# La classe de Brauer de l'algèbre d'endomorphismes d'une variété abélienne modulaire

Jordi Quer*

15–7–98

**Résumé**

On donne une formule pour la classe de Brauer de l'algèbre d'endomorphismes $\mathbf{Q}\otimes\mathrm{End}(A_f)$ de la variété abélienne $A_f/\mathbf{Q}$ attachée par Shimura a une forme primitive $f \in S_2(N,\varepsilon)$ comme un produit d'algèbres de quaternions et d'un facteur provenant du caractère $\varepsilon$.

**Algèbre d'endomorphismes des variétés abéliennes modulaires.** Soit $f = \sum a_n q^n \in S_2(N,\varepsilon)$ une forme primitive, normalisée avec $a_1 = 1$, et soit $E = \mathbf{Q}(\{a_n\})$. Shimura construit une variété abélienne $A_f/\mathbf{Q}$, isogène à un quotient de $J_1(N)$, avec

$$\dim A_f = [E:\mathbf{Q}], \qquad \mathbf{Q}\otimes \mathrm{End}_{\mathbf{Q}}(A_f) \simeq E.$$

Soit $\mathcal{X}$ l'algèbre $\mathbf{Q}\otimes\mathrm{End}(A_f)$ des endomorphismes de $A_f$ définis sur $\overline{\mathbf{Q}}$. Si $f$ est de type CM (voir [4]) on sait que la variété $A_f$ est isogène sur $\overline{\mathbf{Q}}$ à une puissance d'une courbe elliptique $C$ à multiplications complexes ; cela entraîne que $\mathcal{X}$ est une algèbre de matrices à coefficients dans le corps des multiplications complexes de $C$. Dans la suite nous supposerons que $f$ n'est pas de type CM. Dans ce cas (voir [4, Theorem 5.1 et Remark 5.8]) $\mathcal{X}$ est une algèbre simple ayant pour centre le corps totalement réel $F = \mathbf{Q}(\{a_p^2/\varepsilon(p)\}_{p\nmid N})$ ; de plus le corps $E$ est un sous-corps commutatif maximal de $\mathcal{X}$ et l'indice de Schur de $\mathcal{X}$ est égal à 1 ou à 2. La classe de $\mathcal{X}$ dans le groupe de Brauer de $F$ appartient au sous-groupe de 2-torsion $\mathrm{Br}_2(F)$. Notons $[\mathcal{X}]$ cette classe.

Dans [4] et aussi dans [3] l'algèbre $\mathcal{X}$ est décrite comme l'algèbre produit croisé d'un 2-cocycle du groupe $\mathrm{Gal}(E/F)$ défini par certaines sommes de Jacobi. Comme Ribet l'a remarqué dans [6, pag. 271] "it seems that this two-cocycle masks quite effectively the fact that the class of $\mathcal{X}$ in the Brauer group of $F$ has order 1 or 2".

Du théorème de Skolem-Noether et du fait que $E$ est un sous-corps commutatif maximal de $\mathcal{X}$ on déduit que l'action de $\sigma \in G_{\mathbf{Q}}$ sur $\mathcal{X}$ se fait par conjugaison par un élément $\alpha(\sigma) \in E^*$, déterminé à un élément non nul du centre $F$ près : ${}^{\sigma}\varphi = \alpha(\sigma)\varphi\alpha(\sigma)^{-1}$ pour tout $\varphi \in \mathcal{X}$. Un calcul montre que l'application définie par $c(\sigma,\tau) = \alpha(\sigma)\alpha(\tau)\alpha(\sigma\tau)^{-1}$ est un 2-cocycle du groupe $G_{\mathbf{Q}}$ à valeurs dans $F^*$, vu comme $G_{\mathbf{Q}}$-module discret à action triviale. D'après [5, Theorem 5.6], $[\mathcal{X}]$ est l'image de la classe de cohomologie $[c] \in H^2(G_{\mathbf{Q}}, F^*)$ par les homomorphismes

$$H^2(G_{\mathbf{Q}},F^*) \xrightarrow{\mathrm{Res}} H^2(G_F,F^*) \xrightarrow{\iota_*} H^2(G_F,\overline{F}^*) \simeq \mathrm{Br}(F),$$

où $\iota_*$ est induit par l'inclusion $F^* \to \overline{F}^*$.

Le but de cette note est de donner une formule pour cet élément. Dans la pratique, il arrive souvent que l'on connaisse seulement quelques coefficients de Fourier de la forme $f$. Alors, en

*Travail réalisé pendant un séjour à l'Institut für Experimentelle Mathematik (Essen) financé par la DGES

utilisant la formule du théorème 3 ci-dessous, on peut décider aisément si $[\mathcal{X}]$ est d'ordre 1 ou 2 dans $\mathrm{Br}(F)$ et, en particulier, calculer la dimension des variétés abéliennes dans une $\overline{\mathbf{Q}}$-décomposition de $A_f$ à isogénie près.

**Une formule pour $[\mathcal{X}]$.** D'après [5, Theorem 5.5], on a $\alpha^2 \equiv \varepsilon \pmod{F^*}$. Soit $d$ l'application $\alpha^2/\varepsilon$. Du fait que $\alpha$ est déterminé au produit par des éléments de $F^*$ près, on peut voir $d$ comme un homomorphisme $G_{\mathbf{Q}} \to F^*/F^{*2}$. En exprimant $\alpha(\sigma) = \sqrt{\varepsilon(\sigma)}\sqrt{d(\sigma)}$ on obtient, pour $\sigma, \tau \in G_F$,

$$c(\sigma,\tau) = \sqrt{\varepsilon(\sigma)}\sqrt{\varepsilon(\tau)}\sqrt{\varepsilon(\sigma\tau)}^{-1} \, \frac{\sqrt{d(\tau)}}{{}^\sigma\sqrt{d(\tau)}} \, \sqrt{d(\sigma)}\,{}^\sigma\sqrt{d(\tau)}\sqrt{d(\sigma\tau)}^{-1} = c_\varepsilon(\sigma,\tau)c_d(\sigma,\tau)\gamma(\sigma,\tau).$$

Les trois applications $c_\varepsilon, c_d$ et $\gamma$ sont des 2-cocycles de $G_F$ à valeurs dans $\overline{F}^*$ ; les deux premières prennent leurs valeurs dans $\{\pm 1\}$. Vu que $\gamma$ est un cobord, on obtient une décomposition de la classe de cohomologie de la restriction du cocycle $c$ au groupe $G_F$, considéré à valeurs dans $\overline{F}^*$, comme le produit des deux classes $[c_\varepsilon]$ et $[c_d]$.

Soit $L$ le corps fixé par $\ker\varepsilon$. Le cocycle $c_\varepsilon$ est la restriction du cocycle de $G_{\mathbf{Q}}$ défini par la même expression, que nous notons aussi $c_\varepsilon$. La classe $[c_\varepsilon] \in \mathrm{Br}_2(\mathbf{Q})$ peut être interprétée comme l'obstruction à l'existence d'une extension cyclique $\widetilde{L}/\mathbf{Q}$ de degré $2[L:\mathbf{Q}]$ contenant $L$. Dans certains cas (quand l'ordre de $\varepsilon$ est divisible par une puissance de 2 pas trop grande) on dispose de formules exprimant cette classe comme un produit d'algèbres de quaternions. Dans le cas général, on peut la caractériser par ses composantes locales dans $\mathrm{Br}_2(\mathbf{Q}_p)$, qui sont données par la parité des $p$-composantes du caractère $\varepsilon$. Dans ce qui suit nous étudions l'autre facteur $[c_d]$.

Soit $K$ le corps fixé par $\ker d$, qui est un composé de corps quadratiques. Soient $\sigma_1, \dots, \sigma_m$ des éléments de $G_{\mathbf{Q}}$ qui, par restriction à $K$, fournissent une base de $\mathrm{Gal}(K/\mathbf{Q}) \simeq (\mathbf{Z}/2\mathbf{Z})^m$. Soient $t_1, \dots, t_m$ des éléments de $\mathbf{Q}^*$ avec ${}^{\sigma_i}\sqrt{t_j} = \delta_{ij}\sqrt{t_j}$ (delta de Kronecker), et soient $d_i = d(\sigma_i) \in F^*/F^{*2}$. Pour $t, d \in F^*$, soit $(t,d)$ l'algèbre de quaternions sur $F$ selon la notation habituelle.

**Lemme 1** *La classe $[c_d] \in \mathrm{Br}_2(F)$ est égale au produit des algèbres de quaternions suivantes :*

$$[c_d] = (t_1, d_1) \dots (t_m, d_m).$$

Preuve: Pour $i = 1, \dots, m$, soient $x_i : G_{\mathbf{Q}} \to \mathbf{Z}/2\mathbf{Z}$ et $y_i : G_F \to \mathbf{Z}/2\mathbf{Z}$ les homomorphismes determinés par

$${}^\sigma\sqrt{t_i} = (-1)^{x_i(\sigma)}\sqrt{t_i}, \qquad {}^\sigma\sqrt{d_i} = (-1)^{y_i(\sigma)}\sqrt{d_i}.$$

Tout $\tau \in G_F$ (ou $\in G_{\mathbf{Q}}$) peut s'écrire comme le produit $\prod_{i=1}^m \sigma_i^{x_i(\tau)}$ à un élément de $G_K$ près. Il s'ensuit que $d(\tau) \equiv \prod_{i=1}^m d_i^{x_i(\tau)} \pmod{F^{*2}}$. D'où, pour tout $\sigma \in G_F$,

$${}^\sigma\sqrt{d(\tau)} = w\prod_{i=1}^m {}^\sigma\sqrt{d_i}^{x_i(\tau)} = w\prod_{i=1}^m (-1)^{y_i(\sigma)x_i(\tau)}\sqrt{d_i}^{x_i(\tau)} = \sqrt{d(\tau)}\prod_{i=1}^m (-1)^{y_i(\sigma)x_i(\tau)}$$

où $w \in F^*$, et l'on a

$$c_d(\sigma,\tau) = \prod_{i=1}^m (-1)^{y_i(\sigma)x_i(\tau)}.$$

Cette identité montre que le 2-cocycle $c_d$ est le produit des $m$ 2-cocycles définis par $c_i(\sigma,\tau) = (-1)^{y_i(\sigma)x_i(\tau)}$. Chaque $c_i$ est la version multiplicative du 2-cocycle à valeurs dans $\mathbf{Z}/2\mathbf{Z}$ défini par $(\sigma,\tau) \mapsto y_i(\sigma)x_i(\tau)$, qui a pour classe dans $H^2(G_F, \mathbf{Z}/2\mathbf{Z})$ celle du cup-produit des deux 1-cocycles $y_i$ et (la restriction au groupe $G_F$ de) $x_i$. Il est bien connu que ce cup-produit fournit la classe de l'algèbre de quaternions $(t_i, u_i)$. $\square$

Soit $\sigma$ un plongement de $E$ dans $\overline{\mathbf{Q}}$. La *forme conjuguée* $\sum {}^\sigma a_n q^n$ est aussi une forme primitive, que l'on note par ${}^\sigma f$. Si $\chi$ est un caractère de Dirichlet primitif, il existe une unique *forme primitive tordue* $\sum b_n q^n$ pour laquelle on ait $b_p = \chi(p) a_p$ pour presque tout nombre premier $p$, que l'on note par $\chi \otimes f$. Un couple $(\sigma, \chi)$ est une *torsion intérieure* (inner twist) pour la forme $f$ si ${}^\sigma f = \chi \otimes f$.

La forme $f$ est de type CM si $f = \chi \otimes f$ pour un caractère $\chi$ non trivial (primitif). Dans notre cas, comme $f$ n'est pas de type CM, dans $(\sigma, \chi)$ le caractère $\chi$ est déterminé par le plongement $\sigma$. L'ensemble des $\sigma : E \to \overline{\mathbf{Q}}$ appartenant à des torsions intérieures est un sous-groupe abélien de $\mathrm{Aut}(E)$ qui a pour sous-corps fixé le corps $F$ (voir [4, Proposition 3.3]).

**Lemme 2** *Si $p \nmid N$, posons $u_p = a_p^2/\varepsilon(p)$. Pour chaque $\sigma \in G_F$, il existe un unique caractère de Dirichlet (primitif) $\psi_\sigma$ tel que*

$$ {}^\sigma\sqrt{u_p} = \psi_\sigma(p)\sqrt{u_p}, \qquad \textit{pour tout} \ \ p \nmid N. $$

*De plus, $\{\psi_\sigma | \sigma \in G_{\mathbf{Q}}\}$ est le groupe des caractères de $G_{\mathbf{Q}}$ qui se factorisent par* $\mathrm{Gal}(K/\mathbf{Q})$.

Preuve: Pour chaque $\sigma \in G_F$ il y a un caractère de Dirichlet $\chi_\sigma$ tel que la paire $(\sigma|_E, \chi_\sigma)$ soit une torsion intérieure pour $f$. Écrivons $a_p = \sqrt{u_p}\sqrt{\varepsilon(p)}$. Comme ${}^\sigma a_p = \chi_\sigma(p) a_p$ pour $p \nmid N$, on a :

$$ {}^\sigma\sqrt{u_p}\,{}^\sigma\sqrt{\varepsilon(p)} = \chi_\sigma(p)\sqrt{u_p}\sqrt{\varepsilon(p)} \quad \Rightarrow \quad {}^\sigma\sqrt{u_p} = \chi_\sigma(p)\frac{\sqrt{\varepsilon(p)}}{{}^\sigma\sqrt{\varepsilon(p)}}\sqrt{u_p}, \qquad p \nmid N. $$

Si $\varepsilon$ est défini modulo $r$, l'application définie pour les $n$ tels que $(n, r) = 1$ par $n \mapsto \sqrt{\varepsilon(n)}/{}^\sigma\sqrt{\varepsilon(n)}$ est aussi un caractère de Dirichlet défini modulo $r$. On pose $\psi_\sigma = \chi_\sigma\sqrt{\varepsilon}/{}^\sigma\sqrt{\varepsilon}$. L'unicité provient du fait que, si $\psi_\sigma$ satisfait à l'identité de l'énoncé, alors le caractère $\chi_\sigma = \psi_\sigma{}^\sigma\sqrt{\varepsilon}/\sqrt{\varepsilon}$ appartient à $(\sigma|_E, \chi_\sigma)$.

D'après [5, Theorem 5.5], $\alpha(\mathrm{Frob}_p) \equiv a_p \pmod{F^*}$ pour tout nombre premier $p \nmid N$ avec $a_p \neq 0$. On en déduit que $d(\mathrm{Frob}_p) \equiv u_p \pmod{F^{*2}}$ pour ces nombres premiers. Comme la forme $f$ n'est pas de type CM, le sous-ensemble des $p$ avec $a_p \neq 0$ est de densité 1 dans l'ensemble de tous les nombres premiers.

Soit $p \nmid N, a_p \neq 0$. Soit $\sigma_p \in G_{\mathbf{Q}}$ un élément de Frobenius pour $p$. Si $\sigma_p \in G_F$, alors $u_p \in F^{*2}$ et $\psi_\sigma(p) = 1$. On en déduit que les caractères $\psi_\sigma$ se factorisent par $\mathrm{Gal}(K/\mathbf{Q})$. En outre, d'après le théorème de densité de Chebotarev, les $u_p \neq 0$ engendrent le sous-groupe $d(G_{\mathbf{Q}})$ de $F^*/F^{*2}$. Par conséquent, le nombre des caractères $\psi_\sigma$ différents est égal à l'ordre de $d(G_{\mathbf{Q}})$, qui est égal à l'ordre du groupe $\mathrm{Gal}(K/\mathbf{Q})$. $\square$

**Théorème 3** *Soit $\{\psi_1, \dots, \psi_m\}$ une base du groupe des caractères $\{\psi_\sigma | \sigma \in G_{\mathbf{Q}}\}$ et soient $\mathbf{Q}(\sqrt{t_i})$ les corps quadratiques fixés par les* $\ker \psi_i$. *Soient $p_1, \dots, p_m$ des nombres premiers avec $p_i \nmid N, a_{p_i} \neq 0$, pour lesquels $\psi_i(p_j) = \delta_{ij}$. La classe de Brauer de $\mathcal{X}$ est*

$$ [\mathcal{X}] = [c_\varepsilon](t_1, u_{p_1}) \cdots (t_m, u_{p_m}) \in \mathrm{Br}_2(F). $$

Preuve: L'existence de nombres premiers satisfaisant aux conditions de l'énoncé est conséquence du théorème de densité de Chebotarev (et du fait que $f$ n'est pas de type CM).

Soient $\sigma_1, \dots, \sigma_m \in G_{\mathbf{Q}}$ des éléments de Frobenius pour les nombres premiers $p_i$. Du lemme 2, on déduit que la restriction des $\sigma_i$ à $K$ fournit une base du groupe $\mathrm{Gal}(K/\mathbf{Q})$. D'après la définition des $t_j$, on a ${}^{\sigma_i}\sqrt{t_j} = \psi_j(\sigma_i)\sqrt{t_j} = \delta_{ij}\sqrt{t_j}$. On peut donc appliquer le lemme 1 et, compte tenu que $d(\sigma_i) \equiv u_{p_i} \pmod{F^{*2}}$, on obtient la formule de l'énoncé. $\square$

**Remarques.** (a) Grâce aux propriétés bien connues des torsions de formes modulaires, on voit aisément que les conducteurs des caractères $\psi_\sigma$ du lemme 2 divisent le conducteur de la forme $f$. On peut alors calculer ces caractères en connaissant quelques coefficients de Fourier de la forme $f$.

(b) (voir [6]) : (1) si tous les endomorphismes de $A_f$ sont définis sur $\mathbf{R}$, alors $[\mathcal{X}]$ est triviale (il est facile de voir que tous les endomorphismes de $A_f$ sont définis sur $\mathbf{R}$ si, et seulement si, les nombres $t_i$ sont tous positifs) ; (2) si $A_f$ a réduction potentiellement multiplicative en un nombre premier, alors $[\mathcal{X}]$ est triviale.

(c) Considérons le cas $F = \mathbf{Q}$. La condition que $[\mathcal{X}]$ soit triviale est équivalente au fait que $A_f$ soit $\overline{\mathbf{Q}}$-isogène à une puissance d'une courbe elliptique $C/\overline{\mathbf{Q}}$, qui est une $\mathbf{Q}$-courbe au sens de [5]. Le cas particulier de Nebentypus trivial et $E$ quadratique a été étudié par Cremona dans [1] : il prouve que $\mathcal{X}$ est isomorphe à une algèbre de quaternions $(\frac{d,r}{\mathbf{Q}})$ (l'algèbre $(t_1, u_{p_1})$ dans notre notation) et détermine des équations de Weierstrass pour les courbes $C$ dans certains cas.

(d) Admettons la conjecture de modularité des $\mathbf{Q}$-courbes, cf. [5]. Les exemples donnés dans [2] montrent alors qu'il existe des formes primitives $f$ avec $F = \mathbf{Q}$ et $m = 1, 2, 3, 4$ (cf. théorème 3), pour lesquelles $A_f$ est $\overline{\mathbf{Q}}$-isogène à une puissance d'une $\mathbf{Q}$-courbe. En outre, les conjectures standard sur les points rationnels des courbes modulaires suggèrent que dans ce cas (avec $F = \mathbf{Q}$ et $[\mathcal{X}]$ triviale) seulement un nombre fini de valeurs de $m$ peuvent apparaître (mieux : seulement un nombre fini de groupes $d(G_{\mathbf{Q}})$ peuvent apparaître). Par contre, et en attendant de disposer de tables de formes modulaires plus étendues, les seuls exemples de formes $f$ avec $F = \mathbf{Q}$ et $[\mathcal{X}]$ non triviale que nous connaissons proviennent de [1] avec $m = 1$.

# Références


[1] J. E. Cremona, *Abelian varieties with extra twist, cusp forms, and elliptic curves over imaginary quadratic fields*, J. London Math. Soc. (2) 45, (1992), 401–416.

[2] J. González, J. C. Lario, *Rational and elliptic parametrizations of* $\mathbf{Q}$*-curves*, preprint, 1997.

[3] F. Momose, *On the l-adic representations attached to modular forms*, J. Fac. Sci. Univ. Tokyo (1) 28, (1981), 89–109.

[4] K. Ribet, *Twists of modular forms and endomorphisms of abelian varieties*, Math. Ann. 253 (1980), 43–62.

[5] K. Ribet, *Abelian varieties over* $\mathbf{Q}$ *and modular forms*, Proceedings of KAIST Mathematics Workshop (1992), 53–79.

[6] K. Ribet, *Endomorphism algebras of abelian varieties attached to newforms of weight 2*, Progress in Math. 12 (1981), 263–276.