§1. Introduction.

In [T1] M.J.Taylor began the study of the Galois module structure of certain Kummer orders arising from group laws of abelian varieties defined over number fields (see also [ST], [CN-S] and [CN-T]). The purpose of this paper is to study similar Kummer orders which are derived from CM abelian varieties over global function fields.

For any field F we shall write F^c for a separable closure of F and Ω_F for $\mathrm{Gal}(F^c/F)$. Let C be a smooth, geometrically irreducible curve defined over a field $k \subseteq \mathbb{F}_p^c$. Set $L = k(C)$, the function field of C over k. Let $S = \{v_1, \ldots, v_t\}$ be a fixed nonempty set of places of L and let $\mathfrak{O}_L = \mathfrak{O}_{L,S}$ denote the ring of functions in L which are regular away from S. $\mathfrak{O}_L$ is the function field analogue of the ring of integers of a number field. Write $\mathfrak{O}^c$ for the integral closure of $\mathfrak{O}_L$ in L^c.

Let A/L be a simple abelian variety defined over L with complex multiplication. This implies (see [M] p.220) that A is either a constant or a twisted constant variety over L. In what follows, we shall always assume that S contains all places of bad reduction of A. We shall also suppose that all endomorphisms of A that we consider are defined over L. The endomorphism ring $\mathcal{D}$ =End(A) of A is an order in a finite-dimensional semisimple division algebra $\mathcal{K}$ over $\mathbb{Q}$. If $\mathcal{K}$ is non-abelian, then (since A is simple) A is isogenous (possibly after an extension of L) to a supersingular elliptic curve and $\mathcal{K}$ is isomorphic to the quaternion division algebra over $\mathbb{Q}$ which splits at all primes $l \neq p, \infty$ (see e.g. [Mu] p. 256). Choose an endomorphism $\lambda \in \mathcal{D}$ such that the degree of λ is both greater than one and coprime to p.

Denote by G the group of all points of $A(L^c)$ which are killed by λ. The $\mathfrak{O}_L$-

group scheme of λ-torsion points on A is affine and etale (since $(|G|, p) = 1$) and is therefore equal to $\mathrm{Spec}(\mathfrak{B}(L;\lambda))$, where $\mathfrak{B}(L;\lambda) = \mathrm{Map}_{\Omega_L}(G, \mathfrak{O}^c)$, the $\mathfrak{O}_L$-Hopf algebra consisting of Ω_L-maps from G to $\mathfrak{O}^c$. It follows that the $\mathfrak{O}_L$-Cartier dual of $\mathfrak{B}(L;\lambda)$ is $\mathfrak{A}(L;\lambda) = (\mathfrak{O}^c G)^{\Omega_L}$ (here Ω_L acts on both $\mathfrak{O}^c$ and G). $\mathfrak{A}(L;\lambda)$ is thus the unique $\mathfrak{O}_L$-maximal order in the L-algebra $\mathcal{A}(L;\lambda) = (L^c G)^{\Omega_L}$ since $\mathfrak{O}^c G$ is the unique $\mathfrak{O}^c$-maximal order in the algebra $L^c G$.

Now suppose that $Q \in A(L)$ and write

$$G_Q(\lambda) = \{Q' \in A(L^c) \quad | \quad \lambda Q' = Q\}.$$

Define the L-algebra $L_Q(\lambda)$ (the Kummer algebra) by $L_Q(\lambda) = \mathrm{Map}_{\Omega_L}(G_Q, L^c)$, and let $L(\frac{1}{\lambda}Q)$ be the field obtained by adjoining the coordinates of the points of $G_Q(\lambda)$ to L. Let $Q'^{(1)}, \ldots, Q'^{(s)}$ be a set of representatives of Ω_L-orbits of $G_Q(\lambda)$. Then (as an L-algebra),

$$L_Q(\lambda) \simeq \prod_{i=1}^{s} L[Q'^{(i)}] \tag{1.1}$$

where $L[Q'^{(i)}]$ is the field obtained by adjoining the coordinates of $Q'^{(i)}$ to L. (Explicitly, the isomorphism is given by $f \mapsto \prod_{i=1}^{s} f(Q'^{(i)})$, for $f \in L_Q(\lambda)$. Note also that if $G \subseteq A(L)$, then all the fields $L[Q'^{(i)}]$ are the same.) Hence $[L_Q(\lambda) : L] = |G|$. $\mathcal{A}(L;\lambda)$ acts on $L_Q(\lambda)$ via

$$(f. \sum_g a_g g)(Q') = \sum_g a_g f(Q' + g),$$

for $f \in L_Q(\lambda)$ and $\sum_g a_g g \in \mathcal{A}(L;\lambda)(L)$.

Let $\mathfrak{O}_Q(L;\lambda)$ denote the integral closure of $\mathfrak{O}_L$ in $L_Q(\lambda)$. Then $\mathfrak{O}_Q(L;\lambda)$ (the Kummer order) is an $\mathfrak{A}(L;\lambda)$-module. Since S contains all places of bad reduction

of A and $(|G|, p) = 1$, it follows from (1.1) above and the criterion of Neron-Ogg-Shafarevitch that $L_Q(\lambda)/L$ is unramified at all places of $\mathfrak{O}_L$. (This fact, and slight variants of it will be used several times in the sequel.) As $\mathfrak{A}(L;\lambda)$ is the maximal order of $\mathcal{A}(L;\lambda)$, it follows that $\mathfrak{O}_Q(L;\lambda)$ is a locally free $\mathfrak{A}(L;\lambda)$ module (see e.g. [CR] Proposition 31.2). Thus, if $\mathrm{Cl}(\mathfrak{A}(L;\lambda))$ denotes the locally free classgroup of $\mathfrak{A}(L;\lambda)$, then we have a map

$$\psi : A(L)/\lambda A(L) \longrightarrow \mathrm{Cl}(\mathfrak{A}(L;\lambda))$$

given by $\psi(Q) = (\mathfrak{O}_Q(L;\lambda))$, where $(\mathfrak{O}_Q(L;\lambda))$ is the class of $\mathfrak{O}_Q(L;\lambda)$ in $\mathrm{Cl}(\mathfrak{A}(L;\lambda))$. As A has good reduction at all places of $\mathfrak{O}_L$, it follows exactly as in [T1] that ψ is a homomorphism, and so in particular the image of ψ is annihilated by $|G|$. Observe that since G is abelian, $\mathfrak{A}(L;\lambda)$ satisfies the Eichler condition. Hence $\mathfrak{O}_Q(L;\lambda)$ is a free $\mathfrak{A}(L;\lambda)$-module if and only if $\psi(Q) = 0$.

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

THEOREM 1.2. *Let $Q \in A(L)$ be a point of infinite order. Suppose that the image of Q has order $m > 1$ in $A(L)/(\lambda A(L) + A(L)_{tors})$, where $A(L)_{tors}$ denotes the torsion subgroup of $A(L)$ Then there is an integer N_1 (which is independent of Q) such that $\psi(Q) \neq 0$ if $m > N_1$. Furthermore, if A is a constant variety and if S consists of a single place of degree one, then $\psi(Q) \neq 0$, i.e. we may take $N_1 = 1$.*

We refer the reader to [A] and [AT] for an analysis of the Galois module structure of Kummer orders arising from points of infinite order on CM elliptic curves defined over number fields.

The first three sections of this paper are devoted to the proof of Theorem 1.2.

In the fourth section, we give a geometric interpretation of the homomorphism ψ when A is a constant variety over L. We then show how the zeta function of A/k may be used to obtain precise information concerning the image of ψ in the case that λ is a cyclic endomorphism of prime degree.

The results contained in this paper formed a portion of my Ph.D. thesis (Columbia University 1991). It is with the greatest of pleasure that I thank my advisor, Professor T. Chinburg for all of his help, kindness and encouragement. I also wish to thank Professor M. J. Taylor for suggesting that I look at function fields and for much generous advice, and Professor K. Rubin for many very helpful conversations. Thanks also to Dr. R. J. Chapman, Professor R. Friedman, and Mr. J. McKernan for interesting discussions.

§2. Preliminary Remarks

We shall first prove Theorem 1.2 for constant varieties and then deduce the result for twisted constant varieties. *Thus, from now on until further notice, A denotes a constant abelian variety.* We remark that in this case, $A(L)_{tors} = A(k)$.

The following proposition is an extension of a result shown to me by Professor K. Rubin.

Proposition 2.1. *Let $Q \in A(L)$ be a point of infinite order and write $L' = L \otimes_k k^c$. If Q has order m' in $A(L')/\lambda A(L')$, then Q has order dividing m' in $A(L)/(\lambda A(L) + A(k))$.*

Thus, if Q is not divisible by λ in $A(L)/A(k)$, then Q is not divisible by λ in $A(L_1)/A(k_1)$, where k_1/k is any finite extension and $L_1 = L \otimes_k k_1$. Hence

$L'(\frac{1}{\lambda}Q)/L'$ is a nontrivial finite extension.

Proof. Consider the natural homomorphism $\eta : A(L)/\lambda A(L) \to A(L')/\lambda A(L')$ induced by the inclusion $A(L) \hookrightarrow A(L')$. We have the following commutative diagram

$$\begin{array}{ccccc} & & A(L)/\lambda A(L) & \xrightarrow{\eta} & A(L')/\lambda A(L') \\ & & \downarrow i & & \downarrow \\ H^1(\mathrm{Gal}(L'/L), G) & \longrightarrow & H^1(\mathrm{Gal}(L^c/L), G) & \underset{Res}{\longrightarrow} & H^1(\mathrm{Gal}(L^c/L'), G) \end{array} \tag{2.2}$$

where the vertical arrows are injective and the bottom row is exact.

From the exactness of the bottom row, we deduce that Ker(Res) has order at most $|H^1(\mathrm{Gal}(L'/L), G)|$. On the other hand, the natural homomorphism $A(k)/\lambda A(k) \to A(L)/\lambda A(L)$ is an injection because k is the constant subfield of L. Clearly $A(k)/\lambda A(k) \subset \mathrm{Ker}(\eta)$, from which it follows that Ker(Res) has order at least $|A(k)/\lambda A(k)|$.

Now $\mathrm{Gal}(L'/L) \simeq \Omega_k$, and the isomorphism respects the action of these groups on G because G is defined over k^c. Hence $H^1(\mathrm{Gal}(L'/L), G) \simeq H^1(\Omega_k, G)$. Kummer theory on $A(k^c)$ yields the exact sequence

$$0 \to A(k)/\lambda A(k) \to H^1(\Omega_k, G) \to H^1(\Omega_k, A(k^c)).$$

It is a theorem of Lang (see [L]) that a principal homogeneous space of any algebraic group defined over a finite field is trivial. Hence $H^1(\Omega_k, A(k^c)) = 0$ and so $|A(k)/\lambda A(k)| = |H^1(\Omega_k, G)|$. Thus $\mathrm{Ker(Res)} = i(A(k)/\lambda A(k))$.

Now since $m'Q = 0$ in $A(L')/\lambda A(L')$ i.e. $m'Q \in \mathrm{Ker}(\eta)$, we have that $i(m'Q) \in i(A(k)/\lambda A(k))$. Therefore $m'Q \in A(k) + \lambda A(L)$, and so Q has order dividing m' in $A(L)/(A(k) + \lambda A(L))$.

The final paragraph of the proposition now follows immediately. $\square$

Now let k_1/k be any finite extension such that $G \subseteq A(k_1)$, and write $L_1 = L \otimes_k k_1$. Then $\mathcal{A}(L_1;\lambda) = L_1 G = \mathcal{A}(L;\lambda) \otimes_k k_1$, $\mathfrak{A}(L_1;\lambda) = \mathfrak{O}_{L_1} G = \mathfrak{A}(L;\lambda) \otimes_k k_1$, and $\mathfrak{O}_Q(L_1;\lambda) = \mathfrak{O}_Q(L;\lambda) \otimes_k k_1$. Hence if $\mathfrak{O}_Q(L_1;\lambda)$ is not free over $\mathfrak{A}(L_1;\lambda)$ then $\mathfrak{O}_Q(L;\lambda)$ is not free over $\mathfrak{A}(L;\lambda)$. Furthermore, it follows from Proposition 2.1 and the hypotheses of Theorem 2.2 that the order of Q in $A(L_1)/(A(k_1) + \lambda A(L_1))$ is at least as large as the order of Q in $A(L)/(A(k) + \lambda A(L))$ Thus, for the proof of Theorem 1.2, we may assume without loss of generality that $G \subset A(L)$, $\mathcal{A}(L;\lambda) = LG$, $\mathfrak{A}(L;\lambda) = \mathfrak{O}_L G$, and that L contains the $|G|$th roots of unity. We shall make these assumptions.

We caution the reader that where there is no danger of ambiguity, we shall feel free to drop the dependence on L and/or λ in our notation for $\mathfrak{A}(L;\lambda)$, $\mathfrak{O}_Q(L;\lambda)$, $L_Q(\lambda)$, etc.

§3. Classgroup Theory

We now recall some elementary facts from the theory of tame classgroups over global function fields. For details of these results we refer the reader to [C1] or [C3].

Let R_G denote the ring of virtual characters of G and write $\hat{G}$ for the group of irreducible characters of G. Since L contains the $|G|$th roots of unity, the maximal order $\mathfrak{O}_L G$ of LG splits, i.e. $\mathfrak{O}_L G \simeq \prod_{\chi \in \hat{G}} \mathfrak{O}_L$. Hence we have

$$\mathrm{Cl}(\mathfrak{O}_L G) \simeq \mathrm{Map}(\hat{G}, \mathrm{Cl}(\mathfrak{O}_L)) \simeq \frac{\mathrm{Hom}(R_G, \mathrm{Div}_S(L))}{\mathrm{Hom}(R_G, D_S(L^*))}.$$

Here $\mathrm{Div}_S(L)$ is the group of divisors of L with support away from S. $D_S(L^*)$ is the subgroup of $\mathrm{Div}_S(L)$ consisting of the image of the natural map that sends an

element $x \in L^*$ to its associated divisor $\sum_{\mathfrak{P} \text{ prime of } \mathfrak{O}_L} v_{\mathfrak{P}}(x)\mathfrak{P}$. We shall sometimes view elements of $\mathrm{Div}_S(L)$ as ideals of $\mathfrak{O}_L$.

A homomorphism in $\mathrm{Hom}(R_G, \mathrm{Div}_S(L))$ which represents the class $(\mathfrak{O}_Q(L)) \in \mathrm{Cl}(\mathfrak{O}_L G) = \mathrm{Cl}(\mathfrak{A}(L))$ may be contructed as follows:

Suppose that $a \in L_Q$ and $\chi \in \hat{G}$. Then the resolvent of a at χ is

$$(a|\chi) = \sum_{g \in G} \chi(g^{-1}) a^g \in L_Q.$$

Choose $d_Q \in L_Q$ such that $L_Q = d_Q.LG$. For each place $\mathfrak{P}$ of $\mathfrak{O}_L$, let $\mathfrak{O}_{L,\mathfrak{P}}$ (resp. $\mathfrak{O}_{Q,\mathfrak{P}}(L)$) denote the semi-localisation of $\mathfrak{O}_L$ (resp. $\mathfrak{O}_Q(L)$) at $\mathfrak{P}$. Choose $a_{\mathfrak{P}} \in \mathfrak{O}_{Q,\mathfrak{P}}(L)$ such that $\mathfrak{O}_{Q,\mathfrak{P}}(L) = a_{\mathfrak{P}}.\mathfrak{O}_{L,\mathfrak{P}}G$. Then $(a_{\mathfrak{P}}|\chi)(d_Q|\chi)^{-1} \in L$, and the homomorphism we require is given by

$$\chi \mapsto \sum_{\mathfrak{P} \text{ of } \mathfrak{O}_L} v_{\mathfrak{P}}((a_{\mathfrak{P}}|\chi)(d_Q|\chi)^{-1})\mathfrak{P} \tag{3.1}$$

extended to R_G via linearity.

We now make some further remarks on resolvents. Since

$$(d_Q|\chi)^g = \chi(g)(d_Q|\chi) \tag{3.1(a)}$$

and $[L_Q : L] = |G|$, we have the following direct sum decomposition of L_Q into G-eigenspaces:

$$L_Q = \bigoplus_{\chi \in \hat{G}} L.(d_Q|\chi) \tag{3.2}$$

It thus follows from (1.1) and (3.2) that

$$L(\frac{1}{\lambda}Q) = L(\{(d_Q|\chi)(Q')\}_{\chi \in \hat{G}}), \tag{3.3}$$

where Q' is any fixed element of G_Q. Since

$$[(d_Q|\chi_1)(d_Q|\chi_2)]^g = \chi_1(g)\chi_2(g)[(d_Q|\chi_1)(d_Q|\chi_2)] \tag{3.3(a)}$$

for all $\chi_1, \chi_2 \in \hat{G}$, we conclude that, for all $\chi \in \hat{G}$

$$(d_Q|\chi)^r = \gamma_\chi(d_Q|\chi^r) \tag{3.4}$$

for some $\gamma_\chi \in L$.

As A/L has good reduction at all places of L (since A/L is a constant variety) and $(|G|, p) = 1$, it follows from the criterion of Neron-Ogg-Shafarevitch and the definition of L_Q that L_Q/L is unramified at all places of L (and not just at all places of $\mathfrak{O}_L$ as in §1). The following result is a simple extension of Proposition 4.3 in Ch. I of [F] from fields to Galois algebras.

Proposition 3.5. *Let $a_\mathfrak{P} \in \mathfrak{O}_{Q,\mathfrak{P}}(L)$ be such that $\mathfrak{O}_{Q,\mathfrak{P}}(L) = a_\mathfrak{P}.\mathfrak{O}_{L,\mathfrak{P}}G$. Then for all $\chi \in \hat{G}$, we have $(a_\mathfrak{P}|\chi) \in \mathfrak{O}^*_{Q,\mathfrak{P}}$.* $\square$

Let us now recall the isomorphism (1.1) and focus our attention on a fixed component $L[Q'^{(j)}]$ say, of L_Q. Write $\mathfrak{O}(Q'^{(j)})$ for the integral closure of $\mathfrak{O}_L$ in $L[Q'^{(j)}]$. From (3.1(a)), we deduce that $(d_Q|\chi)(Q'^{(j)})^{|G|} \in L^*$ for all $\chi \in \hat{G}$. As $L[Q'^{(j)}]/L$ is unramified at all places of L, it follows that the $\mathfrak{O}(Q'^{(j)})$-submodule $(d_Q|\chi)(Q'^{(j)}).\mathfrak{O}(Q'^{(j)})$ of $L[Q'^{(j)}]$ is an ambiguous ideal, i.e. that

$$(d_Q|\chi)(Q'^{(j)}).\mathfrak{O}(Q'^{(j)}) = \mathfrak{D}_\chi\mathfrak{O}(Q'^{(j)}) \tag{3.6}$$

where $\mathfrak{D}_\chi$ is a fractional $\mathfrak{O}_L$ ideal. (Here, by a fractional $\mathfrak{O}_L$-ideal, we mean a finitely generated $\mathfrak{O}_L$-submodule of L. Note that the remarks immediately after

(1.1) together with (3.2) and the fact that L contains the $|G|$th roots of unity imply that $\mathfrak{D}_\chi$ is independent of the choice of component $L[Q'^{(j)}]/L$.)

Write

$$\mathfrak{d}_\chi = \sum_{\mathfrak{P} \text{ of } \mathfrak{O}_L} v_{\mathfrak{P}}(\mathfrak{D}_\chi)\mathfrak{P}. \tag{3.7}$$

From (3.1), (3.5) and (3.6), we deduce that $(\mathfrak{O}_Q) \in \mathrm{Cl}(\mathfrak{O}_L G)$ is represented by the element of $\mathrm{Map}(\hat{G}, \mathrm{Cl}(\mathfrak{O}_L))$ given by

$$\chi \mapsto (\mathfrak{d}_\chi)^{-1} \tag{3.8}$$

where $(\mathfrak{d}_\chi)$ denotes the class of $\mathfrak{d}_\chi$ in $\mathrm{Cl}(\mathfrak{O}_L)$.

We remark that this map in fact lies in $\mathrm{Hom}(\hat{G}, \mathrm{Cl}(\mathfrak{O}_L))$ since it follows from equation (3.4) that

$$(\mathfrak{d}_{\chi^r}) = (\mathfrak{d}_\chi)^r. \tag{3.9}$$

§4. Kummer Theory.

Consider the homomorphism $\varepsilon' : A(L) \to \mathrm{Hom}_{\Omega_L}(\hat{G}, L^*/L^{*|G|})$ given by $Q \mapsto \{\chi \mapsto (d_Q|\chi)^{|G|}\}$. Suppose that $Q \in \mathrm{Ker}(\varepsilon')$. Then $(d_Q|\chi) \in L^*$ for all $\chi \in \hat{G}$, and so from (3.3(a)) we deduce that $L(\frac{1}{\lambda}Q) = L$ i.e. that $Q \in \lambda A(L)$. Hence ε' induces an injective homomorphism $\varepsilon : A(L)/\lambda A(L) \to \mathrm{Hom}_{\Omega_L}(\hat{G}, L^*/L^{*|G|})$. The following proposition is essentially the same as Proposition 8 of [T1].

PROPOSITION 4.1. *Let U denote the group of units of $\mathfrak{O}_L$. Then $Q \in \mathrm{Ker}(\psi)$ if and only if $\varepsilon(Q) \in \mathrm{Hom}_{\Omega_L}(\hat{G}, U.L^{*|G|}/L^{*|G|})$.*

Proof. Using the notation of §3, we have that $\psi(Q) = 0$ if and only if for all $\chi \in \hat{G}$,

$\mathfrak{d}_\chi = X_\chi \mathfrak{O}_L$ for some $X_\chi \in L^*$. If this is the case, then $(d_Q|\chi)X_\chi^{-1}$ is a unit of $\mathfrak{O}_Q$ and so $\varepsilon(Q)(\chi)$ is represented by $[(d_Q|\chi)X_\chi^{-1}]^{|G|} \in U$. $\square$

Now since $L(\frac{1}{\lambda}Q) = L(\{(d_Q|\chi)\}_{\chi \in \hat{G}})$, it follows from Proposition 4.1 that if $\psi(Q) = 0$, then $L(\frac{1}{\lambda}Q)/L$ is a Kummer extension of L obtained by adjoining $|G|$th roots of various units of $\mathfrak{O}_L$. Moreover, from Proposition 2.1, $L(\frac{1}{\lambda}Q)/L$ is a non-trivial, non-constant extension. Also, as remarked in §3, $L(\frac{1}{\lambda}Q)/L$ is unramified at all places of L since A/L is a constant variety. An element of L is a unit of $\mathfrak{O}_L$ if and only if it is an S-unit of L. In particular, we may observe at this point that if S consists of a single place of degree one, then $\mathfrak{O}_L^* = k^*$, and Theorem 1.2 in this case follows immediately from Propositions 2.1 and 4.1 above. To proceed further, we need the following result.

Proposition 4.2. *Write $L' = L \otimes_k k^c$ and let $n \in \mathbb{N}$ with n coprime to p. Let S' denote the set of places of L' lying above S and suppose that there is an S'-unit α of L' such that $L'(\alpha^{1/n})/L'$ is an everywhere unramified extension of degree n. Then there is an integer N depending only upon S' and L' such that $n|N$.*

Proof. Write $U(S')$ for the group of S'-units of L', and let $\mathrm{Div}^0(S')$ be the group of divisors of degree zero of C/k^c whose support is contained in S'. Then we have an exact sequence

$$0 \to k^{c*} \to U(S') \to \mathrm{Div}^0(S') \to T \to 0, \tag{4.3}$$

where T is a finite group.

Write (α) for the divisor of α, and suppose that

$$(\alpha) = \sum_{i=1}^{d} a_i v_i,$$

where $a_i \in \mathbb{Z}$ and the v_i are places of L'. Since $L'(\alpha^{1/n})/L'$ is everywhere unramified, we have that $n|a_i$ for $i = 1, \ldots d$. Set

$$D = \sum_{i=1}^{d} \frac{a_i}{n} v_i.$$

As $L'(\alpha^{1/n})/L'$ has degree n and $k^c \subset L'$, it follows that the image of D in T has order n. Hence, taking $N = |T|$, the proposition follows. $\square$

The next result relates the order of Q in $A(L')/\lambda A(L')$ to the degree of the extension $L'(\frac{1}{\lambda}Q)/L'$.

LEMMA 4.4. *Let $d = [L'(\frac{1}{\lambda}Q) : L']$ and write m' for the order of Q in $A(L')/\lambda A(L')$. Then $m'|d$.*

Proof. Write $H = \mathrm{Gal}(L'(\frac{1}{\lambda}Q)/L')$, and fix $Q' \in G_Q$. For each $h \in H$, we have ${Q'}^h = Q' + s_h$, with $s_h \in G \subset A(k^c)$. Hence

$$P = \sum_{h \in H} {Q'}^h = d.Q' + s, \tag{4.5}$$

with $P \in A(L')$ and $s \in A(k^c)$. Thus $d.Q = \lambda(P - s)$, i.e. $d.Q = 0$ in $A(L')/\lambda A(L')$, and now the result follows. $\square$

Now suppose that A has dimension t, and write $A_{|G|}$ for the group of $|G|$-torsion points of $A(k^c)$. Then $A_{|G|} \simeq (\mathbb{Z}/|G|\mathbb{Z})^{2t}$, and G is a subgroup of $A_{|G|}$. Hence there exist $\chi_1, \ldots, \chi_s$ with $1 \leq s \leq 2t$ such that $\hat{G} =< \chi_1, \ldots, \chi_s >$. From (3.3)

and (3.3(a)), it follows that $L'(\frac{1}{\lambda}Q) = L'(\{d_Q|\chi_i)(Q')\}_{i=1}^s)$. Thus if for example $d = [L'(\frac{1}{\lambda}Q) : L'] \geq 2N^{2t}$, then we must have $[L'((d_Q|\chi_j)(Q') : L'] > N$ for at least one j, $1 \leq j \leq s$. If this is the case, then we deduce using Proposition 4.2 that $(d_Q|\chi_j)(Q')^{|G|} \notin U.L^{*|G|}/L^{*|G|}$ (where $U = \mathfrak{O}_L^*$), which (from Proposition 4.1) implies that $\psi(Q) \neq 0$.

Recall that $m > 1$ is the order of Q in $A(L)/(\lambda A(L) + A(L)_{tors})$ and that $A(L)_{tors} = A(k)$, since A is a constant variety. From Proposition 2.1 and Lemma 4.4, we have that $m \leq m' \leq d$. Hence if e.g. $m \geq 2N^{2t}$, then $\psi(Q) \neq 0$, which completes the proof of Theorem 1.2 for constant abelian varieties.

We now turn to the case in which A is a twisted constant variety. Thus, from now on until further notice, assume that A is a twisted constant variety and let M/L be a finite extension over which A becomes isomorphic to a constant variety. Write $d_1 = [M : L]$ and let $d_2 = |A(M)_{tors}|$.

Associated to the field M and the set of places S_M of M lying above S is an integer N_M as in Proposition 4.2. Suppose e.g. that $m \geq 2d_1d_2N_M^{2t}$. It follows via the natural injections $A(L)/\lambda A(L) \to H^1(Gal(L^c/L), G)$ and $A(M)/\lambda A(M) \to H^1(Gal(M^c/M), G)$, together with the inflation-restriction sequence of Galois cohomology, that the kernel of the natural map $A(L)/\lambda A(L) \to A(M)/\lambda A(M)$ is killed by d_1. Hence the image of Q in $A(M)/(\lambda A(M) + A(M)_{tors})$ has order at least $m/d_1d_2 = 2N_M^{2t}$. Now reasoning exactly as in the already treated constant case, we deduce that $(\mathfrak{O}_Q(M; \lambda)) \neq 0$ in $Cl(\mathfrak{A}(M; \lambda))$. As $\mathfrak{O}_Q(M; \lambda) = \mathfrak{O}_Q(L; \lambda) \otimes_{\mathfrak{O}_L} \mathfrak{O}_M$ and $\mathfrak{A}_Q(M; \lambda) = \mathfrak{A}_Q(L; \lambda) \otimes_{\mathfrak{O}_L} \mathfrak{O}_M$, this implies that $(\mathfrak{O}_Q(L; \lambda)) \neq 0$ in $Cl(\mathfrak{A}(L; \lambda))$, as required.

Let us now return to the case of an arbitrary CM abelian variety A as in the statement of Theorem 1.2. We conclude this section with some remarks on a simple consequence of the proof of that theorem. It is well known that $A(L')/A(L')_{\mathrm{tors}}$ is a finitely generated $\mathcal{D}$-module. Hence, if $Q \in A(L)$ is a point of infinite order, then Q is not infinitely divisible by λ in $A(L')$. This implies that the degree of the extension $L'(\frac{1}{\lambda^n}Q)/L'$ tends to infinity with n.

THEOREM 4.5. *Let $Q \in A(L)$ be a point of infinite order. Then for all sufficiently large n, $\mathfrak{O}_Q(L;\lambda^n)$ is not a free $\mathfrak{A}_Q(L;\lambda^n)$-module.*

Proof. Let M, N_M, and t be as above (so in particular if A is a constant variety, then $M = L$). Suppose that n is sufficiently large that $[M'(\frac{1}{\lambda^n}Q) : M'] > 2d_1N_M^{2t}$. Then $\mathfrak{O}_Q(M;\lambda^n)$ is not a free $\mathfrak{A}(M;\lambda^n)$-module, which in turn implies that $\mathfrak{O}_Q(L;\lambda^n)$ is not $\mathfrak{A}(L;\lambda^n)$-free. $\square$

§5. Realisable Classes.

In this section we give a geometric interpretation of the homomorphism ψ which enables us to relate the image of ψ to the Hasse-Weil zeta function of A when A is a constant variety. This raises interesting questions regarding the analogous situation over number fields which we hope to pursue elsewhere.

Let us begin by recalling certain basic facts regarding the theory of classgroups of sheaves (see [C2]). We identify C with its associated scheme over Spec k^c, and we write $\mathcal{O}$ for the structure sheaf of C/k^c. Set $L' = L \otimes_k k^c$. The places of L' may be identified with the set of closed points of C/k^c. Let G be a finite group with $(|G|, p) = 1$. Define $\mathcal{O}G$ to be the sheaf of rings whose sections over each open set

U of C/k^c are given by $\mathcal{O}G(U) = \mathcal{O}(U)G$. If S is a finite collection of closed points of C and $U = C - S$ then $\mathcal{O}G(C - S) = \mathfrak{O}_{L',S}G$, where here $\mathfrak{O}_{L',S}G$ denotes the ring of functions in L' which are regular away from S.

Let $\mathfrak{M}$ be a sheaf of $\mathcal{O}G$-modules. $\mathfrak{M}$ is said to be *locally free of rank* r if each stalk $\mathfrak{M}_P$ is a free $\mathcal{O}_P G$-module of rank r. Thus, if $U = C - S$ is an open subset of C as above, then $\mathfrak{M}(U)$ is a locally free $\mathcal{O}G$-module. The locally free classgroup $\mathrm{Cl}(\mathcal{O}G)$ of $\mathcal{O}G$ is defined to be $\mathrm{Map}(\hat{G}, \mathrm{Pic}(C))$, where $\mathrm{Pic}(C)$ denotes the Picard group of C. Each locally free $\mathcal{O}G$-module $\mathfrak{M}$ defines an element $(\mathfrak{M}) \in \mathrm{Cl}(\mathcal{O}G)$ as described in §2 of [C2]. It is shown in [C2] that for all such open subsets U of C, $(\mathfrak{M}(U)) \in \mathrm{Cl}(\mathcal{O}G(U)) = \mathrm{Cl}(\mathfrak{O}_{L',S}G)$ is completely determined by $(\mathfrak{M}) \in \mathrm{Cl}(\mathcal{O}G)$.

Assume throughout this section that A/k is a constant variety. Suppose that $\lambda \in \mathrm{End}(A)$ is such that the kernel of $\lambda : A(k^c) \to A(k^c)$ is cyclic of prime order l with $(l, p) = 1$. Suppose that $Q \in A(L)$. Then Q defines a k-rational section $\tilde{Q} : C \to A$ of the structure map $A \to C$, and for each $i \in \mathbb{N}$, we may form the pullback diagram (of varieties over k^c):

$$\begin{array}{ccc} A & \longleftarrow & C_Q(i) \\ {\scriptstyle \lambda^i}\downarrow & & \downarrow{\scriptstyle \eta(i)} \\ A & \underset{\tilde{Q}}{\longleftarrow} & C \end{array} \tag{5.1}$$

$C_Q(i)/C$ is a possibly reducible, everywhere unramified Galois cover with Galois group $G_i \simeq \mathrm{Ker}(\lambda^i : A(k^c) \to A(k^c))$ which is cyclic of order l^i. As $C_Q(i)/C$ is Galois, all of the irreducible components of $C_Q(i)$ are isomorphic to a variety B_i, say. Since (5.1) is a pullback diagram, it follows that the function field $k^c(B_i)$ of B_i/k^c is isomorphic to the field $L'(\frac{1}{\lambda^i}Q)$. We deduce from this and from (1.1) that the algebra

of functions on $C_Q(i)/k^c$ is isomorphic to $\mathrm{Map}_{\Omega_{L'}}(G_Q(\lambda^i), L^c) = L'_Q(\lambda^i) = L'_Q(i)$, say.

Let $\mathcal{O}_Q(i)$ be the structure sheaf of the variety $C_Q(i)/k^c$. Since $C_Q(i)/C$ is everywhere unramified, the direct image sheaf $\eta(i)_*\mathcal{O}_Q(i)$ is a locally free $\mathcal{O}G_i$-module, and so it yields an element $(\eta(i)_*\mathcal{O}_Q(i)) \in \mathrm{Cl}(\mathcal{O}G_i)$. We have a decomposition (see e.g. [M] p.72)

$$\eta(i)_*\mathcal{O}_Q(i) = \bigoplus_{\chi\in\hat{G}_i} \mathcal{L}_\chi \tag{5.2}$$

where

$$\mathcal{L}_\chi = \{\alpha \in \eta(i)_*\mathcal{O}_Q(i) : \alpha^g = \chi(g)\alpha\} \qquad \forall g \in G_i \tag{5.3}$$

Let $(\mathcal{L}_\chi)$ denote the class of $\mathcal{L}_\chi$ in $\mathrm{Pic}(C)(k^c)$. The following proposition is simply a reformulation of certain results contained in §2 of [C2].

Proposition 5.4. *The class of $\eta(i)_*\mathcal{O}_Q(i)$ in $Cl(\mathcal{O}G_i)$ is given by the map $\chi \mapsto (\mathcal{L}_\chi)$.*

Proof. Write ξ for the generic point of $C_Q(i)/C$. Then $(\mathcal{O}_{G_i})_\xi = L'G_i$ and $(\eta(i)_*\mathcal{O}_Q(i))_\xi = L'_Q(i)$. If P is a closed point of C, then $(\mathcal{O}G_i)_P = \mathcal{O}_PG_i$, while the stalk $(\eta(i)_*\mathcal{O}_Q(i))_P$ is equal to the semilocal ring of L_Q at P. Since $\eta(i)_*\mathcal{O}_Q(i)$ is a locally free $\mathcal{O}G_i$ module of rank one, we may choose $d_Q \in L'_Q(i)$ such that $(\eta(i)_*\mathcal{O}_Q(i))_\xi = d_Q.(\mathcal{O}G_i)_\xi$, and $a_P \in L'_Q(i)$ such that $(\eta(i)_*\mathcal{O}_Q(i))_P = a_P.(\mathcal{O}G_i)_P$ for each closed point P. This implies that the stalks of the line bundle $\mathcal{L}_\chi$ are given by

$$\mathcal{L}_{\chi,\xi} = (d_Q|\chi).\mathcal{O}_\xi \tag{5.5(a)}$$

$$\mathcal{L}_{\chi,P} = (a_P|\chi).\mathcal{O}_P, \quad P \quad \text{closed} \tag{5.5(b)}$$

Hence the Weil divisor associated to $\mathcal{L}_\chi$ is given by

$$D_\chi = \sum_{P\text{closed}} v_P((a_P|\chi)(d_Q|\chi)^{-1})P \tag{5.6}$$

However it is shown in §2 of [C2] (see Proposition 1 and the remarks following Lemma 4) that $(\eta(i)_*\mathcal{O}_Q(i)) \in \mathrm{Cl}(\mathcal{O}G_i)$ is given by the map $\chi \mapsto (D_\chi)$, where (D_χ) denotes the class of (D_χ) in $\mathrm{Pic}(C)(k^c)$. This establishes the result. $\square$

Now if S is a non-empty set of closed points of C/k^c and $U = C - S$, then $\eta(i)_*\mathcal{O}_Q(i)(U) = \mathfrak{O}_Q(L';\lambda^i)$, and $\mathcal{O}G_i(U) = \mathfrak{O}_{L'}G_i = \mathfrak{A}(L';\lambda^i)$, using the notation of §1. Thus $(\eta(i)_*\mathcal{O}_Q(i)) \in \mathrm{Cl}(\mathcal{O}G_i)$ completely determines $(\mathfrak{O}_Q(L';\lambda^i)) \in \mathrm{Cl}(\mathfrak{A}(L';\lambda^i))$ for all choices of S.

If S consists of a single place of degree one over k, then somewhat more is true. For each i, we have a Wedderburn decomposition

$$\mathcal{A}(L;\lambda^i) = (L^cG_i)^{\Omega_L} = \prod_{r=1}^{t} L_r \tag{5.7}.$$

Each L_r/L is a constant field extension, since the values taken by the characters in $\hat{G}_i$ lie in k^c. It follows from (5.7) that

$$\mathfrak{A}(L;\lambda^i) = (\mathfrak{O}^cG_i)^{\Omega_L} = \prod_{r=1}^{t} \mathfrak{O}_{L_r} \tag{5.8}$$

where $\mathfrak{O}_{L_r}$ denotes the integral closure of $\mathfrak{O}_L$ in L_r.

Since S consists of a single place of degree one over k, the natural homomorphism $\mathrm{Cl}(\mathfrak{O}_{L_r}) \to \mathrm{Cl}(\mathfrak{O}_{L'})$ is injective for each r (see e.g. [C3], Lemma 2). This implies that the natural homomorphism $\mathrm{Cl}(\mathfrak{A}(L;\lambda^i)) \to \mathrm{Cl}(\mathfrak{A}(L';\lambda^i))$ is also injective. Hence, in this case $(\mathfrak{O}_Q(L;\lambda^i)) \in \mathrm{Cl}(\mathfrak{A}(L;\lambda^i))$ is determined by $(\eta(i)_*\mathcal{O}_Q(i)) \in$

$\mathrm{Cl}(\mathcal{O}G_i)$. In particular, if λ^i does not divide Q in $A(L')$, then it follows from Theorem 1.2 that $(\eta(i)_*\mathcal{O}_Q(i)) \neq 0$ in $\mathrm{Cl}(\mathfrak{O}G_i)$.

Suppose for the rest of this section that $\lambda \in \mathrm{End}(A)$ is such that the kernel of $\lambda : A(k^c) \to A(k^c)$ is cyclic of prime order l with $(l,p) = 1$. We now turn our attention to the line bundles $\mathcal{L}_\chi$, $\chi \in \hat{G}_i$. Since $C_Q(i)/C$ is everywhere unramified, the degree of the line bundle $\det(\eta(i)_*\mathcal{O}_Q(i))$ is zero (see e.g. [H] Ch. IV Ex. 2.6). As $C_Q(i)/C$ is cyclic and $\mathcal{L}_{\chi_1} \otimes \mathcal{L}_{\chi_2} = \mathcal{L}_{\chi_1\chi_2}$ for $\chi_1, \chi_2 \in \hat{G}_i$, we deduce that $\mathcal{L}_\chi$ is a line bundle of degree zero for all $\chi \in \hat{G}_i$. Thus in fact $(\mathcal{L}_\chi) \in \mathrm{Pic}^0(C)(k^c) = J(k^c)$, where J denotes the Jacobian of C. Let $H_Q(i)$ be the subgroup of $J(k^c)$ generated by $\{(\mathcal{L}_\chi)\}_{\chi \in \hat{G}_i}$. We shall refer to $H_Q(i)$ as the associated subgroup of Q (at level i). $H_Q(i)$ is cyclic of order dividing l^i, and it determines $C_Q(i)$ up to isomorphism. It follows immediately from the definitions of $C_Q(i)$ and $H_Q(i)$ that $H_Q(i-1) = l.H_Q(i)$.

Let $Q_1, \ldots, Q_r$ be a basis of $A(L)$ modulo torsion. For each Q_j, let λ^{s_j} denote the highest power of λ which exactly divides Q_j in $A(L')$. (So $(\eta(i)_*\mathcal{O}_Q(i))) \in \mathrm{Cl}(\mathcal{O}G_i)$ is trivial for $0 \leq i \leq s_j$ and is non-trivial otherwise.) Write $H_j = \varprojlim_i H_{Q_j}(i + s_j)$, where the inverse limit is taken with respect to the multiplication by l map. Theorem 1.2 implies that $H_{j_1} \cap H_{j_2} = 0$ if $j_1 \neq j_2$. Set $H = H_1 \times \cdots \times H_r$. Then H is a subgroup of $T_l(J)$, the l-adic Tate module of J.

Suppose that $\mathcal{H} = \varprojlim_i \mathcal{H}_i$ is a subgroup of $T_l(J)$ with each $\mathcal{H}_i$ cyclic of order dividing l^i. We shall say that $\mathcal{H}$ is *realisable* if $\mathcal{H}$ is a subgroup of H. This is equivalent to saying that for each i, there is a point $Q^{(i)} \in A(L)$ such that $\mathcal{H}_i = H_{Q^{(i)}}(i)$.

Let $\sigma \in \Omega_k$ denote the Frobenius element of k. Write $P_A(x)$ for the characteristic polynomial of σ acting on $T_l(A)$. The following result characterises realisable subgroups.

THEOREM 5.9. *Let $\mathcal{H}$ be a subgroup of $T_l(J)$ as above. Then $\mathcal{H}$ is realisable if and only if $\mathcal{H}^{P_A(x)} = 0$.*

Proof. Let $\mathcal{O}_A$ denote the structure sheaf of A/k^c. Exactly as in the discussion concerning the sheaf $\eta(i)_*\mathcal{O}_Q(i)$, we have a direct sum decomposition

$$\lambda^i_*\mathcal{O}_A = \bigoplus_{\chi \in \hat{G}_i} \mathcal{L}'_\chi \tag{5.10}$$

where the $\mathcal{L}'_\chi$ are line bundles of degree zero. For any point $Q \in A(L)$, the group $H_Q(i)$ is generated by $\{(\tilde{Q}^*\mathcal{L}'_\chi)\}_{\chi \in \hat{G}_i}$, where $\tilde{Q}^*\mathcal{L}'_\chi$ denotes the pullback of $\mathcal{L}'_\chi$ along $\tilde{Q}$. As A and C are defined over k, we have

$$(\tilde{Q}^*\mathcal{L}'^{\sigma}_{\chi}) = (\tilde{Q}^*\mathcal{L}'_\chi)^\sigma \qquad \forall \chi \in \hat{G}_i. \tag{5.11}$$

It is a theorem of Tate (see e.g. the Main Theorem of [Ta] or Theorem 1 of Appendix 1 of [M]) that the natural homomorphism

$$\mathbb{Z}_l \otimes_{\mathbb{Z}} \mathrm{Hom}_k(A, A) \to \mathrm{Hom}_{\mathbb{Z}_l}(T_l(A), T_l(A))^{\Omega_k} \tag{5.12}$$

is an isomorphism. This implies that $P_A(\sigma)$ annihilates $\mathrm{Pic}^0(A)(k^c)$. It follows from (5.11) that $H^{P_A(\sigma)} = 0$, and so in particular that $\mathcal{H}^{P_A(\sigma)} = 0$.

For the converse, recall that from standard theory we have

$$r = \mathrm{rank}(A(L)) = \mathrm{rank}_{\mathbb{Z}}[\mathrm{Hom}_k(J, A)]. \tag{5.13}$$

Via the theorem of Tate quoted earlier,

$$\mathrm{rank}_{\mathbb{Z}}[\mathrm{Hom}_k(J, A)] = \mathrm{rank}_{\mathbb{Z}_l}[\mathrm{Hom}_{\mathbb{Z}_l}(T_l(J), T_l(A))^{\Omega_k}]. \tag{5.14}$$

As σ acts semisimply on $T_l(J)$ and $T_l(A)$, it follows that

$$\mathrm{Ker}(P_A(\sigma) : T_l(J) \to T_l(J)) \simeq \mathbb{Z}_l^r \tag{5.15}$$

(c.f. e.g. Theorem 1 of [Ta] or Theorem 2 of Appendix I of [M]). Write $H' = \mathrm{Ker}(P_A(\sigma) : T_l(J) \to T_l(J))$. Then $H \subseteq H'$, $H \simeq \mathbb{Z}_l^r$, and H_j is not contained in $l.T_l(J)$ for $j = 1, \ldots, r$. Hence $H' = H$. $\square$

Recall that $P_A(x)$ is the numerator of the zeta function of A/k. Thus, as in the tame number field case (see [T2] or [F]), and the cyclotomic function field case (see [C2]), we have yet another instance of the Galois module structure of rings of integers being determined by an L-function.

§5. References.

[A] A. Agboola, 'Iwasawa theory of elliptic curves and Galois module structure of rings of integers', to appear in *Duke Math Journal.*

[AT] A. Agboola, M. J. Taylor, 'Class invariants of Mordell-Weil groups', to appear.

[C1] R. J. Chapman, 'Galois module structure in global function fields', Ph.D. Thesis, Faculty of Technology, University of Manchester, 1988.

[C2] R. J. Chapman, 'Classgroups of sheaves of locally free modules over global function fields'. In: *The Arithmetic of Function Fields*, eds D. Goss, D. R. Hayes and M. I. Rosen, Walter de Gruyter, Berlin, 1992.

[C3] R. J. Chapman, 'Kummer theory and Galois module structure in global function fields', *Math. Z.,* **108**, 375-388, (1991).

[CN-S] Ph. Cassou-Noguès, A. Srivastav, 'On Taylor's conjecture for Kummer orders', *Séminaire de Théorie des Nombres, Bordeaux,* **2**, 349-363, (1990).

[CN-T] Ph. Cassou-Noguès, M. J. Taylor, *Elliptic functions and rings of integers*, Birkhauser, Boston, (1987).

[CR] C. W. Curtis and I. Reiner, *Methods of representation theory Vol. 1*, Wiley, 1981.

[F] A. Fröhlich, *Galois module structure of algebraic integers*, Springer Verlag, New York, 1983.

[H] R. Hartshorne, *Algebraic Geometry*, Springer Verlag, New York, 1977.

[L] S. Lang, 'Algebraic groups over finite fields', *American J. of Math.* **78**, 555-563, (1956).

[M] D. Mumford, *Abelian varieties*, Oxford University Press, Oxford, 1974.

[ST] A. Srivastav and M. J. Taylor, 'Elliptic curves with complex multiplication and Galois module structure', *Inv. Math.*, **99**, 165-184, (1990).

[Ta] J. Tate, 'Endomorphisms of abelian varieties over finite fields', *Inv. Math.*, **2**, 134-144, (1966).

[T1] M. J. Taylor, 'Mordell-Weil groups and the Galois module structure of rings of integers', *Ill. J. Math.*, **32**, 428-452, (1988).

[T2] M. J. Taylor, 'On Fröhlich's conjecture for rings of integers of tame extensions', *Invent. Math.*, **63**, 41-79, (1981).

Abelian Varieties and Galois Module Structure

In Global Function Fields

A. Agboola

Department of Mathematics

University of California

Berkeley, CA 94720

U. S. A.

Email: agboola@math.berkeley.edu

Fax: (510)-642-8204

Running Title: Abelian Varieties and Galois Module Structure

August 19, 2001

Abstract

The purpose of this paper is to study the Galois module structure of certain principal homogeneous spaces constructed via points of infinite order on a CM abelian variety defined over a global function field. We prove that, in general, such principal homogeneous spaces have non-trivial Galois structure. Under suitable hypotheses, we show how this fact may be described in terms of the zeta function of the abelian variety.