# ENDOMORPHISM ALGEBRAS OF ABELIAN VARIETIES ATTACHED TO NEWFORMS OF WEIGHT 2

K. A. Ribet

1. Let $f = \Sigma a_n q^n$ be a weight-2 newform on $\Gamma_1(N)$ with character $\varepsilon$. Let $E = \mathbb{Q}(\ldots a_n \ldots)$ be the subfield of $\mathbb{C}$ generated by the coefficients of $f$. Let $A$ be the abelian variety attached to $f$ (see, e.g., [7, Th. 7.14]), viewed as an abelian variety _up to isogeny_ over $\mathbb{Q}$. One knows that the $\mathbb{Q}$-algebra of endomorphisms of $A$ over $\mathbb{Q}$ is equal to $E$.

On the other hand, let $D$ be the algebra of _all_ endomorphisms of $A$ (defined over $\overline{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$). If $f$ is a form with complex multiplication by an imaginary quadratic field $k$ (in the sense of [3]), then $D$ is a matrix algebra over $k$. We shall suppose, to the contrary, that $f$ is _not_ a form with complex multiplication. One then sees easily that $E$ is its own commutant in $D$, implying that $D$ is a central simple algebra over some subfield $F$ of $E$. The determination of the structure of $D$ (and in particular of the subfield $F$) has been carried out in [2] and in [4]. As we shall recall below, this structure depends on the "self twists" which $f$ possesses.

Before discussing these twists, we will prove three simple results concerning $D$, of which the first is contained in [2].

_Theorem 1_:

The algebra $D$ is either a matrix algebra over $F$, or else a matrix algebra over a quaternion division algebra with center $F$.

_Proof_ (suggested by J. Tunnell):

We know _a priori_ that $D$ is isomorphic to a matrix algebra over some division algebra $C$ with center $F$. Let $n$ be such that $D$ is isomorphic to $\mathbb{M}(n,C)$. We must show that $[E:F]/n$ divides 2.

Consider the cohomology group $V = H_1(A(\mathbb{C}),\mathbb{Q})$, which is of dimension

$$2 \cdot \dim(A) = 2[E:\mathbb{Q}]$$

over $\mathbb{Q}$. By functoriality, $D$ acts on $V$; in particular, $V$ is a $C$-vector space. Because of the $D$-action, the $C$-dimension of $V$ is a multiple of $n$. We have now

$$2[E:F] = \dim_F(V) = (\dim_F C)\cdot(\dim_C V)$$
$$= \left(\frac{[E:F]}{n}\right)^2 \cdot \dim_C V \quad ,$$

so that $2 = \frac{[E:F]}{n} \cdot \frac{\dim_C V}{n}$ as desired.

Remark. This result will be proved in Section 3 by another method.

Theorem 2:

Suppose that all endomorphisms of $A$ are defined over the field $\mathbb{R}$ of real numbers. Then $D$ is in fact a matrix algebra over $F$.

Proof:

To begin, suppose that $D$ is not a matrix algebra. Then in the above notation, the algebra $C$ is a quaternion division algebra over $F$, $[E:F]/n = 2$, and $\dim_C V = n$. Now the action of $D$ on $V$ breaks up $V$ into the direct sum of $n$ copies of a subspace $W$ of $V$ which is stable by $C$. We have

$$\mathrm{End}_D V = \mathrm{End}_C W \quad .$$

On the other hand, the $C$-dimension of $W$ is 1, so that $\mathrm{End}_C W$ is a division algebra (in fact, isomorphic to $C$). In particular, the only involutions in $\mathrm{End}_D V$ are the scalars $+1$ and $-1$.

If we assume, however, that all endomorphisms of $A$ are defined over $\mathbb{R}$, then the endomorphism of $V$ induced by "complex conjugation" on $A(\mathbb{C})$ is $D$-linear. This endomorphism is an involution, and therefore a scalar. One knows that this is not the case, for example because the two summands in the Hodge decomposition of $V \otimes \mathbb{C}$ are permuted by the complex conjugation.

Remarks

1. It is easy to see under what conditions the hypothesis to this theorem is satisfied (cf. Theorem 4 below and its corollary).

2. This theorem is obviously closely related to the results of Shimura in [6]. The proof given above was suggested by the discussion on pp. 137-139 of [6].

3. Another proof of the theorem may be given using the $\ell$-adic representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ defined by $f$ (cf. [3, (5.2)]).

Theorem 3:

Suppose that $D$ is not a matrix algebra over $F$. Then $A$ has everywhere potential good reduction.

Proof:

Let $k$ be a finite extension of $\mathbb{Q}$ over which $A$ has semistable reduction. Let $v$ be an ultrametric place of $k$, and denote by $A^{\sim}$ the connected component of the special fibre of the Néron model for $A$ at $v$. Then $A^{\sim}$ is an extension of an abelian variety by a torus $T$. Let $r = \dim T$. By functoriality, we find a representation

$$D \to (\mathrm{End}\ T) \otimes \mathbb{Q} \approx \mathbb{M}(r,\mathbb{Q}) \quad .$$

It is obvious that $[E:\mathbb{Q}]$ divides $r$ , and the proof of Theorem 1 shows that $2[E:\mathbb{Q}]$ divides $r$ when $D$ is not a matrix algebra over $F$ . Since we have

$$r \le \dim A = [E:\mathbb{Q}] \quad ,$$

we must have $r = 0$ under the hypothesis of the theorem.

Remark. According to the criterion of Néron-Ogg-Shafarevich, the behavior of $A$ at a prime $v$ is determined by the $\ell$-adic representations (of a decomposition group for $v$ in $\mathrm{Gal}(\overline{\mathbb{Q}}/k)$) attached to $f$ . Except in certain cases where $v$ is of residue characteristic 2, these representations have been determined by Deligne (unpublished). Thus, given $f$ , it may happen that we are able to say *a priori* that $A$ does not have everywhere potential good reduction; in that case, $D$ must be a matrix algebra. As an example, suppose that there is a prime $p$ which exactly divides $N$ at which the character $\varepsilon$ is trivial. By a well known result of Deligne-Rapoport [1], the abelian variety $A$ has purely multiplicative reduction at $p$ . Hence $D$ is a matrix algebra in that case.

## 2. The Action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $D$ .

When $\gamma \in \mathrm{Hom}(E,\mathbb{C})$ is an embedding of $E$ into $\mathbb{C}$ , we denote by $\gamma f$ the newform $\Sigma \gamma a_n q^n$ . Similarly, for $\chi$ a Dirichlet character, let $f \otimes \chi$ be the newform whose $p^{th}$ coefficient is $\chi(p)a_p$ for all primes $p$ prime to $N \cdot \mathrm{cond}(\chi)$ . Let

$$\Gamma = \{\gamma : E \longrightarrow \mathbb{C} \mid \gamma f = f \otimes \chi \text{ for some character } \chi\} \quad .$$

One knows ([2],[4]) that $\Gamma$ is an abelian subgroup of

Aut(E) . Further, for $\gamma \in \Gamma$ there is a unique Dirichlet character $\chi$ (which we call $\chi_\gamma$) such that $\gamma f = f \otimes \chi$ . For $\gamma, \gamma' \in \Gamma$ we have the cocycle rule

$$\chi_{\gamma\gamma'} = \chi_\gamma \chi_{\gamma'}^\gamma \quad .$$

Also, $\chi_\gamma^2 = \varepsilon^{\gamma-1}$ for each $\gamma$ . Finally, we recall (<u>loc. cit.</u>) that F <u>is precisely the fixed field of</u> $\Gamma$ .

Now each element g of $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts in the usual way to give an automorphism of the algebra D , and this automorphism is the identity on the field E (which is a maximal commutative subfield of D). (The action is as follows: for $d \in D$ , we define $(gd)(x) = g(d(g^{-1}x))$.) By the Skolem-Noether theorem, this automorphism is an inner automorphism

$$d \mapsto ede^{-1}$$

for an element e of $E^*$ which is well defined modulo $F^*$ . The numbers $\gamma e/e$ (for $\gamma \in \Gamma$) are well defined, and they together determine e as an element of the group $E^*/F^*$ . The map $g \mapsto e$ defines a continuous character $\alpha$ on G with values in the discrete group $E^*/F^*$ .

<u>Theorem 4</u>:

For each $g \in G$ and all $\gamma \in \Gamma$ we have

$$\alpha(g)^{\gamma-1} = \chi_\gamma(g) \quad .$$

<u>Proof</u>:

Let $\ell$ be a prime number, and let V now be the $\mathbb{Q}_\ell$-adic Tate module attached to A . The action of D on V defines an inclusion

$$D \otimes \mathbb{Q}_\ell \hookrightarrow \mathrm{End}\, V \quad ,$$

and the action of G on V defines a homomorphism

$$\rho : G \to \mathrm{Aut}_{E \otimes \mathbb{Q}_\ell} V \quad ,$$

which is known to be the $\ell$-adic representation attached to $f$. For $g \in G$, the automorphism of $D$ induced by $g$ is the restriction to $D$ of the automorphism of $D \otimes \mathbb{Q}$ obtained by conjugating by $\rho(g)$ in $\mathrm{End}\, V$.

To compute this automorphism, we suppose that $\ell$ has been chosen to split completely in $E$. Then, in a well known way, $V$ becomes the direct sum of $\mathbb{Q}_\ell$-submodules $V_\sigma$ of dimension 2, indexed by the various embeddings $\sigma$ of $E$ into $\mathbb{Q}_\ell$.

Let $\sigma$ and $\tau$ be two such embeddings, and let $H$ be an open normal subgroup of $G$. It is easy to see that we have

$$\mathrm{Hom}_H(V_\sigma, V_\tau) = 0$$

unless $\tau = \sigma\gamma$ for some $\gamma \in \Gamma$. Moreover, if $\tau = \sigma\gamma$, then $\mathrm{Hom}_H(V_\sigma, V_\tau)$ is of dimension 1 if $H$ is "small" and again 0 if $H$ is not. The action of $G$ on $\mathrm{Hom}_H(V_\sigma, V_\tau)$ is via the $\mathbb{Q}_\ell$-valued character $\sigma\chi_\gamma$.

Now the $V_\sigma$ are stable under $E$ (as a result of their construction); an $e \in E$ acts on $V_\sigma$ by multiplication by $\sigma e$. Hence conjugation by $e$ in $\mathrm{End}\, V$ preserves each group $\mathrm{Hom}(V_\sigma, V_\tau)$ and more precisely acts on this group by the scalar $\tau e/\sigma e$. In the case where $\tau = \sigma\gamma$, this quotient becomes $\sigma(e^{\gamma-1})$.

For $H$ sufficiently "small," it was proved in [4] that we have

$$D \otimes \mathbb{Q}_\ell = \mathrm{End}_H V = \bigoplus_{\sigma,\tau} \mathrm{Hom}_H(V_\sigma, V_\tau) \quad .$$

If $e \in E$ is such that conjugation by $e$ agrees on $D \otimes \mathbb{Q}_\ell$ with conjugation by $\rho(g)$, then we have

$$\sigma\chi_\gamma(g) = \sigma(e^{\gamma-1})$$

for all $\sigma \in \mathrm{Hom}(E, \mathbb{Q}_\ell)$ and $\gamma \in \Gamma$. This proves the theorem.

Corollary:

All endomorphisms of A are defined over $\mathbb{R}$ if and only if $\chi_\gamma(-1) = 1$ for all $\gamma \in \Gamma$ .

3. The Algebra D as a Crossed Product Algebra

Let $\mathfrak{X} = \mathrm{Hom}(G, \overline{\mathbb{Q}}^*)$ be the G-module of Dirichlet characters. For $\chi \in \mathfrak{X}$ , we define a Gauss sum $\tau(\chi)$ in the usual way: if $\chi$ has conductor r , we view $\chi$ as a function on $(\mathbb{Z}/r\mathbb{Z})^*$ and set

$$\tau(\chi) = \sum_{a \bmod r} \chi(a) e^{2i\pi/r} .$$

For $g \in G$ we then have

$$g(\tau(\chi)) = \tau(\chi^g) \cdot \chi^{-g}(g) .$$

Especially, if $\chi$ and $\chi'$ are Dirichlet characters, the "Jacobi sum"

$$j(\chi,\chi') = \tau(\chi)\tau(\chi')/\tau(\chi\chi')$$

satisfies

$$j(g\chi, g\chi') = gj(\chi,\chi') .$$

With this notation, we have

Theorem 5 ([2],[4]):

The algebra D is isomorphic to the crossed product algebra

$$\bigoplus_{\gamma\in\Gamma} E \cdot X_\gamma$$

furnished with the multiplication table

$$X_\gamma \cdot e = \gamma(e) X_\gamma \qquad (e \in E\ ,\ \gamma \in \Gamma) \quad ,$$

$$X_\gamma X_{\gamma'} = j(\chi_\gamma^{-1}, \chi_{\gamma'}^{-\gamma}) X_{\gamma\gamma'} \qquad (\gamma, \gamma' \in \Gamma) .$$

The multiplication described by the theorem arises quite naturally in the proof of the theorem, the $X_\gamma$ being given by certain "twisting operators" generalizing those occurring in [5]. However, it seems that the two-cocycle $j(\chi_\gamma^{-1}, \chi_{\gamma'}^{-\gamma})$ masks quite effectively the fact that the class of $D$ in the Brauer group of $F$ has order 1 or 2. We will now make a few comments on such cocycles, hoping that these comments will clarify the relation between the algebra $D$ and the $\mathfrak{X}$-valued 1-cocycle $\gamma \mapsto \chi_\gamma$ on $\Gamma$.

For this, we allow $F$ briefly to be an arbitrary finite extension of $\mathbb{Q}$ (in $\overline{\mathbb{Q}}$) and consider a 1-cocycle $\Phi\colon g \mapsto \chi_g$ on $\mathrm{Gal}(\overline{F}/F)$ with values in $\mathfrak{X}$. (Of course, we obtain such a cocycle from the 1-cocycle on $\Gamma$ defined by $f$ by inflation.) It is easy to see that the formula

$$g,h \mapsto \dot{j}(\chi_g^{-1}, \chi_h^{-g})$$

defines a 2-cocycle $\psi$ on $\mathrm{Gal}(\overline{F}/F)$ with values in $\mathfrak{X}$.

<u>Proposition 1</u>:

The class in $H^2(\mathrm{Gal}(\overline{F}/F), \overline{F}^*)$ of $\psi$ is equal to the class of the 2-cocycle

$$g,h \mapsto \chi_g(h) .$$

In particular, this class depends only on the restrictions of the $\chi_g$ to $\mathrm{Gal}(\overline{F}/F)$.

<u>Proof</u>:

We must show that the map

$$g,h \mapsto \chi_g(h)^{-1} j(\chi_g^{-1}, \chi_h^{-g})$$

is a 2-coboundary, i.e., that it may be written in the form $\alpha(g)\alpha(h)^g/\alpha(gh)$ for a suitable (continuous) function $\alpha$ on $\mathrm{Gal}(\overline{F}/F)$ . Taking

$$\alpha(g) = \tau(\chi^{-1}) \cdot \chi_g(g) \quad ,$$

we find after a short computation the required identity.

For $E$ a finite extension of $\mathbb{Q}$ , we let $\mathfrak{X}(E) \subseteq \mathfrak{X}$ be the G-module of $E^*$-valued Dirichlet characters.

<u>Proposition 2</u>:

The map on cocycles $\phi \mapsto \psi$ defines a homomorphism

$$\delta_F : H^1(\mathrm{Gal}(\overline{F}/F),\mathfrak{X}) \to H^2(\mathrm{Gal}(\overline{F}/F),\overline{F}^*) \quad .$$

If $E$ is a finite Galois extension of $F$ , the subgroup $H^1(\mathrm{Gal}(E/F),\mathfrak{X}(E))$ of the source is mapped by $\delta_F$ to the subgroup $H^2(\mathrm{Gal}(E/F),E^*)$ of the target.

<u>Proof</u>:

The first statement is most easily proved by writing the class of $\psi$ as the class of the cocycle given in Proposition 1. For example, we must show that multiplying $\phi$ by a 1-coboundary $g \mapsto \varepsilon^{g-1}$ does not change the class of $\psi$ . For this, we observe that the expression $\chi_g(h)$ gets multiplied by $\varepsilon(h)^g/\varepsilon(h)$ , a factor which may be written in the form $\varepsilon(g)\varepsilon(h)^g/\varepsilon(gh)$ . Thus the map $\phi \mapsto \psi$ indeed induces a map between the indicated cohomology groups, and we see immediately from Proposition 1 that the map is a homomorphism.

For the second statement, we have only to show that $\psi$ is $E^*$-valued if $\phi$ is obtained by inflation from a cocycle on $\mathrm{Gal}(E/F)$ with values in $\mathfrak{X}(E)$ . This follows from the formula at the beginning of this section which gives the behavior of Jacobi sums under automorphisms of $\overline{\mathbb{Q}}$ .

We now return to the context of Theorem 5. We remark that, once the dimension of D over F is known to be $[E:F]^2$ , the algebra D is determined by its class in the Brauer group of F , i.e., in $H^2(\mathrm{Gal}(\overline{F}/F),\overline{F}^*)$ . This class is the class of the 2-cocycle $\psi$ described by Jacobi sums, i.e., it is the image under $\delta_F$ of the class of the 1-cocycle $\gamma \mapsto \chi_\gamma$ on $\Gamma$ . This latter class already has order dividing 2, as we see from the formula $\chi_\gamma^2 = \varepsilon^{\gamma-1}$ , in which $\varepsilon$ is the (Nebentypus) character of the form f . Since $\delta_F$ is a homomorphism, we obtain an alternate proof of Theorem 1. Similarly we have

Proposition 3:

The class of D in Br(F) does not change if we replace f by a twist $f \otimes \chi_o$ of f .

Proof:

By inflation, we view the cocycle $\gamma \mapsto \chi_\gamma$ as a 1-cocycle on $\mathrm{Gal}(\overline{F}/F)$ with values in $\mathfrak{X}$ . When we twist f by $\chi_o$ , we multiply this 1-cocycle by the 1-coboundary $g \mapsto (\chi_o)^{g-1}$ . Hence twisting does not affect the class of this cocycle in $H^1(\mathrm{Gal}(\overline{F}/F),\mathfrak{X})$ ; a fortiori, twisting does not affect its image under $\delta_F$ .

Remark. Proposition 3 may also be obtained as a corollary of [4, (4.7)].

## 4. Concerning Local Triviality of D

If v is a place of F , we let $F_v$ be the completion of F at v and set

$$D_v = D \otimes_F F_v \quad .$$

Since $D$ has order dividing 2 in the Brauer group of $F$, $D_v$ has order dividing 2 in the Brauer group $Br(F_v)$ of $F_v$. In case $v$ is an archimedean (i.e., real) place of $F$, the order of $D_v$ in $Br(F_v)$ is already known to be 1 [2]. (This means that the algebra $C$ of Section 1 is either $F$ itself or else a totally indefinite quaternion algebra over $F$.) Therefore, we will discuss only non-archimedean places of $F$.

Suppose that $v$ is such a place, say of residue characteristic $p$. Suppose further that $p$ is prime to the level of $f$. We say that $f$ is ordinary at $v$ if the number $a_p^2\varepsilon(p)^{-1}$, easily seen to be in $F$, is prime to $v$.

Theorem 6:

If $v$ is ordinary, then $D_v$ is a matrix algebra over $F_v$.

Proof:

Our hypothesis on $p$ implies that $A$ has good reduction at $p$. Let $\tilde{A}$ be the reduction of $A$ at $p$, and let $V$ be the $\mathbb{Q}_p$-adic Tate module made from points of $p$-power order in $\tilde{A}(\overline{\mathbb{F}}_p)$. As is well known, the $\mathbb{Q}_p$-dimension of $V$ is equal to the number of $p$-adic unit roots of the characteristic polynomial of the Frobenius endomorphism of $\tilde{A}/\mathbb{F}_p$. This polynomial is the norm from $E$ to $\mathbb{Q}$ of the polynomial

$$\phi(t) = T^2 - a_p T + p\varepsilon(p) \in E[T] \quad .$$

The polynomial $\phi(T)$ itself controls the structure of $V$ as an $E \otimes \mathbb{Q}_p$-module.

Namely, we first remark that the endomorphisms of $A$ act on $V$, so that $V$ may be considered as a $D \otimes \mathbb{Q}_p$-module and hence in particular as an $E \otimes \mathbb{Q}_p$-module or an $F \otimes \mathbb{Q}_p$-module. As an $E \otimes \mathbb{Q}_p$-module, $V$ becomes the sum of subspaces $V_w$ corresponding to the various completions $E_w$ of $E$ at the primes $w$ of $E$ dividing $p$. Each $V_w$ is an $E_w$-vector space of dimension 1 or 0, and the dimension is more precisely the number of unit roots of $\phi(T)$, considered as a polynomial over $E_w$. Clearly $\phi(T)$ has a unit root if and only if the prime $v$ of $F$ induced by $w$ is ordinary.

It follows that if $v$ is an ordinary prime of $F$, the $F_v$-vector space

$$V_v = V \otimes_{(F\otimes\mathbb{Q}_p)} F_v = \bigoplus_{w|v} V_w$$

has dimension $\sum_{w|v} [E_w:F_v] = [E:F]$. It is, on the other hand, a $D_v$-module. Reasoning identical to that used in Section 1 shows that $D_v$ is a matrix algebra over $F_v$.

## References


1. Deligne, P. and Rapoport, P. Les shémas de modules de courbes elliptiques, Lecture Notes in Math. 349, 143-316 (1973).

2. Momose, F. On the ℓ-adic representations attached to modular forms, to appear.

3. Ribet, K. Galois representations attached to eigenforms with nebentypus, Lecture Notes in Math. 601, 17-52 (1977).

4. Ribet, K. Twists of modular forms and endomorphisms

of abelian varieties, Math. Ann, to appear.

5. Shimura, G. On the factors of the Jacobian variety of a modular function field, J. Math. Soc. Japan 25, 523-544 (1973).

6. Shimura, G. On the real points of an arithmetic quotient of a bounded symmetric domain, Math. Ann. 215, 135-164 (1975).

7. Shimura, G. Introduction to the Arithmetic Theory of Automorphic Functions, Princeton: Princeton University Press, 1971.

Ecole Polytechnique

Current Address:

Mathematics Department
University of California
Berkeley, California 94720 USA