



Project  
**MUSE**<sup>®</sup>

*Scholarly journals online*

# A NOTE ON ELLIPTIC CURVES AND GALOIS MODULE STRUCTURE IN GLOBAL FUNCTION FIELDS

By A. AGBOOLA

---

*Abstract.* In this paper we study the Galois module structure of certain Kummer orders obtained by dividing torsion points on an elliptic curve defined over a global function field. We prove that such Kummer orders are globally free as Galois modules. This is the analogue over function fields of a conjecture first stated by M. J. Taylor for CM elliptic curves defined over number fields.

**0. Introduction and statement of results.** The purpose of this paper is to study the Galois module structure of certain Kummer orders obtained by dividing torsion points on an elliptic curve defined over a global function field.

For any field  $L$ , we shall write  $L^c$  for a separable closure of  $L$ , and  $\Omega_L$  for  $\text{Gal}(L^c/L)$ . Let  $r$  be a prime, and let  $\mathbb{F}_r$  denote the finite field containing  $r$  elements. Let  $k$  be a field such that either  $k \subseteq \mathbb{F}_r^c$  or  $k \subseteq \mathbb{C}$ . Suppose that  $C$  is a smooth, geometrically irreducible curve defined over  $k$ . Set  $F = k(C)$ , the function field of  $C$  over  $k$ . Let  $S = \{v_1, \dots, v_i\}$  be a fixed, non-empty, finite set of places of  $F$ , and let  $O_{F,S} = O_F$  denote the ring of functions in  $F$  which are regular away from  $S$ .  $O_F$  is the function field analogue of the ring of integers of a number field. Write  $O^c$  for the integral closure of  $O_F$  in  $F^c$ . If  $L/F$  is any finite extension of  $F$ , then we shall write  $O_L$  for the integral closure of  $O_F$  in  $L$ .

Let  $E/F$  be an abelian variety defined over  $F$ . In what follows, we shall always assume that  $S$  contains all places of bad reduction of  $E$ . We shall also suppose that all endomorphisms of  $E$  that we consider are defined over  $F$ . We write  $\underline{O}$  for the origin of the group law on  $E$ .

Let  $p > 3$  be a rational prime with  $p \neq r$  if  $k \subseteq \mathbb{F}_r^c$ , and write  $G_i$  for the subgroup of elements of  $E(F^c)$  which are killed by the endomorphism  $[p^i]$  of  $E$ . The  $O_F$ -group scheme of  $p^i$ -torsion points on  $E$  is affine and étale and is therefore equal to  $\text{Spec}(\mathfrak{B}_i(F))$ , where  $\mathfrak{B}_i(F) = \mathfrak{B}_i = \text{Map}(G_i, O^c)^{\Omega_F}$  is the  $O_F$ -Hopf algebra consisting of  $\Omega_F$ -maps from  $G_i$  to  $O^c$ . (Thus  $\mathfrak{B}_i$  is the unique  $O_F$ -maximal order in the algebra  $B_i(F) := \text{Map}(G_i, F^c)^{\Omega_F}$ .) It follows that the  $O_F$ -Cartier dual of  $\mathfrak{B}_i$  is  $\mathfrak{A}_i(F) = \mathfrak{A}_i = (O^c G_i)^{\Omega_F}$  (here  $\Omega_F$  acts on both  $O^c$  and  $G_i$ ).  $\mathfrak{A}_i(F)$  is thus the unique  $O_F$ -maximal order in the  $F$ -algebra  $A_i(F) = A_i = (F^c G_i)^{\Omega_F}$ .

---

Manuscript received June 10, 1994; revised June 26, 1995.

Research supported in part by an NSF Postdoctoral Research Fellowship.

*American Journal of Mathematics* 118 (1996), 427–438.

Now suppose that  $Q \in E(F)$ , and write

$$(0.1) \quad G_Q(i) = \{Q' \in E(F^c): [p^i]Q' = Q\}.$$

Define the Kummer algebra  $F_Q(i)$  by

$$(0.2) \quad F_Q(i) = \text{Map}(G_Q(i), F^c)^{\Omega_F}.$$

Then  $[F_Q(i): F] = |G_i|$ , and  $A_i$  acts on  $F_Q(i)$  via

$$(0.3) \quad \left( f \cdot \sum_{g \in G_i} a_g g \right) (Q') = \sum_{g \in G_i} a_g f(Q' + g).$$

for  $f \in F_Q(i)$  and  $\sum_{g \in G_i} a_g g \in A_i$ .

The  $F$ -algebra structure of  $F_Q(i)$  may be described as follows. Let  $Q^{(1)}, \dots, Q^{(s)}$  be a set of representatives of the  $\Omega_F$ -orbits of  $G_Q(i)$ . Then, as an  $F$ -algebra, we have

$$F_Q(i) \simeq \prod_{i=1}^s F[Q^{(i)}]$$

where  $F[Q^{(i)}]$  is the field obtained by adjoining the coordinates of  $Q^{(i)}$  to  $F$ . Explicitly, the isomorphism is given by  $f \mapsto \prod_{i=1}^s f(Q^{(i)})$  for  $f \in F_Q(i)$ . Note also that if  $G_i \subseteq E(F)$ , then all the fields  $F[Q^{(i)}]$  are the same.

Let  $O_Q(i)$  denote the integral closure of  $O_F$  in  $F_Q(i)$ . Then  $O_Q(i)$  (the *Kummer order*) is an  $\mathfrak{A}_i$ -module. As  $\mathfrak{A}_i$  is the maximal order of  $A_i$ , it follows that  $O_Q(i)$  is a locally free  $\mathfrak{A}_i$ -module (see e.g. [CR], proposition 31.2). Thus, if  $Cl(\mathfrak{A}_i)$  denotes the locally free classgroup of  $\mathfrak{A}_i$ , then we have a map

$$(0.4) \quad \psi_i: E(F) \longrightarrow Cl(\mathfrak{A}_i)$$

given by  $\psi_i(Q) = (O_Q(i))$ , where  $(O_Q(i))$  is the class of  $O_Q(i)$  in  $Cl(\mathfrak{A}_i)$ . As  $E$  has good reduction at all places of  $O_F$ , it follows exactly as per theorem 1 of [T] that  $\psi_i$  is a homomorphism, and so in particular that the image of  $\psi_i$  is annihilated by  $|G_i|$ . Observe that since  $G_i$  is abelian,  $\mathfrak{A}_i$  satisfies that Eichler condition. Hence  $O_Q(i)$  is a globally free  $\mathfrak{A}_i$ -module if and only if  $\psi_i(Q) = 0$ .

We are now able to state the main result of this paper.

**THEOREM 1.** *Suppose that  $E$  is an elliptic curve. Then  $E(F)_{\text{torsion}} \subseteq \ker(\psi_i)$ .*

Theorem 1 is the function field analogue of a conjecture first stated by M. J. Taylor for CM elliptic curves over number fields (see [T]). A large part of this conjecture (for CM elliptic curves) was proved in [ST]. The main technique

of proof in [ST] was the use of modular functions and the  $q$ -expansion principle to prove integrality statements concerning certain resolvent elements that arise as special functions on  $E$ . A different proof relying upon elementary intersection theory rather than modular functions, and valid for all elliptic curves with everywhere good reduction, was given in [A2]. The techniques used in proving Theorem 1 of the present paper are very similar to (albeit somewhat easier than) those used in treating the corresponding result over number fields as described in [A2]. For further results on the class invariant homomorphism over function fields, we refer the reader to [A1].

**1. Preliminary results.** In this section we recall certain preliminary results concerning Kummer orders that we shall require. We first of all give an alternative description of  $O_Q(i)$  as a  $Q$ -twist of the algebra  $\mathfrak{B}_i$  (cf. §4 of [T]).

Let  $N/F$  be a finite extension containing the coordinates of  $G_i$  and  $G_Q(i)$ . Then there is an isomorphism of  $N$ -algebras (and  $A_i$ -modules)  $B_i(N) \simeq N_{O_Q(i)}$  induced by translation by any  $Q' \in G_Q(i)$ . So there is an isomorphism of  $N$ -algebras and  $A_i$ -modules given by

$$(1.1) \quad \xi: B_i \otimes_F N \longrightarrow F_{O_Q(i)} \otimes_F N$$

where  $\xi(b \otimes n)(Q' + g) = b(g)n$  for  $b \in B_i$ ,  $n \in N$ , and  $g \in G_i$ . (Here  $\Omega_F$  acts on both terms of (1.1) via the second factor.) Then we have

$$(1.2) \quad O_Q(i) = [\xi(\mathfrak{B}_i \otimes_{O_F} O_N)]^{\Omega_F}.$$

For any finite extension  $M$  of  $F$ , it follows that

$$(1.3) \quad O_Q(i)(M) = O_Q(i)(F) \otimes_{O_F} O_M, \quad O_Q(i)(F) = O_Q(i)(M)^{\Omega_F}.$$

We shall now describe the relationship between  $(O_Q(i)) \in Cl(\mathfrak{A}_i)$  and  $(O_Q(j)) \in Cl(\mathfrak{A}_j)$  for  $0 < j < i$ , using the methods of §2 of [ST].

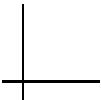
The natural surjection  $[p^{i-j}]: G_i \rightarrow G_j$  induces a surjective homomorphism  $A_i \rightarrow A_j$  of Hopf algebras (which we shall also denote by  $[p^{i-j}]$ ) given by

$$(1.4) \quad [p^{i-j}] \left( \sum_{g \in G_i} \alpha_g g \right) = \sum_{g \in G_j} \alpha_g ([p^{i-j}]g).$$

Similarly, the inclusion  $G_j \rightarrow G_i$  induces an inclusion  $A_j \rightarrow A_i$  of Hopf algebras. Since these maps are induced by homomorphisms of group schemes, we deduce that  $\mathfrak{A}_j$  may be viewed as either a quotient algebra or a subalgebra of  $\mathfrak{A}_i$ .

Next, we observe that  $G_i$  acts on  $\text{Map}(G_i, F^c)$  via translations, i.e.

$$(1.5) \quad f^g(h) = f(g+h) \quad \forall f \in \text{Map}(G_i, F^c) \quad \text{and} \quad g, h \in G_i.$$



The isomorphism  $G_i/G_j \simeq G_{i-j}$  induces identifications

$$(1.6) \quad F^c G_{i-j} = (F^c G_i)^{G_j}$$

and

$$(1.7) \quad \text{Map}(G_{i-j}, F^c) = \text{Map}(G_i, F^c)^{G_j}.$$

The identifications (1.6) and (1.7) in turn induce isomorphisms of  $\mathfrak{A}_{i-j}$  with a subalgebra of  $\mathfrak{A}_i$  and  $\mathfrak{B}_{i-j}$  with a subalgebra of  $\mathfrak{B}_i$ .

PROPOSITION 1.1. *There are isomorphisms*

$$(1.8) \quad F_Q(j) \simeq \Sigma_{i-j} \cdot F_Q(i)$$

as  $A_j$ -modules, and

$$(1.9) \quad O_Q(j) \simeq \Sigma_{i-j} \cdot O_Q(i)$$

as  $\mathfrak{A}_j$ -modules. These isomorphisms are compatible with the inclusions  $O_Q(j) \rightarrow F_Q(j)$  and  $O_Q(i) \rightarrow F_Q(i)$ .

Here  $\Sigma_{i-j} = \Sigma_{g \in G_{i-j}} g$  is viewed as an element of  $A_i$ , and  $A_j$  (resp.  $\mathfrak{A}_j$ ) acts on the right-hand side of (1.8) (resp. (1.9)) via the surjective homomorphism  $[p^{i-j}]$ .

*Proof.* Via (1.3), together with the fact that  $\otimes_{O_F} O_N$  is faithfully flat, we may assume that the field  $F$  contains the coordinates of  $G_i$  and  $G_Q(i)$ . Next, we observe that (1.2) allows us to assume in addition that  $P = \underline{Q}$ , i.e. that  $O_Q(i) = \mathfrak{B}_i$  and  $O_Q(j) = \mathfrak{B}_j$ . The result now follows via the discussion immediately preceding the statement of Proposition 1.1.  $\square$

Proposition 1.1 implies that in order to prove Theorem 1, we may replace  $p^i$  by a higher power of  $p$ . Let  $l$  and  $l'$  be distinct odd primes not equal to  $p$ . Suppose further that  $(r, ll') = 1$  if  $k \subseteq \mathbb{F}_r$ . Then, by replacing  $p^i$  by a higher power of  $p$  if necessary, we shall henceforth assume that

$$(1.10) \quad p^i \equiv 1 \pmod{ll'}.$$

We next observe that it follows from the definition of  $O_Q(i)$  that  $\psi_i(Q)$  in fact depends only upon the image of  $Q$  in  $E(F)/p^i E(F)$ . Hence, in order to prove Theorem 1, we may in fact assume that  $Q \in E(F)$  is a  $p$ -power torsion point. We

shall make this assumption from now on. Observe that, with this assumption, we have

$$(1.11) \quad p^i \cdot (\mathcal{C}_Q(i)) = 0$$

in  $Cl(\mathfrak{A}_i)$ .

Our next result deals with the valuations of certain Lagrange resolvents. Suppose that  $a \in F_Q(i)$  and  $\chi$  is a character of  $G$ . The resolvent of  $a$  at  $\chi$  is defined by

$$(a|\chi) = \sum_{g \in G_i} \chi(g^{-1})a^g \in F_Q(i).$$

For each place  $v$  of  $O_F$ , let  $O_{F,v}$  (resp.  $O_{Q,v}(i)$ , resp.  $\mathfrak{A}_{i,v}(F)$ ) denote the semi-local completion of  $O_F$  (resp.  $O_Q(i)$ , resp.  $\mathfrak{A}_i(F)$ ) at  $v$ . Choose  $a_v \in O_{Q,v}(i)$  such that  $O_{Q,v}(i) = a_v \cdot \mathfrak{A}_{i,v}(F)$ . As  $E/F$  has good reduction at all places of  $O_F$ , it follows from the criterion of Néron-Ogg-Shafarevitch and the description of  $F_Q(i)$  given in §0 that  $F_Q(i)/F$  is unramified at all places of  $O_F$ . The following result is a simple extension of proposition 4.3 in chapter 1 of [F] from fields to Galois algebras.

PROPOSITION 1.3. *Let  $a_v$  be as above. Then for all  $\chi \in \hat{G}_i$ , we have that  $(a_v|\chi) \in O_{Q,v}(i)^*$ .*

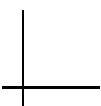
We conclude this section by recalling the following result from [T] regarding a change of basefields. (The result in [T] is proved for number fields, but it is easy to see that the proof given there carries over to our present situation.) For any finite extension  $M/F$ , there is a commutative diagram

$$(1.12) \quad \begin{array}{ccc} E(M) & \xrightarrow{\psi_{i,M}} & Cl(\mathfrak{A}_i(M)) \\ Tr_{M/F} \downarrow & & \downarrow Res \\ E(F) & \xrightarrow{\psi_{i,F}} & Cl(\mathfrak{A}_i(F)) \end{array}$$

where  $Tr_{M/F}$  is the trace map, and  $Res$  is the restriction map on classgroups defined as per §4 of [T].

**2. Intersection multiplicities and an integrality principle.** In this section we shall describe a method for proving integrality statements about special values of functions defined on  $E$ .

Write  $Div^0(E)$  for the group of divisors of degree zero on  $E$ . If  $Z \in Div^0(E)$  is the divisor of a rational function  $f$  on  $E$ , and  $Z' = \sum n_i(P_i)$  is a 0-cycle on  $E$



whose support is disjoint from that of  $Z$ , then we set

$$(2.1) \quad f(Z') = \prod_i f(P_i)^{n_i}.$$

It is easy to see that this is well-defined.

Let  $\mathcal{E}/O_F$  denote the Nèron minimal model of  $E/F$  over  $O_F$ . If  $Z = \sum_i n_i(P_i)$  is any divisor on the generic fibre  $\mathcal{E}_F$  of  $\mathcal{E}$ , then we write  $\mathbf{Z} = \sum_i n_i(\mathbf{P}_i)$  for the Zariski closure of  $Z$  on  $\mathcal{E}$ . If  $v$  is a place of  $O_F$ , and  $\mathbf{D}_1, \mathbf{D}_2$  are horizontal divisors on  $\mathcal{E}$  which intersect properly, then we write  $i_v(\mathbf{D}_1, \mathbf{D}_2)$  for the intersection multiplicity of  $\mathbf{D}_1$  and  $\mathbf{D}_2$  at  $v$  (see e.g. chapter III of [L] for definitions and further details regarding intersection multiplicities). Our principal tool for proving integrality results will be the following proposition.

**PROPOSITION 2.1.** *Let  $f$  be a function on  $E$  with divisor  $Z$ , and suppose that  $Z' \in \text{Div}^0(E)$  with  $\text{supp}(Z)$  disjoint from  $\text{supp}(Z')$ . (Here  $\text{supp}(Z)$  denotes the support of  $Z$ , with similar notation for  $Z'$ .) Assume that all components of  $Z, Z'$  are rational over  $F$ . Then for each place  $v$  of  $O_F$ , we have that*

$$(2.2) \quad \text{ord}_v(f(Z')) = i_v(\mathbf{Z}, \mathbf{Z}').$$

*In particular,  $f(Z')$  is integral at  $v$  if and only if  $i_v(\mathbf{Z}, \mathbf{Z}') \geq 0$ .*

*Proof.* This proposition simply summarises certain elementary facts concerning intersection multiplicities. See e.g. chapter III of [L] (especially theorems 5.1 and 5.2) for full details.  $\square$

Let us now explain how we use this proposition. Suppose that  $P_1, P_2$  are distinct torsion points on  $E(F)$ , with each of order prime to the characteristic of  $F$ . Let  $v$  be a place of  $O_F$ . Then  $P_1, P_2$  remain disjoint when reduced modulo  $v$ , and so we have that  $i_v(\mathbf{P}_1, \mathbf{P}_2) = 0$ . The following result is now immediate.

**PROPOSITION 2.2.** *Let the notation be as in Proposition 2.1. Suppose in addition that  $\text{supp}(Z)$  and  $\text{supp}(Z')$  consist of disjoint sets of torsion points of  $E(F)$  of order prime to the characteristic of  $F$ . Then*

$$(2.3) \quad \text{ord}_v(f(Z')) = i_v(\mathbf{Z}, \mathbf{Z}') = 0$$

*for each place  $v$  of  $O_F$ . Hence  $f(Z')$  is integral over  $O_F$ .*

We conclude this section by introducing a piece of notation. Suppose that  $a, b \in O^c$ . Then we write  $a \sim b$  if  $a/b \in O^{c*}$ .

**3. Special functions.** The purpose of this section is to describe two special functions that will play a major role in the proof of Theorem 1. These functions

are the same as those used to prove the corresponding result in the number field case (cf. §4 of [A2]).

Recall that  $E/F$  is an elliptic curve with good reduction at all places of  $F$  not in  $S$ . The numbers  $l$  and  $l'$  are distinct odd primes not equal to  $p$  or  $r$ , and  $Q \in E(F)$  is a  $p$ -power torsion point. We suppose further that  $p$  satisfies  $p^i \equiv 1(l')$ .

Let  $E_l$  (resp.  $E_{l'}$ ) denote the group of  $l$  (resp.  $l'$ ) torsion points of  $E$ , and write  $F(E_l)$  for the field obtained by adjoining the coordinates of the points in  $E_l$  to  $F$ . Let  $\theta$  and  $\phi$  be two independent  $l$ -torsion points. Choose a function  $D_{\theta,\phi}$ , rational over  $F(E_l)$  such that the divisor of  $D_{\theta,\phi}$  is given by

$$(3.1) \quad (D_{\theta,\phi}) = \sum_{k=0}^{l-1} (k\theta) - \sum_{k=0}^{l-1} (\phi + k\theta).$$

(In what follows, we shall write  $D$  for  $D_{\theta,\phi}$ .)  $D(z)$  and  $D(z + \theta)$  have the same divisor, and so,

$$(3.2) \quad D(z + \theta) = \omega.D(z) \quad \omega \in F(E_l).$$

Since  $l.\theta = Q$ , it follows that  $\omega^l = 1$ .

Write

$$(3.3) \quad w: G_i \times G_i \longrightarrow \mu_{p^i}$$

for the Weil pairing on  $G_i \times G_i$ . Suppose that  $\nu \in G_i$ . Then we define a homomorphism  $\chi_\nu: G_i \rightarrow \mu_{p^i}$  by

$$(3.4) \quad \chi_\nu(\gamma) = w(l.\gamma, \nu), \quad \gamma \in G_i.$$

It follows that the characters of  $G_i$  are precisely the  $\chi_\nu$ 's.

Next, consider the function  $H(z) = D(p^i z)/D(z)$ .  $H(z)$  has neither a zero nor a pole at  $z = Q$  and  $H(Q) = p^i$ . The following result is immediate.

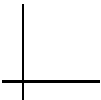
LEMMA 3.1. *The divisor of the function  $H(z)$  is given by*

$$(H(z)) = \sum_{g \in G_i \setminus Q} \left[ \sum_{k=0}^{l-1} (k\theta + g) - \sum_{k=0}^{l-1} (\phi + k\theta + g) \right].$$

Define the resolvent function  $R_\nu(z)$  by

$$(3.5) \quad R_\nu(z) = \frac{1}{p^i} \sum_{\gamma \in G_i} \frac{D(p^i z)}{D(z + \gamma)} \chi_\nu(-\gamma).$$

Note that  $R_\nu(z)$  is well-defined independently of the choice of  $D$ , and that  $R_\nu(Q) = 1$ . Our next result tells us about the divisor of  $R_\nu(z)$ .





PROPOSITION 3.2.

- (a) If  $\nu = \underline{O}$ , then  $R_\nu(z) = 1$ .
- (b) If  $\nu \neq \underline{O}$ , then

$$(R_\nu(z)) = \sum_{g \in G_i} \left[ \sum_{k=0}^{l-1} (\nu' + k\theta + g + \phi) - \sum_{k=0}^{l-1} (k\theta + g + \phi) \right]$$

where  $\nu'$  is any point in  $E(F^c)$  satisfying  $[p^i]\nu' = \nu$ .

*Proof.* This may be proved exactly as in the number field case. We refer the reader to proposition 4.2 of [A2] for details. □

**4. Integrality results.** We shall now use the results in §2 and §3 to obtain integrality statements concerning special values of the functions  $R_\nu(z)$  and  $H(z)$ .

We retain the notation of the previous sections. Fix a choice of  $\nu \in G_i$  with  $\nu \neq 0$ , and set  $Z_1 = (R_\nu(x))$ ,  $Z_2 = (H(z))$  (these are divisors on  $\mathcal{E}_F$ ); so,

$$(4.1) \quad Z_1 := \sum_{g \in G_i} \left[ \sum_{k=0}^{l-1} (\nu' + k\theta + \phi + g) - \sum_{k=0}^{l-1} (g + k\theta + \phi) \right]$$

and

$$(4.2) \quad Z_2 := \sum_{g \in G_i \setminus \underline{O}} \left[ \sum_{k=0}^{l-1} (k\theta + g) - \sum_{k=0}^{l-1} (g + k\theta + \phi) \right].$$

(Note that the divisor  $Z_1$  depends upon our choice of  $\nu$ , although we omit this dependence from our notation.)

Now let  $\psi$  be a primitive  $l'$ -torsion point of  $E$ , and let  $\beta$  be any  $p$ -power torsion point of  $E$ . Define a divisor  $Z_3$  on  $E_F$  by

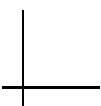
$$(4.3) \quad Z_3 = (\beta + \psi) - (\underline{O}).$$

Choose  $N/F$  to be a sufficiently large extension so that all components of  $Z_1, Z_2, Z_3$  are rational over  $N$ , and regard each  $Z_i$  as being a divisor on  $\mathcal{E}_N$ . We observe that

- (a)  $supp(Z_3)$  is disjoint from  $supp(Z_1) \cup supp(Z_2)$ .
- (b)  $Z_3$  and  $Z_i$  ( $i = 1, 2$ ) do not intersect on any vertical fibre of  $\mathcal{E}$ . This is because for each place  $v$  of  $O_L$ , the divisors  $Z_3$  and  $Z_i$  ( $i = 1, 2$ ) remain distinct when reduced modulo  $v$ .

The following result is an immediate consequence of these observations.

PROPOSITION 4.1. *Let  $v$  be a place of  $O_N$ . Then  $i_v(\mathbf{Z}_i, \mathbf{Z}_2) = 0$  for  $i = 1, 2$ .*



By combining Proposition 4.1 with Proposition 2.2, we obtain the following result.

PROPOSITION 4.2. (a)  $R_\nu(\beta + \psi) \in O^{c*}$  for all  $p$ -power torsion points  $\beta$  of  $E$  and all  $\nu \in G_i$ . Thus, if  $\beta_1, \beta_2$  are any  $p$ -power torsion points of  $E$ , then we have in particular that

$$R_\nu(p^i(\beta_1 + \psi)) \sim R_\nu(p^i(\beta_2 + \psi)) \sim 1$$

for all  $\nu \in G_i$ .

(b)  $H(\beta + \psi) \in O^{c*}$  for all  $p$ -power torsion points  $\beta$  of  $E$ .

**5. Proof of Theorem 1.** In this section we shall use our earlier results to give a proof of Theorem 1. The method used is the same as in the number field case.

Let  $M$  be the field  $F(E_{l'})$ , and define a function  $h$  on  $E$  by

$$(5.1) \quad h(z) = \frac{D(p^l z + \psi)}{D(z + \psi)}.$$

Then the functions  $D(z)$  and  $h(z)$  both lie in the function field  $M(E)$ .

LEMMA 5.1. For the field  $M$  as above, we have

$$[M : F] | [l(l+1)(l-1)^2] [l'(l'+1)(l'-1)^2].$$

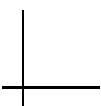
*Proof.* The group  $Gal(M/F)$  is a subgroup of  $GL_2(\mathbb{F}_l) \times GL_2(\mathbb{F}_{l'})$ . The result now follows from the fact that for any prime  $q$ , the group  $GL_2(\mathbb{F}_q)$  is of order  $q(q+1)(q-1)^2$ . □

LEMMA 5.2. Let  $\mathfrak{S}$  be the set of odd rational primes satisfying  $l \neq p$  and (if  $k \subseteq \mathbb{F}_r$ )  $l \neq r$ . (If  $k \subseteq \mathbb{C}$  then we simply ignore this latter condition.) Let  $w = HCF\{l(l+1)(l-1)^2 | l \in \mathfrak{S}\}$ . Suppose that  $q > 3$  is a prime. Then  $q \nmid w$ .

*Proof.* Choose a prime  $l_1 \in \mathfrak{S}$  such that  $l_1 \equiv 3(q)$ . (This may be done via Dirichlet's theorem on primes in an arithmetic progression.) Then  $q \nmid l_1(l_1+1)(l_1-1)^2$ , and the result follows. □

Next, we observe that if  $Q$  is any  $p$ -power torsion point in  $E(F)$ , the function  $h$  defines an element  $h_Q$  of  $M_Q(i)$  by the rule

$$(5.2) \quad h_Q(Q') = h(Q'), \quad Q' \in G_Q(i).$$



Note that  $h_Q(Q')$  is always finite. If we take  $Q = \underline{Q}$ , then we have that  $G_{\underline{Q}}(i) = G_i$ , and (5.2) defines a function  $h_{\underline{Q}}$  on  $G_i$ . We define a resolvent element  $\rho \in A_i(M)$  by

$$(5.3) \quad \rho = \frac{1}{p^i} \sum_{g \in G_i} h_{\underline{Q}}(g)g^{-1}.$$

PROPOSITION 5.3. *Let  $Q \in E(F)$  be a  $p$ -power torsion point. Then  $h_Q \in O_Q(i)(M)$ .*

*Proof.* Let  $N$  be some finite extension of  $F$  containing the coordinates of all points of  $G_i$  and  $G_Q(i)$ . From §1 (see (1.1)-(1.3)) it follows that  $O_Q(i)(M) = \xi(\mathfrak{B}_i(N)) \cap M_Q$ . Hence, since  $h_Q \in M_Q$ , the result will follow if we show that  $h_Q \in \xi(\mathfrak{B}_i(N))$ . But this is certainly the case, because  $\mathfrak{B}_i(N)$  is the unique  $O_N$ -maximal order in  $B_i(N)$ , and so Proposition 4.2(b) implies that  $\xi^{-1}(h_Q) \in \mathfrak{B}_i(N)^*$ .  $\square$

Recall that  $\mathfrak{A}_i(M)$  is the unique  $O_M$ -maximal order in  $A_i(M)$ . The following corollary is an immediate consequence of this fact.

COROLLARY 5.4. *The resolvent element  $\rho$  lies in  $\mathfrak{A}_i(M)$ .*

We now prove a special case of Theorem 1.

THEOREM 5.5. *Let  $Q \in E(F)$  be a  $p$ -power torsion point. Then*

$$O_Q(i)(M) \cdot \rho = h_Q \cdot \mathfrak{A}_i(M),$$

and so  $O_Q(i)(M)$  is  $\mathfrak{A}_i(M)$ -free.

*Proof.* We shall show that the equality holds everywhere locally; this will imply the desired result.

Let  $\nu$  be a place of  $O_M$ . Then we may write  $O_{Q,\nu}(i)(M) = x_\nu \mathfrak{A}_{i,\nu}(M)$ . For some  $\lambda_\nu \in A_i(M_\nu)$ , we have

$$(5.4) \quad x_\nu \cdot \rho \lambda_\nu = h_Q.$$

We shall show that in fact  $\lambda_\nu \in \mathfrak{A}_{i,\nu}(M)^*$ ; this will establish the result.

Recall that if  $x \in M_Q$  and  $\nu \in G_i$ , then we have the Lagrange resolvent

$$(5.5) \quad (x|\chi_\nu) = \sum_{g \in G_i} x^g \chi_\nu(g^{-1}).$$

If  $g' \in G_i$ , then  $(x^{g'}|\chi_\nu) = (x|\chi_\nu) \cdot \chi_\nu(g')$ , and so for each  $\lambda \in F^c G_i$ , we have

$$(5.6) \quad (x\lambda|\chi_\nu) = (x|\chi_\nu) \cdot \chi_\nu(\lambda).$$

Hence, (5.4) implies that

$$(5.7) \quad (x_q | \chi_\nu) \cdot \chi_\nu(\rho) \cdot \chi_\nu(\lambda_q) = (h_Q | \chi_\nu).$$

Now Proposition 1.3 implies that if  $Q' \in G_Q(i)$ , then  $(x_\nu | \chi_\nu)(Q') \sim 1$ . Also, we have that  $\chi_\nu(\rho) = R_\nu(\psi) \sim 1$  and  $(h_Q | \chi_\nu)(Q') = p^i R_\nu(Q' + \psi) \sim 1$  (cf. proposition 4.2). Hence, evaluating (5.7) at  $Q' \in G_Q(i)$ , we obtain

$$(5.8) \quad \chi_\nu(\lambda_\nu) \sim 1.$$

Therefore  $\lambda_\nu \in \mathfrak{A}_{i,\nu}(M)^*$ , and this implies the desired result. □

We now prove Theorem 1.

Consider the trace-restriction square (1.12):

$$(5.9) \quad \begin{array}{ccc} E(M) & \xrightarrow{\psi_{i,M}} & Cl(\mathfrak{A}_i(M)) \\ Tr_{M/F} \downarrow & & \downarrow Res \\ E(F) & \xrightarrow{\psi_{i,F}} & Cl(\mathfrak{A}_i(F)). \end{array}$$

If  $Q \in E(F)$  is a  $p$ -power torsion point, we may regard  $Q$  as lying in  $E(M)$ , and Theorem 5.5 implies that

$$(5.10) \quad \psi_{i,F}(Tr(Q)) = Res(\psi_{i,M}(Q)) = 0.$$

Next, we observe that we also have

$$(5.11) \quad \psi_{i,F}(Tr(Q)) = \psi_{i,F}([M : F]Q) = [M : F] \cdot \psi_{i,F}(Q).$$

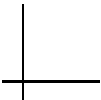
Hence we obtain that

$$(5.12) \quad [M : F] \psi_{i,F}(Q) = 0,$$

i.e.

$$(5.13) \quad [M : F](O_Q(i)) = 0.$$

Now let  $l$  and  $l'$  vary among all odd primes not equal to  $p$  or  $r$ . Then it follows from Lemma 5.1 that  $w^2 \psi_{i,F}(Q) = 0$ . Now recall that  $p^i \psi_{i,F}(Q) = 0$  (see (1.11)). Since  $p > 3$ , we have that  $(p, w) = 1$  by Lemma 5.2, and so finally we deduce that  $(O_Q(i)(F)) = 0$  in  $Cl(\mathfrak{A}_i(F))$ . This completes the proof of Theorem 1. □



DEPARTMENT OF MATHEMATICS, UC SANTA BARBARA, SANTA BARBARA, CA 93106

*Current address:* SCHOOL OF MATHEMATICS, INSTITUTE FOR ADVANCED STUDY, PRINCETON,  
NJ 08540

*Electronic mail:* AGBOOLA@MATH.UCSB.EDU

---

REFERENCES

---

- [A1] A. Agboola, Abelian varieties and Galois module structure in global function fields, *Math. Z.* **271** (1994), 407–419.
- [A2] ———, Torsion points on elliptic curves and Galois module structure, *Invent. Math.* **123** (1996), 105–122.
- [CR] C. W. Curtis and I. Reiner, *Methods of Representation Theory Vol. 1*, Wiley, New York, 1981.
- [F] A. Fröhlich, Galois Module Structure of Algebraic Integers, Springer-Verlag, New York, 1983.
- [L] S. Lang, Introduction to Arakelov Theory, Springer-Verlag, New York, 1988.
- [ST] A. Srivastav and M. J. Taylor, Elliptic curves with complex multiplication and Galois module structure, *Invent. Math.* **99** (1990), 165–184.
- [T] M. J. Taylor, Mordell-Weil groups and the Galois module structure of rings of integers, *Illinois J. Math.* **32** (1988), 428–452.