Ulam Quarterly — Volume 1, Number 1, 1992

Products of Symbol Algebras That Ramify Only on a Nonsingular Plane Elliptic Curve

Timothy J. Ford

Department of Mathematics
Florida Atlantic University
Boca Raton, FL 33431
e-mail address: ford@acc.fau.edu

Abstract

The elements of the Brauer group of the complement of a plane elliptic curve are presented as products of symbol algebras over the field of rational functions on the plane.

Acknowledgements

The author was supported in part by the National Science Foundation under grant DMS-8822944. The author also wishes to thank Professors David Saltman and John Tate for their help and encouragement on this project.

Let k be an algebraically closed field of characteristic zero and $C \subseteq \mathbf{P}^2$ a nonsingular plane elliptic curve, defined by the cubic polynomial $F \in k[x, y, z]$. In this note we study central division algebras D over $K = k(x/z, y/z)$ which ramify only on C. Algebras representing the Brauer classes of such D have recently been constructed using methods of Quantum Groups. Work along these lines has been done by M. Artin, J. Tate, M. Van den Bergh, W. Schelter, A. B. Odeskii and B. L. Feigin (see [1], [2], [3], [4], [8], [9]). It follows from their work, for example, that for any such central division algebra D over K the index of $D = \sqrt{(D : K)}$ is equal to the exponent of D in the Brauer group $B(K)$. David Saltman immediately posed some related questions to the author. First, if D has index n, does there exist a cyclic extension $K(\alpha^{1/n})$ which splits D? That is, is D a cyclic algebra of degree n? Secondly, is D split by the specific cyclic extension $L = K(F(x/z, y/z, 1)^{1/n})$? To the second question the answer is yes for

$n \leq 4$, since in that case L is quickly seen to be a rational function field. For higher n, the question remains open. In view of these results and open questions, it seems interesting and worthwhile to have a formula if not for D at least for a representative of the Brauer class of D in terms of cyclic algebras. The purpose of this note is to give such an explicit formula. As our title suggests, we prefer to write our cyclic algebras as symbol algebras. If α, β are elements of the field K and ζ is a fixed n^{th} root of unity, the symbol algebra $(\alpha, \beta)_n$ is the free associative K-algebra generated by 2 elements u, v subject to the relations $u^n = \alpha$, $v^n = \beta$, $uv = \zeta vu$. The symbol algebra $(\alpha, \beta)_n$ is split by $K(\alpha^{1/n})$, hence is a cyclic algebra.

From [5, Theorem 5], for example, it follows that the Brauer group of the complement of C $B(\mathrm{P}^2 - C)$ is isomorphic to the group $H^1(C, \mathbf{Q}/\mathbf{Z})$ which parametrizes the unramified cyclic Galois extensions of C. The isomorphism is described in [6] and associates to an algebra class A in $B(\mathbf{P}^2 - C)$ a cyclic Galois cover L of C. This L is loosely called the ramification of A on C. Fix an isomorphism $\mathbf{Q}/\mathbf{Z} \cong \mu$, where μ is the sheaf of all roots of unity. From Kummer theory [7, p. 126], the sequence

$$0 \to C^*/C^{*n} \to H^1(C, \mu_n) \to {}_nPic\ C \to 0 \tag{1}$$

is exact for all $n \geq 2$, where ${}_nPic\ C$ denotes the elements annihilated by n in $Pic\ C$. Since $C^* = k^*$, we see that $H^1(C, \mathbf{Q}/\mathbf{Z})$ is isomorphic to the torsion subgroup of $Pic\ C$. Since C is nonsingular the Picard group $Pic\ C$ is isomorphic to the divisor class group $Cl(C)$. Pick an identity element Q_0 for the group law on C. Since C is an elliptic curve, torsion elements in the Picard group of C correspond up to linear equivalence to Weil divisors of the form $Q - Q_0$ where $nQ - nQ_0$ is principal for some $n > 0$. In this note we intend to explicitly construct in terms of symbol algebras an algebra A whose class in $B(\mathbf{P}^2 - C)$ corresponds to $Q - Q_0$ where $Q - Q_0$ is a divisor of order $n = p^s$ and p is a prime. Since $B(\mathbf{P}^2 - C)$ can be identified with the subgroup of $B(K(\mathbf{P}^2))$ consisting of algebra classes which ramifiy only along C, we construct the algebra A over the field $K(\mathbf{P}^2)$.

Suppose the Weil divisor $Q - Q_0$ has order n in $Cl(C)$ and α is a rational function on C such that the divisor of α is $(\alpha) = nQ - nQ_0$. Using [7, p. 125] one sees that the unramified cyclic extension of C corresponding to $Q - Q_0$ is the integral closure of C in $K(C)[T]/(T^n - \alpha)$.

In order to simplify notation, we assume the curve C intersects the line at infinity $z = 0$ in the point Q_0, with multiplicity 3, and dehomogenize the projective plane with respect to z. Let $\mathbf{A}^2$ denote the affine plane $z \neq 0$ and $C' = C - Q_0$. From [5, Theorem 5] the rows of the diagram

$$\begin{tikzcd} B(\mathbf{P}^2) \arrow[r] \arrow[d] & B(\mathbf{P}^2 - C) \arrow[r] \arrow[d] & H^1(C, \mathbf{Q}/\mathbf{Z}) \arrow[r] \arrow[d] & H^3(\mathbf{P}^2, \mathbf{Q}/\mathbf{Z}) \arrow[d] \\ B(\mathbf{A}^2) \arrow[r] & B(\mathbf{A}^2 - C') \arrow[r] & H^1(C', \mathbf{Q}/\mathbf{Z}) \arrow[r] & H^3(\mathbf{A}^2, \mathbf{Q}/\mathbf{Z}) \end{tikzcd} \tag{2}$$

are exact. Since $B(\mathbf{P}^2) = B(\mathbf{A}^2) = 0$ and $H^3(\mathbf{P}^2, \mathbf{Q}/\mathbf{Z}) = H^3(\mathbf{A}^2, \mathbf{Q}/\mathbf{Z}) = 0$, the four remaining groups in (2) are isomorphic. From now on we write C for the affine curve C' and proceed as follows. Let Q be a point on C of order $n = p^s$. We find a function $\alpha \in k(x,y)$ of the form $\alpha = t_1^{e_1} \cdots t_m^{e_m}$ where $e_i \in \mathbf{Z}$, each t_i is a linear polynomial in $k[x,y]$ and such that α restricts to a function on C whose divisor is $(\alpha) = nQ$. Using the description of symbol algebras in [6, Section 2], the ramification of the symbol algebra $A_1 = (f, \alpha)_n$ on C is the cyclic extension corresponding to the point Q. By [6, Theorem 2.1] if Y is the curve $t_1 \cdots t_m = 0$, there is an algebra A_2 in $B(\mathbf{A}^2 - Y)$ such that $A_1 A_2$ represents the desired algebra class in $B(\mathbf{A}^2 - C)$. Using [5, Theorem 4] A_2 is Brauer equivalent to a product of the form $\prod (t_i, t_j)_n^{r_{ij}}$. With this introduction we state our first result.

Theorem 1. *Let C be a nonsingular affine plane elliptic curve defined by $f = 0$. Assume the projective completion of C is nonsingular and C has only 1 point at infinity. Given any point Q on C of order $n = p^s$ for some prime p, there are lines defined by equations $t_1 = 0, \ldots, t_m = 0$ and integers p^u, $\{e_i\}_{i=1}^m$, $\{r_{ij}\}_{1 \le i < j \le m}$ such that the product of symbol algebras over $k(x,y)$*

$$A = (f, t_1^{e_1} \cdots t_m^{e_m})_{p^u} \cdot \prod_{i<j} (t_i, t_j)_{p^u}^{r_{ij}}$$

ramifies only on C with ramification corresponding to the point Q.

Proof. By the above discussion, it suffices to find lines $t_1, \ldots, t_m$ and integers $e_1, \ldots, e_m$ satisfying the property that if $\alpha = t_1^{e_1} \cdots t_m^{e_m}$, then the divisor of α on C is $(\alpha) = nQ$. We consider 3 cases.

Case 1. $n = 3$. In this case, Q is a flex on C. Let $t = 0$ be the tangent line to C at Q. Then the divisor of $\alpha = t$ is $(\alpha) = 3Q$, so the function α does the job. In this case $A = (f, \alpha)_3$ is an algebra with ramification Q.

Case 2. $n = 2^s$. Consider the s points $Q, (-2)Q, (-2)^2 Q, \ldots, (-2)^{s-1} Q$. Let $t_i = 0$ be the tangent line to C at $(-2)^i Q$, $i = 0, \ldots, s-1$. Then for $i = 0, \ldots, s-2$, t_i intersects C at the point $(-2)^i Q$ with multiplicity 2 and at the point $(-2)^{i+1} Q$ with multiplicity 1. The divisor of $\alpha = t_0^{e_0} \cdots t_{s-1}^{e_{s-1}}$ on C is $w_0 Q + w_1(-2)Q + w_2(-2)^2 Q + \ldots + w_{s-1}(-2)^{s-1} Q$ where the integers $w_0, \ldots, w_{s-1}$ are given by the matrix product

$$\begin{bmatrix} w_0 \\ \vdots \\ w_{s-1} \end{bmatrix} = \begin{bmatrix} 2 & & & & & 0 \\ 1 & 2 & & & & 0 \\ & 1 & 2 & \ldots & & 0 \\ 0 & & & & 1 & 2 \end{bmatrix} \begin{bmatrix} e_0 \\ \vdots \\ e_{s-1} \end{bmatrix} = \begin{bmatrix} 2e_0 \\ \vdots \\ e_{s-2} + 2e_{s-1} \end{bmatrix}$$

If we take $e_0 = (-2)^{s-1}$, $e_1 = (-2)^{s-2}$, $\ldots$, $e_{s-2} = -2$, $e_{s-1} = 1$, then $(w_0, \ldots, w_{s-1}) = (-(-2)^s, 0, \ldots, 0)$. Therefore, the divisor of α is $(\alpha) = \pm nQ$ and either α or $1/\alpha$ is the desired function.

Case 3. $n = p^s$ where $p \neq 2$ and $n > 3$. Say -2 has order m (mod p^s). That is, m is the smallest positive integer such that $1 - (-2)^m$ is divisible by p^s. I don't know whether it is possible for there to exist $r > s$ such that p^r divides $1-(-2)^m$, but if so, choose r to be the largest positive integer such that p^r divides $1-(-2)^m$. Since the group law on the elliptic curve C is divisible, there exists a point P of order p^r and $p^{r-s}P \sim Q$. Therefore, it suffices to prove the theorem for the point P. Consider the points P, $(-2)P$, $\ldots$, $(-2)^{m-1}P$. Because $p \neq 2$, none of these points is a flex. Let $t_i = 0$ be the tangent line to C at $(-2)^iP$, $i = 0, \ldots, m-1$. The tangent line $t_i = 0$ intersects C at $(-2)^iP$ with intersection multiplicity 2 and at $(-2)^{i+1}P$ with intersection multiplicity 1. The divisor of the function $\alpha = t_0^{e_0} \cdots t_{m-1}^{e_{m-1}}$ on C is $w_0P + w_1(-2)P + w_2(-2)^2P + \ldots + w_{m-1}(-2)^{m-1}P$ where the integers $w_0, \ldots, w_{m-1}$ are given by the matrix product

$$\begin{bmatrix} w_0 \\ \vdots \\ w_{m-1} \end{bmatrix} = \begin{bmatrix} 2 & & & & 0 & 1 \\ 1 & 2 & & & & 0 \\ & 1 & 2 & \ldots & & 0 \\ 0 & & & & 1 & 2 \end{bmatrix} \begin{bmatrix} e_0 \\ \vdots \\ e_{m-1} \end{bmatrix} = \begin{bmatrix} e_{m-1} + 2e_0 \\ \vdots \\ e_{m-2} + 2e_{m-1} \end{bmatrix}$$

If we let $e_0 = (-2)^{m-1}$, $e_1 = (-2)^{m-2}$, $\ldots$, $e_{m-2} = -2$, $e_{m-1} = 1$, then $(w_0, \ldots, w_{m-1}) = (1-(-2)^m, 0, \ldots, 0)$. So the divisor of α is $(\alpha) = (1-(-2)^m)P = p^r vP$ where we factor $1-(-2)^m = p^r v$ and v is relatively prime to p. There is a function $\gamma \in k[x,y]$ such that the divisor of γ restricted to C is $vP - P_1$, where P_1 is a point of order p^r on C. Therefore, the divisor of α/γ^{p^r} is $(\alpha) - p^r(\gamma) = p^r P_1$. So the unramified extension of C obtained by adjoining a $p^r - th$ root of α corresponds to the point P_1 in the group law on C. Since P and P_1 generate the same group on C, it suffices to prove the theorem for P_1, and α is the desired function. Q.E.D.

Our second result uses the techniques of [6, Section 2] to determine the integers r_{ij} of Theorem 1 explicitly in terms of the exponents e_i.

Theorem 2. *(1) Let p be an odd prime and P a point on C of order $p^r > 3$ where -2 has order m mod(p^r) and p^r is the largest power of p dividing $1-(-2)^m$. Let $\alpha = t_0^{e_0} \cdots t_{m-1}^{e_{m-1}}$ be as in Case 3 of the proof of Theorem 1. Then the Brauer class of the algebra in $B(\mathbf{P}^2 - C)$ corresponding to the point P is represented by*

$$A = \left(f, t_0^{e_0} \cdots t_{m-1}^{e_{m-1}}\right)_{p^r} (t_{m-1}, t_{m-2})_{p^r}^{-e_{m-2}} \cdots (t_i, t_{i-1})_{p^r}^{-e_{i-1}} \\ \cdots (t_1, t_0)_{p^r}^{-e_0} (t_0, t_{m-1})_{p^r}^{-e_{m-1}}$$

(2) Let Q be a point of order 2^s on C and $\alpha = t_0^{e_0} \cdots t_{s-1}^{e_{s-1}}$ as in Case 2 of the proof of Theorem 1. Then the Brauer class of the algebra in $B(\mathbf{P}^2 - C)$ corresponding to the point Q is represented by

$$A = \left(f, t_0^{e_0} \cdots t_{s-1}^{e_{s-1}}\right)_{2^s} (t_{s-1}, t_{s-2})_{2^s}^{-e_{s-2}} \cdots (t_i, t_{i-1})_{2^s}^{-e_{i-1}} \cdots (t_1, t_0)_{2^s}^{-e_0}$$

Proof. (1) We use the notation and terminology of [6, Section 2]. In Case 3 of the proof of Theorem 1, the graph corresponding to the symbol algebra $(f,t_i)_n^{e_i}$ is

$$\begin{tikzcd}
f \arrow[r, "2e_i"] & (-2)^i P \arrow[d, "-2e_i"] \\
(-2)^{i+1}P \arrow[u, "e_i"] & t_i \arrow[l, "-e_i"']
\end{tikzcd}$$

Now C intersects the divisor of α only at the points P, $(-2)P$, $\dots$, $(-2)^{m-1}P$. Therefore, the algebra class $\prod_{i<j}(t_i,t_j)_{p^u}^{r_{ij}}$ of Theorem 1 corresponds to the weighted cyclic graph

$$\begin{tikzcd}
(-2)^i P \arrow[r, "e_{i-1}"] & t_{i-1} \arrow[dr] & \\
t_i \arrow[u, "2e_i"] & & \vdots \arrow[dl] \\
(-2)^{i+1}P \arrow[u, "e_i"] & t_{i+1} \arrow[l, "2e_{i+1}"'] &
\end{tikzcd}$$

Since $-2e_i = e_{i-1}$, this cycle corresponds to the product of symbol algebras $(t_{m-1},t_{m-2})_n^{-e_{m-2}} \cdots (t_i,t_{i-1})_n^{-e_{i-1}} \cdots (t_0,t_{m-1})_n^{-e_{m-1}}$. The proof of (2) is similar. Q.E.D.

References

[1] M. Artin and W. Schelter, *Graded algebras of global dimension 3,* Advances in Math. 66 (1987), pp. 171–216.

[2] M. Artin, J. Tate, and M. Van den Bergh, *Modules over regular algebras of dimension 3,* preprint.

[3] M. Aartin, *Some algebras associated to automorphisms of elliptic curves,* in The Grothendieck Festschrift, vol. 1, 1990, Birkhäuser, Boston, pp. 33–85.

[4] M. Artin and M. Van den Bergh, *Twisted homogeneous coordinate rings,* J. Algebra, 133 (1990), pp. 249–271.

[5] T. J. Ford, *On the Brauer group of* $k[x_1,...,x_n,1/f]$, J. Algebra, 122 (1989), pp. 410–424.

[6] T. J. Ford, *On the Brauer group of a localization,* J. Algebra, (to appear).

[7] J. Milne, *Etale Cohomology,* Princeton University Press, Princeton, N.J., 1980.

[8] A. B. Odeskii and B. L. Feigin, *Sklyanin algebras associated to elliptic curves,* preprint.

[9] M. Van den Bergh, *Regular algebras of dimension 3,* in Séminaire Dubreil-Malliavin 1986, vol. 1296 of Lecture Notes in Math., 1987, Springer-Verlag, Berlin, pp. 228–234.