Φ

D. Bertrand May 2006

Updated May 2007

On a formula of Shimura and Taniyama : a Note on the Note [BM].

Abstract : in a recent work with David Masser, we proved a formula concerning the order of certain subgroups of torsion points of complex abelian varieties (see the "Proposition" of [BM], §3). We here show that this proposition holds in any characteristic, and for all simple abelian varieties X whose endomorphism ring is a maximal order.

Updated abstract : I recently realized that the formula in question is established in the same degree of generality in the classical work [ST], see §7.2, Proposition 10. Furthermore, various methods of proof later appear in the literature, albeit in special cases: see [W], [G] and the Remark below. The present argument is still different, and it seems not totally useless to make it available here.

---

1. Introduction

Let k be an algebraically closed field of arbitray characteristic, and let X be an arbitrary abelian variety defined over k. Denote by $\Lambda = End(X)$ the ring of endomorphisms of X over k, put $A = \Lambda \otimes \mathbf{Q}$, and write d (resp. g) for the rank of Λ over $\mathbf{Z}$ (resp. the dimension of X). For any left ideal I of Λ (by which we mean, as in [CR], line before (26.13), a full left ideal: one such that $I \otimes \mathbf{Q} = A$), the abstract group Λ/I is finite, of order $[\Lambda : I]$, while the "I-torsion of X"

$$X[I] := \cap_{\alpha \in I} Ker\alpha$$

is a finite subgroup scheme of X, whose order will be denoted by $\#X[I]$. This coincides with the order of the abstract group $X[I](k) := \{x \in X(k), \forall \alpha \in I, \alpha x = 0\}$ when k has characteristic 0, but must in general be viewed as the rank of the finite k-algebra $\mathcal{O}_{X[I]}$.

(New) Proposition: *Assume that A is a simple $\mathbf{Q}$-algebra, and that $\Lambda = End(X)$ is a maximal order in A. For any (full) left ideal I of Λ, one has*

$$\#X[I] = [\Lambda : I]^{2g/d}.$$

In the situation of [BM], take $X = X_0^L$, where X_0 is simple of dimension g_0 and $\mathcal{O} = EndX_0$ is a maximal order of $\mathbf{Z}$-rank d_0. Then, $\Lambda = Mat_{LL}(\mathcal{O})$ is a maximal order in a simple algebra A. For a finite $\phi \in Hom(X_0^L, X_0^N)$, represented by a matrix B in $Mat_{NL}(\mathcal{O})$, let I be the left ideal of Λ generated by the various LL-matrices extracted from B. Then, $Ker\phi = X[I]$, while $\Lambda/I \simeq (\mathcal{O}^L/\mathcal{O}^N B)^L$. From the NP above, we get $\deg \phi = \#Ker\phi = [\mathcal{O}^L : \mathcal{O}^N B]^{L.2g_0L/d_0L^2} = [\mathcal{O}^L/\mathcal{O}^N B]^{2g_0/d_0}$. Therefore, the Proposition of [BM], §3, also holds in finite characteristic, under the general form alluded to after its enunciation. Along the lines of [BM] (whose §2 was already set in a general framework), this provides an extension to all characteristics of Theorem 5.1 of [LR2], where the authors compared their newly defined $\mathcal{O}$-heights with degrees in the context of complex abelian varieties.

Remark : the formula above is easily seen to be the same as [ST], §7.2, Prop. 10 (bearing in mind that at that time, "principal" meant "maximal order", and that the notion of I-transform takes into account degrees of inseparability). The formula was reproved in [W], Theorem 3.15 (1) under the assumption that the base field k is finite, building on Serre's point of view on I-transforms (see [S], beginning of §2, as well as the appendix to [C]). The formula is also proven in [G], at least in the commutative case, but now in the setting of group schemes.

In fact, we shall establish the following (apparent) generalization of the New Proposition. For all positive integers n, consider Λ^n as a free left Λ-module, which we identify with $Hom(X^n, X)$. In other words, we view the elements $\lambda = (\lambda_1, ..., \lambda_n)$ of Λ^n as row vectors (on which the matrix ring $M_{nn}(\Lambda)$ acts on the right), while the elements $(x_1, ..., x_n)^t$ of X^n are viewed as column vectors (on which $End(X^n) \simeq M_{nn}(\Lambda)$ acts on the left). A lattice $\mathbf{I}$ in Λ^n is a left Λ-submodule of Λ^n such that $\mathbf{I} \otimes \mathbf{Q} = A^n$. For such a lattice, $X^n[\mathbf{I}] := \cap_{\lambda \in \mathbf{I}} Ker(\lambda : X^n \to X)$ is a finite subgroup scheme of X^n, which satisfies:

(Lattice) Proposition: *Same assumptions as in NP. For any $n > 0$ and any lattice $\mathbf{I}$ in Λ^n, one has: $\#X^n[\mathbf{I}] = [\Lambda^n : \mathbf{I}]^{2g/d}$.*

This can actually be viewed as a corollary of the NP, applied to the abelian variety $\tilde{X} = X^n$, and to the left ideal $\tilde{I}$ of $\tilde{\Lambda} := End(X^n) = Mat_{nn}(\Lambda)$ formed by the matrices all of whose rows lie in $\mathbf{I}$. Indeed, $\tilde{X}[\tilde{I}] = X^n[\mathbf{I}]$, $[\tilde{\Lambda} : \tilde{I}] = [\Lambda^n : \mathbf{I}]^n$ and $\tilde{g} := dim\tilde{X} = ng$, $\tilde{d} := rk_{\mathbf{Z}}\tilde{\Lambda} = n^2 d$. The NP then implies $\#X^n[\mathbf{I}] = \#\tilde{X}[\tilde{I}] = [\tilde{\Lambda} : \tilde{I}]^{2\tilde{g}/\tilde{d}} = [\Lambda^n : \mathbf{I}]^{2g/d}$.

(1) Notice a misprint in this reference : the reduced norm should be raised to the power $m = 2g/e\delta$, where $d = [\Lambda : \mathbf{Z}] = e^2\delta$.

2. Restating the Proposition

The notation $X^n[\mathbf{I}]$ does not make it clear that the ambiant free module Λ^n in which $\mathbf{I}$ lives is already identified to $Hom(X^n, X)$. For instance, a change of basis of Λ^n would provide an isomorphic, but different, subscheme $X^n[\mathbf{I}]$. More generally, the following statement shows that its isomorphism class, hence its order, depends only on the isomorphism class of the finite (left) Λ-module $\Lambda^n/\mathbf{I}$ (by a finite Λ-module, we mean one of finite cardinality)

Lemma 0: *let $\mathbf{I} \subset \Lambda^n$ and $\mathbf{U} \subset \Lambda^m$ be two lattices such that the (finite) Λ-modules $\Lambda^n/\mathbf{I}$ and $\Lambda^m/\mathbf{U}$ are isomorphic. Then, the finite group schemes $X^n[\mathbf{I}]$ and $X^m[\mathbf{U}]$ are isomorphic.*

Proof: wlog, assume $n = m + m'$ with $m' \geq 0$, and consider $\mathbf{U}' = U \oplus \Lambda^{m'}$ in $\Lambda^m \oplus \Lambda^{m'} = \Lambda^n$. Clearly, $\Lambda^m/\mathbf{U} \simeq \Lambda^n/\mathbf{U}'$ and $X^m[\mathbf{U}] \simeq X^n[\mathbf{U}']$. So, we may assume that $n = m$. The isomorphism between $\Lambda^n/\mathbf{I}$ and $\Lambda^n/\mathbf{U}$, and its inverse, are then given by two elements B, C in $Mat_{nn}(\Lambda)$ satisfying $\mathbf{I}B \subset \mathbf{U}, \mathbf{U}C \subset \mathbf{I}$, and $BC \equiv \mathbf{1}_n \mod \tilde{I}$, $CB \equiv \mathbf{1}_n \mod \tilde{U}$, where the tilde has the same meaning as some lines above. Consider the isogenies $\beta : (x_1, ..., x_n)^t \mapsto C(x_1, ..., x_n)^t$, $\gamma : (y_1, ..., y_n)^t \mapsto B(y_1, ..., y_n)^t$ of X^n. Then, β maps $X^n[\mathbf{I}]$ into $X^n[\mathbf{U}]$, γ maps $X^n[\mathbf{U}]$ into $X^n[\mathbf{I}]$, and $\gamma\beta$ (resp. $\beta\gamma$) induces the identity on $X^n[\mathbf{I}]$, (resp. on $X^n[\mathbf{U}]$). They therefore induce isomorphisms between these subgroups schemes.

Conversely, let F be a finite Λ-module. Looking at sets of generators of F, we may write it, in many ways, as a quotient $\Lambda^n/\mathbf{I}$, where $\mathbf{I}$ is a lattice in Λ^n, but by Lemma 0, the resulting finite group schemes $X^n[\mathbf{I}]$ will be all isomorphic. Their order $\#X^n[\mathbf{I}]$ may therefore be denoted by $d(F)$. Similarly, the indices $[\Lambda^n : \mathbf{I}]$ are all equal to the cardinality $|F|$ of F; we may therefore set $i(F) := [\Lambda^n : \mathbf{I}]^{2g/d}$. We must now prove

(*) Proposition : *for all finite Λ-modules F, the quantities just defined above satisfy*

$$d(F) = i(F). \qquad (*)$$

As in Lemmas 4 and 5 of [BM], from which these notations are borrowed (with a slighlty different meaning), the proof will consist in a reduction to the case $F = \Lambda/\Lambda\gamma$, reminiscent of the reduction to diagonal matrices which these lemmas enable (see also [LR1]).

We close these preparations by collecting the results on Λ-modules (always on the left in what follows) and on finite group schemes which will be needed for the proof.

MO 1: maximal orders are hereditary, hence any lattice in Λ^n is a direct factor of a free Λ-module. [Cf. [CR], Prop. 26.12 (ii).]
MO 2: for any maximal two sided ideal $\wp$ of Λ, $\Lambda/\wp$ is a simple artinian ring [cf. [CR], Ex. 26.4]. In particular, there exists a unique isomorphism class of simple $\Lambda/\wp$-modules (equivalently, of simple Λ-modules annihilated by $\wp$); we shall denote by $S(\wp)$ a representative of this class. [See [CR], Ex. 3.2 and 3 for a description of these rings.]
MO 3: norm-form principle for the simple algebra A; cf. [M], p. 179, Lemma.

GS 1: if $0 \to A \to B \to C \to 0$ is an exact sequence of finite commutative group schemes over k, then $\#B = \#A \times \#C$. [See [MG], Ex. 4.4, or [M], p. 121, Thm. 2.]
GS 2: let $\beta \in \Lambda = End(X)$ be an isogeny of the abelian variety X, set $X[\beta] := X[\Lambda\beta]$, and let I be a left submodule of Λ. Then, the restriction $\overline{\beta}$ of β to $X[I\beta]$ induces an exact sequence $0 \to X[\beta] \to X[I\beta] \to X[I] \to 0$ of subgroup schemes of X. Indeed, the isogeny $\beta : X \to X$ is epimorphic, so that $\overline{\beta} : X[I\beta] \to X[I]$, which is deduced from β by the base extension $X[I] \to X$, is again epimorphic, while $Ker(\overline{\beta})$ coincides with $Ker(\beta)$, since they are both defined by base extension to the zero section. Conclude by [M], p. 118, Cor. 1.

We shall need GS2 only when I is a full ideal, i.e. when the involved subgroup schemes are finite. In this case, we deduce from GS1 that $\#X[I\beta] = \#X[I] \times \#X[\beta]$.

3. Proof of the (*) Proposition

Step 1

We first show how to reduce the claim (*) to the case of a *simple* finite left Λ-module F. Let

$$0 \to E \to F \to G \to 0$$

be an exact sequence of finite left Λ-modules. Then $|F| = |E|.|G|$ (hence $i(F) = i(E)i(G)$), and it suffices to check that the LHS of $(*)$ shares the same multiplicative property.

Write F as a quotient $\Lambda^n/\mathbf{I}$ of a free left module by a left sub-module $\mathbf{I}$. Then, $E = \mathbf{J}/\mathbf{I}$ for a left sub-module $\mathbf{J} \supset \mathbf{I}$, and $G = \Lambda^n/\mathbf{J}$. Since Λ is hereditary, $\mathbf{J}$ is by **MO1** a direct factor of a free Λ-module $N \simeq \Lambda^m$, and there exists a Λ-module $\mathbf{J}' \subset \Lambda^{n'}$ with $n + n' = m$ such that $N = \mathbf{J} \oplus \mathbf{J}'$. Let M be the big $\Lambda^n \oplus \Lambda^{n'} = \Lambda^m$ in which $\mathbf{J} \oplus \mathbf{J}'$ naturally lives, and let $B \in Mat_{mm}(\Lambda)$ be the matrix whose rows form a basis of N in terms of a basis of M; in other words, $N = MB$, where we write the elements of $M = \Lambda^m$ as row vectors. For rank reasons, B is invertible in $Mat_{mm}(A)$ and the endomorphism $\beta : X^m \to X^m : (x_1, ..., x_m)^t \mapsto B(x_1, ..., x_m)^t$ attached to B is an isogeny of X^m.

The inclusions of left Λ-modules $\mathbf{I} \oplus \mathbf{J}' \subset \mathbf{J} \oplus \mathbf{J}' = MB \subset \Lambda^n \oplus \Lambda^{n'} = M$ (which are all lattices in M) ensures the existence of a lattice $\mathbf{U} := (\mathbf{I} \oplus \mathbf{J}')B^{-1}$ in M such that

$\mathbf{U}B = \mathbf{I} \oplus \mathbf{J}'$. Now, in view of **GS2**, the isogeny β of X^m induces on $X^m[\mathbf{U}\beta]$ an exact sequence of finite subgroup schemes of X^m:

$$0 \to X^m[\beta] \to X^m[\mathbf{U}\beta] \to X^m[\mathbf{U}] \to 0.$$

By definition, the first term is the group scheme $X^m[\mathbf{J} \oplus \mathbf{J}'] \simeq X^n[\mathbf{J}] \times X^{n'}[\mathbf{J}']$, hence has order equal to $d(G).d(F')$, where we set $F' = \Lambda^{n'}/\mathbf{J}'$; the second one is $X^m[\mathbf{I} \oplus \mathbf{J}'] \simeq X^n[\mathbf{I}] \times X^{n'}[\mathbf{J}']$, whose order is $d(F).d(F')$; and since $\Lambda^m/\mathbf{U} = M/\mathbf{U} \simeq MB/\mathbf{U}B = (\mathbf{J} \oplus \mathbf{J}')/(\mathbf{I} \oplus \mathbf{J}') \simeq \mathbf{J}/\mathbf{I} = E$, the third one has order $d(E)$. By **GS1**, we therefore have: $d(F)d(F') = d(E)d(G)d(F')$, i.e. $d(F) = d(E)d(G)$, as was to be checked.

Step 2

Let now F be a simple finite left Λ-module. By [CR], proof of (26.19), there exists a maximal two-sided ideal $\wp$ of Λ such that $\wp F = 0$. We can therefore view F as a simple left module over the ring $\Lambda/\wp$. But this is a simple artinian ring, which by **MO2** admits a unique isomorphism class, say $F = S(\wp)$, of simple left modules. In particular, if Φ is any left Λ-module admitting a descending chain of submodules whose successive quotients are annihilated by $\wp$, then, it admits a (Jordan-Hölder, see [CR], Prop. 3.9]) composition series whose quotients are all isomorphic to $S(\wp)$ (as modules over Λ, or over $\Lambda/\wp$, cela revient au même). We are going to check $(*)$ not on F itself, but on a conveniently chosen module Φ of this type. By the multiplicativity of both sides of $(*)$ in exact sequences from Step 1, this is will ensure that F itself satisfies $(*)$.

The Φ we choose is $\Lambda/\wp^{eh}$, where h is the class number of the number field $K = Z(A)$, and e is the unique integer such that the prime ideal $P = R \cap \wp$ of $R = O_K$ satisfies $\Lambda P = \wp^e$ (cf. [CR], Exercise 26.5; as in [CR], I here denote by R the ring of integers of the center K of the simple $\mathbf{Q}$-algebra A). In particular, $\wp^{eh}$ is a principal two-sided ideal $\Lambda\gamma$, with $\gamma \in R$, and $\Phi = \Lambda/\Lambda\gamma$. On the other hand, Φ admits the descending chain $\{\wp^i/\wp^{eh}, i = 0, ..., eh\}$, whose quotients $\wp^i/\wp^{i+1}$ are anihilated by $\wp$. Refining this filtration gives a composition series with (say ℓ) simple factors, all isomorphic to $S(\wp) = F$. In particular,

$$i(\Phi) = i(F)^\ell \ , \ d(\Phi) = d(F)^\ell,$$

and it remains to check $(*)$ on $\Phi = \Lambda/\Lambda\gamma$.

Step 3

For this principal ideal case $I = \Lambda\gamma$, we appeal as in [LR1,2] and [BM] to the standard

MO 3 : the function $\alpha \in \Lambda \mapsto [\Lambda : \Lambda\alpha]$ extends to a norm form on A with degree of homogeneity equal to d, while by [M], p. 175, the function $\alpha \in \Lambda \mapsto deg(\alpha) := \#X[\alpha]$

extends to a norm form on A of degree of homogeneity equal to $2g$. Since A is a simple algebra, we obtain

$$\#X[\alpha] = [\Lambda : \Lambda\alpha]^{2g/d}$$

for all $\alpha \in \Lambda$.

Applying this to our $\alpha = \gamma \in R$, we finally deduce that Φ does satisfy $d(\Phi) = i(\Phi)$, and the proof of $(*)$ is completed. (See "Question" after the references for another possible way of applying **MO3**.)

References

[BM] D. Bertrand and D. Masser: Heights and degrees: a note on [LR 1], Monatshefte Math., 148, 2006 , 19-27.

[C] C. Cornut: Réduction de Familles de points CM; Thèse Univ. Strasbourg, 2000.

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

[GM] G. van der Geer and B. Moonen: Abelian varieties; Prep. 2005-2006-..., file available on 2nd author's home page.

[G] J. Giraud: Remarque sur une formule de Shimura-Taniyama; Invent. math., 5, 1968, 231-236.

[LR 1] C. Liebendörfer and G. Rémond: Duality of heights over quaternion algebras, Monatshefte Math., 145, 2005, 61-72.

[LR 2] C. Liebendörfer and G. Rémond: Hauteurs de sous-espaces sur les corps non commutatifs; Math. Zeitschrift, 255, 2007, 549-577.

[M] D. Mumford: *Abelian varieties*, Tata/Oxford UP, 1970.

[S] J-P. Serre: Complex multiplication; in *Oeuvres*, vol. II, 455-459.

[ST] G. Shimura and Y. Taniyama: *Complex multiplication of abelian varieties ...*; Publ. MS Japan, 6, 1961. Reprinted in G. Shimura: *Abelian varieties with CM and modular functions*, Princeton UP, 1998.

[W] W. Waterhouse: Abelian varieties over finite fields; Ann. ENS, 2, 1969, 521-560.

Question on non maximal orders

Is it true that for any (non necessarily maximal) order $\Lambda = End(X)$ in a simple $\mathbf{Q}$-algebra A, any $n > 0$, and any lattice $\mathbf{I}$ in Λ^n, one would always have

$$[\Lambda^n : \mathbf{I}]^{2g/d} \leq X^n[\mathbf{I}] \quad ?$$

(Probably, a divisibility relation would then always occur.)

If so, a much simpler proof of the LP could be given, as follows: if Λ is a maximal order, $\mathbf{I}$ will admit by **MO1** a supplement $\mathbf{I}' \subset \Lambda^{n'}$ such that $N := \mathbf{I} \oplus \mathbf{I}'$ is a free submodule of rank $m = n + n'$ of $M := \Lambda^n \oplus \Lambda^{n'} = \Lambda^m$. Write $N = MB$ for some $B \in Mat_{m,m}(\Lambda)$ in a manner similar to Step 1, and interpret B as an isogeny β of X^m. Clearly, we then have $\#X^m[\beta] = \#X^n[\mathbf{I}] \times \#X^{n'}[\mathbf{I}']$, while $[\Lambda^m : \Lambda^m B] = [\Lambda^n : \mathbf{I}] \times [\Lambda^{n'} : \mathbf{I}']$. Now, repeating the NP $\Rightarrow$ LP trick, we have $[\Lambda^m : \Lambda^m B]^{2g/d} = [Mat_{mm}(\Lambda) : Mat_{mm}(\Lambda)B]^{2g/dm} = [End(X^m) : End(X^m)\beta]^{2gm/dm^2}$, which, by the (easy) Step 3, applied to X^m, is equal to $\#X^m[\beta]$. Consequently,

$$[\Lambda^n : \mathbf{I}]^{2g/d} \times [\Lambda^{n'} : \mathbf{I}']^{2g/d} = \#X^n[\mathbf{I}] \times \#X^{n'}[\mathbf{I}'].$$

If the inequalities (?) hold for the two lattices $\mathbf{I}$ and $\mathbf{I}'$, this relation will force both to become equalities !

See [BM] and [LR2] for counterexamples to the equality in the non maximal case. Note, however, that since the deduction of Theorem 5.1 of [LR2] from the method of [BM], §5, uses the duality Theorem 7.1 of [LR2], it is not clear whether Inequality (?) would imply a similar "height $\geq$ degree" inequality in [LR2] for non maximal orders (recall that $\Delta_{fin}(\phi) = (deg\phi)^{-1}$).