ON PRIMITIVE AND REALISABLE CLASSES

A. Agboola

Version of January 11, 2000

Abstract. Let S be a scheme, and let G be a finite, flat, commutative group scheme over S. In this paper we show that (subject to a mild technical assumption) every primitive class in $\mathrm{Pic}(G)$ is realisable. This gives an affirmative answer to a question of Waterhouse. We also discuss applications to locally free classgroups and to Selmer groups of abelian varieties.

Introduction

Let F be a number field with ring of integers O_F, and suppose that G/O_F is a finite, flat, commutative group scheme of exponent N. Then $G = \mathrm{Spec}(\mathfrak{B})$, where $\mathfrak{B}$ is an O_F-Hopf algebra. Let $H^1(O_F, G)$ denote flat cohomology of $\mathrm{Spec}(O_F)$ with coefficients in G, and write $G^D = \mathrm{Spec}(\mathfrak{A})$ for the Cartier dual of G. The group $H^1(O_F, G)$ parametrises isomorphism classes of twisted forms of $\mathfrak{B}$. It may be shown that each twisted form $\mathfrak{C}$ of $\mathfrak{B}$ is a locally free $\mathfrak{A}$-module, and so determines a class $(\mathfrak{C})$ in the Picard group $\mathrm{Pic}(G^D)$ of G^D.

In recent years, a large amount of work has been done concerning the $\mathfrak{A}$-module structure of twisted forms of $\mathfrak{B}$. The initial motivation for this work was the study of the Galois module structure of rings of integers : in many cases, the twisted form $\mathfrak{C}$ may be viewed as an order in the ring of integers of some (in general wildly ramified) extension of F. An important aspect of this theory is the class invariant homomorphism ψ which is defined by

$$\begin{aligned} \psi : H^1(O_F, G) &\longrightarrow \mathrm{Pic}(G^D) \\ \mathfrak{C} &\longmapsto (\mathfrak{C})(\mathfrak{B})^{-1}. \end{aligned} \tag{1}$$

1991 *Mathematics Subject Classification.* 11G, 11R, 14K.

Key words and phrases. Class invariants, classgroups, realisable classes, primitive classes, group schemes, twisted forms.

Partially supported by NSF grant no. DMS 9700937.

This homomorphism was first introduced by W. Waterhouse (see [Wa]), and it provides a measure of the $\mathfrak{A}$-module structure of twisted forms of $\mathfrak{B}$. For example, in many cases of arithmetic interest, one can show that $\mathfrak{B}$ is $\mathfrak{A}$-globally free. If this holds, then it follows that $\mathfrak{C}$ is a globally free $\mathfrak{A}$-module if and only if it lies in the kernel of ψ.

In this note, we shall be concerned with describing the image of ψ. In order to explain our result, we first give two definitions. Let $p_i : G^D \times G^D \to G^D$ $(i = 1, 2)$ denote projection onto the ith factor, and write $m : G^D \times G^D \to G^D$ for the multiplication map on G^D. Each of these maps induce corresponding pullback homomorphisms $p_i^* : \mathrm{Pic}(G^D) \to \mathrm{Pic}(G^D \times G^D)$ and $m^* : \mathrm{Pic}(G^D) \to \mathrm{Pic}(G^D \times G^D)$ on Picard groups. We shall say that an element in $\mathrm{Pic}(G^D)$ is *primitive* if it lies in the kernel of the homomorphism $m^* - p_1^* - p_2^*$. We shall say that an element in $\mathrm{Pic}(G^D)$ is *realisable* if it lies in the image of the homomorphism ψ.

It was shown by Childs and Magid (see [CM]) that every realisable class is primitive, and Waterhouse has raised the question as to whether the converse is true. If the converse does hold, then this gives an analogue for finite group schemes of a standard result concerning extensions of abelian varieties by commutative, connected linear groups (see [S], Chapter VII, no. 15, Theorem 5). The purpose of this note is to point out that Waterhouse's question does indeed have an affirmative answer in almost all cases of arithmetic interest: it follows by combining the work of Childs and Magid with a vanishing theorem of Breen.

We remark that Waterhouse's question has been considered by a number of other authors (see e.g. [By1], [C], [C1], [C2], [CP]). Also, by extending earlier work of L. McCulloh on relative abelian Galois module structure (see [M]), N. Byott has given a precise description of the realisable classes of $\mathrm{Pic}(G^D)$ in terms of certain resolvend maps (see [By2]). However, it does not seem to be easy to use this description to determine whether or not every primitive class is realisable. It would be interesting to obtain an answer to Waterhouse's question in terms of Byott's description.

In Section 1 of this note, we recall work of Childs and Magid, and of Breen, and we state our main result. In Section 2, we explain how this result may be used to study the Galois structure of rings of integers of unramified extensions of F and to analyse the structure of certain locally free classgroups. Finally, in Section 3, we apply our earlier results to the case of class invariants arising via abelian varieties, and we explain how to obtain a new description of a certain flat

Selmer group in some cases. (In fact, it was this last application that originally aroused our interest in Waterhouse's question.)

Part of the work described in this paper was carried out while I was visiting the Université de Bordeaux I. I am extremely grateful to the members of the Mathematics Department there for their generous hospitality. I am also very grateful to G. Pappas and R. Schoof for useful conversations, and to L. Breen and L. Childs for helpful remarks via email. I would like to thank the referee for a number of very useful comments.

1. We begin by briefly reviewing certain aspects of the work of Childs and Magid. The reader may find further details in [CM].

Let S be any scheme, and let G be any finite, flat, commutative group scheme over S of exponent N. It is not hard to show, using Yoneda's lemma, that the primitive elements of $\mathrm{Pic}(G^D)$ correspond to the natural homomorphisms between the group-valued functors G^D and $H^1(-, \mathbb{G}_m)$. In particular, this implies that the group of primitive classes in $\mathrm{Pic}(G^D)$ is annihilated by N.

Let $\mathcal{P}$ and $\mathcal{S}$ denote the categories of abelian presheaves and sheaves respectively for the fpqc topology on S. Childs and Magid show that there is a spectral sequence

$$\mathrm{Ext}^p_{\mathcal{P}}(G^D, H^q(-, \mathbb{G}_m)) \Rightarrow \mathrm{Ext}^{p+q}_{\mathcal{S}}(G^D, \mathbb{G}_m). \tag{2}$$

The exact sequence of terms of low degree of (2) yields

$$0 \to \mathrm{Ext}^1_{\mathcal{P}}(G^D, \mathbb{G}_m) \to \mathrm{Ext}^1_{\mathcal{S}}(G^D, \mathbb{G}_m) \to \mathrm{Hom}_{\mathcal{P}}(G^D, H^1(-, \mathbb{G}_m)) \to \mathrm{Ext}^2_{\mathcal{P}}(G^D, \mathbb{G}_m). \tag{3}$$

Now Waterhouse (see Theorem 2 of [W]) has shown that $\mathrm{Ext}^1_{\mathcal{S}}(G^D, \mathbb{G}_m)$ is isomorphic to $H^1(S, G)$. Hence (3) yields an exact sequence

$$H^1(S, G) \to \mathrm{Prim}(H^1(G^D, \mathbb{G}_m)) \to \mathrm{Ext}^2_{\mathcal{P}}(G, \mathbb{G}_m), \tag{4}$$

where $\mathrm{Prim}(H^1(G^D, \mathbb{G}_m))$ denotes the group of primitive classes of $H^1(G^D, \mathbb{G}_m)$.

The first arrow of (4) is the class invariant homomorphism ψ. Hence, (4) implies that the image of ψ is contained in the group of primitive classes of $H^1(G^D, \mathbb{G}_m)$, i.e. that every realisable class is primitive. Furthermore, if $\mathrm{Ext}^2_{\mathcal{P}}(G^D, \mathbb{G}_m) = 0$, then it follows from (4) that the image of ψ consists precisely of the primitive classes, i.e. that every primitive class is realisable. (See Proposition 1.1 of [CM].)

We now give the statement of Breen's vanishing theorem. Although the following result is not explicitly stated in [Br1] in quite this form, it is a direct consequence of the results described that paper (cf. [Br1], Théorème 3).

Theorem 1.1 (Breen). *Let S be any scheme, and let G be a finite, flat commutative group scheme over S. Suppose that the composition series of every geometric fibre of G of residue characteristic 2 does not contain a factor of local-local type. Then* $\mathrm{Ext}^2_{\mathcal{P}}(G, \mathbb{G}_m) = 0$. $\square$

Proof. We shall briefy explain how the results of [Br1] imply Theorem 1.1, and we refer the reader to [Br1] for full details. We shall follow the notation of [Br1] as closely as possible in our explanation below.

Suppose first that G is just an ordinary abelian group, and consider the following complex $L.(G)$:

$$0 \to \mathbb{Z}[G \times G] \times \mathbb{Z}[G \times G \times G] \xrightarrow{d_1} \mathbb{Z}[G \times G] \xrightarrow{d_0} \mathbb{Z}[G] \xrightarrow{\varepsilon} G \to 0.$$

Here

$$\begin{aligned} \varepsilon[p] &= p \\ d_0[p,q] &= [p+q] - [p] - [q] \\ d_1[p,q] &= [p,q] - [q,p] \\ d_1[p,q,r] &= [p+q,r] - [p,q+r] - [p,q] - [q,r], \end{aligned}$$

and we set $L_0(G) = \mathbb{Z}[G]$, $L_1(G) = \mathbb{Z}[G \times G]$, $L_2(G) = \mathbb{Z}[G \times G] \times \mathbb{Z}[G \times G \times G]$. Then (see [G], Exposé VII, 3.5)

$$\begin{aligned} H_0(L.(G)) &= G, \\ H_1(L.(G)) &= 0. \end{aligned}$$

Now the above construction is functorial in G (*loc. cit.*). Hence given any finite, flat commutative group scheme G over S (viewed as an object of $\mathcal{P}$), we may construct a complex $L.(G)$ of abelian presheaves over S exactly as above. (We remark that Breen uses a different complex, denoted by $A(G)$ in [Br1]. We use the complex $L.(G)$ here in order to be able to treat group schemes G of even order (cf. Remarque 3 of [Br1]).)

Now suppose that $\mathcal{A}$ is any abelian category which has enough injectives. Let X_* be a complex in $\mathcal{A}$, and let H be any object of $\mathcal{A}$. Then there are two spectral sequences whose abutment is the hypercohomology of X_* with values in H (see [Br2], Sections 4 and 5):

$$'E_1^{i,j} = \mathrm{Ext}^j(X_i, H) \implies \mathbf{Ext}^{i+j}(X_*, H),$$
$$''E_2^{i,j} = \mathrm{Ext}^i(H_j(X_*), H) \implies \mathbf{Ext}^{i+j}(X_*, H).$$

We now take $\mathcal{A} = \mathcal{P}$, $X_* = L.(G)$, and $H = \mathbb{G}_m$. Since $L.(G)$ is a partial free resolution of G, we have

$$\mathrm{Ext}^j(G, \mathbb{G}_m) \simeq \mathbf{Ext}(L.(G), \mathbb{G}_m) \qquad 0 \leq j \leq 2.$$

Next, we note that, for any scheme X, we have

$$\mathrm{Ext}^j(\mathbb{Z}[X], \mathbb{G}_m) = H^j(X, \mathbb{G}_m) = 0 \qquad (j > 0)$$

in $\mathcal{P}$, since the global sections functor $H \mapsto H^0(X, H)$ is exact in $\mathcal{P}$. This implies that the spectral sequence $'E_{i,j}$ degenerates. Hence its abutment $\mathrm{Ext}^i(G, \mathbb{G}_m)$ $(0 \leq i \leq 2)$ is the ith cohomology group of the complex

$$'E_1^{*,0} : \mathrm{Hom}(L_0(G), \mathbb{G}_m) \to \mathrm{Hom}(L_1(G), \mathbb{G}_m) \xrightarrow{f} \mathrm{Hom}(L_2(G), \mathbb{G}_m).$$

Thus, to show that $\mathrm{Ext}^2(G, \mathbb{G}_m) = 0$, we have to show that f is surjective.

For each $0 \leq i \leq 2$, the presheaf $\mathrm{Hom}(L_i(G), \mathbb{G}_m)$ is represented by a smooth group scheme over S. Hence, via the argument given on p. 345-347 of [Br1], it suffices to show that f is surjective whenever $S = \mathrm{Spec}(k)$, where k is an algebraically closed field, i.e. that $\mathrm{Ext}^2(G, \mathbb{G}_m) = 0$ in this case. If $\mathrm{char}(k) > 2$, this follows immediately from Proposition 2 of [Br1]. On the other hand, if $\mathrm{char}(k) = 2$, then $\mathrm{Ext}^2(\mathbb{Z}/2\mathbb{Z}, \mathbb{G}_m) = \mathrm{Ext}^2(\mu_2, \mathbb{G}_m) = 0$, while $\mathrm{Ext}^2(\alpha_2, \mathbb{G}_m) \neq 0$ (see [Br3], Remark 5). Hence it follows via devissage that if the composition series of G does not have a factor of local-local type, then $\mathrm{Ext}^2(G, \mathbb{G}_m) = 0$. This completes the proof. $\square$

The next result now follows immediately from Theorem 1.1 and the exact sequence (4).

Theorem 1.2. *Let S be any scheme, and let G be a finite, flat commutative group scheme over S. Suppose that the composition series of every geometric fibre of G of residue characteristic 2 does not contain a factor of local-local type. Then every primitive class of* $\mathrm{Pic}(G^D)$ *is realisable.* $\square$

Remark 1.3. If $S = \mathrm{Spec}(O_F)$ (or more generally, if $S = \mathrm{Spec}(R)$, where R is any Dedekind domain), then $\mathrm{Pic}(G^D)$ may be identified with the locally free classgroup $\mathrm{Cl}(\mathfrak{A})$ of the Hopf algebra $\mathfrak{A}$. Theorem 1.2 then asserts that (under the given hypotheses on G), every primitive class in $\mathrm{Cl}(\mathfrak{A})$ is realisable. We remark that most authors have considered Waterhouse's question in terms of classgroups of Hopf algebras.

2. Suppose now that $S = \mathrm{Spec}(O_F)$ and that $G = \oplus_i \mathbb{Z}/n_i\mathbb{Z}$ is a constant group scheme over S. Then $G^D = \oplus_i \mu_{n_i}$. If we set $\Gamma = G(F)$, then $\mathfrak{A} = O_F\Gamma$, and $\mathfrak{B} = \mathrm{Map}(\Gamma, O_F)$. In this situation, the twisted forms of $\mathfrak{B}$ are the rings of integers in unramified Galois algebra extensions of F with Galois group Γ which are unramified at all finite primes of F (see e.g. [BT]).

Theorem 2.1. *(a) We have* $\mathrm{Im}(\psi) = \mathrm{Prim}(\mathrm{Cl}(\mathfrak{A}))$.

(b) Suppose that $|\Gamma|$ *is coprime to* $|\,\mathrm{Cl}(O_F)|$. *If either*

(i) F is totally imaginary, or

(ii) F is not totally imaginary and $|\Gamma|$ is odd,

then $\mathrm{Prim}(\mathrm{Cl}(\mathfrak{A})) = 0$.

If F is not totally imaginary and $|\Gamma|$ is even, then $2.\,\mathrm{Prim}(\mathrm{Cl}(\mathfrak{A})) = 0$.

Proof. (a) This follows from Theorem 1.2 and Remark 1.3.

(b) Let C/F be a Galois algebra extension of F with Galois group Γ, and assume that C/F is unramified at all finite places of F. Suppose either that F is totally imaginary, or that F is not totally imaginary and $|\Gamma|$ is odd. Then classfield theory implies that each Wedderburn component of C is isomorphic to F. Hence the subgroup of realisable classes of $\mathrm{Cl}(\mathfrak{A})$ is trivial, and so it follows from Theorem 1.2 that $\mathrm{Prim}(\mathrm{Cl}(\mathfrak{A}))$ is also trivial.

On the other hand, if F is not totally imaginary and $|\Gamma|$ is even, then each Wedderburn component of C is isomorphic either to F or to a quadratic extension of F which is unramified at all finite places of F. This implies that, in this case, the subgroup of realisable classes of $\mathrm{Cl}(\mathfrak{A})$ is annihilated by 2. Hence we deduce from Theorem 1.2 that $2.\,\mathrm{Prim}(\mathrm{Cl}(\mathfrak{A})) = 0$. $\square$

Remark 2.2. Theorem 2.1(b) is rather striking because it gives quite fine information concerning the structure of $\mathrm{Cl}(\mathfrak{A})$ solely in terms of the classgroup $\mathrm{Cl}(O_F)$ of the base O_F. In some sense, it may be viewed as a sort of analogue of Vandiver's conjecture for classgroups of integral group rings. We shall illustrate this point via a simple example. (It is possible to construct more complicated examples by using work of Ullom ([U]) on the fine structure of certain classgroups.)

Suppose that Γ is cyclic of prime order $p > 2$, and let $\hat{\Gamma}$ be the group of characters of Γ. Write $K = F(\zeta_p)$, where ζ_p is a primitive pth root of unity, and set $\Delta = \mathrm{Gal}(K/F)$. Let $\mathrm{Map}_\Delta(\hat{\Gamma}, \mathrm{Cl}(O_K))$ denote the group of Δ-equivariant maps from $\hat{\Gamma}$ to $\mathrm{Cl}(O_K)$. If $\mathcal{M}$ denotes the maximal O_F-order in $F\Gamma$, then it follows from the theory of locally free classgroups (see e.g. Chapter 1 of [T]) that $\mathrm{Cl}(\mathcal{M}) \simeq \mathrm{Map}_\Delta(\hat{\Gamma}, \mathrm{Cl}(O_K))$. Let us now assume that $\mathrm{Cl}(\mathfrak{A}) \simeq \mathrm{Cl}(\mathcal{M})$. We therefore regard each element of $\mathrm{Cl}(\mathfrak{A})$ as being an element of $\mathrm{Map}_\Delta(\hat{\Gamma}, \mathrm{Cl}(O_K))$.

Next, we recall that for each integer r with $0 \leq r \leq p-1$, there is an Adams operator Ψ_r on $\mathrm{Cl}(\mathfrak{A})$ which is defined as follows (see Chapter 9 of [T1]). Suppose that $f \in \mathrm{Map}_\Delta(\hat{\Gamma}, \mathrm{Cl}(O_K))$. Then $\Psi_r f(\chi) = f(\chi^r)$ for each $\chi \in \hat{\Gamma}$. Set

$$\mathrm{Cl}(\mathfrak{A})^{(1)} := \{f \in \mathrm{Cl}(\mathfrak{A}) | \Psi_r(f) = f^r \quad \text{for all } r \text{ with } 1 \leq r \leq p-1\}.$$

Then it is easy to see that $\mathrm{Cl}(\mathfrak{A})^{(1)} \simeq \mathrm{Hom}_\Delta(\hat{\Gamma}, \mathrm{Cl}(O_K)) \subseteq \mathrm{Map}_\Delta(\hat{\Gamma}, \mathrm{Cl}(O_K))$.

Let D denote the p-part of $\mathrm{Cl}(O_K)$, and write $\omega : \Delta \to \mathbb{Z}_p^*$ for the character giving the action of Δ on the pth roots of unity in K. Then we have

$$\mathrm{Hom}_\Delta(\hat{\Gamma}, \mathrm{Cl}(O_K)) \simeq \mathrm{Hom}_\Delta(\hat{\Gamma}, D) \simeq D(\omega),$$

where $D(\omega)$ denotes the ω-eigenspace for the action of Δ on D. Hence

$$\mathrm{Cl}(\mathfrak{A})^{(1)} \simeq D(\omega).$$

Now consider the following examples:

(a) Suppose that $F = \mathbb{Q}$. Then it is a theorem of Rim (see [R] or Theorem 50.2 of [CR]) that $\mathrm{Cl}(\mathfrak{A}) \simeq \mathrm{Cl}(\mathcal{M})$. Also, it follows from Herbrand's theorem (see [W], Proposition 6.16 and Theorem 6.17) that $D(\omega) = 0$. Hence we deduce that $\mathrm{Prim}(\mathrm{Cl}(\mathfrak{A})) = \mathrm{Cl}(\mathfrak{A})^{(1)} = 0$. (So in fact this gives another proof of Theorem 2.1(b) in this special case.)

(b) Suppose that $F = \mathbb{Q}(\zeta_p)^+$, the maximal real subfield of $K = \mathbb{Q}(\zeta_p)$, and that p is an irregular prime, i.e. that p divides $|\operatorname{Cl}(O_K)|$. (There are infinitely many irregular primes.) Suppose further that Vandiver's conjecture holds, i.e. that p does not divide $|\operatorname{Cl}(O_F)|$. Then Theorem 2.1(b) implies that $\operatorname{Prim}(\operatorname{Cl}(\mathfrak{A})) = 0$.

On the other hand, via an argument virtually identical to that given in Theorem 50.2 of [CR], it may be shown that $\operatorname{Cl}(\mathfrak{A}) \simeq \operatorname{Cl}(\mathcal{M})$. Hence, since $\operatorname{Gal}(K/F)$ is generated by complex conjugation, we have that $\operatorname{Cl}(\mathfrak{A})^{(1)} \simeq D(\omega) = D^-$, where D^- denotes the minus-eigenspace for the action of complex conjugation on D. Since D is non-trivial, and p does not divide $|\operatorname{Cl}(O_F)|$, it follows that D^- is non-trivial.

Hence, if Vandiver's conjecture is true, then for infinitely many p, we have $\operatorname{Prim}(\operatorname{Cl}(\mathfrak{A})) = 0$, whilst $\operatorname{Cl}(\mathfrak{A})^{(1)} \neq 0$. $\square$

Remark 2.3. Let F be a real quadratic field of odd discriminant and odd classnumber. Then F has at most one quadratic extension L that is unramified at all finite primes. This extension L exists if and only if the norm of a fundamental unit of F is $+1$ (cf. [FT], Chapter V, 1.14). Hence it follows from a theorem of Brinkhuis (cf. [Bri], Theorem 2.2) that if H denotes $\operatorname{Gal}(L/F)$, then O_L is a free $O_F H$-module.

Now suppose that Γ is any finite abelian 2-group. Let C/F be any Galois algebra extension of F with Galois group Γ, and assume that C/F is unramified at all finite places of F. Then each Wedderburn component of C is isomorphic either to F or to L. Hence the ring of integers of C is a free $O_F\Gamma$-module. This implies that the subgroup of realisable classes of $O_F\Gamma$ is trivial, and so it follows from Theorem 1.2 that $\operatorname{Prim}(\operatorname{Cl}(O_F\Gamma)) = 0$.

It would be interesting to know whether a similar strengthening of Theorem 2.1(b) holds for other fields F which are not totally imaginary and which have odd classnumber. $\square$

3. We shall now describe the application that led to our interest in these problems. For further details, the reader may consult [A1], [A2], and [AT].

Let A/F be an abelian variety with everywhere good reduction, and let $\mathcal{A}/O_F$ denote its Néron model. Write $\mathcal{A}^D/O_F$ for the dual abelian scheme of $\mathcal{A}/O_F$. Fix a prime p, and let $\mathcal{A}_{p^n}$ denote the O_F-group scheme of p^n-torsion on $\mathcal{A}/O_F$. Then $\mathcal{A}_{p^n}$ is a finite, flat, commutative group scheme, and its Cartier dual is $\mathcal{A}^D_{p^n}$, the O_F-group scheme of p^n-torsion on $\mathcal{A}^D/O_F$. We therefore have a class invariant homomorphism

$$\psi_n : H^1(O_F, \mathcal{A}_{p^n}) \longrightarrow \mathrm{Prim}(\mathrm{Pic}(\mathcal{A}^D_{p^n}))$$

as described in Section 1. The study of the class invariant homorphism in this context was first introduced by M. J. Taylor in [T2].

The natural inclusion map $\mathcal{A}^D_{p^n} \hookrightarrow \mathcal{A}^D_{p^{n+1}}$ induces natural homomorphisms $H^1(O_F, \mathcal{A}_{p^{n+1}}) \to H^1(O_F, \mathcal{A}_{p^n})$ and $\mathrm{Prim}(\mathrm{Pic}(\mathcal{A}^D_{p^{n+1}})) \to \mathrm{Prim}(\mathrm{Pic}(\mathcal{A}^D_{p^n}))$. It may be shown that the following diagram is commutative:

$$\begin{array}{ccc} H^1(O_F, \mathcal{A}_{p^{n+1}}) & \xrightarrow{\psi_{n+1}} & \mathrm{Prim}(\mathrm{Pic}(\mathcal{A}^D_{p^{n+1}})) \\ \downarrow & & \downarrow \\ H^1(O_F, \mathcal{A}_{p^n}) & \xrightarrow{\psi_n} & \mathrm{Prim}(\mathrm{Pic}(\mathcal{A}^D_{p^n})). \end{array}$$

Passing to inverse limits yields a homomorphism

$$\psi_\infty : \varprojlim H^1(O_F, \mathcal{A}_{p^n}) \longrightarrow \varprojlim \mathrm{Prim}(\mathrm{Pic}(\mathcal{A}^D_{p^n})).$$

We now observe that for all odd primes p (and for all positive integers n), the group schemes $\mathcal{A}_{p^n}$ satisfy the hypotheses of Theorem 1.2. Furthermore, this is also the case when $p = 2$ provided that $\mathcal{A}$ has ordinary reduction at all places dividing 2. Hence we have the following result.

Theorem 3.1. *The homomorphism ψ_∞ is surjective whenever p is odd. If $\mathcal{A}$ has ordinary reduction at all places dividing 2, then ψ_∞ is also surjective when $p = 2$.*

Remarks 3.2. (1) Theorem 3.1 gives an affirmative answer to Question 1 (ii) of [A1] if in addition the p-primary part of the Tate-Shafarevich group of A/F is assumed to be finite.

(2) Suppose that the kernel of ψ_∞ is finite. (The author believes that this is the case for all abelian varieties A/F with everywhere good reduction, and for all primes p.) Then Theorem 3.1 implies that there is an isomorphism

$$\{\varprojlim H^1(O_F, \mathcal{A}_{p^n})\}/\{\text{a finite group}\} \simeq \varprojlim \mathrm{Prim}(\mathrm{Pic}(\mathcal{A}^D_{p^n})).$$

Hence we obtain a new description of the flat Selmer group $\varprojlim H^1(O_F, \mathcal{A}_{p^n})$ (modulo a finite subgroup) in terms of the Galois structure of twisted forms of Hopf orders.

It is shown in [AT] that, (subject to certain technical hypotheses), if A/F is a CM elliptic curve and p is an odd prime of ordinary reduction, then the kernel of ψ_∞ is indeed finite.

(3) Observe that the kernel of ψ_∞ is finite if and only if the order of the kernel of ψ_n is bounded independently of n. The exact sequence (3) implies that this is equivalent to the assertion that the order of the group$\mathrm{Ext}^1_{\mathcal{P}}(\mathcal{A}^D_{p^n}, \mathbb{G}_m)$ is bounded independently of n. It would be very interesting to have an answer to the following question. Suppose that $(G_n)_{n\geq 0}$ is any p-divisible group scheme over O_F. Under what conditions is the order of the group $\mathrm{Ext}^1_{\mathcal{P}}(G_n, \mathbb{G}_m)$ bounded independently of n?

I am gateful to R. Schoof for drawing my attention to the following example. Let $(\mathbb{Z}/p^n\mathbb{Z})_{n\geq 0}$ denote the constant p-divisible group scheme over O_F, and suppose that $p \nmid |\mathrm{Cl}(O_F)|$. Then, for each n, the p-primary part of $H^1(\mathbb{Z}/p^n\mathbb{Z}, \mathbb{G}_m)$ is trivial, and so it follows that

$$\mathrm{Ext}^1_{\mathcal{P}}(\mathbb{Z}/p^n\mathbb{Z}, \mathbb{G}_m) = \mathrm{Ext}^1_{\mathcal{S}}(\mathbb{Z}/p^n\mathbb{Z}, \mathbb{G}_m).$$

Now Theorem 2 of [W] implies that

$$\mathrm{Ext}^1_{\mathcal{S}}(\mathbb{Z}/p^n\mathbb{Z}, \mathbb{G}_m) \simeq H^1(O_F, \mu_{p^n}),$$

and this last group is of exponent p^n. Hence we deduce that the order of $\mathrm{Ext}^1_{\mathcal{P}}(\mathbb{Z}/p^n\mathbb{Z}, \mathbb{G}_m)$ increases with n.

This suggests that, in general, perhaps the exponent of $\mathrm{Ext}^1_{\mathcal{P}}(G_n, \mathbb{G}_m)$ remains bounded if the p-divisible group $(G_n)_{n\geq 0}$ does not have a subquotient of twisted constant type. We remark that if $\mathcal{A}/O_F$ is any abelian scheme, then the p-divisible group scheme $(\mathcal{A}_{p^n})_{n\geq 0}$ does not have a subquotient of twisted constant type (see [MW], Chapter 3, Section 7).

References

[A1] A. Agboola, *A geometric description of the class invariant homomorphism*, Journal de la Théorie des Nombres de Bordeaux **6** (1994), 273-280.

[A2] A. Agboola, *Iwasawa theory of elliptic curves and Galois module structure*, Duke Math. J. **71** (1993), 441-462.

[AT] A. Agboola, M. J. Taylor, *Class invariants of Mordell-Weil groups*, Crelle **447** (1994), 23-61.

[Br1] L. Breen, *Une théorème d'annulation pour certains Ext^i de faisceaux abéliens*, Ann. scient. Éc. Norm. Sup. **5** (1975), 339-352.

[Br2] L. Breen, *Extensions of abelian sheaves and Eilenberg-Mac Lane algebras*, Invent. Math. **9** (1969), 1249-1253.

[Br3] L. Breen, *On a non-trivial higher extension of representable abelian sheaves*, AMS Bull. **75** (1969), 1249-1253.

[Bri] J. Brinkhuis, *On the Galois module structure over CM-fields*, Manuscripta Math. **75** (1992), 333-347.
[By1] N. Byott, *Picard invariants of Galois algebras over a class of Hopf orders*, preprint (1997).
[By2] N. Byott, *Tame realisable classes over Hopf orders*, J. Algebra **210** (1998), 284-316.
[BT] N. Byott, M. J. Taylor, *Hopf orders and Galois module structure*, In: Group rings and classgroups, K. W. Roggenkamp, M. J. Taylor (eds), Birkhauser, 1992, pp. 153-210.
[C] S. Caenepeel, *Kummer theory for monogenic Larson orders*, In: Rings, Hopf algebras and Brauer groups. Lecture Notes Pure Appl. Math 197, S. Caenepeel (ed) et. al., Marcel Dekker, 1998, pp. 85-102.
[C1] L. N. Childs, *The group of unramified Kummer extensions of prime degree*, Proc. London Math. Soc. **35** (1977), 407-422.
[C2] L. N. Childs, *Abelian Galois extensions of rings containing roots of unity*, Ill. J. Math. **15** (1971), 273-280.
[CM] L. Childs, A. Magid, *The Picard invariant of a principal homogeneous space*, J. Pure and Appl. Alg. **4** (1974), 273-286.
[CP] M. P. Cox Paul, *The image of the Picard invariant map for Hopf Galois extensions*, Ph.D. Thesis, SUNY Albany (1994).
[CR] C. W. Curtis and I. Reiner, *Methods of Representation Theory, Volume II*, Wiley, 1987.
[FT] A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*, Cambridge University Press, 1991.
[G] A. Grothendieck et al., *Groupes de monodromie en géometrie algébrique (SGA 7)*, Lecture Notes in Mathematics **288** (1972), Springer Verlag.
[MW] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbb{Q}$, Invent. Math. **76** (1984), 179-330.
[M] L. R. McCulloh, *Galois module structure of abelian extensions*, Crelle **375/376** (1987), 259-306.
[R] D. S. Rim, *Modules over finite groups*, Ann. Math. **69** (1959), 700-712.
[T1] M. J. Taylor, *Classgroups of Group Rings*, Cambridge University Press, 1984.
[T2] M. J. Taylor, *Mordell-Weil groups and the Galois module structure of rings of integers*, Ill. J. Math. **32** (1988), 428-452.
[U] S. V. Ullom, *Fine structure of class groups of cyclic p-groups*, J. Algebra **49** (1977), 112-124.
[W] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, 1997.
[Wa] W. Waterhouse, *Principal homogeneous spaces and group scheme extensions*, AMS Transactions **153** (1971), 181-189.

Department of Mathematics, University of California, Santa Barbara, CA 93106, USA
E-mail address: agboola@math.ucsb.edu