

A. AGBOOLA

**A geometric description of the class invariant
homomorphism**

Journal de Théorie des Nombres de Bordeaux, tome 6, n° 2 (1994),
p. 273-280

http://www.numdam.org/item?id=JTNB_1994__6_2_273_0

© Université Bordeaux 1, 1994, tous droits réservés.

L'accès aux archives de la revue « Journal de Théorie des Nombres de Bordeaux » (<http://jtnb.cedram.org/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

A geometric description of the class invariant homomorphism

par A. AGBOOLA

In recent years, a certain amount of work has been done on the Galois structure of principal homogeneous spaces of finite group schemes that are constructed via dividing points on abelian varieties. This study was begun by M. J. Taylor in [T1] and was originally motivated by the fact that such principal homogeneous spaces are very closely connected with certain rings of integers. The starting point of the theory is the so-called class invariant homomorphism which was first introduced by Waterhouse in [W]. The purpose of this note is to point out a simple geometric description of this homomorphism (as considered in [T1]) in terms of the restriction of certain line bundles to torsion subgroup schemes of the abelian variety in question. We shall also make a number of remarks concerning both old results and new questions that arise in light of this description.

In what follows, we shall confine ourselves to the case of abelian varieties defined over number fields. It should however be noted that there is no difficulty in carrying out a similar analysis of the analogous situation over global function fields (cf. [A3]).

I would like to thank K. Ribet for drawing my attention to [R]. I am also grateful to T. Chinburg, M. J. Taylor, and W. Messing for interesting conversations.

1. In this section we shall recall the definition of the class invariant homomorphism for abelian varieties. We refer the reader to [W], [T1] and [BT] for further details.

Let F be a number field with ring of integers \mathcal{O}_F . Suppose that A/F is an abelian variety with everywhere good reduction, and let $\mathcal{A}/\mathcal{O}_F$ denote the Néron model of A/F . Write \hat{A} (resp. $\hat{\mathcal{A}}$) for the dual abelian variety of A (resp. \mathcal{A}). (We shall frequently omit the dependence upon F from our notation when there is no danger of confusion.) It follows from the universal property of the Néron model that there are natural isomorphisms $\mathcal{A}(\mathcal{O}_F) \simeq A(F)$ (resp. $\hat{\mathcal{A}}(\mathcal{O}_F) \simeq \hat{A}(F)$); we shall feel free to make such identifications without further notice.

Let \mathcal{A}_{p^n} denote the \mathcal{O}_F -group scheme of p^n -torsion on \mathcal{A} . Then \mathcal{A}_{p^n} is affine with Cartier dual $\hat{\mathcal{A}}_{p^n}$, and both \mathcal{A}_{p^n} and $\hat{\mathcal{A}}_{p^n}$ are twisted constant groups. Hence we may apply Theorem 2 of [W] and deduce that there is an isomorphism

$$\nu_1 : \text{Ext}(\mathcal{A}_{p^n}, \mathbb{G}_m) \longrightarrow H^1(\mathcal{O}_F, \hat{\mathcal{A}}_{p^n}).$$

(Here $\text{Ext}(\mathcal{A}_{p^n}, \mathbb{G}_m)$ is computed in the category of fpqc group schemes, and we take cohomology with respect to the fpqc site.)

This isomorphism may be described as follows. Let \mathcal{V} be an extension of \mathcal{A}_{p^n} by \mathbb{G}_m ; then there is an exact sequence of commutative group schemes

$$(1) \quad 1 \longrightarrow \mathbb{G}_m \longrightarrow \mathcal{V} \longrightarrow \mathcal{A}_{p^n} \longrightarrow 0.$$

Applying the functor $\text{Hom}(\mathcal{A}_{p^n}, -)$ to (1) yields the exact sequence

$$(2) \quad 0 \longrightarrow \text{Hom}(\mathcal{A}_{p^n}, \mathbb{G}_m) \longrightarrow \text{Hom}(\mathcal{A}_{p^n}, \mathcal{V}) \longrightarrow \text{Hom}(\mathcal{A}_{p^n}, \mathcal{A}_{p^n})$$

i.e.

$$(3) \quad 0 \longrightarrow \hat{\mathcal{A}}_{p^n} \longrightarrow \text{Hom}(\mathcal{A}_{p^n}, \mathcal{V}) \longrightarrow \text{Hom}(\mathcal{A}_{p^n}, \mathcal{A}_{p^n}).$$

Let $\iota \in \text{Hom}(\mathcal{A}_{p^n}, \mathcal{A}_{p^n})$ denote the identity map, and define Y to be the inverse image of ι in (3) above (i.e. Y is the sheaf of group-theoretic sections of (1)). Then Y is a principal homogeneous space of $\hat{\mathcal{A}}_{p^n}$ (see e.g. Theorem 2' of [W]) and so determines an element $\nu_1(\mathcal{V})$ of $H^1(\mathcal{O}_F, \hat{\mathcal{A}}_{p^n})$.

We next observe that there is an obvious natural homomorphism

$$\nu_2 : \text{Ext}(\mathcal{A}_{p^n}, \mathbb{G}_m) \longrightarrow H^1(\mathcal{A}_{p^n}, \mathbb{G}_m) = \text{Pic}(\mathcal{A}_{p^n})$$

and that Kummer theory on \mathcal{A} affords us a natural map

$$\nu_3 : \hat{\mathcal{A}}(F) \simeq \hat{\mathcal{A}}(\mathcal{O}_F) \longrightarrow \hat{\mathcal{A}}(\mathcal{O}_F)/p^n \hat{\mathcal{A}}(\mathcal{O}_F) \longrightarrow H^1(\mathcal{O}_F, \hat{\mathcal{A}}_{p^n}).$$

The class invariant homomorphism

$$\psi_n : \hat{\mathcal{A}}(F) \longrightarrow \text{Pic}(\mathcal{A}_{p^n})$$

is defined by $\psi_n = \nu_2 \circ \nu_1^{-1} \circ \nu_3$.

This homomorphism may be described somewhat more concretely as follows. Let F^c be an algebraic closure of F , and write Ω_F for the absolute Galois group of F . Let G denote the group of F^c -valued points of $\hat{\mathcal{A}}_{p^n}$, and

let \mathfrak{H} (resp. \mathfrak{B}) be an \mathfrak{D}_F -Hopf algebra that represents the group scheme $\hat{\mathcal{A}}_{p^n}/\mathfrak{D}_F$ (resp. $\mathcal{A}_{p^n}/\mathfrak{D}_F$). It is shown in [T1] that \mathfrak{H} (resp. \mathfrak{B}) is an \mathfrak{D}_F -order in the algebra $\mathcal{H} = (F^cG)^{\Omega_F}$ (resp. $\text{Map}(G, F^c)^{\Omega_F}$), where here Ω_F acts on both G and F^c .

Let $Q \in \hat{A}(F)$, and set

$$G_Q = \{Q' \in \hat{A}(F^c) \mid p^n Q' = Q\}.$$

Define the Kummer algebra F_Q by $F_Q = \text{Map}(G_Q, F^c)^{\Omega_F}$, and write \mathfrak{D}_Q for the integral closure of \mathfrak{D}_F in F_Q . The algebra \mathcal{H} acts on F_Q by

$$(f \cdot \alpha)(Q') = \sum_{g \in G} \alpha_g f(Q' + g)$$

for $f \in F_Q$ and $\alpha = \sum_{g \in G} \alpha_g g \in \mathcal{H}$.

In general \mathfrak{D}_Q is not acted upon by \mathfrak{H} . Define the Kummer order \mathfrak{C}_Q to be the largest \mathfrak{H} -module contained in \mathfrak{D}_Q . It is shown in §3 of [T1] (see also p.186 of [BT]) that \mathfrak{C}_Q is a principal homogeneous space of the algebra \mathfrak{B} , and that \mathfrak{C}_Q is a locally free \mathfrak{H} -module. Then (ibid.) $\psi_n(Q) = (\mathfrak{C}_Q) \in \text{Pic}(\mathcal{A}_{p^n})$.

2. Recall that, via standard theory, there are canonical isomorphisms

$$(4) \quad \hat{A} \simeq \text{Pic}^0(\mathcal{A}) \simeq \text{Ext}(\mathcal{A}, \mathbb{G}_m).$$

Thus each point $Q \in \hat{A}(F)$ determines a (rigidified) line bundle \mathcal{L}_Q on \mathcal{A} , and an extension

$$(5) \quad 1 \longrightarrow \mathbb{G}_m \longrightarrow \mathcal{G}(Q) \longrightarrow \mathcal{A} \longrightarrow 0$$

of \mathcal{A} by \mathbb{G}_m (cf. [Mu, §13 and §23] or [Mi, §11]).

The inclusion map $\mathcal{A}_{p^n} \hookrightarrow \mathcal{A}$ induces a natural homomorphism

$$\nu_4 : \text{Ext}(\mathcal{A}, \mathbb{G}_m) \longrightarrow \text{Ext}(\mathcal{A}_{p^n}, \mathbb{G}_m).$$

Hence, from (5), we obtain an extension $\mathcal{G}(Q)^{(n)} := \nu_4(\mathcal{G}(Q))$

$$(6) \quad 1 \longrightarrow \mathbb{G}_m \longrightarrow \mathcal{G}(Q)^{(n)} \longrightarrow \mathcal{A}_{p^n} \longrightarrow 0$$

of \mathcal{A}_{p^n} by \mathbb{G}_m .

We thus have a homomorphism

$$(7) \quad \psi'_n : \hat{A}(F) \longrightarrow \text{Pic}(\mathcal{A}_{p^n}/\mathfrak{D}_F)$$

defined by $\psi'_n = \nu_2 \circ \nu_4$. Note that the map ψ'_n is simply that induced by restricting the line bundle \mathcal{L}_Q to the subgroup scheme \mathcal{A}_{p^n} of \mathcal{A} .

We are now in a position to state the main result of this note.

THEOREM 1. $\psi_n = \psi'_n$.

Proof. To prove the result it suffices to show that

$$(8) \quad \nu_1 \circ \nu_4(\mathcal{G}(Q)) = \nu_3(Q).$$

We first of all note that the natural homomorphism

$$\eta : H^1(\mathcal{O}_F, \hat{A}_{p^n}) \longrightarrow H^1(F, G)$$

is an injection (see e.g. [BT, Lemma 2.1]), and so (8) will follow if we show that

$$(9) \quad \eta \circ \nu_1 \circ \nu_4(\mathcal{G}(Q)) = \eta \circ \nu_3(Q).$$

We next observe that by reasoning exactly as above in the definition of ν_i 's, but this time working over $\text{Spec}(F)$ rather than $\text{Spec}(\mathcal{O}_F)$, we may define natural homomorphisms ν'_i :

$$\begin{aligned} \nu'_1 : \text{Ext}(A_{p^n}, \mathbb{G}_m) &\longrightarrow H^1(F, \hat{A}_{p^n}) \\ \nu'_2 : \text{Ext}(A_{p^n}, \mathbb{G}_m) &\longrightarrow H^1(A_{p^n}, \mathbb{G}_m) = \text{Pic}(A_{p^n}) \\ \nu'_3 : \hat{A}(F) &\longrightarrow H^1(F, \hat{A}_{p^n}) \\ \nu'_4 : \text{Ext}(A, \mathbb{G}_m) &\longrightarrow \text{Ext}(A_{p^n}, \mathbb{G}_m) \end{aligned}$$

(It is perhaps worth remarking that $\text{Pic}(A_{p^n}) = 0$, and so the map ν'_2 is not particularly interesting!)

Let $G(Q)$ (resp. $G(Q)^{(n)}$) denote the generic fibre of $\mathcal{G}(Q)/\mathcal{O}_F$ (resp. $\mathcal{G}(Q)^{(n)}/\mathcal{O}_F$), and set $\theta = \nu'_1 \circ \nu'_4$. Then $G(Q)$ is the extension of A/F by \mathbb{G}_m afforded by $Q \in A(F)$, and so by functoriality we have

$$\eta \circ \nu_1 \circ \nu_4(\mathcal{G}(Q)) = \theta(G(Q))$$

and

$$\eta \circ \nu_3(Q) = \nu'_3(Q)$$

However, Proposition 3.1 of [R] asserts that

$$(10) \quad \theta(G(Q)) = \nu'_3(Q)$$

(note that Ribet's ξ is our ν'_3 , and his P is our Q), and this implies the result.

For the sake of completeness, we shall now give a brief sketch of the proof of (10). The reader may refer to §3 of [R] for full details.

Let D be the divisor on A determined by the point Q (cf. (4) above). Let $F^c(A)$ denote the function field of A/F^c , and for each $a \in A(F^c)$, write $T_a : A \rightarrow A$ for the translation-by- a map. Ribet shows that $G(Q)^{(n)}(F^c)$ is isomorphic to the group of pairs $(a, f) \in A_{p^n}(F^c) \times F^c(A)^x$ satisfying:

$$(11) \quad (f) = T_a^*D - D$$

$$(12) \quad f(x)f(x+a) \dots f(x+(p^n-1)a) = 1$$

under the multiplication

$$(a_1, f_1)(a_2, f_2) = (a_1 + a_2, g)$$

where $g(x) = f_2(x + a_1)f_1(x)$.

Now choose a p^n th root Q' , say, of Q on $\hat{A}(F^c)$, and let E be the corresponding divisor on A/F^c . Then

$$[p^n]^*(E) = D + (h)$$

for some function $h \in F^c(A)$, and it may be shown that the map $s : A_{p^n}(F^c) \rightarrow G(Q)^{(n)}(F^c)$ defined by

$$a \longmapsto (a, h(x)/h(x+a))$$

is a group-theoretic section of the natural epic $G(Q)^{(n)}(F^c) \rightarrow A_{p^n}(F^c)$. It follows that $\theta(G(Q)) \in H^1(F, \hat{A}_{p^n})$ is represented by the cocycle $\delta_\sigma = \sigma.s - s$ (where $\sigma \in \Omega_F$). By explicitly computing δ_σ , it may be deduced that

$$\delta_\sigma(a) = e_n(a, (\sigma - 1)Q'),$$

where e_n denotes the Weil pairing. This establishes (10), as required.

It follows from Theorem 1 that there are certain constraints on the image of ψ_n . Let \mathcal{W} be any flat, commutative \mathfrak{D}_F -group scheme, and write $m : \mathcal{W} \times \mathcal{W} \rightarrow \mathcal{W}$ for the multiplication map. Let $p_i : \mathcal{W} \times \mathcal{W} \rightarrow \mathcal{W}$ ($i = 1, 2$) denote projection onto the i th factor. Recall (see eg [Se, Chapter VII, §3]) that a class $c \in \text{Pic}(\mathcal{W})$ is said to be *primitive* if $m^*(c) = p_1^*(c) + p_2^*(c)$. Let $\text{PPic}(\mathcal{W})$ denote the subgroup of $\text{Pic}(\mathcal{W})$ consisting of the primitive elements of $\text{Pic}(\mathcal{W})$. Then (*op. cit.*) $\text{PPic}(\mathcal{W})$ is an additive functor of \mathcal{W} ,

and if \mathcal{W} is an abelian variety, then $\text{PPic}(\mathcal{W}) = \text{Pic}^0(\mathcal{W})$. Hence we deduce that the image of ψ_n is contained in $\text{PPic}(\mathcal{A}_{p^n})$, i.e. that we in fact have

$$\psi_n : \hat{A}(F) \longrightarrow \text{PPic}(\mathcal{A}_{p^n}/\mathcal{O}_F).$$

We remark that this fact also follows from the results contained in §1 of [CM].

3. Theorem 1 implies that the study of the homomorphism ψ_n is really the study of the behaviour of line bundles on \mathcal{A} under restriction to certain torsion subgroup schemes of \mathcal{A} . It is interesting to reformulate the results of [A], [AT] and [ST] in light of this fact. For example, combining Proposition 1 above with Theorem 1 of [ST] immediately yields the following result.

THEOREM 2 (SRIVASTAV-TAYLOR). *Let A/F above be a CM elliptic curve. Suppose that $p > 3$, and let $\mathcal{L} \in \text{Pic}^0(\mathcal{A})(\mathcal{O}_F)$ be a torsion line bundle. Then $\mathcal{L}|_{\mathcal{A}_{p^n}}$ is trivial for all $n \geq 1$.*

It is conjectured that a similar result holds for an arbitrary CM abelian variety with everywhere good reduction. (Note added in proof: The author has recently shown that Theorem 2 also holds in the non-CM case. See his forthcoming paper ‘Torsion points on elliptic curves and Galois module structure’.)

We shall now introduce some further notation. Let $\mathcal{A}'_{p^n}/\mathcal{O}_F$ denote the normalisation of $\mathcal{A}_{p^n}/\mathcal{O}_F$. Composing ψ_n with the natural map $\text{Pic}(\mathcal{A}_{p^n}) \rightarrow \text{Pic}(\mathcal{A}'_{p^n})$ gives us a homomorphism

$$\varphi_n : \mathcal{A} \longrightarrow \text{PPic}(\mathcal{A}'_{p^n}/\mathcal{O}_F).$$

The map φ_n may be described in terms of Kummer orders (cf. §1) as follows. By definition, $\mathcal{A}'_{p^n}/\mathcal{O}_F = \text{Spec}(\mathcal{M})$, where \mathcal{M} is the unique maximal \mathcal{O}_F -order contained in \mathcal{H} . Suppose that $Q \in \hat{A}(F)$. Then $\varphi_n(Q) = (\mathcal{C}_Q \otimes_{\mathcal{H}} \mathcal{M}) \in \text{PPic}(\mathcal{A}'_{p^n})$.

Next, we recall that ψ_n (and hence also φ_n) factors through the projection $\hat{A}(F) \rightarrow \hat{A}(F)/p^n \hat{A}(F)$. Also, the inclusion map $\mathcal{A}_{p^n} \hookrightarrow \mathcal{A}_{p^{n+1}}$ induces natural morphisms $H^1(\mathcal{O}_F, \mathcal{A}_{p^{n+1}}) \rightarrow H^1(\mathcal{O}_F, \mathcal{A}_{p^n})$ and $H^1(\mathcal{A}_{p^{n+1}}, \mathbb{G}_m) \rightarrow H^1(\mathcal{A}_{p^n}, \mathbb{G}_m)$. Taking inverse limits of ψ_n and φ_n with respect to these maps, and identifying $\hat{\mathcal{A}}$ with $\text{Pic}^0(\mathcal{A})$ as per (4) above yields homomorphisms

$$\psi_\infty : \hat{\mathcal{A}}(\mathcal{O}_F) \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq \text{Pic}^0(\mathcal{A})(\mathcal{O}_F) \otimes_{\mathbb{Z}} \mathbb{Z}_p \longrightarrow \varprojlim \text{PPic}(\mathcal{A}_{p^n})$$

and

$$\varphi_\infty : \hat{\mathcal{A}}(\mathcal{O}_F) \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq \text{Pic}^0(\mathcal{A})(\mathcal{O}_F) \otimes_{\mathbb{Z}} \mathbb{Z}_p \longrightarrow \varprojlim \text{PPic}(\mathcal{A}'_{p^n}).$$

We remark that a line bundle $\mathcal{L} \in \text{Pic}^0(\mathcal{A})(\mathcal{O}_F)$ lies in the kernel of φ_∞ if and only if $\mathcal{L}|_{\mathcal{A}_{p^n}}$ is trivial for all $n \geq 1$. We may now pose the following question.

- QUESTION 1. (i) *Is the kernel of φ_∞ finite?*
 (ii) *Is φ_∞ surjective (possibly only up to finite index)?*

It seems possible to regard an affirmative answer to these questions as a loose analogue of the Tate conjecture for abelian varieties (now a theorem of Faltings (see [F] or [CS])). This states that the natural map

$$\text{End}_F(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p \longrightarrow \text{End}_F(T_p(A))$$

is an isomorphism. (Here $T_p(A)$ is the p -adic Tate module of A , and $\text{End}_F(A)$ (resp. $\text{End}_F(T_p(A))$) is the ring of endomorphisms of A (resp. $T_p(A)$) that are defined over F .) It is shown in [AT] that Question 1(i) has an affirmative answer (subject to certain technical hypotheses) in the case that A/F is a CM elliptic curve and p is a prime of good ordinary reduction.

We may also ask similar questions about the kernel of φ_∞ . When A/F is a CM elliptic curve and p is an ordinary prime, it is shown in [A1] and [AT] that the kernel of φ_∞ is equal to a canonical subgroup of $A(F) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ first defined by R. Greenberg using Iwasawa theory (see [G]). This subgroup may be described in terms of the p -adic height pairing on A (see [P]) and is in general of infinite order. (See also [A2] for a discussion of φ_∞ in the context of p -adic representations.) It would be of some interest to obtain a better understanding of the relationship between class invariants and p -adic heights. (See [A4] for further remarks on this in the case of CM elliptic curves.) We conclude with the following question.

- QUESTION 2. *Suppose that the kernel of φ_∞ is of infinite order. Does this imply that the p -adic height pairing on A (cf. [PR] or [Sc]) is degenerate?*

BIBLIOGRAPHIE

- [A1] A. Agboola, *Iwasawa theory of elliptic curves and Galois module structure*, Duke Math. J. **71** (1973), 441-462.
- [A2] A. Agboola, *p-adic representations and Galois module structure*, preprint.
- [A3] A. Agboola, *Abelian varieties and Galois module structure in global function fields*, Math. Z. (to appear).
- [A4] A. Agboola, *On p-adic height pairings and locally free classgroups of Hopf orders*, in preparation.
- [AT] A. Agboola, M. J. Taylor, *Class invariants of Mordell-Weil groups*, J. reine angew. Math. **447** (1994), 23-61.
- [BT] N. P. Byott, M. J. Taylor, *Hopf orders and Galois module structure*, in: Group rings and classgroups, K. W. Roggenkamp, M. J. Taylor (eds.), Birkhauser, 1992.
- [CM] L. Childs, A. Magid, *The Picard invariant of a principal homogeneous space*, J. Pure and Appl. Alg. **4** (1974), 273-286.
- [CS] G. Cornell, J. Silverman (eds.), *Arithmetic Geometry*, Springer, 1986.
- [F] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349-366.
- [G] R. Greenberg, *Iwasawa theory for p-adic representations*, Advanced Studies in Pure Mathematics **17** (1989), Academic Press, 97-137.
- [Mi] J. Milne, *Abelian varieties*, in: Arithmetic Geometry, G. Cornell, J. Silverman (eds.), Springer, 1986.
- [Mu] D. Mumford, *Abelian Varieties*, OUP, 1970.
- [PR] B. Perrin-Riou, *Théorie d'Iwasawa et hauteurs p-adique*, Invent. Math. **109** (1992), 137-185.
- [P] A. Plater, *Height Pairings on Elliptic Curves*, Ph.D. Thesis, Cambridge University, 1991.
- [R] K. Ribet, *Kummer theory on extensions of abelian varieties by tori*, Duke Math. J. **49** (1979), 745-761.
- [Sc] P. Schneider, *Iwasawa theory for abelian varieties—a first approach*, Invent. Math. **71** (1983), 251-293.
- [Se] J.-P. Serre, *Algebraic Groups and Class Fields*, Springer, 1988.
- [ST] A. Srivastav, M. J. Taylor, *Elliptic curves with complex multiplication and Galois module structure*, Invent. Math. **99** (1990), 165-184.
- [T1] M. J. Taylor, *Mordell-Weil groups and the Galois module structure of rings of integers*, Ill. J. Math. **32** (1988), 428-452.
- [W] W. Waterhouse, *Principal homogeneous spaces and group scheme extensions*, AMS Transactions **153** (1971), 181-189.

A. Agboola
 Department of Mathematics
 UC Berkeley Berkeley
 CA 94720
 USA