Division Algebras, the Brauer Group, and Galois Cohomology

Robert Hines

January 5, 2015

Introduction

Classifying (or even finding) non-commutative division algebras is a difficult task. Here are two examples:

- (Cyclic algebras) Given a finite cyclic extension $K/k$ with galois group generated by $\sigma$ and an element $a \in k^\times$, define the **cyclic algebra** $(K/k, a)$ as the quotient of the twisted polynomial algebra $K[x]_\sigma$ ($bx = x\sigma(b)$ for $b \in K$) by the two-sided ideal generated by $x^n - a$. For instance, the quaternions are $\mathbb{C}[x]_{\tau}/(x^2 + 1)$, $\tau$ complex conjugation.

- (Crossed product algebras) The previous example can be generalized. Let $K/k$ be a finite galois extension with galois group $G$, and consider the $K$ vector space $A = \langle x_\sigma : \sigma \in G \rangle_K$ with multiplication defined by

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

where the $a_{\sigma,\tau} \in K^\times$ satisfy (forced by associativity $x_\rho(x_\sigma x_\tau) = (x_\rho x_\sigma)x_\tau$)

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

With this multiplication, $A$ becomes a finite dimensional $k$-central division algebra containing $K$ as a maximal subfield, the **crossed product algebra** $(K, G, a)$. We will see these again when we discuss the relation of the Brauer group to cohomology.

Examples of finite dimensional central division algebras not given as a crossed product were not found until the ’70s (by Amitsur).

The Brauer group is a tool for organizing information about all of the finite dimensional division algebras with a given center. As we shall see, the Brauer group can be realized as a cohomology group.
The Brauer Group of a Field

A central simple $k$-algebra $A$ is a ring with no non-trivial two-sided ideals and center $k$. For a fixed field $k$, we define an equivalence relation on the collection of finite dimensional central simple $k$-algebras, $A \sim B$, if there is a division ring $D$ (a ring such that every non-zero $d \in D$ has an inverse $d^{-1}$ such that $dd^{-1} = d^{-1}d = 1$) and positive integers $n, m$ such that $A \cong M_n(D), B \cong M_m(D)$. Equivalently, $A \sim B$ if there are positive integers $m, n$ such that $A \otimes M_n(k) \sim B \otimes M_m(k)$. We denote the equivalence class of $A$ by $[A]$. (It is a fact that any finite dimensional central simple $k$-algebra is isomorphic to a matrix ring over a division ring so that a $D$ as described above exists (a consequence of the Artin-Wedderburn theorem).)

The tensor product of two finite dimensional central simple $k$-algebras is also a central simple $k$-algebra, and this can be used to define a product on the set of equivalence classes, $[A] \cdot [B] := [A \otimes B]$, with identity $[k]$ and inverse $[A]^{-1} = [A^{op}]$ ($A \otimes A^{op} \cong M_n(k)$, $n = \dim_k A$, by sending $a \otimes b$ to the matrix of $x \mapsto axb$). With this product, the equivalence classes of central simple $k$-algebras form an abelian group, the **Brauer Group** $Br(k)$.

Some examples:

- (Wedderburn) $Br(\mathbb{F}_q) = 0$ because any finite division ring is a field.
- $Br(\bar{k}) = 0$ as there are no finite dimensional division algebras $D$ with center an algebraically closed field. (Proof: The action of $D$ on itself by left multiplication is $\bar{k}$-linear. Considering the minimal polynomial of this linear transformation shows that every element of $D$ is algebraic over $\bar{k}$.)
- (Frobenius) $Br(\mathbb{R})$ is cyclic of order two, generated by the class of the quaternions $\mathbb{H}$ (we have $\mathbb{H} \otimes \mathbb{H} \cong M_4(\mathbb{R})$).
- $Br(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}$ (local class field theory).
- $Br(\mathbb{Q})$ fits into the exact sequence

$$0 \to Br(\mathbb{Q}) \to \bigoplus_{\nu} Br(\mathbb{Q}_\nu) \to \mathbb{Q}/\mathbb{Z} \to 0$$

where $\nu$ ranges over all completions of $\mathbb{Q}$ (a similar result holds for other number fields).

The Brauer group is functorial in the following sense. Given an extension $K/k$, extension of scalars gives a homomorphism $Br(k) \to Br(K)$, $[A] \mapsto [A \otimes_k K]$. We define the relative Brauer group, $Br(K/k)$, to be the kernel of this homomorphism, consisting of the (equivalence classes) of finite central simple $k$-algebras split by $K$ ($A \otimes K \cong M_n(K)$ for some $n$).

Every finite dimensional central division algebra $D/k$ is split by any maximal subfield of $D$; furthermore we can find a finite galois extension of $k$ which splits $D$. Hence we have $Br(k) = \bigcup Br(K/k)$, the union taken over all finite galois extensions $K/k$. The relative Brauer groups are computable as cohomology groups. We will see that there is an isomorphism, $Br(K/k) \cong H^2(\text{Gal}(K/k), K^\times)$, for a finite galois extension $K/k$. 

Group Cohomology

Let $G$ be a group, and $M$ a $G$-module (an abelian group with a $G$-action). We define co-chain groups

$$C^n(G,M) := \{ f : G^n \to M \} \quad (C^0(G,M) = M),$$

with point-wise addition, $G$-action given by $(gf)(g_1,...,g_n) = g \cdot f(g_1,\ldots,g_n)$, and differential $\delta_n : C^n(G,M) \to C^{n+1}(G,M)$ given by

$$(\delta_n f)(g_1,\ldots,g_{n+1}) = g_1 \cdot f(g_2,\ldots,g_{n+1}) + \sum_{i=1}^{n} (-1)^i f(g_1,\ldots,g_ig_i+1,\ldots,g_{n+1}) + (-1)^{n+1} f(g_1,\ldots,g_n).$$

For $n = 0, 1, 2$ we have

$$(\delta^0 m) = g \cdot m - m$$

$$(\delta^1 f)(g_1,g_2) = g_1 \cdot f(g_2) - f(g_1 g_2) + f(g_1),$$

$$(\delta^2 f)(g_1,g_2,g_3) = g_1 \cdot f(g_2,g_3) - f(g_1 g_2,g_3) + f(g_1,g_2 g_3) - f(g_1,g_2).$$

The first two cohomology groups are

- $H^0(G,M) = M^G = \{ m \in M | g \cdot m = m \}$

  $H^0(\text{Gal}(K/k),K^\times) = k^\times$

- $H^1(G,M) =$ “crossed homomorphisms” / “principal crossed homomorphisms”

  $H^1(\text{Gal}(K/k),K^\times) = 1$ (Hilbert’s Satz 90).

Let $G = \text{Gal}(K/k)$ and switch to multiplicative notation to analyze $H^2(G,K^\times)$. The cocycles $Z^2$ are functions

$$a : G \times G \to K^\times \text{ such that } (\delta^2 a)(\rho,\sigma,\tau) = 1 = \rho(a(\sigma,\tau))a(\rho\sigma,\tau)^{-1}a(\rho,\sigma\tau)a(\rho,\sigma)^{-1},$$

i.e.

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

These were exactly the conditions on the structure constants given for crossed product algebras.

The coboundaries $B^2$ are given by functions of the form

$$(\delta^1 f)(\sigma,\tau) = \frac{\sigma(f(\tau))f(\sigma)}{f(\sigma\tau)} \text{ where } f : G \to K^\times.$$

The coboundary condition is the equivalence obtained by considering different bases for a crossed product algebra, as we will now discuss in more detail. First an important theorem:

**Theorem** (Skolem-Noether). *If $f, g : R \to S$ are $k$-algebra homomorphisms, $R$ simple and $S$ finite central simple, then there is an inner automorphism $\phi$ of $S$ such that $\phi f = g$.**
So if $(K, G, a) = \langle x_\sigma \rangle_K = S = \langle x'_\sigma \rangle_K = (K, G, b)$ then the fact that 
\[ x_\sigma \alpha x_\sigma^{-1} = \sigma(\alpha) = x'_\sigma \alpha x'_\sigma^{-1} \]
implies that conjugation by $x'_\sigma x_\sigma^{-1}$ induces the identity on $K$, hence $x'_\sigma x_\sigma^{-1} = f_\sigma \in K^\times$ as $K$ is its own centralizer in $S$. Multiplying $x'_\sigma x'_\sigma = b_{\sigma, \tau} x'_{\sigma, \tau}$ using the above, we get 
\[ b_{\sigma, \tau} = \frac{\sigma(f_\tau f_\sigma^{-1})}{f_\sigma^{-1}} a_{\sigma, \tau} \]
which is the coboundary condition.

Next we’d like to see that every element of the relative Brauer group $Br(K/k)$ ($K/k$ finite galois) is represented uniquely by a crossed product $(K, G, a)$.

**Lemma.** Given an extention $K/k$ of degree $n$, any element of $Br(K/k)$ has a unique representative $S$ of degree $n^2$ over $k$, with subfield $K$ satisfying $C_S(K) = K$ (K is its own centralizer in $S$).

**Proof.** (Sketch) Let $D$ be the division algebra equivalent to $S$, $K \otimes D^{op} \cong M_n(K)$, and $V$ the simple $K \otimes D^{op}$-module. Let $S = M_{[V, D]}(D)$ and check the details ($K \subseteq S$ satisfies $C_S(K) = K$, etc.).

Any $S$ as in the lemma is a crossed product algebra when $K/k$ is galois (take $x_\sigma$ to be the elements satisfying $x_\sigma \alpha x_\sigma^{-1} = \sigma(\alpha)$ for $\alpha \in K$ which exist by the Skolem-Noether theorem). So far we have a bijection between $H^2(\text{Gal}(K/k), K^\times)$ and $Br(K/k)$, which is actually a group isomorphism. The proof is a bit lengthy and is omitted.

**Theorem.** The map $\psi : H^2(G, K^\times) \to Br(K/k)$, $a \mapsto [(K, G, a)]$ is a group isomorphism.

We can now apply a a few results from group cohomology to get information about the Brauer group. For instance,

**Proposition.** The Brauer group $Br(k)$ is torsion.

**Proof.** For any finite group $G$ and $G$-module $M$, we have $|G|H^n(G, M) = 0$ for $n \geq 1$. To see this for $n = 2$, let $f$ be a 2-cocycle,
\[ f(g_1, g_2) = g_1 \cdot f(g_2, g_3) - f(g_1g_2, g_3) + f(g_1, g_2g_3). \]

Summing over $g_3$ gives
\[ |G|f(g_1, g_2) = \sum_{g_3 \in G} g_1 \cdot f(g_2, g_3) - f(g_1g_2, g_3) + f(g_1, g_2g_3). \]

Let $h(g_2) = \sum_{g_3 \in G} f(g_2, g_3)$ and rewrite the above to get
\[ |G|f(g_1, g_2) = g_1 \cdot h(g_2) - h(g_1g_2) + h(g_1) = (\delta^1 h)(g_1, g_2) \in B^2. \]

Since $Br(k)$ is the union of $Br(K/k)$ over finite galois extenstions $K/k$, the Brauer group is torsion. 

\[ \square \]
Proposition. If $K/k$ is a cyclic extension with $G = \text{Gal}(K/k) = \langle \sigma \rangle$ and the norm map $N : K^\times \to k^\times$ is not surjective, then there is a noncommutative division algebra over $k$.

Proof. We have a free resolution of $\mathbb{Z}[G]$ given by

$$\ldots \to \mathbb{Z}[G] \xrightarrow{D} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{D} \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

where $D = \sigma - 1$ and $N = \sum_i \sigma^i$ is the norm. Applying $\text{Hom}(\_ , K^\times)$ and taking cohomology gives $H^2(G, K^\times) = k^\times / N(K^\times)$.

For instance, if $p$ is an odd prime and $k = \mathbb{F}_p(x)$, $K = k(\sqrt{x})$, then $x^2 + x$ is not a norm.

That’s all I have to say about that.

References


[4] THE INTERNET