GT VACHES : exposé 3

Virgile Ducet

12 février 2015

Objectif : Construire une famille de surfaces abéliennes principalement polarisées sur $\mathbb{C}$ et interpréter leur espace de module comme une courbe de Shimura.

On se donne une algèbre de quaternions indéfinie B sur $\mathbb{Q}$ de discriminant D. Comme nous supposons que B est indéfinie, on a un isomorphisme $B \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathrm{M}_2(\mathbb{R})$. Soit $\phi : B \hookrightarrow \mathrm{M}_2(\mathbb{R})$ un plongement de B dans $\mathrm{M}_2(\mathbb{R})$.

1 Isomorphismes entre surfaces abéliennes complexes

Une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{R})$ agit sur $\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \in \mathbb{C}^2$ suivant la règle

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} a\omega_1 + b\omega_2 \\ c\omega_1 + d\omega_2 \end{pmatrix}.$$

Rappelons également que le sous-groupe $\mathrm{GL}_2^+(\mathbb{R})$ de $\mathrm{GL}_2(\mathbb{R})$ des matrices à déterminant positif agit sur $\mathcal{H}$ comme suit :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d}.$$

Un *ordre* est un $\mathbb{Z}$-module libre de rang 4 qui est aussi un anneau. On appelle ordre *maximal* tout ordre n'étant inclus strictement dans aucun autre ordre.

Soit $u = \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \in \mathbb{C}^2$. Nous allons considérer l'orbite de u sous l'action de $\mathcal{O}$:

$$\Lambda_u = \phi(\mathcal{O}) \cdot u.$$

Lemme 1.1. *L'ensemble Λ_u est un réseau de $\mathbb{C}^2$ si et seulement si $\omega_1\omega_2 \neq 0$ et $\Im(\omega_1/\omega_2) \neq 0$.*

Preuve. Soit $\alpha_i \in \mathrm{M}_2(\mathbb{R}),\ i = 1, \ldots, 4$ une base du $\mathbb{Z}$-module $\phi(\mathcal{O})$ telle que les α_i soit $\mathbb{R}$-linéairement indépendant. Si ω_1 ou ω_2 est nul, ou si ω_1 et ω_2 sont multiples réels l'un de l'autre, on peut trouver une relation de dépendance linéaire

$$\sum_{i=1}^{4} a_i \alpha_i u = 0,\ \ a_i \in \mathbb{R}.$$

Inversement, supposons que $\Im(\omega_1/\omega_2) \neq 0$. En multipliant par w_2^{-1}, on se ramène au cas où

$$u = \begin{pmatrix} \tau \\ 1 \end{pmatrix},$$

où $\tau = \omega_1/\omega_2$. Dans ce cas, le fait que les α_i soient $\mathbb{R}$-linéairement indépendants et la relation

$$\Im\left(\frac{a\omega_1/\omega_2 + b}{c\omega_1/\omega_2 + d}\right) = \frac{ad - bc}{|c\omega_1/\omega_2 + d|^2}\Im(z)$$

impliquent qu'il est impossible de trouver une relation de dépendance linéaire. □

Soit

$$u = \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \in \mathbb{C}^2$$

tel que $\omega_1\omega_2 \neq 0$ et $\Im(\omega_1/\omega_2) \neq 0$. L'ensemble Λ_u est donc un réseau et $A_u = \mathbb{C}^2/\Lambda_u$ est un tore complexe. Nous allons maintenant construire une forme de Riemann sur A_u, ce qui prouvera que A_u est une variété abélienne. Pour cela, notons tout d'abord le théorème suivant (voir le livre de Vignéras pour une preuve) :

Théorème 1.2. *Un corps quadratique $K/\mathbb{Q}$ se plonge dans B si et seulement si tout nombre premier p où B est ramifiée ne se décompose pas dans K.*

Ainsi on voit par exemple que tout corps quadratique imaginaire $\mathbb{Q}(\sqrt{-d})$ où $D|d$ se plonge dans B. Il existe donc toujours un élément $\gamma \in B$ tel que $\gamma^2 = -1/D < 0$, $\gamma^2 \in \mathbb{Q}$ et $\bar{\gamma} = -\gamma$. On définit une application $E : \Lambda_u \times \Lambda_u \to \mathbb{Q}$ par

$$E(\phi(\alpha)u, \phi(\beta)u) = \mathrm{trd}(\gamma\alpha\bar{\beta}).$$

Rappelons que comme $\bar{\cdot}$ est une involution, pour deux éléments $x, y \in B$ on a $\overline{xy} = \bar{y}\bar{x}$ et donc $\mathrm{trd}(xy) = \mathrm{trd}(\overline{xy}) = \mathrm{trd}(\bar{y}\bar{x})$.

Proposition 1.3. *L'application E est une forme de Riemann.*

Preuve.
1. E est anti-symétrique :

$$E(\phi(\alpha)u, \phi(\beta)u) = \mathrm{trd}(\gamma\alpha\bar{\beta}) = \gamma\alpha\bar{\beta} + \beta\bar{\alpha}\bar{\gamma} = \gamma\alpha\bar{\beta} - \beta\bar{\alpha}\gamma$$

et de même

$$E(\phi(\beta)u, \phi(\alpha)u) = \gamma\beta\bar{\alpha} - \alpha\bar{\beta}\gamma.$$

Ainsi

$$E(\phi(\alpha)u, \phi(\beta)u) + E(\phi(\beta)u, \phi(\alpha)u) = \gamma\mathrm{trd}(\alpha\bar{\beta}) - \mathrm{trd}(\alpha\bar{\beta})\gamma = 0$$

car $\mathrm{trd}(\alpha\bar{\beta}) \in \mathbb{Q}$, donc $E(\phi(\alpha)u, \phi(\beta)u) = -E(\phi(\beta)u, \phi(\alpha)u)$.

2. $E(iz, z')$ est symétrique : vu notre choix de u, $\phi(B \otimes \mathbb{R}) \cdot u = \mathbb{C}^2$, donc il existe $\eta \in B \otimes \mathbb{R}$ tel que $\eta^2 = -1$ et $\bar{\eta} = -\eta$. En notant que $i\phi(\alpha)u = \phi(\alpha\eta)u$, on obtient donc

$$E(i\phi(\alpha)u, \phi(\beta)u) = \mathrm{trd}(\gamma\alpha\eta\bar{\beta}) = \mathrm{trd}(\beta\eta\bar{\alpha}\gamma),$$

puis

$$E(i\phi(\alpha)u, \phi(\beta)u) - E(i\phi(\beta)u, \phi(\alpha)u) = \gamma \cdot \mathrm{trd}(\beta\eta\bar{\alpha}) - \mathrm{trd}(\beta\eta\bar{\alpha}) \cdot \gamma = 0$$

car $\mathrm{trd}(\beta\eta\bar{\alpha}) \in \mathbb{Q}$.

3. $E(iz, z')$ est définie positive : comme ci-dessus on a
$$E(i\phi(\alpha)u, \phi(\alpha)u) = \mathrm{trd}(\gamma\alpha\eta\bar{\alpha}) = \mathrm{trd}(\alpha\eta\bar{\alpha}\gamma).$$
Soit $s \in \mathbb{R}$ positif tel que $\gamma^2 = -s^2$. On a $(\gamma^{-1}s)^2 = -1$, donc par le théorème des automorphismes intérieurs il existe $\delta \in B \otimes \mathbb{R}$ tel que
$$\gamma^{-1}s = \delta^{-1}\eta\delta.$$
Pour tout $\mu \in B^\times$, notons $\mu^* = \gamma^{-1}\bar{\mu}\gamma$. Comme $\gamma^2 < 0$, un lemme de Lang implique que l'application
$$\mu \mapsto \mathrm{trd}(\mu\mu^*)$$
est définie positive. Maintenant, le terme $\mathrm{trd}(\alpha\eta\bar{\alpha}\gamma)$ est égal à
$$s \cdot \mathrm{trd}(\alpha\delta\gamma^{-1}\delta^{-1}\bar{\alpha}\gamma) = s \cdot \mathrm{trd}(\alpha\delta\gamma^{-1}\delta^{-1}\bar{\delta}^{-1}\bar{\delta}\bar{\alpha}\gamma) = s \cdot \mathrm{nrd}(\delta)^{-1}\mathrm{trd}((\alpha\delta)(\alpha\delta)^*),$$
donc en remplaçant si besoin est E par $c \cdot E$ pour un réel c tel que $c \cdot \mathrm{nrd}(\delta)^{-1} > 0$, on obtient que E est définie positive.
4. E est entière : comme $\mathcal{O}$ est un $\mathbb{Z}$-module de dimension 4, il suffit de considérer $c \cdot E$, où c est un entier tel que les $c \cdot E(\gamma\alpha_i\beta_j)$, pour des éléments α_i et β_j parcourant une $\mathbb{Z}$-base de $\mathcal{O}$, soient à valeurs entières. Notons que l'on prendra garde au signe de c pour que $c \cdot E$ soit définie positive.
5. E s'étend en une forme sesquilinéaire. On a
$$E(i\phi(\alpha)u, i\phi(\beta)u) = E(\gamma\alpha\eta\bar{\eta}\bar{\beta}) = \mathrm{nrd}(\eta)E(\phi(\alpha)u, \phi(\beta)u) = E(\phi(\alpha)u, \phi(\beta)u),$$
car $\mathrm{nrd}(\eta) = 1$.

Corollaire 1.4. *Le quotient $\mathbb{C}^2/\Lambda_u$ est une surface abélienne principalement polarisée.*

PREUVE. Il reste à montrer que la polarisation donnée par E est principale. Pour cela, considérons une base $b_1, \ldots, b_4$ de $\mathcal{O}$. Les vecteurs $\phi(b_i) \cdot u$ forment une base de Λ_u, donc on peut évaluer le déterminant de E sur cette base. On peut supposer que γ vérifie $\gamma^2 = -1/D$. On obtient :
$$\begin{aligned}\det(E(\phi(b_i)u, \phi(b_j)u) &= \det(\mathrm{trd}(\gamma b_i\bar{b}_j)) \\ &= \mathrm{nrd}(\gamma)^2 \det(\mathrm{trd}(b_i\bar{b}_j)) \\ &= D^{-2}\mathrm{Disc}(\mathcal{O})^2 \\ &= D^{-2}D^2 \\ &= 1,\end{aligned}$$
ce qui montre que la polarisation induite par E est principale. □

La preuve montre que le choix de γ est fondamental : le fait que γ^2 soit négatif est nécessaire pour que $E(iz, z')$ soit définie positive, et le fait que $\gamma^2 = -1/D$ est nécessaire pour que E induise une polarisation principale.

Finalement, nous décrivons les isomorphismes entre deux variétés abéliennes construites comme ci-dessus. Soit

$$u = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}.$$

D'après le théorème des normes d'Eichler,

$$\mathrm{nrd}(\mathcal{O}^\times) = \mathbb{Z}^\times.$$

Prenons $\epsilon \in \mathcal{O}^\times$ tel que $\mathrm{nrd}(\epsilon) = 1$ si u_1/u_2 est dans $\mathcal{H}$, et ϵ tel que $\mathrm{nrd}(\epsilon) = -1$ sinon. Alors

$$\phi(\epsilon) \cdot u = \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$$

avec $\tau = \omega_1/\omega_2 \in \mathcal{H}$, et on a un isomorphisme

$$\mathbb{C}/\Lambda_u \overset{\cong}{\to} \mathbb{C}/\Lambda_{u'}, \text{ où } u' = \begin{pmatrix} \tau \\ 1 \end{pmatrix},$$

défini pour tout $z \in \mathbb{C}^2$ par

$$z \mapsto \omega_2^{-1}\phi(\epsilon)z.$$

On peut donc se ramener au cas où

$$u = \begin{pmatrix} \tau \\ 1 \end{pmatrix} \text{ et } u' = \begin{pmatrix} \tau' \\ 1 \end{pmatrix}$$

pour deux éléments $\tau, \tau' \in \mathcal{H}$. On note $A_\tau = A_u$ et $\Lambda_\tau = \Lambda_u$.

Le plongement ϕ étant fixé, considérons un homomorphisme

$$\psi : (A_\tau, \phi) \to (A_{\tau'}, \phi)$$

qui commute avec ϕ. Un tel morphisme ψ peut être représenté par une matrice complexe $M \in \mathrm{M}_2(\mathbb{C})$ qui commute avec $\phi(\alpha)$ pour tout $\alpha \in \mathcal{O}$. Ainsi

$$M = m \cdot \mathrm{Id}$$

pour un élément $m \in \mathbb{C}$. Supposons que $\psi \neq 0$. Comme $M\Lambda_\tau \subset \Lambda_{\tau'}$, il existe $\lambda \in \mathcal{O}$ tel que

$$M \cdot \begin{pmatrix} \tau \\ 1 \end{pmatrix} = m \cdot \begin{pmatrix} \tau \\ 1 \end{pmatrix} = \phi(\lambda) \cdot \begin{pmatrix} \tau' \\ 1 \end{pmatrix}.$$

Notons

$$\phi(\lambda) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

On obtient

$$m \cdot \begin{pmatrix} \tau \\ 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} \tau' \\ 1 \end{pmatrix} = (c\tau' + d) \cdot \begin{pmatrix} \phi(\lambda) \cdot \tau' \\ 1 \end{pmatrix},$$

d'où

$$c\tau' + d = m \text{ et } \tau = \phi(\lambda) \cdot \tau'.$$

Vu que les parties imaginaires de τ et τ' ont le même signe, on voit alors que

$$\mathrm{nrd}(\lambda) = \det \phi(\lambda) > 0.$$

Théorème 1.5. *Soient $\tau, \tau' \in \mathcal{H}$. Deux triplets (A_τ, ϕ, E) et $(A_{\tau'}, \phi, E')$ sont isomorphes si et seulement s'il existe un élément $\lambda \in \mathcal{O}^\times$ de norme réduite 1 tel que $\phi(\lambda)\tau' = \tau$, et tous les isomorphismes sont décrits par les $\phi(\epsilon)$.*

Preuve. Supposons que ψ est un isomorphisme ; on a donc $M\Lambda_\tau = \Lambda_{\tau'}$. De manière équivalente

$$\phi(\mathcal{O})\phi(\lambda) = \phi(\mathcal{O}),$$

ou encore $\mathcal{O}\lambda = \mathcal{O}$, ce qui signifie que λ est une unité, donc $\mathrm{nrd}(\lambda) = 1$. Nous avons déjà vu que $\phi(\lambda) \cdot \tau' = \tau$.

Inversement, étant donné un élément $\lambda \in \mathcal{O}^\times$ tel que $\phi(\lambda) \cdot \tau' = \tau$, notons

$$\phi(\lambda) = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

et $m = c\tau' + d$. On a donc

$$\phi(\lambda) \cdot \begin{pmatrix} \tau' \\ 1 \end{pmatrix} = m \cdot \begin{pmatrix} \tau \\ 1 \end{pmatrix}.$$

Comme λ est une unité, $m.\Lambda_\tau = \Lambda_{\tau'}$ et λ induit ainsi un isomorphisme.

Il reste à vérifier qu'un isomorphisme préserve la polarisation. La polarisation associée au morphisme décrit par M vérifie

$$\begin{aligned} E(\phi(\alpha) \cdot (M \cdot u), \phi(\beta) \cdot (M \cdot u)) &= E(\phi(\alpha\lambda)u', \phi(\beta\lambda)u') \\ &= \mathrm{trd}(\gamma\alpha\lambda\bar{\lambda}\bar{\beta}) \\ &= \mathrm{nrd}(\lambda)E'(\phi(\alpha)u', \phi(\beta)u') \\ &= E'(\phi(\alpha)u', \phi(\beta)u'), \end{aligned}$$

qui est bien la polarisation de $A_{\tau'}$. □

On définit le groupe

$$\mathcal{O}^1 = \{x \in \mathcal{O} : \mathrm{nrd}(x) = 1\},$$

et son image

$$\Gamma^1 = \phi(\mathcal{O}^1) \subset \mathrm{SL}_2(\mathbb{R}).$$

On voit donc que les classes d'isomorphisme de triplets (A_τ, ϕ, E) sont paramétrisées par le quotient $\Gamma^1 \backslash \mathcal{H}$.

2 Compacité du quotient $\Gamma \backslash \mathcal{H}$

Le groupe Γ^1 est un *groupe Fuchsien du premier ordre*, c'est-à-dire qu'il est discret et que le quotient $\Gamma^1 \backslash \mathcal{H}$ est de volume fini. On a le théorème fondamental suivant (voir par exemple Katok pour une preuve).

Théorème 2.1. *Supposons que $B \neq \mathrm{M}_2(\mathbb{Q})$. Alors le quotient $\Gamma^1 \backslash \mathcal{H}$ est compact.*

Le quotient $\Gamma^1\backslash\mathcal{H}$ est donc une surface de Riemann compacte, à laquelle on peut également donner une structure de courbe algébrique projective, lisse et irréductible appelée *courbe de Shimura*.

Si $B = \mathrm{M}_2(\mathbb{Q})$, le cas des courbes modulaires, le résultat n'est plus vrai, et il faut alors compactifier en considérant l'action de B sur les *pointes* $\mathbb{P}^1(\mathbb{Q})$. On considère alors l'ensemble

$$\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$$

et le quotient $\Gamma^1\backslash\mathcal{H}^*$.