Perspectives on the Albert-Brauer-Hasse-Noether Theorem for Quaternion Algebras

Thomas R. Shemanske

17 May 2007

Abstract

1 Introduction

In his book on *Associate Algebras* [2], Richard Pierce characterizes the Albert-Brauer-Hasse-Noether theorem as "the most profound result in the theory of central simple algebras." The theorem has numerous formulations in the literature (some repeated here), but even the most general one stated in this note is not the most general which appeared in 1932 papers of Brauer-Hasse-Noether and Albert-Hasse. There is a wonderful historical and mathematical discussion of the Albert-Brauer-Hasse-Noether theorem in the book by Roquette [4].

This note simply represents some background for a talk I gave recently at a local seminar; it is far from complete in scope or detail, but intended only to draw attention to the remarkable confluence of ideas which this theorem embodies. The focus here is restricted to the quaternion case. There are many good reasons for this including accessibility in a seminar talk, the quaternion context affords many alternate characterizations of the main theorem which do not generalize to higher dimensions, and last but not least because the first version of this theorem ever stated to the author concerned embedding quadratic extensions in quaternion algebras. As an embedding theorem, I have only rarely seen it stated in the literature, never proven, and a bit more surprisingly not even stated in the standard books on books treating the subject, e.g., [2], [3].

It is quite surprising to those who have not seen the theorem before that while the main theorem characterizes division algebras over number fields, it is completely equivalent to the Hasse Norm theorem which concerns only extensions of number fields.

2000 *Mathematics Subject Classification.* Primary 11R52
Key Words and Phrases. Cyclic Algebra, Quaternion Algebra, Class Field Theory

2 Background on Quaternion Algebras

Let F be a field, $a, b \in F^\times$. Denote by $A = \left(\frac{a,b}{F}\right)$ the quaternion algebra over F with basis $\{1, i, j, k\}$ and defining relations $i^2 = a$, $j^2 = b$, $ij = k = -ji$. A quaternion algebra is a central simple algebra of dimension 4 over F, and except when F has characteristic 2, any 4-dimensional central simple algebra over F is a quaternion algebra. In our case we are interested when F is a number field or one of its completions, all of which have characteristic zero.

Associated to A is an involution $\alpha \mapsto \bar{\alpha}$, defined by

$$\bar{\alpha} = \overline{w + xi + yj + zk} = w - xi - yj - zk$$

with which we define a (reduced) norm and trace $A \to F$:

$$N(\alpha) = \alpha\bar{\alpha} = w^2 - ax^2 - by^2 + abz^2 \text{ and } Tr(\alpha) = \alpha + \bar{\alpha} = 2w.$$

It is easy to check that an element $\alpha \in A$ is invertible iff $N(\alpha) \neq 0$ in which case $\alpha^{-1} = \bar{\alpha}/N(\alpha)$. The subset $A_0 = \{\alpha \in A \mid Tr(\alpha) = 0\}$ is called the set of pure quaternions.

Theorem 2.1 (Theorem II.2.7 [1])**.** *Let F be a field, $a, b \in F^\times$, and $A = \left(\frac{a,b}{F}\right)$. The following are equivalent:*

1. $A \cong \left(\frac{1,-1}{F}\right) \cong M_2(F)$.
2. *A is not a division algebra.*
3. *A is isotropic as a quadratic space (i.e., there exists $\alpha \neq 0$ in A with $N(\alpha) = 0$).*
4. *A_0 (pure quaternions) is isotropic as a quadratic space.*
5. *$ax^2 + by^2 = 1$ is solvable over F.*
6. *$a \in N_{E/F}(E)$, where $E = F(\sqrt{b})$, and $N_{E/F}$ is the field norm.*

If any of these conditions holds for A, we say A is split *or A* splits *over F.*

Remark 2.2. *Note that this theorem says many interesting things. The theory of quaternion algebras over fields is only really interesting in the context of division algebras, as all other quaternion algebras are isomorphic to $M_2(F)$.*

When $F = \mathbb{Q}_p$ the field of p-adic numbers, $\left(\frac{a,b}{\mathbb{Q}_p}\right)$ is usually associated to the Hilbert symbol, $(a, b)_p$. We write $(a, b)_p = 1$ iff $ax^2+by^2 = 1$ is solvable over $\mathbb{Q}_p$. The Hilbert symbols satisfy what is known as the Hilbert reciprocity law which says for $a, b \in \mathbb{Q}^\times$, $\prod_{p \leq \infty} (a, b)_p = 1$. In particular, $(a, b)_p = -1$ for a finite even number of primes. Said another way, given a quaternion algebra $A = \left(\frac{a,b}{\mathbb{Q}}\right)$, the local algebra $A_p = \left(\frac{a,b}{\mathbb{Q}_p}\right)$ is a division algebra at a finite even (we shall see not zero) number of primes. This association will be clearer when we state the Albert-Brauer-Hasse-Noether theorem.

Proof. While essentially all of the above criteria are needed for what follows, I sketch only a couple of implications as the proofs of many depend on some basic quadratic forms theory.

Clearly (1) implies (2), and given that $\alpha \in A$ is invertible iff $N(\alpha) \neq 0$, we see (2) iff (3). The interest for this talk lies in the equivalence of (1), (5), (6).

To show the equivalence of (5) and (6), we may assume that b is not a square in $F^\times$, otherwise both statements are obvious. Suppose $ax^2 + by^2 = 1$. We have that $x \neq 0$ since b is not a square, thus $a + b(y/x)^2 = 1/x^2$ or $a = (1/x)^2 - b(y/x)^2 = N_{E/F}(1/x + (y/x)\sqrt{b})$.

Conversely, suppose that $a = x^2 - by^2$ is the norm of an element in E. If $x \neq 0$, we have $a(1/x)^2 + b(y/x)^2 = 1$. If $x = 0$, $a = -by^2$, and we need to fuss a bit more. The equation $au^2 + bv^2 = 1$ is solvable iff $-by^2u^2 + bv^2 = b(v^2 - y^2u^2) = 1$ is solvable. As y cannot also be zero, using the change of variable $v' = v, u' = yu$, we need only show that $v'^2 - u'^2$ represents the value $1/b$. In fact, this quadratic form (actually the associated quadratic space) is a "hyperbolic plane" which represents everything as is clear from the change of variable (assuming $\chi(F) \neq 2$): $v' = (U + V)/2, u' = (U - V)/2$ in which case $v'^2 - u'^2 = UV$ which clearly represents all elements of F.

Finally it is clear that (5) implies (1), since if $ax^2+by^2 = 1$, then the norm of $\alpha = 1+xi+yj$ is $1 - ax^2 - by^2 = 0$, so α has no inverse and A is not a division algebra. □

We can now state two versions of the theorem of interest to me.

Theorem 2.3 (Albert-Brauer-Hasse-Noether)**.** *Let A be a central simple algebra over an algebraic number field F. Then A splits over F iff $A_\mathfrak{p}$ splits over $F_\mathfrak{p}$ for all primes of F (including the infinite ones).*

For quaternion algebras, the above theorem implies and is often restated as:

Theorem 2.4. *Let A be a quaternion algebra over a number field F, and let L be a quadratic extension of F. Then there is an embedding of L into A over F iff no prime of F which ramifies in A splits in L.*

One key to the connection of these two theorems is the following standard result:

Theorem 2.5 (Theorem III.4.1 [1])**.** *Let F be a field, $a, b \in F^\times$, and $A = \left(\frac{a,b}{F}\right)$. For $c \in F^\times \setminus (F^\times)^2$, let $K = F(\sqrt{c})$ be a quadratic field extension of F. The following are equivalent:*

1. *A splits over K.*
2. *$A \cong \left(\frac{c,d}{F}\right)$ for some $d \in F^\times$.*
3. *K can be embedded (over F) in A.*

Proof. Again we only indicate some of the implications.

(1) implies (2) needs quadratic form theory.

(2) implies (3) is easy: If $A \cong \left(\frac{c,d}{F}\right)$, then $i \in A$ satisfies $i^2 = c$ and $K = F(\sqrt{c}) \cong F[i] = F(i) \subset A$ (since the center of A is F).

For (3) implies (1), assume without loss of generality that $F \subset K \subset A$. Then as K-algebras, we have (the last isomorphism by the Chinese Remainder Theorem),

$$K \otimes_F A \supseteq K \otimes_F K \cong K \otimes_F F[x]/(x^2 - c) \cong K[x]/(x^2 - c) \cong K \oplus K$$

which contains zero divisors. □

Crucial to the classification of simple (even semisimple) algebras over a field is the famous theorem of Wedderburn.

Theorem 2.6 (Wedderburn)**.** *Let A be a simple algebra over a field F. Then $A \cong M_n(D)$ where D is a division algebra over F. The integer n is unique, and D uniquely determined up to isomorphism.*

For central simple algebras, more can be said.

Theorem 2.7. *Let A be a central simple algebra over a field F with $A \cong M_n(D)$. Then $[D : F] = m^2$ and so $[A : F] = n^2m^2$. The integer m is called the* index *of A.*

Remark 2.8. *Every central simple algebra A of dimension 4 over a field (at least if the characteristic is not two) is a quaternion algebra, and for $[A : F] = 4 = n^2m^2$ we have but two cases:*

- *$n = 1, m = 2$ in which case $A \cong D$ is a division algebra*
- *$n = 2, m = 1$ in which case $A \cong M_2(F)$ is split.*

It is here that Brauer's contributions are quite visible. For central simple algebras $A \cong M_n(D)$, $A' \cong M_{n'}(D')$ over a fixed field K, we call A and A' *similar* (denoted $A \sim A'$) if their associated division rings D and D' are isomorphic as K-algebras. Similarity is an equivalence relation, and the elements of the Brauer group of K are the similarity classes of central simple algebras over K. The group law is $[A][B] = [A \otimes_K B]$ with $[K] = [M_n(K)]$ the identity, and $[A^{\text{op}}]$ the inverse of $[A]$.

The index plays a critical role in the splitting of central simple algebras (sections 13.3 and 13.4 of [2], and (7.15) of [3]). In particular, we have the following proposition:

Proposition 2.9. *Let A be a central simple algebra over a field F. If E/F is a finite field extension so that E splits A, then the index m of A divides $[E : F]$. Conversely, if E/F is a finite extension of fields with $F \subset E \subset A$, and $[E : F] = m$, then E splits A.*

It turns out that the index is an exponent for $[A]$ in the Brauer group. Another absolutely critical theorem which we show is equivalent to the ABHN theorem in the quaternion case (and deeply connected in the general case) is the Hasse Norm Theorem.

Theorem 2.10 (Hasse Norm Theorem [2])**.** *Let L/K be a finite cyclic extension of number fields. Then an element $a \in K$ is in the image of the norm $N_{L/K}$ if and only if a is in the image of each norm $N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$ for each prime $\mathfrak{p}$ of K (including the infinite ones) and for each prime $\mathfrak{P}$ of L lying above $\mathfrak{p}$.*

Remark 2.11. *It turns out that since the Galois group $Gal(L/K)$ acts transitively on the primes $\mathfrak{P}$ of L lying above $\mathfrak{p}$, for any two such primes $\mathfrak{P}$ and $\mathfrak{P}'$, the completions $L_{\mathfrak{P}} \cong L_{\mathfrak{P}'}$ over $K_{\mathfrak{p}}$, from which it follows that $N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} = N_{L_{\mathfrak{P}'}/K_{\mathfrak{p}}}$.*

It is also quite easy to see that if an element is in the image of the global norm, it is also a local norm, so the content of the Hasse theorem is the converse.

3 Implications and equivalences of the ABHN theorem

3.1 Implications

First we show that the Albert-Brauer-Hasse-Noether theorem in the context of quaternion algebras implies Theorem 2.4. Actually it is only required for one direction.

Suppose that $A = \left(\frac{a,b}{F}\right)$ is a quaternion algebra over a number field F and that L/F a quadratic extension of fields with $F \subset L \subset A$. It is quite easy to see that the condition 'no prime of F which ramifies in A splits in L' is necessary: Let $\mathfrak{p}$ be a prime of F with ramifies in A, i.e., $A_{\mathfrak{p}} = F_{\mathfrak{p}} \otimes A \cong \left(\frac{a,b}{F_{\mathfrak{p}}}\right)$ is a division algebra. Then $F_{\mathfrak{p}} \otimes_F F \cong F_{\mathfrak{p}} \subset F_{\mathfrak{p}} \otimes_F L \subset F_{\mathfrak{p}} \otimes_F A$.

The following are two standard results in algebraic number theory: Given an extension of number fields L/F, and $\mathfrak{p}$ a prime of F, $F_{\mathfrak{p}} \otimes_F L \cong \oplus_{\mathfrak{P}|\mathfrak{p}} L_{\mathfrak{P}}$, the direct sum being over all completions of L at primes $\mathfrak{P}$ of L lying over $\mathfrak{p}$. The second result is for a prime $\mathfrak{p}$ of F, $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ with $\sum_{i=1}^{g} e_i f_i = [L : F]$. Appropriate interpretations also exist for the infinite primes.

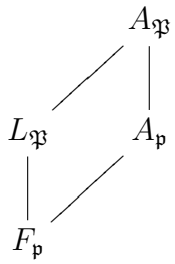
For quadratic extensions, the possibilities are quite simple:

- $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^2$ ($\mathfrak{p}$ ramifies),
- $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}$ is prime ($\mathfrak{p}$ is inert),
- $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1\mathfrak{P}_2$ ($\mathfrak{p}$ splits).

Only in the last case is $F_{\mathfrak{p}} \otimes_F L$ a direct sum of fields producing zero divisors within the division algebra $F_{\mathfrak{p}} \otimes A$. The case of a complex prime $\mathfrak{p}$ ($F_{\mathfrak{p}} = \mathbb{C}$) cannot occur, $A_{\mathfrak{p}}$ is split. If $\mathfrak{P}$ is a real prime ($F_{\mathfrak{p}} = \mathbb{R}$) which ramifies in A, then $A_{\mathfrak{p}}$ is Hamilton's quaternions. If $\mathfrak{p}$ split in L, once again $F_{\mathfrak{p}} \otimes_F L = \mathbb{R} \otimes_F L \cong \mathbb{R} \oplus \mathbb{R}$ producing zero divisors in the division algebra. Thus it is clear that no prime of L which ramifies in A can split in L.

Conversely, assume Theorem 2.3, and that no prime of F which ramifies in A splits in L. By Theorem 2.5, L can be embedded in A over F iff L splits A, that is $\left(\frac{a,b}{L}\right)$ is split. By Theorem 2.3, L splits A iff $L_{\mathfrak{P}}$ splits $A_{\mathfrak{P}}$ for every prime $\mathfrak{P}$ of L.

Let $\mathfrak{P}$ a prime of L and $\mathfrak{p} = \mathcal{O}_F \cap \mathfrak{P}$ the unique prime of F lying below it. We have the following inclusions (see diagram): $F_\mathfrak{p} \subset L_\mathfrak{P} \subset A_\mathfrak{P}$ and $F_\mathfrak{p} \subset A_\mathfrak{p} \subset A_\mathfrak{P}$ since $A_\mathfrak{P} = L_\mathfrak{P} \otimes_L A \cong L_\mathfrak{P} \otimes_{F_\mathfrak{p}} F_\mathfrak{p} \otimes_F A \cong L_\mathfrak{P} \otimes_{F_\mathfrak{p}} A_\mathfrak{p}$. Now if $F_\mathfrak{p}$ splits $A_\mathfrak{p}$, then $L_\mathfrak{P}$ splits $L_\mathfrak{P} \otimes_{F_\mathfrak{p}} A_\mathfrak{p} \cong A_\mathfrak{P}$ (i.e., $A_\mathfrak{p} \cong M_2(F_\mathfrak{p})$ implies $L_\mathfrak{P} \otimes_{F_\mathfrak{p}} A_\mathfrak{p} \cong M_2(L_\mathfrak{P})$.)



If $F_\mathfrak{p}$ does not split $A_\mathfrak{p}$, then $A_\mathfrak{p}$ is a division algebra over $F_\mathfrak{p}$ (i.e., $\mathfrak{p}$ ramifies in A), so $\mathfrak{p}$ does not split in L by assumption. That $[L_\mathfrak{P} : F_\mathfrak{p}] = ef$ and $\mathfrak{p}$ does not split in L means either $e = 2$ or $f = 2$, so $[L_\mathfrak{P} : F_\mathfrak{p}] = 2$. Moreover, $\mathfrak{p}$ not split in L means there is only one prime of L lying above $\mathfrak{p}$ so $F_\mathfrak{p} \otimes L \cong L_\mathfrak{P} \subset F_\mathfrak{p} \otimes A = A_\mathfrak{p}$. Since $F_\mathfrak{p} \subset L_\mathfrak{P} \subset A_\mathfrak{p}$ and $[L_\mathfrak{P} : F_\mathfrak{p}] = 2$, Proposition 2.9 implies $L_\mathfrak{P}$ splits A_p, i.e., $L_\mathfrak{P} \otimes_{F_\mathfrak{p}} A_\mathfrak{p} = A_\mathfrak{P}$ is split. Thus, $L_\mathfrak{P}$ splits $A_\mathfrak{P}$ for every prime $\mathfrak{P}$ of L, and by Theorem 2.3, A is split over L which means L is embeddable in A. This completes this direction of the proof.

3.2 Equivalent formulations

Here we show that the Albert-Brauer-Hasse-Noether theorem is equivalent to the Hasse Norm theorem in the context of quaternion algebras. The equivalence is true more generally.

Let A be a quaternion algebra over F. Since F is contained in each of its completions, if F splits A, it follows easily that $F_\mathfrak{p}$ splits $A_\mathfrak{p}$ for all primes $\mathfrak{p}$ since $F \otimes_F A \cong M_2(F)$ implies $A_\mathfrak{p} = F_p \otimes_F A \cong (F_\mathfrak{p} \otimes_F F) \otimes_F A \cong F_p \otimes_F M_2(F) \cong M_2(F_\mathfrak{p})$.

Now we assume that $F_\mathfrak{p}$ splits $A_\mathfrak{p}$ for all primes $\mathfrak{p}$ in F, and write $A = \left(\frac{a,b}{F}\right)$. By Theorem 2.1, $F_\mathfrak{p}$ splits $A_\mathfrak{p}$ iff $a \in N_{E_\mathfrak{p}/F_\mathfrak{p}}(E_\mathfrak{p})$ with $E_\mathfrak{p} = F_\mathfrak{p}(\sqrt{b})$. Now let $E = F(\sqrt{b})$. To apply the Hasse norm theorem, we have to know $a \in N_{E_\mathfrak{P}/F_\mathfrak{p}}(E_\mathfrak{P})$ for all primes $\mathfrak{p}$ in F and all primes $\mathfrak{P}$ in E lying above $\mathfrak{p}$ (actually since E/F is Galois, it suffices for any $\mathfrak{P}$ lying above a given $\mathfrak{p}$).

For any $\mathfrak{P}$ lying above a given $\mathfrak{p}$, we have $[E_\mathfrak{P} : F_\mathfrak{p}] = ef$ so $[E_\mathfrak{P} : F_\mathfrak{p}] = 1$ iff $\mathfrak{p}$ splits in E and is 2 otherwise. In the split case, for each of the two primes $\mathfrak{P}$ lying above $\mathfrak{p}$ we have $E_\mathfrak{P} = F_\mathfrak{p}$ contains $\sqrt{b}$ (since $E \subset E_\mathfrak{P}$). In the nonsplit case, $[E_\mathfrak{P} : F_\mathfrak{p}] = 2$, so $\sqrt{b} \notin F_\mathfrak{p}$. Thus $\sqrt{b} \in F_\mathfrak{p}$ iff $\mathfrak{p}$ is split. It now follows that for all $\mathfrak{p}$, $E_\mathfrak{P} = E_\mathfrak{p}$. Thus a is a local norm at all primes and by the Hasse norm theorem, $a \in N_{E/F}(E)$ which means that $A = \left(\frac{a,b}{F}\right)$ is split as required.

Conversely, we assume the validity of the Albert-Brauer-Hasse-Noether theorem. Let E/F be a quadratic extension of number fields, say $E = F(\sqrt{b})$. If $a \in N_{E/F}(E)$ then it follows easily that a is a local norm at all primes. So suppose that $a \in F$ is in the image of the norm $N_{E_{\mathfrak{P}}/F_{\mathfrak{p}}}$ for all primes $\mathfrak{P} \mid \mathfrak{p}$ of E. Consider the quaternion algebra $A = \left(\frac{a,b}{F}\right)$. By Theorem 2.1, the local norm condition is equivalent to $A_{\mathfrak{p}}$ splitting over each completion $F_{\mathfrak{p}}$. By the Albert-Brauer-Hasse-Noether theorem, A is split over F, and by Theorem 2.1 once again, $a \in N_{E/F}(E)$.

3.3 Implications of Hilbert Reciprocity

Recall the characterization of the Hilbert symbol. Let F be a number field and $a, b \in F$, $\mathfrak{p}$ a prime of F. The Hilbert symbol $(a,b)_{\mathfrak{p}} = \pm 1$ with value $+1$ iff $ax^2 + by^2 = 1$ is solvable in $F_{\mathfrak{p}}$, which by Theorem 2.1 is true iff $\left(\frac{a,b}{F_{\mathfrak{p}}}\right)$ is split.

As we have mentioned before, the Hilbert Reciprocity Law says that $\prod_{p \leq \infty} (a,b)_{\mathfrak{p}} = 1$. The Albert-Brauer-Hasse-Noether theorem says that $\left(\frac{a,b}{F}\right)$ is split iff $(a,b)_{\mathfrak{p}} = 1$ for all $\mathfrak{p}$. In particular, $\left(\frac{a,b}{F}\right)$ is a division algebra iff $(a,b)_{\mathfrak{p}} = -1$ for at least two (and always a finite even number of) primes in F.

Interestingly given any choice of a finite even number of primes, there is (up to isomorphism) a unique quaternion algebra over F ramified at precisely those primes.

3.4 Hasse-Minkowski Theorem

The quaternion algebra $\left(\frac{a,b}{K}\right)$ is split iff the norm form $w^2 - ax^2 - by^2 + abz^2$ is isotropic (i.e., represents zero nontrivially). Hasse-Minkowski says that over a global field, a quadratic form is isotropic iff it is isotropic over all completions providing yet another local-global characterization of the main theorem (at least in the quaternion case).

References

[1] T. Y. Lam, *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics, vol. 67, American Mathematical Society, Providence, RI, 2005. MR MR2104929 (2005h:11075)

[2] Richard S. Pierce, *Associative algebras*, Graduate Texts in Mathematics, vol. 88, Springer-Verlag, New York, 1982, , Studies in the History of Modern Science, 9. MR MR674652 (84c:16001)

[3] I. Reiner, *Maximal orders*, Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1975, London Mathematical Society Monographs, No. 5. MR MR0393100 (52 #13910)

[4] Peter Roquette, *The Brauer-Hasse-Noether theorem in historical perspective*, Schriften der Mathematisch-Naturwissenschaftlichen Klasse der Heidelberger Akademie der Wissenschaften [Publications of the Mathematics and Natural Sciences Section of Heidelberg Academy of Sciences], vol. 15, Springer-Verlag, Berlin, 2005. MR MR2222818 (2006m:11160)

DEPARTMENT OF MATHEMATICS, 6188 KEMENY HALL, DARTMOUTH COLLEGE, HANOVER, NH 03755

Fax: (603) 646-1312

E-mail address: thomas.r.shemanske@dartmouth.edu

URL: http://www.math.dartmouth.edu/~trs/