ILLINOIS JOURNAL OF MATHEMATICS
Volume 32, Number 3, Fall 1988

MORDELL-WEIL GROUPS AND THE GALOIS MODULE STRUCTURE OF RINGS OF INTEGERS

BY

M.J. TAYLOR[1]

This paper is dedicated to the memory of Irv Reiner in recognition of much kindness shown

1. Introduction and statement of results

In [5], A. Fröhlich introduced the notion of a Kummer order—taken with respect to the multiplicative group law. The Galois module structure (at rational level) of such orders was then determined by the author in [20]. The purpose of this article is to introduce and study the corresponding Galois module properties of analogous orders, when the multiplicative group law is replaced by the group law of an abelian variety.

Before stating our results, we first fix some notation. Let $\mathbf{Q}^c$ denote the algebraic closure of $\mathbf{Q}$, which we view as embedded in $\mathbf{C}$ once and for all; we write ρ for the complex conjugation automorphism of $\mathbf{C}$; given a number field $L \subseteq \mathbf{Q}^c$, we put $\Omega_L = \mathrm{Gal}(\mathbf{Q}^c/L)$.

We let K denote a CM number field, that is to say K is a totally imaginary extension of a totally real field. We then fix a CM type Φ of K; thus $\Phi = \{\varphi_1, \ldots \varphi_n\}$, is a transversal, modulo the action of ρ, of the set of field embeddings from K into $\mathbf{Q}^c$. We write K' for the field generated by all elements of the form $\sum_i x^{\varphi_i}$ for $x \in K$: we call K' the reflex field of K with respect to Φ. In the sequel we shall always suppose the CM type (K, Φ) to be simple, that is to say K identifies with the reflex of K'. We write N_Φ: $K^* \to K'^*$ for the reflex norm $N_\Phi(x) = \prod_i x^{\varphi_i}$, and we shall also write N_Φ for the corresponding norm map on idèles and ideals.

Let A denote an Abelian variety of dimension $n = \frac{1}{2}[K : \mathbf{Q}]$ which admits complex multiplication by $\mathfrak{O}_K$. For points P, Q on A we write $P +_A Q$ for

Received July 20, 1987.

[1]Much of the work for this paper was done whilst I was Professeur Associé at Bordeaux University, and also whilst I was a visitor at the MSRI at Berkeley. I am deeply grateful to these two institutions for their hospitality. I should particularly like to thank Ph. Cassou-Noguès and J. Boxall for many helpful remarks concerning the preparation of this manuscript.

their sum with respect to the group law of the variety; and for $\alpha \in \mathfrak{O}_K$ we write $[\alpha]P$ for the point obtained by applying the endomorphism corresponding to α to P. We suppose that A, together with the endomorphisms $\mathfrak{O}_K$, are all defined over a given number field H. Furthermore we suppose that A has CM type Φ; that is to say $A \times_H \mathbf{C}$ has a basis of differentials of the first kind $\{dz_1, \ldots, dz_n\}$ such that $[\alpha]\, dz_i = \alpha^{\varphi_i}\, dz_i$. By general theory we know that $K' \subseteq H$.

Let $\mathfrak{a} = a\mathfrak{O}_K$ denote an integral $\mathfrak{O}_K$ ideal, we then choose $\pi \in H$ such that $\pi = N_\Phi a$, and we henceforth write S for the set of primes of $\mathfrak{O}_H$ which divide π.

It is well-known that the co-ordinates of a torsion point of A generate an abelian extension of H. The Galois action on such torsion points is described by Shimura's reciprocity law (see Theorem 11 in [11]). In the sequel we shall freely use this result without further reference.

We write G for the sub-group of elements in $A(\mathbf{Q}^c)$ which are killed by all elements of $\mathfrak{a}$; we put $r = |G|$ and we let L denote a finite extension of H with the property that A acquires everywhere good reduction over L; we note that this can always be achieved by Theorem 6 of [11].

For $Q \in A(L)$ we define the corresponding G-space of points on A by

$$G_Q = \{Q' \in A(\mathbf{Q}^c) | [a]Q' = Q\}$$

and we note that G_Q is Ω_L stable. We define the Kummer algebra L_Q by

$$L_Q = \mathrm{Map}_{\Omega_L}(G_Q, \mathbf{Q}^c)$$

where the addition and multiplication are given by value-wise addition and multiplication of Ω_L-maps from G_Q to $\mathbf{Q}^c$.

L_Q is an L-algebra. To understand why we use L_Q rather than $L(Q)$, the field generated over L by the co-ordinates of all points of G_Q, we note that $[L_Q : L] = |G|$, whereas, in general, $[L(Q) : L]$ will vary with the choice of Q; thus the algebra L_Q enables us to treat all points in $A(L)$ in a uniform fashion.

In §2 we construct an $\mathfrak{O}_L$-algebra $\mathfrak{B}$ which represents the $\mathfrak{O}_L$ group scheme of $\mathfrak{a}$ points of A: although $\mathfrak{B}$ depends on A, $\mathfrak{a}$, and L, we shall only include such dependence in our notation when there is any ambiguity. We write $\mathfrak{A}$ for the $\mathfrak{O}_L$ Cartier dual of $\mathfrak{B}$.

More explicitly, we shall see that $\mathfrak{B}$ is an $\mathfrak{O}_L$ order in the algebra $\mathscr{B} = \mathrm{Map}_{\Omega_L}(G, \mathbf{Q}^c)$, while $\mathfrak{A}$ is an $\mathfrak{O}_L$ order in the algebra $\mathscr{A} = (\mathbf{Q}^c G)^{\Omega_L}$. (Here Ω_L has its natural Galois action on both $\mathbf{Q}^c$ and G.) Thus L_Q is an $\mathscr{A}$ module via the rule that for $f \in L_Q$, $Q' \in G_Q$,

$$\left[f\left(\sum_{a_g} g\right)\right](Q') = \sum_g f(Q' + g)\, a_g.$$

At the integral level we define $\mathfrak{O}_Q$ to be the integral closure of $\mathfrak{O}_L$ in L_Q, and we let $\tilde{\mathfrak{O}}_Q$ denote the largest $\mathfrak{A}$-module contained in $\mathfrak{O}_Q$:

$$\tilde{\mathfrak{O}}_Q = \{x \in \mathfrak{O}_Q | x\mathfrak{A} \subseteq \mathfrak{O}_Q\}. \tag{1.1}$$

Thus $\tilde{\mathfrak{O}}_Q$ is naturally isomorphic to $\mathrm{Hom}_{\mathscr{A}}(\mathfrak{A}, \mathfrak{O}_Q)$, the $\mathfrak{O}_L$ lattice of homomorphisms in $\mathrm{Hom}_{\mathscr{A}}(\mathscr{A}, L_Q)$ which take $\mathfrak{A}$ into $\mathfrak{O}_Q$. In §3 we shall see that $\tilde{\mathfrak{O}}_Q$ is a twisted Q-form of $\mathfrak{B}$, in the sense of Galois cohomology, and that it is an $\mathfrak{O}_L$-order which is $\mathfrak{A}$-locally free. We call $\tilde{\mathfrak{O}}_Q$ a Kummer order. The main goal of this paper is the study of $(\tilde{\mathfrak{O}}_Q) \in \mathrm{Cl}(\mathfrak{A})$, the classgroup of locally free $\mathfrak{A}$-modules.

We remark that in many respects the above framework generalises the Normal Integral Basis problem, where one studies rings of integers which are locally free over the (minimal) Hopf order $\mathfrak{O}_L G$; by Noether's criterion such an extension can be at most tamely ramified. Here we replace $\mathfrak{O}_L G$ by the Hopf order $\mathfrak{A}$, and the full ring of integers is replaced by $\tilde{\mathfrak{O}}_Q$; we remark that the result of Childs-Hurley (see Proposition 5) furnishes us with a generalisation of Noether's projectivity criterion for $\mathfrak{A}$-modules. Pursuing the analogy with Normal Integral Bases a little more closely, the fact that we use only Abelian varieties with everywhere good reduction is the analogue of using only non-ramified extensions (compare Theorem 1 with the work in [2]). One obtains the analogue of (genuinely) tamely ramified extensions by permitting bad reduction on A.

The notion of Kummer orders over a split commutative maximal order was first introduced by Fröhlich in [5]. Such orders were further studied in [20], and in particular such Kummer orders were completely described as Galois modules at the rational level: Theorem 2 below may be thought of as an analogue of this result. We remark that the situation where we use a split maximal order, corresponds to replacing the group law of A, by the multiplicative group law. We note that the (local) Kummer orders associated to Lubin-Tate formal groups have recently been studied in [15].

We now conclude this introductory section by describing our main results.

Let V denote the multiplicative monoid of elements in $\mathfrak{O}_K$, which are coprime to $\mathfrak{a}$. In §4 we shall define a natural V-action on $\mathfrak{A}$, which extends the $\mathfrak{O}_K$ action on G: for $g \in G$ (resp. $a \in \mathfrak{A}$), $v \in V$, we write this action exponentially as g^v (resp. a^v). Thus, to sum up, V acts as automorphisms of the group $\mathrm{Cl}(\mathfrak{A})$, and this action factors through $V \bmod^* \mathfrak{a}$. Let ψ: $A(L) \to \mathrm{Cl}(\mathfrak{A})$ denote the map induced by $Q \to (\tilde{\mathfrak{O}}_Q)$. We note from the definition of $\tilde{\mathfrak{O}}_Q$, that $\psi(Q)$ only depends on the class of $Q \bmod [a]A(L)$. In §5 we show:

THEOREM 1. *ψ is a group homomorphism which respects V-action.*

COROLLARY 1. *Let e denote the exponent of G; then $(\tilde{\mathfrak{O}}_Q)^e = 1$.*

We let $\mathfrak{D}_Q^{-1}$ denote the inverse different of L_Q/L. By standard theory, $\mathfrak{D}_Q^{-1} \cdot \mathfrak{A}$ identifies as the dual of $\tilde{\mathfrak{D}}_Q$; in §5 we show that the inverse class of the dual of a module corresponds to the action of $[-1]$ on $\mathrm{Cl}(\mathfrak{A})$.

COROLLARY 2. *$\tilde{\mathfrak{D}}_Q$ is a self-dual $\mathfrak{A}$-module, that is to say there is an isomorphism of $\mathfrak{A}$-modules*: $\tilde{\mathfrak{D}}_Q \cong \mathfrak{D}_Q^{-1} \cdot \mathfrak{A}$.

Proof. From the above it suffices to note that

$$1 = \psi(Q + [-1]Q) = \big(\tilde{\mathfrak{D}}_Q\big)\big(\tilde{\mathfrak{D}}_Q\big)^{[-1]}. \qquad \square$$

Remark 1. In practice when calculating $(\tilde{\mathfrak{D}}_Q)$ one has to admit a limited amount of bad reduction on A: $\tilde{\mathfrak{D}}_Q$ is then defined in the same way see; see the remark after Theorem 5. However, in this case, ψ apparently ceases to be a homomorphism. Given this proviso, one can show that if $a = 1 + i$ and $Q = (1 + 2i, \sqrt{-10})$ on $y^2 = x^3 + x$, then $(\tilde{\mathfrak{D}}_Q)$ has order 2. Bryan Birch has shown that if $a = \sqrt{-3}$ and

$$Q = \left[\frac{5 + 4\omega}{1 + 4\omega}, \frac{\sqrt{-26} \cdot (3 + 2\omega)}{(1 + 4\omega)^2}\right] \quad \text{on } y^2 = x^3 + 1, \text{ with } \omega = \frac{-1 + \sqrt{-3}}{2},$$

then $(\tilde{\mathfrak{D}}_Q)$ has order 3.

Remark 2. In the case where A is a Fueter elliptic curve and Q is some torsion point, then it is shown in [17] and [1] that $\tilde{\mathfrak{D}}_Q = \mathfrak{D}_Q$, and that $\tilde{\mathfrak{D}}_Q$ is $\mathfrak{A}$-free when 2 splits in K (see Theorem 7).

Remark 3. It is interesting to note that the annihilators for $\mathrm{Im}(\psi)$ are of the same nature as a number of L. McCulloh's annihilators in [7] and [8].

Next we consider the behaviour of the homomorphism ψ with respect to restriction. We therefore let F denote a finite extension of L. In §6 we shall show that the following diagram commutes:

$$\begin{array}{ccc} A(F) & \xrightarrow{\psi_F} & \mathrm{Cl}(\mathfrak{A}(F)) \\ \Big\downarrow{\scriptstyle \mathrm{Tr}_{F/L}} & & \Big\downarrow{\scriptstyle \mathrm{Res}} \\ A(L) & \xrightarrow[\psi_L]{} & \mathrm{Cl}(\mathfrak{A}(L)) \end{array} \tag{1.2}$$

where Res denotes the restriction map (see §5), and $\mathrm{Tr}_{F/L}$ is the trace map. We

can then deduce:

THEOREM 2. *Suppose that $A(L)$ is torsion, with $\mathfrak{O}_K$-annihilator coprime to a; then for all $Q \in A(F)$ we have an isomorphism of $\mathfrak{A}(L)$-modules*

$$\tilde{\mathfrak{O}}_Q \cong \mathfrak{A}(F)$$

Remark. This result can be seen as an Abelian variety analogue of the (classical) Kummer order classification theorem in [20]. The proof of this result depends critically on Stickelberger's annihilation theorem for classgroups.

Our next result concerns the evaluation of resolvents. In general one can only obtain Galois module results for rings of integers by making some kind of statement about Lagrange resolvents in the abelian case, or, more generally, about Fröhlich's generalised resolvents. The result which we give below may be viewed as an analogue of Fröhlich's evaluation of tame resolvents (see Theorem 23 in [4]).

Given a map $m \in \mathrm{Map}_{\mathfrak{Q}_L}(G_Q, \mathbf{Q}^c)$ and $g \in G$, we define

$$m^g \in \mathrm{Map}_{\mathfrak{Q}_{L(Q)}}\left(G_Q, \mathbf{Q}^c\right) = \mathrm{Map}\left(G_Q, \mathbf{Q}^c\right)$$

by the rule

$$m^g(Q') = m(Q' + g) \quad \text{for } Q' \in G_Q.$$

Fixing $Q' \in G_Q$, we define $m_{Q'} \in \mathrm{Map}(G, \mathbf{Q}^c)$ by the rule $m_{Q'}(g) = m(Q' + g)$.

THEOREM 3. *Let $\mathfrak{q}$ denote a prime of $\mathfrak{O}_L$ and choose $m \in \tilde{\mathfrak{O}}_Q$ such that $\tilde{\mathfrak{O}}_{Q,\mathfrak{q}} = m \cdot \mathfrak{A}_{\mathfrak{q}}$; then*

$$\pi^{-1}\left(\sum_g m^g_{Q'} g^{-1}\right)$$

is a unit in the ring $\mathfrak{A}(L(Q))_{\mathfrak{q}}$.

Lastly we consider what happens in a particular case when A is an elliptic curve. More precisely we now suppose that K is a quadratic imaginary number field with class number one. We now take A to be an elliptic curve, which we denote by E, with complex multiplication by $\mathfrak{O}_K$ and which is defined over K. We choose a 'split' prime element π, $\pi \nmid 3$, $\pi \equiv \pm 1 \bmod 8\mathfrak{O}_K$, with the property that $\mathfrak{p} = \pi\mathfrak{O}_K$ is a prime of good reduction for E/K; we set $p = N_{K/\mathbf{Q}}\pi$. Given an $\mathfrak{O}_K$-ideal $\mathfrak{f}$, we shall denote the ray classfield with conductor $\mathfrak{f}$ by $K(\mathfrak{f})$.

Next we choose a finite abelian extension L/K with the following properties:

(a) $p \nmid [L : K]$;

(b) L contains the co-ordinates of a primitive $4\mathfrak{p}$ division point of E.

We set $\Delta = \mathrm{Gal}(L/K)$, and we let $\kappa\colon \Delta \to Z_p^*$ denote the unique character of order $p - 1$, with the property that

$$g^\delta = [n_\delta]g \quad \text{for } g \in G,\ \delta \in \Delta$$

where $n_\delta \in Z$ with $n_\delta \equiv \kappa(\delta) \bmod \mathfrak{p}$. We put $k = \mathfrak{O}_K \bmod \mathfrak{p}$, $\mathscr{E} = E(L) \otimes k$, and we note that ψ factors through $\mathscr{E}$. Given a finite $\mathbf{F}_p\Delta$-module M, we shall denote the κ-eigenspace in M by $M^{(\kappa)}$.

In §7 we shall show:

THEOREM 4. *With the above notations and hypotheses*:

(a) *For each character* $\theta\colon \Delta \to \mathbf{F}_p^*$

$$\dim_{\mathbf{F}_p}(\mathrm{Ker}\, \psi|_{\mathscr{E}^{(\theta)}}) \leq 1.$$

(b) *If* 2 *splits in* K/Q, *then* $\mathrm{Ker}\,(\psi|_{\mathscr{E}^{(\kappa)}}) = G$.

The above result, together with other calculations, leads me to believe the following:

Conjecture. *If* E/L *is an elliptic curve with everywhere good reduction, and with complex multiplications by* $\mathfrak{O}_K$; *then for any* $a \in \mathfrak{O}_K \setminus 0$,

$$E(L)_{\mathrm{torsion}} \subseteq \mathrm{Ker}(\psi).$$

One immediate consequence of this conjecture would be that Theorem 2 could then be strengthened to:

If $E(L)$ *is finite, then for any finite extension* F/L, *we have an isomorphism of* $\mathfrak{A}(L)$ *modules*: $\tilde{\mathfrak{O}}_Q \cong \mathfrak{A}(F)$ *for each* $Q \in E(F)$.

The Birch-Swinnerton-Dyer conjecture asserts that $E(L)$ is finite precisely when the L-function, associated to E/L, is non-zero at 1. As is proven in the tame case, one can therefore again hope for a direct link between the Galois module structure of rings of integers and the behaviour of an L-function.

2. The orders $\mathfrak{A}$ and $\mathfrak{B}$

In this section we give the definitions and a number of basic properties of the orders $\mathfrak{A}$, (resp. $\mathfrak{B}$) in the algebra $(\mathbf{Q}^c G)^{\Omega_L}$ (resp. $\mathrm{Map}_{\Omega_L}(G, \mathbf{Q}^c)$). Clearly,

in defining such an order, it will suffice to describe its localisation at each prime of $\mathfrak{O}_L$.

Given a prime $\mathfrak{q}$ of $\mathfrak{O}_L$, we write $G_{\mathfrak{q}}$ for the $\mathfrak{O}_{L,\mathfrak{q}}$ group scheme obtained by localising the $\mathfrak{O}_L$ group scheme afforded by G at $\mathfrak{q}$. We then let G_1 denote its connected component of the identity, and we write G' for the étale factor G/G_1. From Corollary 2 to Theorem 5 in [11] together with Corollary 2 to Theorem 4 in [14], we have a splitting $G_{\mathfrak{q}} = G_1 \times G'$.

We let $\mathbf{F}(\mathbf{X}, \mathbf{Y}) \in \mathfrak{O}_{L,\mathfrak{q}}[[\mathbf{X}, \mathbf{Y}]]^{(m)}$ denote the formal group over L afforded by the kernel of reduction mod $\mathfrak{q}$ on A, where $\mathbf{X} = (X_1, \ldots, X_m)$ etc. For each $b \in \mathfrak{O}_K$, we let $[b](\mathbf{X})$ denote the vector of formal power series corresponding to the endomorphism b; we then let $\mathfrak{f}_{\mathfrak{q}}$ denote the $\mathfrak{O}_{L,\mathfrak{q}}[[\mathbf{X}]]$ ideal generated by the components of $[a]$ and we define

$$\mathfrak{B}_1 = \frac{\mathfrak{O}_{L,\mathfrak{q}}[[\mathbf{X}]]}{\mathfrak{f}_{\mathfrak{q}}} \tag{2.1}$$

Then $\mathfrak{B}_1$ represents G_1, where we view $\mathfrak{B}_1$ as an $\mathfrak{O}_{L,\mathfrak{q}}$ order in $\mathrm{Map}_{\Omega_L}(G_1, \mathbf{Q}^c)_{\mathfrak{q}}$ via the rule $b(\mathbf{X})(g) = b(\mathbf{g})$ for $g \in G_1$, where $\mathbf{g}$ denotes the co-ordinates of g on the formal group.

$G_{\mathfrak{q}}$ is represented by the $\mathfrak{O}_{L,\mathfrak{q}}$ order $\mathfrak{B}_{\mathfrak{q}}$:

$$\mathfrak{B}_{\mathfrak{q}} = \mathfrak{B}' \otimes_{\mathfrak{O}_{L,\mathfrak{q}}} \mathfrak{B}_1 \quad \text{where } \mathfrak{B}' = \mathrm{Map}_{\Omega_L}(G', \mathfrak{O}^c)_{\mathfrak{q}}.$$

Here $\mathfrak{O}^c$ denotes the ring of all algebraic integers in $\mathbf{Q}^c$.

We note that if $\mathfrak{q} \notin S$, then $G_1 = \{1\}$ and so $\mathfrak{B}_{\mathfrak{q}}$ identifies with $\mathrm{Map}_{\Omega_L}(G, \mathfrak{O}^c)_{\mathfrak{q}}$. We let $\mathfrak{A}(L)$ denote the $\mathfrak{O}_L$-Cartier dual of $\mathfrak{B}(L)$. To describe $\mathfrak{A}(L)$ more explicitly, we first consider the case of a number field M which contains the field $L(Q)$; then $\mathscr{B}(M) = \mathrm{Map}(G, M)$, $\mathscr{A}(M) = MG$, and we have the non-singular pairing

$$\langle \ , \ \rangle : \mathscr{B}(M) \times \mathscr{A}(M) \to M, \quad \langle b, \sum l_g g \rangle = \sum l_g b(g).$$

Furthermore we note that for $\omega \in \Omega_L$,

$$\langle b, a \rangle^{\omega} = \langle b^{\omega}, a^{\omega} \rangle.$$

Thus, since $\mathfrak{B}(L) = \mathfrak{B}(M)^{\Omega_L}$, we note that

$$\mathscr{A}(L) = (MG)^{\Omega_L} \quad \text{and} \quad \mathfrak{A}(L) = \mathfrak{A}(M)^{\Omega_L}.$$

In the opposite direction, since A has everywhere good reduction, from the

above we see that for a finite extension F/L,

$$\mathfrak{B}(F) = \mathfrak{B}(L) \otimes_{\mathfrak{O}_L} \mathfrak{B}_F, \quad \mathfrak{A}(F) = \mathfrak{A}(L) \otimes_{\mathfrak{O}_L} \mathfrak{O}_F.$$

We again view L as fixed, and so write $\mathfrak{A}$ for $\mathfrak{A}(L)$ etc., and we study the orders $\mathfrak{A}$ and $\mathfrak{B}$ in greater detail. We let t: $\mathscr{B} \to L$ denote the trace map $t(b(\mathbf{X})) = \Sigma_{g \in G} b(g)$, and we write $\mathfrak{D}^{-1}(\mathfrak{B})$ for the inverse different of $\mathfrak{B}$:

$$\mathfrak{D}^{-1}(\mathfrak{B}) = \{ b \in \mathscr{B} | t(b\mathfrak{B}) \subseteq \mathfrak{O}_L \}. \tag{2.2}$$

In the same way we write $\mathfrak{D}^{-1}(\mathfrak{A})$ for the inverse different of $\mathfrak{A}$ with respect to the trace pairing $\mathscr{A} \to L$.

LEMMA 1.
(a) $\mathfrak{D}^{-1}(\mathfrak{B}) = \pi^{-1}\mathfrak{B}$;
(b) $\mathfrak{D}^{-1}(\mathfrak{A}) = r^{-1}\pi\mathfrak{A}$, *where* r *denotes* $|G|$.

Proof. Part (a) is a particular case of (2.2) in [14]; (b) then follows from (a) by Proposition 9 in the appendix of [10]. □

In the standard way we have:

LEMMA 2. $\mathfrak{D}^{-1}(\mathfrak{B})$ *identifies with* $\mathrm{Hom}_{\mathfrak{O}_L}(\mathfrak{B}, \mathfrak{O}_L)$ *via the pairing*

$$(d, b) = t(db) \quad \text{for } d \in \mathfrak{D}^{-1}(\mathfrak{B}), \quad b \in \mathfrak{B}.$$

PROPOSITION 1. $\mathfrak{A} = \{ \pi^{-1} \Sigma_{g \in G} f(g) g | f \in \mathfrak{B} \}$.

Proof. This follows easily on piecing together the above information: by Lemma 2 we have a natural isomorphism ξ: $\mathfrak{D}^{-1}(\mathfrak{B}) \cong \mathrm{Hom}_{\mathfrak{O}_L}(\mathfrak{B}, \mathfrak{O}_L)$ where $\xi(d)(b) = t(db)$; furthermore, under the identification

$$\eta\colon \mathrm{Hom}_{\mathfrak{O}_L}(\mathfrak{B}, \mathfrak{O}_L) \cong \mathfrak{A},$$

such a homomorphism h has image $\eta(h) = \Sigma h_g g$ if, and only if, for all $b \in \mathfrak{B}$, $h(b) = \Sigma h_g b(g)$. Thus $\eta \circ \xi(d) = \Sigma d(g) g$; the result then follows from Lemma 1. □

The above map $\eta \circ \xi$: $\mathfrak{D}^{-1}(\mathfrak{B}) \to \mathfrak{A}$ does not respect $\mathfrak{A}$-action; however, this is easily rectified by composing with the antipode $\bar{\ }$: $\mathfrak{A} \to \mathfrak{A}$; we write κ:

$\mathfrak{D}^{-1}(\mathfrak{B}) \to \mathfrak{A}$ for this isomorphism, and we let l: $G \to L$ be defined by

$$l(g) = \begin{cases} 1 & \text{if } g = 1_G, \\ 0 & \text{if } g \neq 1_G. \end{cases}$$

Then from the above,

$$\pi^{-1}\mathfrak{B} = \mathfrak{D}^{-1}(\mathfrak{B}) = \kappa^{-1}(\mathfrak{A}) = \kappa^{-1}(1)\mathfrak{A} = l.\mathfrak{A}.$$

We have therefore shown:

PROPOSITION 2. *$\mathfrak{B}$ is a free $\mathfrak{A}$-module on πl.*

Remark. To see the role of self-duality in Hopf algebras in full generality the reader is referred to [13].

3. Principal homogeneous spaces

We recall that, given $Q \in A(L)$, the $\mathfrak{A}$-module $\tilde{\mathfrak{O}}_Q$ was defined in (1.1). We begin this section by showing:

PROPOSITION 3. *$\tilde{\mathfrak{O}}_Q$ is an $\mathfrak{O}_L$-order in L_Q.*

Proof. Since clearly $\tilde{\mathfrak{O}}_Q \otimes_{\mathfrak{O}_L} L = L_Q$, it suffices to show that $\tilde{\mathfrak{O}}_Q$ is a ring. Firstly we note that for an $a \in \mathfrak{A}$, $1.a = \varepsilon(a)$, where ε is the augmentation map; thus $1 \in \tilde{\mathfrak{O}}_Q$, since $\varepsilon(\mathfrak{A}) = \mathfrak{O}_L$. Next we note that for any two elements $s, t \in L_Q$ and $a \in LG$,

$$(s.t)a = \sum_i (sa_{i1}).(ta_{i2}) \tag{3.1}$$

where $\Delta(a) = \Sigma a_{i1} \otimes a_{i2}$ under the co-multiplication map Δ: $\mathscr{A} \to \mathscr{A} \otimes_L \mathscr{A}$, induced by $g \to g \otimes g$. We are required to show that if $s, t \in \tilde{\mathfrak{O}}_Q$, then $(st)a \in \mathfrak{O}_Q$ for all $a \in \mathfrak{A}$. This, however, is now clear from (3.1), since the sa_{i1} and ta_{i2} all lie in $\mathfrak{O}_Q$. □

Next we give a sufficient condition for the local freedom of a module over a Hopf order in L_qG.

PROPOSITION 4 (See [3] and also more recently [21]). *Let $\mathfrak{E}$ denote a Hopf order in L_qG and suppose that $\mathfrak{E} \cap L_qG = t^{-1}\mathfrak{O}_{L_q}\Sigma$ where $\Sigma = \Sigma_{g \in G} g$. Let M denote a finitely generated $\mathfrak{E}$-module which has no $\mathfrak{O}_{L_q}$-torsion, which has*

$M \otimes_{\mathfrak{D}_{L,\mathfrak{q}}} L$ an $L_{\mathfrak{q}}G$ free module, and which possesses an $\mathfrak{D}_{L,\mathfrak{q}}$ endomorphism f such that $tm = \Sigma_g f(mg)g^{-1}$, for all $m \in M$. Then M is a free $\mathfrak{E}$-module.

Proof. This is a straightforward generalisation of the corresponding well-known result for group rings: we therefore only sketch the details. By hypothesis $t^{-1}\Sigma \in \mathfrak{E}$; we may therefore write

$$\Delta(t^{-1}\Sigma) = \sum \beta_{i1} \otimes_{\mathfrak{D}_{L,\mathfrak{q}}} \beta_{i2} \quad \text{where } \beta_{ij} \in \mathfrak{E}.$$

For $m \in M$, the element

$$\lambda(m) = t^{-1}\Sigma f(mg) \otimes g^{-1}$$

can be written in the form

$$\lambda(m) = (m \otimes 1)\big(\Delta(t^{-1}\Sigma)\big)(\mathrm{id} \otimes {}^{-})(f \otimes 1)$$

and so $\lambda(m) \in M \otimes_{\mathfrak{D}_{L,\mathfrak{q}}} \mathfrak{E}$. Thus λ defines a $\mathfrak{E}$-module map $\lambda\colon M \to M \otimes_{\mathfrak{D}_{L,\mathfrak{q}}} \mathfrak{E}$, with $\mathfrak{E}$ acting on the second factor in the range of λ. Since f has trace t, λ is split by the map $\mu\colon M \otimes_{\mathfrak{D}_{L,\mathfrak{q}}} \mathfrak{E} \to M$ induced by $m \otimes a \to ma$; hence M is certainly $\mathfrak{E}$-projective. The fact that M is actually free, follows from the hypothesis that $M \otimes L_{\mathfrak{q}}$ is $L_{\mathfrak{q}}G$-free and the fact that $L_{\mathfrak{q}}G$ is commutative (for instance, see [6]). □

The main goal of this section is to show:

THEOREM 5. *$\tilde{\mathfrak{D}}_Q$ is a locally free rank one $\mathfrak{A}$-module.*

Remark. If we allow bad reduction on A/L at primes which are coprime to $|G|$; then, for any prime $\mathfrak{q}$ of bad reduction, $\mathfrak{A}_{\mathfrak{q}}$ is the maximal order, and so, of course, $\tilde{\mathfrak{D}}_Q$ will still be locally free over $\mathfrak{A}$.

Before starting to prove this result, we need an alternative description of $\tilde{\mathfrak{D}}_Q$.

Let N/L denote a finite extension field which contains the coordinates of G and G_Q; then by standard Galois theory we have isomorphisms of N-algebras (and $\mathscr{A}$-modules),

$$\mathrm{Map}_{\Omega_L}(G, \mathbf{Q}^c) \otimes_L N \cong \mathrm{Map}_{\Omega_N}(G, \mathbf{Q}^c)$$

$$\mathrm{Map}_{\Omega_L}(G_Q, \mathbf{Q}^c) \otimes_L N \cong \mathrm{Map}_{\Omega_N}(G_Q, \mathbf{Q}^c).$$

Thus translation by $Q' \in G_Q$ yields an isomorphism of N algebras (and

$\mathscr{A}$-modules):

$$\xi\colon \mathscr{B} \otimes_L N \cong L_Q \otimes_L N. \tag{3.2}$$

Here $\xi(b \otimes n)(Q' + g) = b(g)n$, and we view Ω_L as acting on both terms via the second factor. We then define the Q-twist of $\mathfrak{B}$, denoted $\mathfrak{C}_Q$, by

$$\mathfrak{C}_Q = \xi\big(\mathfrak{B} \otimes_{\mathfrak{O}_L} \mathfrak{O}_N\big)^{\Omega_L}. \tag{3.3}$$

Concretely, given a prime $\mathfrak{q}$ of $\mathfrak{O}_L$, $\mathfrak{C}_{Q,\mathfrak{q}}$ is the $\mathfrak{O}_{L,\mathfrak{q}}$ suborder of $\mathfrak{O}_{Q,\mathfrak{q}}$ which is defined as follows: Over $L_\mathfrak{q}$ for $Q' \in G_Q$ we write $Q' = Q_2' + Q_1'$ with Q_2' torsion of order prime to the reflex norm of $\mathfrak{q} \cap K'$, and with Q_1' in the kernel of reduction mod $\mathfrak{q}$. We write $\mathfrak{g}$ for the $\mathfrak{O}_{L,\mathfrak{q}}[[\mathbf{x}]]$ ideal generated by the components of $[a](\mathbf{x}) - {}_F\mathbf{Q}_1$, where $Q_1 = [a]Q_1'$. We then set

$$\mathfrak{C}_1 = \frac{\mathfrak{O}_{L,\mathfrak{q}}[[\mathbf{x}]]}{\mathfrak{g}}, \quad \mathfrak{C}' = \mathrm{Map}_{\Omega_{L_\mathfrak{q}}}\big(Q_2' + G', \mathfrak{O}_q^c\big)$$

$$\mathfrak{C}_\mathfrak{q} = \mathfrak{C}_1 \otimes_{\mathfrak{O}_{L,\mathfrak{q}}} \mathfrak{C}'.$$

Here we identify

$$\mathrm{Map}_{\Omega_{L,\mathfrak{q}}}\big(G_Q, L_\mathfrak{q}^c\big) = \mathrm{Map}_{\Omega_L}\big(G_Q, L_\mathfrak{q} \otimes L^c\big)$$

and

$$\mathrm{Map}_{\Omega_{L,\mathfrak{q}}}\big(Q_1' + G_1, L_\mathfrak{q}^c\big) \otimes_{L_\mathfrak{q}} \mathrm{Map}_{\Omega_{L_\mathfrak{q}}}\big(Q_2' + G', L_\mathfrak{q}^c\big) = \mathrm{Map}_{\Omega_{L_\mathfrak{q}}}\big(G_Q, L_\mathfrak{q}^c\big)$$

We thereby view $\mathfrak{C}$ as an order in L_Q defined by the $\mathfrak{C}_\mathfrak{q}$. Then subtraction by Q' induces an isomorphism of $\mathfrak{O}_{N,\mathfrak{q}}$ algebras:

$$\xi_\mathfrak{q}\colon \mathfrak{B} \otimes_{\mathfrak{O}_L} \mathfrak{O}_{N,\mathfrak{q}} \cong \mathfrak{C}_Q \otimes_{\mathfrak{O}_L} \mathfrak{O}_{N,\mathfrak{q}}. \tag{3.4}$$

We note that for $N \supseteq F \supseteq L$,

$$\mathfrak{C}_Q(F) = \mathfrak{C}_Q(L) \otimes_{\mathfrak{O}_L} \mathfrak{O}_F \quad \mathfrak{C}_Q(L) = \mathfrak{C}_Q(F)^{\Omega_L}.$$

LEMMA 3. *$\mathfrak{C}_Q$ is a locally free, rank one $\mathfrak{A}$-module.*

Proof. We recall that L_Q is an $\mathscr{A}$-module (see §1); so, by (3.2), we see that $\mathfrak{C}_Q$ is $\mathfrak{A}$-stable. Moreover $\mathfrak{C}_{Q,\mathfrak{q}}$ must be $\mathfrak{A}_\mathfrak{q}$-projective since $\mathfrak{B}_\mathfrak{q}$ is $\mathfrak{A}_\mathfrak{q}$-free, while $\mathfrak{O}_{N,\mathfrak{q}}$ is $\mathfrak{O}_{L,\mathfrak{q}}$ free. Thus $\mathfrak{C}_Q$ is in fact $\mathfrak{A}$ locally free since $\mathscr{A}$ is commutative and since $\mathfrak{C}_Q \otimes L$ is $\mathscr{A}$ free. □

In order to prove Theorem 5 it now suffices to show:

PROPOSITION 5. $\tilde{\mathfrak{D}}_Q = \mathfrak{C}_Q$.

Proof. By definition, since $\mathfrak{C}_Q$ is an $\mathfrak{A}$-submodule of $\mathfrak{D}_Q$, we have

$$\mathfrak{C}_Q \subseteq \tilde{\mathfrak{D}}_Q. \tag{3.5}$$

We shall prove Proposition 5 by proving the reverse inclusion at each prime $\mathfrak{q}$ of $\mathfrak{D}_L$. Since in fact it suffices to show $\mathfrak{C}_Q \otimes_{\mathfrak{D}_L} \mathfrak{D}_E = \tilde{\mathfrak{D}}_Q \otimes_{\mathfrak{D}_L} \mathfrak{D}_E$, for any finite extension E of L, we may, without loss of generality, now suppose that L contains the r-th roots of unity, together with the co-ordinates of G and G_Q. Thus if we write $\hat{G} = \mathrm{Hom}_Z(G, L^*)$, then the Hopf algebra LG now identifies with Map $(\hat{G}, L)$. As previously, splitting $\mathfrak{A}_\mathfrak{q}$ into its connected and étale part $\mathfrak{A}_\mathfrak{q} = \mathfrak{A}_1 \otimes_{\mathfrak{D}_{L,\mathfrak{q}}} \mathfrak{A}'$, we have a decomposition of groups $\hat{G}_\mathfrak{q} = \hat{G}_1 \times \hat{G}'$; here explicitly

$$\mathfrak{A}' = \prod_{\chi \in \hat{G}'} \mathfrak{D}_L e_\chi \tag{3.6}$$

where e_χ is the idempotent associated to χ. We therefore have corresponding decompositions:

$$\mathfrak{C}_{Q,\mathfrak{q}} = \prod_{\chi \in \hat{G}'} \mathfrak{C}_\chi, \quad \tilde{\mathfrak{D}}_{Q,\mathfrak{q}} = \prod_{\chi \in \hat{G}'} \mathfrak{D}_\chi \tag{3.7}$$

where for brevity we put $\mathfrak{C}_\chi = \mathfrak{C}_{Q,\mathfrak{q}} e_\chi$, $\mathfrak{D}_\chi = \tilde{\mathfrak{D}}_{Q,\mathfrak{q}} e_\chi$. By Nakayama's lemma and by (3.5) it therefore suffices to show that for each such χ,

$$\mathfrak{C}_\chi + \mathfrak{D}_{\chi'} J_\chi = \mathfrak{D}_\chi$$

where J_χ denotes the Jacobson radical of $\mathfrak{A}_1 e_\chi$. Since $\mathfrak{A}_1$ is connected, it suffices to show

$$\mathfrak{C}_\chi + \mathfrak{D}_\chi I' e_\chi = \mathfrak{D}_\chi$$

where I' is the augmentation ideal of $\mathfrak{A}_1$. We are therefore reduced to showing that, for each χ, $\mathfrak{D}_\chi$ is $\mathfrak{A}_1 e_\chi$ free and that

$$\mathfrak{C}_\chi \Sigma_H = \mathfrak{D}_\chi \Sigma_H \tag{3.8}$$

where Σ_H denotes the sum over all elements of $H = \bigcap_\chi \mathrm{Ker}\, \chi$.

For some $t \in \mathfrak{D}_L$ we know that

$$\mathfrak{A}_1 \cap L_\mathfrak{q} \Sigma_H = t^{-1} \mathfrak{D}_{L,\mathfrak{q}} \Sigma_H. \tag{3.9}$$

Consequently, if M is any free $\mathfrak{A}_1$ module, then

$$M\Sigma_H = tM^H. \tag{3.10}$$

In order to prove (3.8) we begin by considering the special case when χ is the identity character ε in $\hat{G}'$. Then we note that

$$\mathfrak{O}_\varepsilon^H = \mathfrak{O}_{L,\mathfrak{q}} = \mathfrak{C}_\varepsilon^H. \tag{3.11}$$

Thus by (3.10),

$$\frac{\mathfrak{O}_{L,\mathfrak{q}}}{\mathfrak{C}_\varepsilon \Sigma_H} = \frac{\mathfrak{C}_\varepsilon^H}{\mathfrak{C}_\varepsilon \Sigma_H} \cong \frac{\mathfrak{O}_{L,\mathfrak{q}} t^{-1}\Sigma_H}{\mathfrak{O}_{L,\mathfrak{q}}\Sigma_H}. \tag{3.12}$$

We conclude that $\mathfrak{C}_\varepsilon$ contains an element of trace t; hence, by (3.5), $\mathfrak{O}_\varepsilon$ contains such an element; however, since $\tilde{\mathfrak{O}}_Q$ is an order, $\mathfrak{O}_\varepsilon \mathfrak{O}_\chi \subseteq \mathfrak{O}_\chi$ for all $\chi \in \hat{G}'$; therefore by Proposition 4 (using $\mathfrak{A}_1 e_\chi$ in place of $\mathfrak{E}$) we see that $\mathfrak{O}_\chi$ is $\mathfrak{A}_1 e_\chi$ free. From (3.10) we deduce that

$$\mathfrak{O}_\chi \Sigma_H = t\mathfrak{O}_\chi^H, \quad \mathfrak{C}_\chi \Sigma_H = t\mathfrak{C}_\chi^H. \tag{3.13}$$

It therefore suffices to show

$$\mathfrak{C}_\chi^H = \mathfrak{O}_\chi^H. \tag{3.14}$$

To this end we choose $\mathfrak{O}_{L,\mathfrak{q}}$ bases

$$\mathfrak{C}_\chi^H = c_\chi \mathfrak{O}_{L,\mathfrak{q}}, \quad \mathfrak{O}_\chi^H = d_\chi \mathfrak{O}_{L,\mathfrak{q}}.$$

By (3.5) $c_\chi = d_\chi \lambda_\chi$ with $\lambda_\chi \in \mathfrak{O}_{L,\mathfrak{q}}$. We wish to show $\lambda_\chi \in \mathfrak{O}_{L,\mathfrak{q}}^*$; it will therefore suffice to show

$$c_\chi^r \in \mathfrak{O}_{L,\mathfrak{q}}^*. \tag{3.15}$$

With the identifications given at the start of the proof, $\mathfrak{B}^H = \mathfrak{O}_{L,\mathfrak{q}}\hat{G}'$, and so $\mathfrak{B}_\chi^H = \mathfrak{O}_{L,\mathfrak{q}}\chi$. However, we have an isomorphism of $(G, \mathfrak{O}_N)$ algebras ξ: $\mathfrak{B} \otimes \mathfrak{O}_N \cong \mathfrak{C}_Q \otimes \mathfrak{O}_N$; thus $\xi^{-1}(c_\chi) = u\chi$ for $u \in \mathfrak{O}_{N,\mathfrak{q}}^*$, and (3.15) now follows. □

We conclude this section by proving Theorem 3. With the notation of the statement of this result, we choose a prime $\mathfrak{q}$ of $\mathfrak{O}_L$ and we fix $m \in \mathfrak{C}_Q$ such that $\mathfrak{C}_{Q,\mathfrak{q}} = m\mathfrak{A}_\mathfrak{q}$. For a field N as in (3.2), we have an isomorphism of

$(G, \mathfrak{O}_N)$ algebras:

$$\xi_q;\ \mathfrak{B}(N)_q = \mathfrak{B}(L)_q \otimes_{\mathfrak{O}_L} \mathfrak{O}_N \cong \mathfrak{C}_{Q,q} \otimes_{\mathfrak{O}_L} \mathfrak{O}_N$$

and

$$\mathfrak{C}_{Q,q} \otimes_{\mathfrak{O}_L} \mathfrak{O}_N = m.\mathfrak{A}(N)_q.$$

By Proposition 2, $\mathfrak{B}(N)$ is $\mathfrak{A}(N)$ free on πl; thus for some $a \in \mathfrak{A}(N)^*$, $\xi_q^{-1}(m) = \pi l a$; applying the isomorphism κ (prior to Proposition 2), we conclude that

$$\pi^{-1}\left(\sum_g m_Q^g,\ g^{-1}\right) = \bar{a} \in \mathfrak{A}(N)^*.$$

Finally we note that the values of m_Q^g, all lie in $L(Q)$, so that in fact $\bar{a} \in \mathfrak{A}(L(Q))^*$.

4. The *K*-theory of $\mathfrak{A}$

We let $\mathrm{Cl}(\mathfrak{A})$ denote the locally free class group of $\mathfrak{A}$-modules: that is to say $\mathrm{Cl}(\mathfrak{A})$ is the subgroup of elements of zero rank in the Grothendieck group of finitely generated, locally free $\mathfrak{A}$-modules. Given such an $\mathfrak{A}$-module M, the class of M, $(M) \in \mathrm{Cl}(\mathfrak{A})$, denotes the isomorphism class of M minus the isomorphism class of the free $\mathfrak{A}$-module whose rank is the $\mathfrak{A}$-rank of M.

We now briefly recall *A.* Fröhlich's description of $\mathrm{Cl}(\mathfrak{A})$ in terms of character maps (see [4], [16]).

Let Y denote the set of isomorphism classes of simple $\mathscr{A} \otimes_L \mathbf{Q}^c$ representations: we view Y as an Ω_L set in the natural way. We let M denote a finite Galois extension of L which is 'sufficiently large': that is to say M contains the coordinates of G and of all points Q' for Q in $A(L)$, together with the roots of unity of order the exponent of G. We write $J(M)$ for the group of idèles of M, and we let $U(\mathfrak{A})$ denote the group of unit idèles of $\mathfrak{A}$:

$$U(\mathfrak{A}) = \prod_{q<\infty} \mathfrak{A}_q^* \times \prod_{q|\infty} \mathscr{A}_q^*.$$

Given $u \in U(\mathfrak{A})$, we define $\mathrm{Det}(u) \in \mathrm{Map}_{\Omega_L}(Y, J(M))$ where for $\chi \in Y$,

$$(\mathrm{Det}(u)(\chi))_q = \chi(u_q) \in M \otimes_L L_q$$

where we view χ as a homomorphism from $\mathscr{A}$ to M and extend by L_q linearity.

As per Chapter 2 in [4], we have an isomorphism

$$\mathrm{Cl}(\mathfrak{A}) \cong \frac{\mathrm{Map}_{\Omega_L}(Y, J(M))}{\mathrm{Det}(U(\mathfrak{A}))\mathrm{Map}_{\Omega_L}(Y, M^*)}. \tag{4.1}$$

We next describe the construction of a representing map for the class of a given locally free rank one $\mathfrak{A}$-module X under (4.1). We choose bases

$$X_\mathfrak{q} = m_\mathfrak{q}\mathfrak{A}_\mathfrak{q}, \quad X.L = v.\mathscr{A}$$

and we let $\alpha_\mathfrak{q} \in \mathscr{A}_\mathfrak{q}^*$ have the property that $m_\mathfrak{q} = v.\alpha_\mathfrak{q}$; then (X), the class of X in $\mathrm{Cl}(\mathfrak{A})$, is represented by

$$\prod \mathrm{Det}(\alpha_\mathfrak{q}) \in \mathrm{Map}_{\Omega_L}(Y, J(M)). \tag{4.2}$$

We now use a technique, due to Fröhlich, to explicitly construct such a representing map for $(\tilde{\mathfrak{D}}_Q)$. For $\chi \in Y$, $n \in L_Q$, we define the χ resolvent of n, $(n|\chi) \in \mathrm{Map}(G_Q, \mathbf{Q}^c)$, via

$$(n|\chi) = \mathrm{Det}\left(\sum_g n^g g^{-1}\right)(\chi).$$

Note that if $a \in \mathscr{A}$, then

$$(na|\chi) = (n|\chi)\mathrm{Det}(a)(\chi).$$

In conclusion if $\tilde{\mathfrak{D}}_{Q,\mathfrak{q}} = m_{Q,\mathfrak{q}}\mathfrak{A}_\mathfrak{q}$ for each $\mathfrak{q}$, and if $L_Q = d_Q\mathscr{A}$, then we have shown:

PROPOSITION 6. *$(\tilde{\mathfrak{D}}_Q) \in \mathrm{Cl}(\mathfrak{A})$ is represented by the map*

$$h_Q \in \mathrm{Map}_{\Omega_L}(Y, J(M))$$

defined by

$$h_Q(\chi)_\mathfrak{q} = (m_{Q,\mathfrak{q}}|\chi)(d_Q|\chi)^{-1}.$$

Remark. We extend L if necessary to ensure that L contains the coordinates of G. By standard theory we know that L_Q is unramified outside S, since A has everywhere good reduction. Thus, if $\mathfrak{q} \notin S$, then

$$\mathfrak{D}_{Q,\mathfrak{q}} = m_{Q,\mathfrak{q}}\mathfrak{A}_\mathfrak{q} = m_{Q,\mathfrak{q}}\mathfrak{D}_{L,\mathfrak{q}}G \tag{4.3}$$

and by the Frobenius determinant formula, the $(m_{Q,q}|\chi)$ are all units.

Actions on $\mathrm{Cl}(\mathfrak{A})$. Since A admits complex multiplication by $\mathfrak{O}_K$, G is an $\mathfrak{O}_K$-module, and so V acts as L-algebra automorphisms on $\mathscr{A}$ (by L-linearity). Since V acts on $\mathfrak{B}$, it acts by transposition on $\mathfrak{A}$; hence, by functoriality, V acts on $\mathrm{Cl}(\mathfrak{A})$.

The action of V on G induces an action on Y via the rule ${}^v\chi(a) = \chi(a^{(v)})$, for $a \in \mathfrak{A}$. Given a locally free $\mathfrak{A}$-module M, we define the v-twist of M, $M^{(v)}$, via

$$m^{(v)}a^{(v)} = (ma)^{(v)} \quad \text{for } m \in M,\ a \in \mathfrak{A}.$$

The map $M \to M^{(v)}$ then induces the above V-action on $\mathrm{Cl}(\mathfrak{A})$. From the construction (4.2), we see that if M is represented by the map h, then $M^{(v)}$ is represented by the map $h^{(v)}$ where $h^{(v)}(\chi) = h({}^v\chi)$. The V-actions on G and $\mathfrak{A}$ extend, by $\mathbf{Z}$-linearity, to $\mathbf{Z}V$-module structures: we shall write these actions exponentially.

Self-duality. We have already seen in Proposition 2 that $\mathfrak{B}$ is an $\mathfrak{A}$-free module on πl, that is to say we have an isomorphism of $\mathfrak{A}$-modules:

$$\mathfrak{A} \otimes \pi\mathfrak{O}_L l \cong \mathfrak{B}.$$

More generally, if M is a locally free $\mathfrak{A}$-module, then, by the above,

$$M^D = \mathrm{Hom}_{\mathfrak{O}_L}(M, \mathfrak{O}_L)$$

is also a locally free $\mathfrak{A}$-module; thus $M \to M^D$ induces an involution on $\mathrm{Cl}(\mathfrak{A})$. Exactly as in I, §5 of [16], we see that if M is represented by

$$h \in \mathrm{Map}_{\Omega_L}(Y, J(M)),$$

then (M^D) is represented by the map $h(\chi^{-1})^{-1}$. Since $\mathfrak{A}$ is commutative, $\mathfrak{A}$ certainly satisfies the Eichler condition, and so $M \cong M^D$ if, and only if, the map $\chi \to h(\chi + \chi^{-1})$ lies in the denominator of the quotient group in (4.1).

Restriction. Let F denote a finite extension of L, and let $\{\omega_1, \ldots \omega_n\}$ denote a transversal of $\Omega_F \backslash \Omega_L$. We then have the co-restriction map

$$\mathscr{N}\colon \mathrm{Map}_{\Omega_F}(Y, J(M)) \to \mathrm{Map}_{\Omega_L}(Y, J(M)) \tag{4.4}$$

given by

$$\mathcal{N}f(\chi) = \prod_i f\left(\chi^{\omega_i^{-1}}\right)^{\omega_i}.$$

As per the corresponding result for group rings in Theorem 13 of [4], we see that $\mathcal{N}$, on (4.1), corresponds to the restriction map

$$\mathrm{Cl}(\mathfrak{A}(F)) \to \mathrm{Cl}(\mathfrak{A}(L)).$$

5. The homomorphism ψ

The main aim of this section is to prove Theorem 1. We begin by showing that ψ is indeed a group homomorphism; we conclude by showing that ψ commutes with V-action.

Let P, Q denote points of $A(L)$. Addition $G_P \times G_Q \to G_{P+Q}$, given by $(P', Q') \to (P' + Q')$, induces an injection of L-algebras

$$\Delta\colon L_{P+Q} \to L_P \otimes_L L_Q;$$

we have the trace map $T\colon L_P \otimes_L L_Q \to L_{P+Q}$.

(5.1) If L contains the co-ordinates of G, then we note that

$$\Delta\left(L_{P+Q}\right) = \left(L_P \otimes_L L_Q\right)^{\delta(G)},$$

where $\delta\colon G \to G \times G$ is given by $\delta(g) = (g, g^{-1})$; correspondingly

$$T(f \otimes h) = \sum_g f^g \otimes h^{g^{-1}} \quad \text{for } f \in L_P,\ h \in L_Q.$$

We now pass to integral level, and show:

PROPOSITION 7. (a) $\Delta(\mathfrak{C}_{P+Q}) \subseteq \mathfrak{C}_P \otimes \mathfrak{C}_Q$.
(b) $T(\mathfrak{C}_P \otimes \mathfrak{C}_Q) = \pi\mathfrak{C}_{P+Q}$.

Proof. Let N denote a finite extension of L which contains the co-ordinates of G_P and G_Q. Applying $\otimes_{\mathfrak{O}_L} \mathfrak{O}_N$, by (3.3) we are reduced to the case $\mathfrak{C}_P = \mathfrak{C}_Q = \mathfrak{B}$; then (a) follows from the fact that $\mathfrak{B}$ is co-closed; while (b) follows from the formula for the different of $\mathfrak{B}$ given in Lemma 1, together with the tower formula for differents. □

We note the following trivial fact:

LEMMA 4. *For $x \in L_P \otimes L_Q$, and $a, b \in \mathscr{A}$, $T(x(a \otimes b)) = T(x)a.b$.*

We now show that $\psi(P+Q) = \psi(P).\psi(Q)$. With the notation of the previous section we choose $m_{P,\mathfrak{q}}$, d_P etc. such that $\mathfrak{C}_{P,\mathfrak{q}} = m_{P,\mathfrak{q}}\mathfrak{A}_{\mathfrak{q}}$, $L_P = d_P\mathscr{A}$. Identifying $\mathfrak{C}_{P+Q}$ with its image under Δ, by the above proposition we have

$$\mathfrak{C}_{P+Q} = \pi^{-1}T\big(\mathfrak{C}_P \otimes \mathfrak{C}_Q\big);$$

thus

$$\begin{aligned}\mathfrak{C}_{P+Q,\mathfrak{q}} &= \pi^{-1}T\big(\big(m_{P,\mathfrak{q}} \otimes m_{Q,\mathfrak{q}}\big)(\mathfrak{A} \otimes \mathfrak{A})\big)\\ &= \pi^{-1}T\big(m_{P,\mathfrak{q}} \otimes m_{Q,\mathfrak{q}}\big)\mathfrak{A};\end{aligned}$$

and

$$L_{P+Q} = T\big(\big(d_P \otimes d_Q\big)(\mathscr{A} \otimes \mathscr{A})\big) = T\big(d_P \otimes d_Q\big)\mathscr{A}.$$

Since $m_P \otimes m_Q = (d_P \otimes d_Q)(\alpha_P \otimes \alpha_Q)$, by Lemma 4 we conclude that

$$\pi^{-1}T\big(m_P \otimes m_Q\big) = T\big(d_P \otimes d_Q\big) \cdot \big(\alpha_P\alpha_Q\pi^{-1}\big).$$

Therefore, in summary, $\psi(P+Q)$ is represented by $\mathrm{Det}(\alpha_P\alpha_Q\pi^{-1})$, which has the same class under (4.1) as $\mathrm{Det}(\alpha_P) \cdot \mathrm{Det}(\alpha_Q)$, which represents the class $\psi(P) \cdot \psi(Q)$.

We conclude this section by showing that for $v \in V$, we have an isomorphism of $\mathfrak{A}$-modules:

$$\mathfrak{C}_Q^{(v)} \cong \mathfrak{C}_{[v]Q}. \tag{5.2}$$

The map $v\colon G_Q \to G_{[v]Q}$, given by $v(Q') = [v]Q'$, is not a map of G-spaces. It does, however induce an isomorphism of L-algebras (and $\mathscr{A}$-modules):

$$v^*\colon L_{[v]Q} \tilde{\to} \big(L_Q\big)^{(v)}.$$

To see this we are required to show that for $f \in L_{[v]Q}$ and $a \in \mathscr{A}$,

$$v^*(f \cdot a) = \big(v^*(f)^{(v)}\big)a. \tag{5.3}$$

To show this we evaluate on $Q' \in G_Q$:

$$(5.4) \qquad (v^*(f \cdot a))(Q') = (f \cdot a)([v]Q') = \sum f([v]Q' + g)a_g$$

where $a = \sum a_g g$. We choose $u \in V$ such that $uv \equiv 1 \bmod \mathfrak{a}$; then

$$(5.5) \qquad \begin{aligned} \left(\left(v^*(f)^{(v)}\right) \cdot a\right)(Q') &= \left(\left(v^*(f)a^{(u)}\right)^{(v)}\right)(Q') \\ &= \sum v^*(f)(Q' + [u]g)a_g \\ &= \sum f([v]Q' + g)a_g. \end{aligned}$$

Now (5.3) follows from (5.4) and (5.5).

Lastly we note that since $\mathfrak{C}_Q$ (resp. $\mathfrak{C}_{[v]Q}$) is the largest $\mathfrak{A}$-module in $\mathfrak{O}_Q$ (resp. $\mathfrak{O}_{[v]Q}$), we may conclude that v^* induces the required isomorphism (5.2).

6. The Weil pairing

The purpose of this section is to show how the Weil pairing provides a natural tool for calculations with Fröhlich's character-map description of classgroups; in particular we shall thereby obtain a quick proof of (1.3).

We let B denote the isogenous Abelian variety A/G; we let $\hat{B}$ denote the dual Abelian variety of B; then $\mathfrak{O}_K$ acts on $\hat{B}$ by pull-back of divisors; we write this action as $[\hat{\alpha}]$, for $\alpha \in \mathfrak{O}_K$; we let $\hat{G}$ denote the points on $\hat{B}(\mathbf{Q}^c)$ which are killed by $[\hat{a}]$. We then have the Weil pairing

$$(6.1) \qquad w\colon G \times \hat{G} \to \mu$$

where μ denotes the group of roots of unity in $\mathbf{Q}^c$ killed by the exponent of G. (See page 184 of [9].) Thus, by definition, for $\alpha \in \mathfrak{O}_K$ we have the adjoint relation

$$(6.2) \qquad w([\alpha]g, R) = w(g, [\hat{\alpha}]R) \quad \text{for } g \in G,\ R \in \hat{G}.$$

Henceforth we identify Y and $\hat{G}$, by viewing Y as the distinct $\mathbf{Q}^c$ algebra homomorphisms $\mathscr{A} \otimes \mathbf{Q}^c = \mathbf{Q}^c G \to \mathbf{Q}^c$, and where for $R \in \hat{G}$ we define

$$\chi_R\left(\sum a_g g\right) = \sum a_g w(g, R).$$

This identification respects both the V-action and the Ω_L-action.

Let N denote a finite extension of L which contains μ together with the co-ordinates of G. We let f denote a radical element for the Kummer extension $N(A)/N(B)$ - so that $f^e \in N(B)$; then f has class $R \in \hat{G}$, for

some R, and

$$f(z +_A g) = w(g, R) \cdot f(z). \tag{6.3}$$

(6.4) We remark that for any $h \in L(A)$, of course, $(h|R) = \Sigma_g h(z + g)w(-g, R)$ satisfies (6.3).

LEMMA 5. *For any number field N, we write $N(A)_{\text{fin}}$ for the N sub-algebra of $N(A)$ consisting of those functions which are finite at all points of G_Q; then evaluation on G_Q induces a surjection*

$$N(A)_{\text{fin}} \to \text{Map}_{\Omega_N}(G_Q, \mathbf{Q}^c).$$

Proof. It is clear that for some 'sufficiently large' extension M/N,

$$M(A)_{\text{fin}} \twoheadrightarrow \text{Map}(G_Q, M),$$

by use of co-ordinate functions. The result then follows on applying the M/N trace. □

We now show (1.2). We let $\{\omega_1, \ldots \omega_n\}$ denote a transversal of $\Omega_F \setminus \Omega_L$; for $\sigma \in \Omega_L$ we write

$$\omega_i \sigma = \delta_i(\sigma)\omega_{j(i,\sigma)} \quad \text{with } \delta_i \in \Omega_F.$$

We choose $Q \in A(F)$; for $\delta \in \Omega_L$ we shall write $\theta(\delta) = Q'^{\delta} -_A Q' \in G$; for brevity we set $P' = \Sigma_i Q'^{\omega_i} \in A(L)$.

Next, by the above lemma, we choose $f \in F(A)_{\text{fin}}$, $f' \in L(A)_{\text{fin}}$ such that

$$F_Q = f(Q') \cdot \mathscr{A}(F) \quad \text{and} \quad L_P = f'(P')\mathscr{A}(L).$$

By (4.4), Proposition 6 and (4.1), in order to prove (1.2) it suffices to show

$$\left(R \to \mathscr{N}(f(Q')|R)(f'(P')|R)^{-1}\right) \in \text{Map}_{\Omega_L}(\hat{G}, \mathbf{Q}^{c*}). \tag{6.5}$$

$$\left(R \to \pi^{1-[F:L]}\mathscr{N}(m_Q|R)(m_P|R)^{-1}\right) \in \text{Det}(U(\mathfrak{A}(L)). \tag{6.6}$$

Here, as usual, m_Q (resp. m_P) denotes an adèlic basis for $\mathfrak{C}_Q$ (resp. $\mathfrak{C}_P$) over $\mathfrak{A}(F)$ (resp. $\mathfrak{A}(L)$).

Proof of (6.5). The result follows on comparing Galois action formulae:

$$\begin{aligned}\prod_i \left(f^{\omega_i}(Q'^{\omega_i})|R\right)^\sigma &= \prod \left(f^{\delta\omega_j}(Q'^{\delta\omega_j})|R^\sigma\right)\\ &= \prod_j \left(f^{\omega_j}\left(Q'^{\omega_j} + \theta(\delta)^{\omega_j}\right)|R^\sigma\right)\\ &= w\left(\sum \theta(\delta)^{\omega_j}, R^\sigma\right)\prod_i \left(f^{\omega_i}(Q^{\omega_i})|R^\sigma\right) \quad \text{by (6.4).}\end{aligned}$$

Also

$$(6.7)\qquad \left(f'(P')|R\right)^\sigma = \left(f'^\sigma(P'^\sigma)|R^\sigma\right) = \left(f'(P'^\sigma)|R^\sigma\right).$$

However,

$$P'^\sigma = \sum Q'^{\omega_i\sigma} = \sum Q'^{\delta_i\omega_j} = \sum Q'^{\omega_j} + \sum \theta(\delta_i)^{\omega_j} = P' + \sum \theta(\delta_i)^{\omega_j}.$$

Hence by (6.7),

$$\begin{aligned}\left(f'(P')|R\right)^\sigma &= \left(f'\left(P' + \sum \theta(\delta_i)^{\omega_j}\right)|R^\sigma\right)\\ &= w\left(\sum \theta(\delta_i)^{\omega_j}, R^\sigma\right)\left(f'(P)|R^\sigma\right).\end{aligned}$$ □

Proof of (6.6). Since both $\mathcal{N}((f|\ -\ )(m_Q|\ -\ )^{-1})$ and $(f'|\ -\ )(m_P|\ -\ )^{-1}$ are Ω_L maps, by (6.5) we see that the left-hand term in (6.6) is an Ω_L-map. Therefore, by Theorem 3,

$$\pi^{1-[F:L]}\mathcal{N}\left(m_Q|\ -\right)\left(m_P|\ -\right)^{-1} \in \mathrm{Det}\left(\mathfrak{A}(N)\right)^{\Omega_L}$$

where N denotes the normal closure of F/L. However, since LG is commutative and separable, we see that for each prime ideal $\mathfrak{q}$ of $\mathfrak{O}_L$, the homomorphism

$$\mathrm{Det}\colon \mathfrak{A}_{\mathfrak{q}}^* \to \mathrm{Det}\left(\mathfrak{A}_{\mathfrak{q}}^*\right)$$

is injective. Thus $\mathrm{Det}(U(\mathfrak{A}(N))^{\Omega_L} = \mathrm{Det}(U(\mathfrak{A}(N))^{\Omega_L}) = \mathrm{Det}(U(\mathfrak{A}(L))$. □

7. Elliptic results

We now adopt all the notation and hypotheses given prior to the statement of Theorem 4. We note that since $|G| = N_{K/\mathbf{Q}}\pi$ is a prime, p say, $L_Q = L(Q)$ for any non-zero point Q in $\mathscr{E}$; furthermore, $\mathrm{Gal}(L_Q/L)$ identifies with G, since $G \subseteq E(L)$.

We begin this section by observing that $\mathscr{E}^{(\kappa)}$ admits the following interpretation:

LEMMA 7. *For non-zero* $Q \in \mathscr{E}$, L_Q *is abelian over* K *if, and only if,* $Q \in \mathscr{E}^{(\kappa)}$.

Proof. This follows immediately from the Ω_K-equivariance of the Kummer pairing $\mathscr{E} \times \Omega_L^{ab} \otimes \mathbf{F}_p \to G$ of $\mathbf{F}_p$-vector spaces and the fact that $p \nmid [L : K]$. □

From property (b) of L, we deduce that E acquires everywhere good reduction over L, by the standard theory of the Néron minimal model; we may therefore now apply all the preceding results and techniques of this paper to the triple $(E, \mathfrak{p}, L)$.

THEOREM 7. *If* 2 *splits in* K, *then* $G \subseteq \operatorname{Ker} \psi$.

Proof. From (2.10), Chapter XI of [2], we recall that if $N = K(4\mathfrak{p}^2)$, $F = K(4\mathfrak{p})$; then $\mathfrak{O}_N$ is a free $\mathfrak{A}(F)$-module. (N.B. In order to guarantee that $\mathfrak{A}(F)$ agrees with the associated order in [2], we apparently need to assume $\pi \equiv \pm 1 \bmod 8\mathfrak{O}_K$, and not just $\bmod 4\mathfrak{O}_K$—see the remark on page 173 of [2].)

Let P denote a non-zero point of G. Since $G = G_{\mathbf{0}}$, we shall write $K(\mathbf{0})$ for the field generated by K by the co-ordinates of P. Since $\mathfrak{p}$ has ramification index $p - 1$ in both F/K and $K(\mathbf{0})/K$, we deduce that $\mathfrak{p}$ is non-ramified in $J = F(\mathbf{0})/F$; however, N/F is, of course, unramified outside $\mathfrak{p}$; thus $\mathfrak{O}_N \otimes_{\mathfrak{O}_F} \mathfrak{O}_J = \mathfrak{O}_{NJ}$, and moreover this is a free $\mathfrak{A}(J)$ module. By standard complex multiplication theory $N.J = J(P)$; hence, by the above, $\mathfrak{O}_{J(P)}$ admits $\mathfrak{A}(J)$, and so $\tilde{\mathfrak{O}}_P(= \tilde{\mathfrak{O}}_P(J)) = \mathfrak{O}_{J(P)}$. Therefore, on applying $\otimes_{\mathfrak{O}_J} \mathfrak{O}_L$, we conclude that $\psi(P) = 1$. □

Next we rework some of the results of §4 on representative maps for classes in $\mathrm{Cl}(\mathfrak{A})$. We let ζ denote a primitive p-th root of unity in $\mathbf{Q}^c$, and we set $M = L(\zeta)$. We let

$$\varepsilon\colon \mathscr{E} \to \operatorname{Hom}_{\Omega_L}\left(\hat{G}, \frac{M^*}{M^{*p}}\right)$$

denote the injective $\mathbf{F}_p\Omega_K$-homomorphism induced by

$$Q \to \left(R \to \left(d_Q | R\right)(Q')^p\right.$$

where $L_Q = d_Q \cdot \mathscr{A}$ (cf. Theorem 1.1 in Chapter X of [12]).

For the present we fix $R \in \hat{G}$, and let L' denote the field generated over L by the values of R. From Proposition 6 and Theorem 3 we know that

$$c\big(h_Q(R)\big)\cdot \mathfrak{O}_{L'} = \big(d_Q|R\big)(Q')\pi^{-1}\mathfrak{O}_{L'}$$

where c denotes idèle content. Moreover, by choosing d_Q to be an $\mathfrak{A}_{\mathfrak{q}}$ basis of $\tilde{\mathfrak{O}}_{Q,\mathfrak{q}}$ for each $\mathfrak{q}|\pi$, we see that $(d_Q|R)(Q')\pi^{-1}$ is a unit at each such prime (see Theorem 3 again). However, since $\mathfrak{q}$ is non-ramified if $\mathfrak{q} \nmid \pi$, and since $(d_Q|R)(Q')^p \in L_Q$, we have shown that $(d_Q|R)(Q')\mathfrak{O}_{L'(Q)}$ is lifted from an $\mathfrak{O}_{L'}$ ideal,

$$\big(d_Q|R\big)(Q')\mathfrak{O}_{L'(Q)} = \mathfrak{d}_Q(R)\cdot\mathfrak{O}_{L'(Q)} \tag{7.1}$$

with $\mathfrak{d}_Q(R)$ an $\mathfrak{O}_{L'}$-ideal.

Let $\mathfrak{R}$ denote the unique maximal order in LG (note that $\mathscr{A} = LG$, since $E(L) \supseteq G$). Thus we have an isomorphism.

$$\mathrm{Cl}(\mathfrak{R}) = \mathrm{Cl}(\mathfrak{O}_L) \times \prod \mathrm{Cl}(\mathfrak{O}_M) \tag{7.2}$$

where the product extends over the Ω_L-orbits of $\hat{G}\setminus \mathbf{0}$. Of course, $\mathrm{Cl}(\mathfrak{R})$ possesses an idèlic Map-description, as per (4.1); we obtain (7.2) by evaluating on orbit representatives and taking content. Therefore, by naturality together with the above work, we see that the image of $\psi(Q)$ in $\mathrm{Cl}(\mathfrak{R})$, under the extension map e: $\mathrm{Cl}(\mathfrak{A}) \to \mathrm{Cl}(\mathfrak{R})$, is represented by $\prod \mathfrak{d}_Q(R)$. In fact, from the above, we note that $\mathfrak{d}_Q(\mathbf{0})$ is obviously a principal $\mathfrak{O}_L$-ideal.

The proof of the following result, and its subsequent application is similar to part of Leopoldt's Spiegelungsatz:

PROPOSITION 8. *Let U denote the units of $\mathfrak{O}_M$. If $Q \in \mathrm{Ker}(e \circ \psi)$, then*

$$\varepsilon(Q) \in \mathrm{Hom}_{\Omega_L}\left(\hat{G}, \frac{UM^{*p}}{M^{*p}}\right).$$

Proof. We suppose $e \circ \psi(Q) = 1$, and we choose a non-trivial $R \in \hat{G}$. Then, by hypothesis and (7.1),

$$\mathfrak{O}_{L'(Q)}\big(d_Q|R\big)(Q') = X_{R'}\mathfrak{O}_{L'(Q)}$$

for some $X_R \in M^*$. Therefore $\varepsilon(Q)(R)$ is represented by the unit $(d_Q|R)(Q')^p X_R^{-p}$. □

We now conclude by proving Theorem 4. Let θ: $\Delta \to \mathbf{F}_p^*$ denote an abelian character of Δ. We write κ^* (resp. η) for the Ω_K-character given by action on $E(\mathfrak{p}^\rho)$ (resp. the p-th roots of unity); from the Weil pairing we know that

$\kappa \cdot \kappa^* = \eta$. For $\omega \in \Omega_K$, $Q \in \mathscr{E}^{(\theta)}$, $R \in \hat{G}$,

$$(\varepsilon(Q)(R))^{\omega} = \varepsilon(Q^{\omega})(R^{\omega}) = \varepsilon(Q)(R)^{\theta\kappa^*(\omega)}.$$

Writing $\mathscr{E}_0 = \operatorname{Ker} \psi$, we see that

$$\varepsilon\left(\mathscr{E}_0^{(\theta)}\right) \subseteq \operatorname{Hom}_{\Omega_L}\left(\hat{G}, U \otimes \mathbf{F}_p^{(\theta\kappa^*)}\right).$$

However, by Dirichlet's Unit theorem we know that

$$\dim_{\mathbf{F}_p}\left(U \otimes \mathbf{F}_p^{(\eta)}\right) = 2, \dim_{\mathbf{F}_p}\left(U \otimes \mathbf{F}_p^{(\theta\kappa^*)}\right) = 1 \quad \text{if } \theta \neq \kappa.$$

Moreover, if $C \subseteq U \otimes \mathbf{F}_p^{(\eta)}$ denotes the $\mathbf{F}_p$-line represented by ζ, then we note that $\operatorname{Im}(\varepsilon) \cap \operatorname{Hom}_{\Omega_L}(\hat{G}, C) = 1$ since $M(\zeta^{1/p})/M$ is ramified at $\mathfrak{p}^{\rho}$ (by condition (a) for L). Thus we have now shown that for all θ

$$\dim_{\mathbf{F}_p}\left(\varepsilon\left(\mathscr{E}_0^{(\theta)}\right)\right) \leq 1.$$

Part (b) of Theorem 4 now follows from Theorem 7, since ε is injective.

References

1. Ph. Cassou-Noguès and M.J. Taylor, *Rings of integers and elliptic functions*, Progr. Math., vol. 66, Birkhäuser, Boston, 1987.
2. L. Childs, *The group of unramified Kummer extensions of prime degree*, Proc. London Math. Soc. (3), vol. 35 (1977), pp. 407–422.
3. L. Childs and S. Hurley, *Local normal bases for objects of finite commutative, co-commutative Hopf algebras*, pre-print.
4. A. Fröhlich, *Galois module structure of algebraic integers*, Ergeb. Math. Grenzgeb., 3 Folge, Band 1, 1983.
5. _____, *The module structure of Kummer extensions over Dedekind domains*, J. Reine Angew Math., vol. 209 (1962), pp. 39–53.
6. _____, *Invariants for modules over commutative separable orders*, Quart J. Math. Oxford (2), vol. 16 (1965), pp. 193–232.
7. L. McCulloh, *Galois module structure of elementary abelian extensions*, J. Algebra, vol. 82 (1), 1983, pp. 102–134.
8. _____, *Galois module structure of abelian extensions*, to appear.
9. D. Mumford, *Abelian varieties*, Oxford Univ. Press, Oxford, 1974.
10. M. Raynaud, *Schémas en groupes de type* $(p, \ldots, p)$, Bull. Soc. Math. France, vol. 102 (1974), pp. 241–280.
11. J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math., vol. 68 (1968), pp. 492–517.
12. J.H. Silverman, *The arithmetic of elliptic curves*, Springer Text, vol. 106, Springer-Verlag New York, 1985.
13. M.E. Sweedler, *Hopf algebras*, W.A. Benjamin, New York, 1969.
14. J. Tate, *p-divisible groups*, Proc. Conf. Local Fields, Driebergen, ed. T. Springer, New York/Berlin, 1967, pp. 158–183.

15. M.J. TAYLOR, *Hopf structure and the Kummer theory of formal groups*, J. Reine Angew. Math., vol. 375/6 (1987), pp. 1–11.
16. _____, *Classgroups of group rings*, London Math. Soc. Lecture Notes Ser., vol. 91, Camb. Univ. Press, Cambridge, 1984.
17. _____, *Relative Galois module structure of rings of integers and elliptic functions II*, Ann. of Math., vol. 121 (1985), pp. 519–535.
18. _____, *Formal groups and the Galois module structure of local rings of integers*, J. Reine Angew Math., vol. 358 (1985), pp. 97–103.
19. _____, *On the self-duality of a ring of integers as a Galois module*, Invent. Math., vol. 46 (1978), pp. 173–177.
20. _____, *Galois module structure of rings of integers in Kummer extensions*, Bull. London Math. Soc. (12), 1980, pp. 96–98.
21. W.C. WATERHOUSE, *Tame objects for finite commutative Hopf algebras*, preprint.

THE UNIVERSITY OF MANCHESTER INSTITUTE OF SCIENCE AND TECHNOLOGY
MANCHESTER, ENGLAND