{i,j}\}$ is a basis for $M_m(K)$ and $\{e'_{k,l}\}$ is a basis or $M_n(K)$, and $\{f_{p,q}\}$ is a basis for $M_{mn}(K)$, then we map $e_{i,j} \otimes e_{k,l}$ to $f_{i+mk,j+ml}$. Then if $A = (a_{ij})$ is an $m \times m$ matrix and $B = (b_{kl})$ is an $n \times n$ matrix, then the under the isomorphism we get

$$A \otimes B \mapsto \begin{pmatrix} b_{11}A & \dots & b_{1n}A \\ \vdots & \ddots & \vdots \\ b_{n1}A & \dots & b_{nn}A \end{pmatrix},$$

which is a block matrix where each $m \times m$ block is a scalar multiple of A. This allows us to extend our isomorphisms we obtained in the third section to isomorphisms of tensor products of such algebras.

Proposition 6.1: The cocycle for $\left(\frac{a,c}{k}\right) \otimes \left(\frac{b,c}{k}\right)$ in $Br(k(\sqrt{c})|k)$ is given by the table

$\tau \backslash \sigma$	e	g
e	1	1
g	1	ab

Proof. Let $\{1_a, i_a, j_a, k_a\}$ be a basis for $A = \left(\frac{a,c}{k}\right)$, and similarly $\{1_b, i_b, j_b, k_b\}$ for $B = \left(\frac{b,c}{k}\right)$. We define our isomorphism $\phi : (A \otimes B) \otimes K \to M_4(K)$ on the generators $i_a \otimes i_b \otimes 1$, $j_a \otimes i_b \otimes 1$,

$i_a \otimes j_b \otimes 1$, and $j_a \otimes j_b \otimes 1$:

$$\phi(i_a \otimes i_b \otimes 1) = \begin{pmatrix} 0 & 0 & 0 & ab \\ 0 & 0 & b & 0 \\ 0 & a & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \qquad \phi(i_a \otimes j_b \otimes 1) = \begin{pmatrix} 0 & a\sqrt{c} & 0 & 0 \\ \sqrt{c} & 0 & 0 & 0 \\ 0 & 0 & 0 & -a\sqrt{c} \\ 0 & 0 & -\sqrt{c} & 0 \end{pmatrix},$$

$$\phi(j_a \otimes i_b \otimes 1) = \begin{pmatrix} 0 & 0 & b\sqrt{c} & 0 \\ 0 & 0 & 0 & -b\sqrt{c} \\ \sqrt{c} & 0 & 0 & 0 \\ 0 & -\sqrt{c} & 0 & 0 \end{pmatrix}, \qquad \phi(j_a \otimes j_b \otimes 1) = \begin{pmatrix} c & 0 & 0 & 0 \\ 0 & -c & 0 & 0 \\ 0 & 0 & -c & 0 \\ 0 & 0 & 0 & c \end{pmatrix}.$$

These come exactly from the Kronecker product of matrices discussed above, as well as the isomorphism $\left(\frac{x,c}{k}\right) \otimes k(\sqrt{c}) \xrightarrow{\sim} M_2(k(\sqrt{c}))$ that we constructed in Proposition 4.4. The cocycle for e fixes every one of these, so as usual, it is associated to conjugation by the identity I. On the other hand, the cocycle for g fixes $i_a \otimes i_b \otimes 1$ and $j_a \otimes j_b \otimes 1$ while taking $i_a \otimes j_b \otimes 1$ and $j_a \otimes i_b \otimes 1$ to their negatives. At this point, this could be represented by either $\phi(i_a \otimes i_b \otimes 1)$ or $\phi(j_a \otimes j_b \otimes 1)$ in $PGL_4(K)$, but the choice of which to use is made clear when you look at how it acts on $1_a \otimes i_b \otimes 1$ and $i_a \otimes 1_b \otimes 1$ (by fixing them) and on $1_a \otimes j_b \otimes 1$ and $j_a \otimes 1_b \otimes 1$ (by taking them to their negatives). Here it is clear that the 1-cocycle should be:

$$c_e = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad c_g = \begin{pmatrix} 0 & 0 & 0 & ab \\ 0 & 0 & b & 0 \\ 0 & a & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Now taking our usual convention of lifting c_σ to b_σ, (denoting $b_g = M$) noting that $b_g^2 = M^2 = abI_4$, we can fill in our 2-cocycle $a_{\sigma,\tau} : G^2 \to K^\times$ as follows:

σ	τ	$b_\sigma \sigma(b_\tau) b_{\sigma\tau}^{-1}$	$\leftarrow$	$a_{\sigma,\tau}$
e	e	$Ie(I)I^{-1} = I$	$\leftarrow$	1
e	g	$Ie(M)M^{-1} = I$	$\leftarrow$	1
g	e	$Me(I)M^{-1} = I$	$\leftarrow$	1
g	g	$Mg(M)I^{-1} = M^2$	$\leftarrow$	ab

which is exactly the table given in the statement.

The previous proposition suggests that the class of $\left(\frac{a,c}{k}\right) \otimes \left(\frac{b,c}{k}\right)$ should be the same as the class of $\left(\frac{ab,c}{k}\right)$ in $Br(K|k)$ (and thus in $Br(k)$ since $Br(K|k)$ is a subgroup of that), so by looking at degrees we would guess:

$$\left(\frac{a,c}{k}\right) \otimes \left(\frac{b,c}{k}\right) \cong \left(\frac{ab,c}{k}\right) \otimes M_2(k) \cong M_2\left(\left(\frac{ab,c}{k}\right)\right).$$

The next proposition is a direct proof of this statement, taken almost directly from [Lam].

Proposition 6.2: The isomorphism above holds.

Proof. We find a basis for the first algebra that acts like a standard basis for the second algebra, which shows that the first isomorphism holds. The second isomorphism does not need to be proven.

First, let the bases of $\left(\frac{x,c}{k}\right)$ be as in the previous proposition. Then set

$$1 = 1_a \otimes 1_b,\ I = i_a \otimes i_b,\ J = j_a \otimes 1_b,\ K = k_a \otimes i_b,$$
$$1 = 1_a \otimes 1_b,\ I' = 1_a \otimes i_b,\ J' = j_a \otimes k_b,\ K' = -b(j_a \otimes j_b),$$

and let X be the span of $\{1, I, J, K\}$ while Y is the span of $\{1, I', J', K'\}$. Note that

$$I^2 = i_a^2 \otimes i_b^2 = ab1,\ J^2 = j_a^2 \otimes 1_b^2 = c1,\ -JI = -j_a i_a \otimes i_b = i_a j_a \otimes i_b = IJ,$$

so X is isomorphic to $\left(\frac{ab,c}{k}\right)$. Further,

$$I'^2 = 1_a^2 \otimes i_b^2 = b1,\ J'^2 = j_a^2 \otimes k_b^2 = -bc^2 1,\ -J'I' = j_a \otimes -k_b i_b = j_a \otimes i_b k_b = I'J',$$

which means Y is isomorphic to $\left(\frac{b,-bc^2}{k}\right)$, which is split because it is not a division algebra. In particular, $(ci+j)(-ci-j) = -c^2i^2 - cij - cji - j^2 = -c^2b - cij + cij + c^2b = 0$, so we have zero divisors. So $X \otimes Y \cong M_2\left(\left(\frac{ab,c}{k}\right)\right)$. Thus if $A \otimes B \cong X \otimes Y$, we're done. This is true because the elements of X commute with the elements of Y, and because together they generate the whole space $A \otimes B$. This proves the proposition.

Proposition 6.1 gave us insight into the isomorphism class of $\left(\frac{a,c}{k}\right) \otimes \left(\frac{b,c}{k}\right)$, and Proposition 6.2 showed us that the insight was correct. The next proposition will give us a similar insight for cyclic algebras.

Proposition 6.3: Let $K|k$ be a cyclic field extension of degree n with galois group $G = \langle g \rangle$. Let $A = \langle K, x | x^n = a,\ x^{-1}\lambda x = g(\lambda)\, \forall \lambda \in K\rangle$ and $B = \langle K, y | y^n = b,\ y^{-1}\lambda y = g(\lambda)\, \forall \lambda \in K\rangle$ be cyclic algebras over k. Then a cocycle for $A \otimes B$ in $Br(K|k)$ is given by

$$a_{g^p,g^q} = \begin{cases} 1, & p+q < n \\ ab, & p+q \geq n \end{cases}.$$

Thus we have an isomorphism $A \otimes B \cong M_n(C)$, where $C = \langle K, z | z^n = ab,\ z^{-1}\lambda z = g(\lambda)\, \forall \lambda \in K\rangle$ is a cyclic algebra over k.

Proof. Let $K = k(t)$. As in the quaternion case, we start with an isomorphism ϕ from $(A \otimes B) \otimes K$ to $M_{n^2}(K)$. We use block matrices to do this. To make the notation easier, let T, M_a, and M_b be defined as:

$$T = \begin{pmatrix} t & 0 & \dots & 0 \\ 0 & g^{n-1}(t) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & g(t) \end{pmatrix}$$

$$M_a = \left(\begin{array}{c:c} 0 & a \\ \hdashline I_{n-1} & 0 \end{array}\right)$$

$$M_b = \left(\begin{array}{c:c} 0 & b \\ \hdashline I_{n-1} & 0 \end{array}\right)$$

Then for our isomorphism ϕ, we set

$$\phi((t \otimes 1) \otimes 1) = \left(\begin{array}{c:c:c} T & \dots & 0 \\ \hdashline \vdots & \ddots & \vdots \\ \hdashline 0 & \dots & T \end{array}\right),$$

$$\phi((1 \otimes t) \otimes 1) = \left(\begin{array}{c:c:c} tI_n & \dots & 0 \\ \hdashline \vdots & \ddots & \vdots \\ \hdashline 0 & \dots & g(t)I_n \end{array}\right),$$

$$\phi((x \otimes 1) \otimes 1) = \left(\begin{array}{c:c:c} M_a & \dots & 0 \\ \hdashline \vdots & \ddots & \vdots \\ \hdashline 0 & \dots & M_a \end{array}\right),$$

$$\phi((1 \otimes y) \otimes 1) = \left(\begin{array}{c:c} 0 & bI_n \\ \hdashline I_{n^2-n} & 0 \end{array}\right).$$

This gives in particular:

$$\phi((x \otimes y) \otimes 1) = \left(\begin{array}{c:c:c:c} 0 & \dots & 0 & bM_a \\ \hdashline M_a & \dots & 0 & 0 \\ \hdashline \vdots & \ddots & \vdots & \vdots \\ \hdashline 0 & \dots & M_a & 0 \end{array}\right); \quad \phi((x \otimes y) \otimes 1)^n = abI_{n^2}.$$

The 1-cocycle is defined to be $c_\sigma : G \to PGL_{n^2}(K)$ with

$$c_{g^l} = \phi((x \otimes y) \otimes 1)^l.$$

As usual, we lift to b_σ, and set $a_{\sigma,\tau} = b_\sigma \sigma(b_\tau) b_{\sigma,\tau}^{-1}$. This gives, as expected,

$$a_{g^p,g^q} = \begin{cases} 1, & p+q < n \\ ab, & p+q \geq n \end{cases}.$$

Finally, we note that this suggests that $A \otimes B$ is in the same class as $C = \langle K, z | z^n = ab, z^{-1}\lambda z = g(\lambda) \,\forall \lambda \in K\rangle$, and by matching degrees this yields that we suspect $A \otimes B \cong M_n(C)$.

7 References

[Lam]: Lam, T. Y. Introduction to Quadratic Forms over Fields. Providence, RI: American Mathematical Society, 2005.

[GS]: Gille, Philippe, and Tamás Szamuely. Central Simple Algebras and Galois Cohomology. Cambridge, UK: Cambridge UP, 2006.