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, specific examples of cocycles associated to central simple algebras are calculated

1. 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 1.1: 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 the "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 has the addition 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. Central simple algebras are often referred to as CSAs, an abbreviation we will use often.

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 1.2: Common examples of CSAs include:

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

2. Central division algebras, including k itself, are CSAs over k as well.

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 1.4 and proposition 1.6. It relates the tensor product to the properties of central simple algebras.

Lemma 1.3: 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:

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

And 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 $A \otimes span(b_i)_{i \neq j}$ and the right hand side is in $A \otimes span(b_j)$, 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 $z \in I$, where z is represented as the following sum:

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

and we can choose z such that r is minimal. Now, since A is simple, the ideal generated by a_1 in A is all of A – this means that there is an equation $ca_1d = 1$ for some pair $c, d \in A$. Similarly, we have $c'b_1d' = 1$ 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

$$z' = 1 \otimes 1 + \sum_{i=2}^{r} a_i' \otimes b_i'$$

where $a_i' = ca_id$ and $b_i' = c'b_id'$. Then fix some $a_0 \in A$, and note

$$(a_0 \otimes 1)z' - z'(a_0 \otimes 1) = \sum_{i=2}^{r} (a_0a_i' - a_i'a_0) \otimes b_i \in I$$

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

$$(1 \otimes b_0)z' - z'(1 \otimes b_0) = \sum_{i=2}^{r} a_i \otimes (b_0b_i' - b'b_0)$$

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 1.4: 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 1.5: 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 operation on the group 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, of course, have an inverse, with $[A]^{-1} = [A^{op}]$, the class of its 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 1.6: 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 1.3, 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 1.3, 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 1.7: Wedderburn's Theorem. Every CSA over k is isomorphic to $M_n(D)$ 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.

The proof of this theorem is given in the entire section 2.1 of [GS], and since it is so involved, it is not reproduced here. In particular, this means that every element of $Br(k)$ can be represented by a unique central division algebra over k.

Lemma 1.8: If k is algebraically closed, then any CSA over k is isomorphic to $M_n(k)$ for some choice of n.

Proof: By 1.7, 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 1.8, the implicit assumption that every algebra is finite dimensional is integral to the proof. This lemma and proposition 1.6 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 1.9: 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 extension $K|k$ such that $A \otimes K \cong M_n(K)$.

Proof: The reverse implication follows from 1.6, since $M_n(K)$ is central simple over K. Now for the forward direction, first fix $\overline{k}$ an algebraic closure of k. By 1.8, $A \otimes \overline{k} \cong M_n(\overline{k})$ for some choice of n. $\overline{k}|k$ may not be a finite extension, but we show that we can find one.
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.

Definition 1.10: Let k be a field and K a Galois extension. The Brauer group of k relative to K is the subgroup of $Br(k)$ generated by 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 1.9.

2. 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 2.1: 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 $\sigma(\tau a) = (\sigma\tau)a$. Equivalently, it is a module 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 $Hom(P, A) \to Hom(P, B)$ given by $\lambda \mapsto \alpha \circ \lambda$ is surjective. Free modules are always projective.

3. Given any G-module A, a projective resolution 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

$$M_0 \xrightarrow{c_0} M_1 \xrightarrow{c_1} M_2 \xrightarrow{c_2} \dots$$

   Where $c_i \circ c_{i-1} = 0$ for all i. That is, $Im(c_{i-1}) \subset Ker(c_i)$ – if the sets are equal, the chain is 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 $M_i = Hom_G(P_i, A)$, 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 $Hom_G(P_*, A)$. The next definition uses this connection.

Definiton 2.2: 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 $H^i(Hom_G(P_*, A))$, as defined above. It is denoted $H^i(G, A)$. These groups also have the following nice properties:

1. $H^0(G, A) = A^G$ is the set of elements of A fixed by G.
2. Any G-homomorphism $A \to B$ induces a natural map $H^i(G, A) \to H^i(G, B)$ 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

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

starting with $H^0(G, A)$.

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 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.

Definition 2.3: These definitions culminate in the definition of the standard resolution.

1. Define the map $s^i_j : \mathbb{Z}[G^{i+1}] \to \mathbb{Z}[G^i]$ so that

$$s^i_j(g_0, g_1, \dots, g_i) = (g_0, \dots, g_{j-1}, g_{j+1}, \dots, g_i)$$

2. Now define the map $d_i : \mathbb{Z}[G^{i+1}] \to \mathbb{Z}[G^i]$ in terms of the s^i_j:

$$d_i = \sum_{j=0}^{i} (-1)^j s^i_j$$

3. Finally, the standard resolution is the resolution

$$\dots \xrightarrow{d_2} \mathbb{Z}[G^2] \xrightarrow{d_1} \mathbb{Z}[G] \xrightarrow{d_0} \mathbb{Z} \to 0$$

where the d_i are as above.

It's easy to check that $d_{i+1} \circ d_i = 0$ for all i, which shows that $Im(d_{i+1}) \subset Ker(d_i)$. However to show that the standard resolution is exact, we need further that $Ker(d_i) = Im(d_{i+1})$, 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 $h^i(g_0, \dots, g_i) = (g, g_0, \dots, g_i)$.

$$d_{i+1} \circ h^i + h^{i-1} \circ d_i = Id_{\mathbb{Z}[G^{i+1}]}$$

Now take some element $x \in \mathbb{Z}[G^{i+1}]$ which is in the kernel of d_i. Then:

$$x = Id_{\mathbb{Z}[G^{i+1}]}(x) = (d_{i+1} \circ h^i + h^{i-1} \circ d_i)(x) = (d_{i+1} \circ h^i)(x) + (h^{i-1} \circ d_i)(x) = d_{i+1}(h^i(x)) + 0$$

Which shows that $x \in Im(d_{i+1})$, so $Ker(d_i) = Im(d_{i+1})$ 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 2.4:

1. An i-cochain is a G-homomorphism from $\mathbb{Z}[G^{i+1}]$ to A, i.e., an element of $Hom_G(P_i, A)$.
2. An i-cocycle is an element of $Ker(d_i)$.
3. An i-coboundary is an element of $Im(d_{i-1})$. 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.

The next section covers what are called "inhomogeneous cochains" in [GS], which recovers 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 for 1-cocycles is:

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

Definition 2.5: 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 the following:

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

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 $Hom_G(\mathbb{Z}[G^i], A) \to Hom_G(\mathbb{Z}[G^{i+1}], A)$ 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 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

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

for some 1-cochain (not necessarily cocycle) b_σ.

$i = 1$, A not neccesarily commutative: this case is requires a little bit of fudging 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:

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

and 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 $\sigma \in G$.

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

Definition 2.6: Let $K|k$ be a field extension, and let A and B be two algebras over k. A and B are said to be $K|k$-twisted forms if $A \otimes K \cong B \otimes K$.

Theorem 2.7: Let A be an algebra, let $G = Gal(K|k)$, and define the action of G on $Aut(A)$ to be such that $\sigma(\phi) = \sigma\phi\sigma^{-1}$. Then the set of $K|k$-twisted forms of A is isomorphic to $H^1(G, Aut(A))$.

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

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

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 1.9, 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 $Aut(M_n(K)) \cong PGL_n(K)$ (by the Skolem-Noether theorem), we have now identified $CSA_n(K|k)$ with the cohomology group $H^1(Gal(K|k), PGL_n(K))$. 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 $PGL_{1 \cdot 2 \cdot 3 \cdot \cdots \cdot n}(K)$ as $n \to \infty$, such that $PGL_m(K)$ is realized as a subgroup by the inclusion $i_{m,1 \cdot 2 \cdot \cdots \cdot n}$ for every m. This way we can have $Br(K|k) \cong H^1(Gal(K|k), PGL_\infty(K))$.

Theorem 2.8: $H^1(G, GL_n(K)) \cong \{0\}$.

Proof: The proof here uses a more general form of theorem 2.7. 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. 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 twisted forms of V is isomorphic to $H^1(G, GL_n(K))$. But the determining factor of the isomorphism class of a vector space is only the dimension, and the dimension of $V \otimes K$ and of V are the same, so this set is trivial. Then $H^1(G, GL_n(K)) \cong \{0\}$ 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 2.10.

Theorem 2.9: 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:

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

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 $b^*_{\sigma,\tau} = b_\sigma \sigma(b_\tau) b^{-1}_{\sigma\tau} \in B$. 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 ∂.

The final proposition for this section takes us back to the Brauer group by associating it to some cohomology groups. It uses 2.7 as a starting point, associating $Br(K|k)$ to $H^1(Gal(K|k), PGL_\infty(K))$, and then uses 2.8 and 2.9 to show that it is also isomorphic to $H^2(Gal(K|k), K^\times)$, which is easier to deal with.

Theorem 2.10: The groups $Br(K|k)$, $H^1(Gal(K|k), PGL_\infty(K))$, and $H^2(Gal(K|k), K^\times)$ are all isomorphic.

Proof: The first two groups are isomorphic because of 2.7 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 2.9 to it, we get the smaller exact sequence

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

and since the first group is trivial by 2.8, the map ∂ is injective. Then the surjectivity of this map is all that is in doubt.
To show surjectivity of the map $H^1(G, PGL_\infty(K)) \to H^2(G, K^\times)$, we show something stronger: that the natural map $H^1(G, PGL_n(K)) \to H^2(G, K^\times)$ is surjective, where n is the order of G. This is stronger because every natural map $H^1(G, PGL_{mn}(K)) \to H^2(G, K^\times)$ will then be surjective, which implies the result for $PGL_\infty(K)$.
First consider $K \otimes K$ as a vector space, which is isomorphic to K^n. There is an injective homomorphism from the group $(K \otimes K)^\times$ to $GL_n(K)$ where an invertible element $x \in (K \otimes K)^\times$ maps to multiplication by x. This creates a commutative diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^\times & \longrightarrow & (K \otimes K)^\times & \longrightarrow & (K \otimes K)^\times / K^\times & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle id} & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & K^\times & \longrightarrow & GL_n(K) & \longrightarrow & PGL_n(K) & \longrightarrow & 1 \end{array}$$

The properties of cohomology groups give us this next diagram, which is commutative because the previous one is.

$$\begin{array}{ccccc} H^1(G, (K \otimes K)^\times / K^\times) & \xrightarrow{\alpha} & H^2(G, K^\times) & \longrightarrow & H^2(G, (K \otimes K)^\times) \\ \downarrow & & \downarrow{\scriptstyle id} & & \\ H^1(G, PGL_n(K)) & \xrightarrow{\delta} & H^2(G, K^\times) & & \end{array}$$

The top row of that diagram is exact, because it comes from the long exact cohomology sequence. The last group in the top row is trivial by Shapiro's lemma (since $(K \otimes K)^\times \cong K^\times \otimes_{\mathbb{Z}} \mathbb{Z}[G] \cong Hom(\mathbb{Z}[G], K^\times)$, where the last isomorphism is found by choosing a basis for $\mathbb{Z}[G]$ over $\mathbb{Z}$), which means that the morphism α is surjective. By commutativity of the diagram, this shows that δ is surjective, which is what we were trying to prove. Thus the natural map $H^1(G, PGL_n(K)) \to H^2(G, K^\times)$ is surjective, so the natural map $H^1(G, PGL_\infty(K)) \to H^2(G, K^\times)$ is surjective. Along with the injectivity established earlier, this shows that it is an isomorphism, so that all three groups in the proposition are isomorphic.

3. 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.

Proposition 3.1: Let $A = \left(\frac{a,b}{k}\right)$, and let $K = k(\sqrt{b})$ be a splitting field for A. Further let $Gal(K|k) = \{e, g\}$ where g is the non-identity element. Then the class $[A]$ in $Br(K|k)$ is given by $a_{\sigma,\tau}$:

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

Proof: (Note: in this proof and others to come, there is a particular abuse of notation where the elements of $PGL_m(K)$ and the elements of $GL_m(K)$ are not distinguished. This does not cause any problems, especially as most of the calculations themselves occur in $GL_m(K)$.) 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:

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

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 what we wanted. Using the class of I_2 will obviously work for e, since $\phi^{-1}e(\phi)$ fixes everything. The 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 noted 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_σ, τ
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 3.2: 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 $a_{\sigma,\tau}$:

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

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

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

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 easily 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 is easily 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 $\phi(y)$, and $c_{g^p} = \phi(y)^p$. After lifting c_σ to b_σ, we get

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

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 3.2 reduces to proposition 3.1 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 quaternion algebras are cyclic.

2. When the author first found these cocycles, he thought he had done something wrong. He first did it for the quaternion algebras, and this process seems to "forget" about b, because the only constant present in the cocycle is a. In the more general construction, we seem to lose β. However, 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 $\left(\frac{x,b}{k}\right)$ for some x, and the cocycle just gives us a particular value for x. The next two propositions give cocycles for a quaternion algebra over different splitting fields, and transitions us into the next section.

Proposition 3.3: 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. 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 3.4: 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 lead me to believe that we can make 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.

4. 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. Before we define these maps, we first have to show that they apply.

Proposition 4.1 Let $L|K|k$ be a tower of Galois extensions. The groups $Gal(L|k)$, $Gal(L|K)$, and $Gal(K|k)$ fit into the following short exact sequence:

$$1 \to Gal(L|K) \to Gal(L|k) \to Gal(K|k) \to 1$$

Proof: This first requires that $Gal(L|K)$ be a normal subgroup of $Gal(L|k)$.$Gal(L|k)$ is the group of automorphisms of L that fix every element of k, and $Gal(L|K)$ is the subgroup of automorphisms that further fix evey element of K. So to show that $Gal(L|K) \triangleleft Gal(L|k)$, we take an automorphism $h \in Gal(L|K)$ and conjugate by any automorphism $g \in Gal(L|k)$. Then we look at the function ghg^{-1} restricted to K. On K, h is the identity map, so the function $ghg^{-1}|_K$ is the function $g|_K g^{-1}|_K = Id_K$, so ghg^{-1} also fixes all of K, and is in $Gal(L|K)$. This shows $Gal(L|K)$ is a normal subgroup of $Gal(L|k)$.
Note that this requires the fact that g maps K to K. But this must be true since $L|K|k$ is a tower of Galois extensions, so K is the splitting field of some separable polynomial $p \in k[x]$. On L, the isomorphism g must send roots of p to other roots of p. Since all these roots are in K, g fixes K.
Now that we know $Ga(L|K) \triangleleft Gal(L|k)$, we have to find the quotient $Gal(L|k)/Gal(L|K)$. We want to show that this is $Gal(K|k)$. We create an isomorphism between the two by mapping the equivalence class $[g]$ of some automorphism $g \in Gal(L|k)$ to the function g_K, which is g with its domain restricted to K. This is well defined on the equivalence class since composing with elements of $Gal(L|K)$ is like composing with Id_K. Its kernel is $Gal(L|K)$ (and thus trivial) since, if $g_K(x) = h_K(x)$ for all x, we have that $gh^{-1}(x) = x$ for all $x \in K$, so their difference in $Gal(L|k)$ is an element of $Gal(L|K)$. The image is all of $Gal(K|k)$ since each element of $Gal(K|k)$ can be extended to an element of $Gal(L|k)$. Thus we have constructed an isomorphism between the two sets.

The important point here is that, if we take $G = Gal(L|k)$ and $H = Gal(L|K)$, the factor group G/H is isomorphic to $Gal(K|k)$. This is important, as we will see when we define inflation maps:

Definition/Proposition 4.2: Inflation maps. This definition requires a few things:

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.
2. Let $H \triangleleft G$. There exist natural maps $\inf : H^i(G/H, A^H) \to H^i(G, A)$ for all i.

Proof: Each will be proven separately.

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

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

2. We now construct the maps, by setting up the construction of the cohomology groups in 2.2. 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. This gives us natural maps α_i so that the diagram

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

commutes. Each α_i induces a map $Hom_G(Q_i, A^H) \to Hom_G(P_i, A^H)$, 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, $Hom_{G/H}(Q_i, A^H) = Hom_G(Q_i, A^H)$, which means these induce nice maps $Hom_{G/H}(Q_i, A^H) \to Hom_G(P_i, A^H)$. They then induce maps $H^i(G/H, A^H) \to H^i(G, A^H)$, which, after composing with the inclusion map $A^H \to A$, gives us the required 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 proposition in this section. If $L|K|k$ is a tower of galois extensions, we have $Gal(K|k) \cong Gal(L|k)/Gal(L|K)$. 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:

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

which is in fact a map $Br(K|k) \to Br(L|k)$, whose construction is the point of this section. To finish, we try to recover the cocycle for $\left(\frac{a,b}{k}\right)$ we found in 3.3 from the one we found in 3.1.

Construction 4.3: Take k a field, $K = k(\sqrt{b})$, and $L = k(\sqrt{a}, \sqrt{b})$. The Galois groups $G = Gal(L|k)$ and $G/H = Gal(K|k)$ (where $H = Gal(L|K)$) 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 3.1. 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 3.4:

$\tau \backslash^{\sigma}$	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 $Gal(k_{sep}|k)$, 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 $Br(K|k)$.

5. Cocycles for tensor products

In this section we calculate the cocycles associated to certain tensor products of quaternion algebras and cyclic algebras. First, we find a presentation of the tensor products of two quaternion algebras split by the same quadratic extension, and use that to find what we expect the cocycle to be. Then we calculate the cocycle in that case, and finally in the case of two cyclic algebras.

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 isomorphism maps:

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

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.

Propostion 5.1: 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:

$\tau \backslash \sigma$	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 $i_a \otimes i_b$, $j_a \otimes i_b$, $i_a \otimes j_b$, and $j_a \otimes j_b$:

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

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

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 $i_a \otimes i_b$ and $j_a \otimes j_b$ while taking $i_a \otimes j_b$ and $j_a \otimes i_b$ to their negatives. At this point, this could be represented by either $\phi(i_a \otimes i_b)$ or $\phi(j_a \otimes j_b)$ in $PGL_4(K)$, but the choice is made clear when you look at how it acts on $1_a \otimes i_b$ and $i_a \otimes 1_b$ (by fixing them) and on $1_a \otimes j_b$ and $j_a \otimes 1_b$ (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 shows 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 5.2: 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:

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

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 $\left(\frac{b,-bc^2}{k}\right)$. Now the quadratic form $\langle b, -bc^2\rangle$ is isotropic (since $(c^2, 1)$ is mapped to 0), so it is universal. In particular, it represents 1, and thus by Hilbert's Criterion this quaternion algebra is split, and isomorphic to $M_2(k)$. 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 5.1 gave us insight into the isomorphism class of $\left(\frac{a,c}{k}\right) \otimes \left(\frac{b,c}{k}\right)$, and proposition 5.2 showed us that the insight was correct. The next proposition will give us a similar insight for cyclic algebras.

Proposition 5.3: 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:

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

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:

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

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

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

Then for our isomorphism ϕ, we set:

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

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

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

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

which gives in particular:

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

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, this shows 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 the isomorphism $A \otimes B \cong M_n(C)$.

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.