VARIÉTÉS ABÉLIENNES

∼

Université P. & M. Curie

.

Master M2 2010-2011

∼

D. Bertrand

Plan

Références

O. Debarre : *Tores et variétés abéliennes complexes* ; SMF, 1999.

M. Hindry, J. Silverman : *Diophantine geometry* ; Springer, 2000.

H. Lange, C. Birkenhake : *Complex abelian varieties* ; Springer, 1992.

D. Mumford : *Abelian varieties* ; Oxford UP, 1970

Table des matières

Chapitre I

Jacobiennes (non rédigé)

Chapitre II

Variétés abéliennes complexes

Université de Paris VI — Master M2 2010-2011

D. Bertrand — *Variétés abéliennes*

CHAPITRE II

VARIÉTÉS ABÉLIENNES SUR $\mathbb{C}$

II.1 Tores complexes et structures de Hodge

Dans un e-v. V sur $\mathbb{R}$, de dimension finie m, un réseau Γ de V est un sous-groupe discret de V engendrant V sur $\mathbb{R}$ $\Leftrightarrow$ un sous-$\mathbb{Z}$-module libre engendré sur $\mathbb{Z}$ par une base de V de $\mathbb{R}$. Alors, $X := V/\Gamma$ est naturellement muni d'une structure de groupe de Lie réel de dimension m, commutatif et compact. Inversement, tout groupe de Lie commutatif connexe réel est le quotient de son algèbre de Lie $Lie(X) \simeq V$ par le noyau Γ de exp_X, et il n'y a à isomorphisme près qu'un groupe de Lie réel commutatif connexe et compact de dimension m : le tore réel $\mathbb{U}_1^m$, où $\mathbb{U}_1 \simeq \mathbb{R}/\mathbb{Z} \simeq \mathbb{S}_1$.

Un réseau d'un e-v. V sur $\mathbb{C}$, de dimension g sur $\mathbb{C}$, est un réseau Γ de l'e-v réel (de dimension $2g$) sous-jacent. Alors, $X := V/\Gamma$ est naturellement muni d'une structure de groupe de Lie complexe de dimension g, commutatif et compact. Inversement, tout groupe de Lie complexe connexe et compact X est automatiquement commutatif, et est donc le quotient de son algèbre de Lie $Lie(X) \simeq V$ (qui est un $\mathbb{C}$-e-v) par le noyau Γ de exp_X, qui en est un réseau, autrement dit X est un tore complexe. Le cas $g = 1$ (cours de J. Nekovář) montre qu'il y a beaucoup de classes d'isomorphismes de tores complexes. Plus précisément, en notant que V est le revêtement universel de $X = V/\Gamma$, on a dans la catégorie des groupes de Lie complexes :

Théorème II.1.1. $Hom_{Lie/\mathbb{C}}(V'/\Gamma', V/\Gamma) \simeq \{\phi \in End_{\mathbb{C}}(V', V), \phi(\Gamma') \subset \Gamma\}$. *Mieux, tout morphisme de variétés analytiques complexes $f : V'/\Gamma' \to V/\Gamma$ tel que $f(0) = 0$ est un homomorphisme de groupes. Et toute variété analytique Y, munie d'un morphisme $f : Y \to V/\Gamma$ qui est un revêtement étale fini, admet une structure de tore complexe telle que f soit un homomorphisme.*

Pour comprendre comment varient ces classes d'isomorphismes, on peut donc :

* soit fixer le $\mathbb{C}$-e-v ambiant $V = \mathbb{C}^g$, et regarder ses différents réseaux Γ ;

* soit fixer le réseau $\Gamma = \mathbb{Z}^{2g}$, et regarder les différentes structures complexes que porte le $\mathbb{R}$-e-v. $\Gamma \otimes_{\mathbb{Z}} \mathbb{R}$.
Rappelons qu'une structure complexe sur un e-v. $V/\mathbb{R}$ est la donnée d'un homomophisme de $\mathbb{R}$-algèbres $\mathbb{C} \to End_{\mathbb{R}}(V)$ sur V (l'image J de i vérifiant donc $J^2 = -id_V$).

Definition II.1.2. *soient n un entier et Γ un $\mathbb{Z}$-module libre de type fini. On appelle* structure de Hodge *(entière et pure) de poids n sur Γ la donnée d'une décomposition de $W = \Gamma \otimes_{\mathbb{Z}} \mathbb{C}$ en $\mathbb{C}$-ss-evs de la forme $W = \oplus_{p+q=n} W^{p,q}$ tels que pour tout (p,q), $W^{q,p} = \overline{W^{p,q}}$.*

Une structure de Hodge sur Γ revient à la donnée d'une action du groupe algébrique réel

$$\mathbb{S} := Res_{\mathbb{C}/\mathbb{R}} \mathbb{G}_{m/\mathbb{C}} \simeq \{Z = \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \in GL_{2/\mathbb{R}}\}$$

sur $V = \Gamma \otimes_{\mathbb{Z}} \mathbb{R}$, soit $h : \mathbb{S} \to GL_{\mathbb{R}}(V)$, vérifiant la condition suivante : la restriction de h au sous-groupe $\mathbb{G}_{m/\mathbb{R}}(\mathbb{R}) = \mathbb{R}^*$ de $\mathbb{S}(\mathbb{R}) \simeq \mathbb{C}^*$ est isotypique, et donnée par le caractère $r \mapsto r^{-n}$. Posant pour tout couple (p,q) d'entiers rationnels :

$$W^{p,q} = \{w \in W = V \otimes_{\mathbb{R}} \mathbb{C}, \forall (z_1, z_2) \in \mathbb{S}(\mathbb{C}) \simeq \mathbb{C}^* \times \mathbb{C}^*, h(z_1, z_2).w = z_1^{-p} z_2^{-q} w\}$$

$$= \{w \in W = V \otimes_{\mathbb{R}} \mathbb{C}, \forall z \in \mathbb{C}^* \simeq \mathbb{S}(\mathbb{R}), h(z).w = z^{-p} \overline{z}^{-q} w\},$$

on a bien $W^{p,q} = 0$ pour $p+q \neq n$, et $W^{q,p} = \overline{W^{p,q}}$. En particulier, l'opérateur de Weil $C := h(i)$ agit sur $W^{p,q}$ par mutiplication par i^{q-p}, et C^2 par multiplication par $(-1)^n$.

À une structure de Hodge de poids n sur Γ est associée la filtration de Hodge décroissante $F^\bullet W$, donnée par $F^p W := \oplus_{p' \geq p} W^{p', n-p'}$. Elle vérifie $F^p W \oplus \overline{F^q W} = W$ si $p + q = n + 1$. Inversement, toute telle filtration fournit une structure de Hodge de poids n, définie par $F^p W \cap \overline{F^q W} = W^{p,q}$ si $p + q = n$.

Un morphisme entre deux structures de Hodge de même poids est un morphisme $\phi : \Gamma \to \Gamma'$ entre les $\mathbb{Z}$-modules sous-jacents tel que $\phi \otimes 1 : W \to W'$ respecte les décompositions données. De façon équivalente, ϕ commute aux actions h, h' de $\mathbb{S}$ sur V, V'.

La donnée d'une structure complexe sur $V = \Gamma \otimes_{\mathbb{Z}} \mathbb{R}$ équivaut à celle d'une structure de Hodge de poids -1, type $(-1,0), (0,-1)$ sur $W = V \otimes_{\mathbb{R}} \mathbb{C}$:

l'actions de l'opérateur $C \otimes 1 = iId_{W^{-1,0}} \oplus (-i)Id_{W^{0,-1}}$ fournies par une telle structure de Hodge définit un unique homomorphisme de $\mathbb{R}$-algèbre de $\mathbb{C}$ dans $End_{\mathbb{R}}(V)$; inversement, tout $J \in End(V/\mathbb{R})$ de carré $-id_V$ se diagonalise sur $W = V \otimes_{\mathbb{R}} \mathbb{C}$, et si $W^{-1,0}, W^{0,-1}$ désignent les ss-espaces propres pour les valeurs propres $i, -i$ de $J \otimes 1$, ils sont bien complexes conjugués et en somme directe dans W. La projection $\pi : W \to W/W^{0,-1}$ induit alors un $\mathbb{C}$-isomorphisme du $\mathbb{C}$-e-v. V sur $W^{-1,0}$ envoyant le réseau Γ de V sur un réseau $\pi(\Gamma)$ de $W^{-1,0}$, et les tores complexes $X = V/\Gamma$ et $W^{-1,0}/\pi(\Gamma)$ sont isomorphes. On a donc un isomorphisme canonique $Lie(X) \simeq W^{-1,0}$, qui, joint au théorème 1.1 entraîne :

Théorème II.1.3. *: la construction précédente établit une équivalence entre la catégorie des tores complexes et la catégorie des structure de Hodge entières de type* $(-1,0),(0,-1)$.

Plus généralement, toute structure de Hodge entière de poids $n = 2m-1$ impair fournit naturellement un tore complexe : en effet, la filtration $F^\bullet(W)$ de $W = \Gamma \otimes \mathbb{C}$ vérifie alors $W = F^m \oplus \overline{F^m}$, avec $rk_{\mathbb{Z}}(\Gamma) = 2dim_{\mathbb{C}} F^m$. De plus, les éléments v du $\mathbb{R}$-e-v. $V = \Gamma \otimes_{\mathbb{Z}} \mathbb{R} \subset W$ s'écrivent $v = w \oplus \overline{w}$ dans cette décomposition, de sorte que $V \cap \overline{F^m} = 0$, et l'image de Γ par la projection $\pi : W \to W/\overline{F^m} \simeq F^m$ est un réseau du $\mathbb{C}$-e-v. F^m.

Constructions tensorielles, dual, structure de Hodge de Tate : c'est $\mathbb{Z}(1) = 2i\pi\mathbb{Z} \subset \mathbb{C} = W$, avec $W = W^{-1,-1}$, donc de poids -2, munie de $h(z) = z\overline{z}$. Sommes directes de structures de Hodge pures de poids différents. Éléments de type (p,q) ; ceux de type $(0,0)$ sont appelés des classes de Hodge (et ceux de type (p,p) s'en déduisent après tensorisation par $\mathbb{Z}(-p)$). Si Γ, Γ' sont munis de structures de Hodge, les structures de Hodge naturelles sur $W^* \otimes W'$ et sur $H = Hom(W, W')$ coincident, et un élément ϕ de $Hom(\Gamma, \Gamma')$ est un morphisme de structures de Hodge si et slt si $\phi_{\mathbb{R}}$ commute aux actions h, h' de $\mathbb{S}$, i.e. si et slt si $\phi \in H^{0,0}$ est une classe de Hodge.

Groupe de Mumford-Tate

Dans tout ce qui précède, on peut remplacer $\mathbb{Z}$ par un sous-anneau k de $\mathbb{R}$, d'où la notion de k-structures de Hodge. Pour $k = \mathbb{Q}$, le théorème 1.3 devient une équivalence entre la catégorie des tores complexes à isogénie près et la catégorie des structures de Hodge rationelles de type $(-1,0),(0,-1)$.

Soit $h : \mathbb{S} \to GL(V/\mathbb{R})$ une structure de Hodge sur un $\mathbb{Q}$-e-v Γ de dimension (finie) m. Le groupe de Mumford-Tate de cette structure de Hodge est par définition le plus petit sous-groupe algébrique G de $GL(\Gamma) \simeq GL_{m/\mathbb{Q}}$, défini sur $\mathbb{Q}$ et tel que $G(\mathbb{R}) \subset GL_m(\mathbb{R}) \simeq GL(V/\mathbb{R})$ contienne $h(\mathbb{S}(\mathbb{R}))$. Il est donc connexe. Il contient le groupe $\mathbb{G}_{m/\mathbb{Q}}$ des homothéties si h est pure de poids $n \neq 0$, et il est contenu dans $SL_{m/\mathbb{Q}}$ si $n = 0$.

Le groupe de Mumford-Tate G agit sur toutes les constructions tensorielles $T^{a,b} = \Gamma^{*a} \otimes \Gamma^b$ de Γ, et sur leurs sommes directes, et l'on a :

Proposition II.1.4. *Un $\mathbb{Q}$-sous-espace d'une construction tensorielle de Γ en est une sous-structure de Hodge si et seulement s'il est stable sous l'action de G.*

Le théorème 1.3 conduit à la

Definition II.1.5. *Soit $X = V/\Gamma$ un tore complexe. On appelle groupe de Mumford-Tate $MT(X)$ le groupe de Mumford-Tate de la $\mathbb{Q}$-structure de Hodge associée à la classe d'isogénie de X.*

Comme on (ne) le verra (pas) aux chap. IV et VI, ce groupe contrôle les représentations galoisiennes attachées aux variétés abéliennes sur les corps de nombres et les groupes de monodromie attachés aux schémas abéliens.

II.2 Formes différentielles et fibrés

Soit k un corps algébriquement clos. Une *variété abélienne* sur k est un groupe algébrique A/k propre sur k, ce qui entraîne automatiquement que A est commutatif. En particulier, pour $k = \mathbb{C}$, le groupe de Lie A^{an} que définit $A(\mathbb{C})$ est un tore complexe.

On dit qu'un tore complexe X est *polarisable* s'il existe un plongement j de la variété analytique X dans un espace projectif $\mathbb{P}_N(\mathbb{C})$. Comme $j(X)$ est compacte, le théorème de Chow affirme alors que c'est l'ensemble des points complexes d'une sous-variété algébrique fermée A de $\mathbb{P}_{N/\mathbb{C}}$, et que sa structure de groupe de Lie provient d'une structure de groupe algébrique sur $\mathbb{C}$, de sorte que A est une variété abélienne complexe (qu'on identifiera à X). De plus, le théorème GAGA de Serre permet d'identifier le groupe $Pic(A)$ des classes d'isomorphismes de fibrés (algébriques) sur A au groupe $Pic(X)$ des classes d'isomorphismes de fibrés (analytiques) sur X.

En dimension 1, tout tore complexe est isomorphe à une cubique lisse de $\mathbb{P}_2(\mathbb{C})$ et est donc polarisable. En dimension supérieure, cela impose des conditions, dite de Riemann, que la plupart des tores V/Γ ne satisfont pas.

Definition II.2.1. *: soit Γ un réseau d'un $\mathbb{C}$-e-v. V. Une* forme de Riemann *sur Γ est une forme hermitienne définie positive H sur V telle que $Im(H)$ prenne des valeurs entières sur $\Gamma \times \Gamma$.*

Rappelons qu'une forme hermitienne $H(u,v) = B(u,v) + iE(u,v)$ est antilinéaire en u, que $E = ImH$ est alors une forme alternée sur V, et que $B = ReH$ est $\mathbb{R}$-bilinéaire symétrique (et définie positive si H l'est). La donnée de H équivaut à celle d'une forme alternée $E : \wedge^2\Gamma \to \mathbb{Z}$ dont l'extension $\mathbb{R}$-linéaire à V vérifie

$$\forall (u,v) \in V : E(iu,iv) = E(u,v), \text{ et } E(u,iu) > 0 \text{ si } u \neq 0.$$

(Poser $B(u,v) = E(u,iv)$ et $H(u,v) = E(u,iv) + iE(u,v)$; une telle E s'appelle aussi une forme de Riemann.)

Théorème II.2.2. *Un tore complexe $X = V/\Gamma$ est une variété abélienne si et seulement si le réseau Γ admet une forme de Riemann.*

Voici une traduction de cette condition en termes de

Structures de Hodge polarisables : soient $\Gamma := (\Gamma, F^\bullet(W))$ une structure de Hodge de poids n, et $C = h(i)$ l'opérateur de Weil correspondant. Une polarisation de Γ est un morphisme de structures de Hodge $\psi : \Gamma \otimes \Gamma \to \mathbb{Z}(-n)$ telle que la forme $\mathbb{R}$-bilinéaire sur $V = \Gamma \otimes_{\mathbb{Z}} \mathbb{R}$:

$$B : (u,v) \mapsto B(u,v) := (2i\pi)^n \psi(u \otimes Cv)$$

soit symétrique et définie positive. Si n est impair (resp. pair), cela impose que ψ soit alternée (resp. symétrique). Via l'isomorphisme canonique $Hom(\Gamma \otimes \Gamma, \mathbb{Z}(-n)) \simeq \Gamma^* \otimes \Gamma^*(-n)$, on peut voir ψ comme un tenseur de type $(0,0)$. On obtient ainsi une équivalence de catégories

$$\begin{gathered}\{ \text{ variétés abéliennes sur } \mathbb{C} \text{ à isogénie près } \} \\ \Updownarrow \\ \{ \text{ structures de Hodge sur } \mathbb{Q} \text{ de type } (-1,0),(0,-1) \text{ polarisables. } \}\end{gathered}$$

Pour une telle variété abélienne $X = V/\Gamma$, la droite engendrée par la classe rationnelle $E := \frac{1}{2i\pi}\psi$ est stable sous le groupe de Mumford-Tate $MT(X)$, qui est donc contenu dans le groupe $\mathbb{G}_m Sp_{2g/\mathbb{Q}}$ des similitudes symplectiques de Γ. L'hypothèse de positivité de B entraîne de plus que $MT(X)$ est un groupe réductif.

Nous allons montrer de deux façons que l'existence d'un plongement projectif $j : V/\Gamma \hookrightarrow \mathbb{P}_N(\mathbb{C})$ imposent à Γ de vérifier les conditions de Riemann.

2.1. Formes différentielles.

On dispose sur $\mathbb{P}_N(\mathbb{C}) = \mathbb{C}^{N+1}/\sim$ de la 2-forme de Fubini-Study :

$$\omega(z) = \frac{-1}{2i\pi}\partial\overline{\partial}\log(||z||^2),$$

qui ne dépend bien que de la classe de z dans $\mathbb{P}_N$, et qui est de type $(1,1)$, fermée et invariante sous l'action du groupe unitaire $\mathbf{U}_{N+1}$. De plus,

$*$ ω est entière : pour toute sous-variété fermée orientée $C \subset \mathbb{P}_N(\mathbb{C})$ de dimension réelle 2, l'intégrale $\int_C \omega \in \mathbb{Z}$. En effet, toute telle C est homologue à un multiple d'une droite projective $\mathbb{P}_1 \subset \mathbb{P}_N$, et le calcul donne $\int_{\mathbb{P}_1(\mathbb{C})} \omega = 1$..

$*$ ω est définie positive : par invariance sous $\mathbf{U}_{N+1}$, il suffit de le verifier au point $[1 : 0 : ... : 0]$, où elle vaut $\frac{-1}{2i\pi}\Sigma_{k=1,\dots,N} dz_k \wedge d\overline{z}_k = \frac{1}{\pi}\Sigma_{k=1,\dots,N} dx_k \wedge dy_k$, donc est réelle et prend des valeurs positives sur les couples de vecteurs tangents de la forme (u, iu).

L'image réciproque de ω sous j est donc une une forme différentielle sur V/Γ fermée, de type $(1,1)$, définie positive et entière. Dans les coordonnées associées à une base de Γ, elle s'écrit : $j^*\omega = \Sigma_{1\leq i<j\leq 2g} a_{ij}(x) dx_i \wedge dx_j$, où les a_{ij} sont des fonctions C^∞ et Γ-périodiques, qui admettent donc un bon développement de Fourier $a_{ij}(x) = \Sigma_{k\in\mathbb{Z}^{2g}} a_{ij}^k e^{2i\pi k\cdot x}$. Je dis que la classe de cohomologie de $j^*\omega$ dans $H^2_{dR}(V/\Gamma)$ est donnée par sa moyenne (relativement à la mesure de Haar sur V/Γ) :

$$\tilde{\omega} := \Sigma_{1\leq i<j\leq 2g} a_{ij}^0 dx_i \wedge dx_j,$$

i.e. qu'il existe une 1-forme $\Sigma_i A_i(x) dx_i$ telle que $-\Sigma_{i,j;k\neq 0} a_{ij}^k e^{2i\pi k\cdot x} dx_i \wedge dx_j = d(\Sigma_{i;k\in\mathbb{Z}^n} A_i^k e^{2i\pi k\cdot x} dx_i)$, i.e. telle que $k_i A_j^k - k_j A_i^k = \frac{1}{2i\pi} a_{ij}^k$ pour tout $i < j, k \neq 0$. Pour que ce système soit résoluble, il suffit que pour tout i, j, m et $k \neq 0$, on ait : $k_m a_{ij}^k + k_i a_{jm}^k + k_j a_{mi}^k = 0$. C'est le cas, car comme $j^*\omega$ est fermée, $d(j^*\omega) = \Sigma_{i,j,m} \frac{\partial}{\partial x_m} a_{ij} dx_m \wedge dx_i \wedge dx_j = 0$, d'où $\frac{\partial}{\partial x_m} a_{ij} + \frac{\partial}{\partial x_i} a_{jm} + \frac{\partial}{\partial x_j} a_{mi} = 0$.

Dans ces conditions, notons $E \in \wedge^2_{\mathbb{R}} V^*$ la forme $\mathbb{R}$-bilinéaire alternée sur V que $\tilde{\omega}$ définit. Alors,

$*$ $\tilde{\omega}$ est encore entière : pour tout $\gamma \in H_2(X, \mathbb{Z})$, $\int_\gamma \tilde{\omega} = \int_{j_*\gamma} \omega \in \mathbb{Z}$. Autrement dit, pour tout $\gamma_i, \gamma_j \in \Gamma$, $\int_{\gamma_i\wedge\gamma_j} \tilde{\omega} = E(\gamma_i, \gamma_j) \in \mathbb{Z}$.

$*$ $\tilde{\omega}$ est fermée, et est de type $(1,1)$ comme moyenne sur $j(X)$ de formes de type $(1,1)$. Autrement dit, pour tout $u, v \in V$, $E(iu, iv) = E(u, v)$, et la forme $B(u, v) = E(u, iv)$ est symétrique.

$*$ $\tilde{\omega}$ est positive : pour tout $u \in V$, vu comme un vecteur tangent en tout point x de X, le nombre $B(u, u)$ est la moyenne sur $j(X)$ de la fonction $\omega_{j(x)}(j_* u, j_* u)$, qui est > 0.

Ainsi, le réseau Γ, muni de E, vérifie bien les conditions de Riemann.

2.2. Fibrés en droites (et diviseurs)

On dispose sur $\mathbb{P}_N(\mathbb{C}) = \mathbb{C}^{N+1}/\sim$ du fibré tautologique $\mathcal{O}(-1)$, dont le dual $\mathcal{O}(1)$ admet pour sections globales les formes linéaires sur $\mathbb{C}^{N+1}$. Plus généralement, pour tout $r > 0$, le système linéaire $|\mathcal{O}(r)|$ est l'ensemble des hypersurfaces de degré r de $\mathbb{P}_N(\mathbb{C})$. L'image inverse $j^*\mathcal{O}(1)$ de $\mathcal{O}(1)$ est un fibré en droites sur $X = V/\Gamma$.

Le groupe de Picard

Tout fibré en droites $\mathcal{L} \to X$ se relève sur le revêtement universel $V \simeq \mathbb{C}^g$ en un fibré trivial $\mathbb{C} \times V$, et $\mathcal{L}$ est le quotient de $\mathbb{C} \times V$ par une action du groupe $\pi_1(X) = \Gamma$ de la forme

$$\gamma.(t, z) = (e_\gamma(z)t, z + \gamma) \ , t \in \mathbb{C}, z \in V, \gamma \in \Gamma,$$

où les e_γ sont des fonctions holomorphes nulle part nulles sur V vérifiant la condition de cocyle

$$e_{\gamma_1+\gamma_2}(z) = e_{\gamma_1}(z + \gamma_2) e_{\gamma_2}(z).$$

Les sections holomorphes de $\mathcal{L}$ s'identifient aux fonctions holomorphes f sur V telles que

$$f(z + \gamma) = e_\gamma(z) f(z) \ , z \in V, \gamma \in \Gamma.$$

En particulier, si $q \in H^0(V, \mathcal{O}_V^*)$ ne s'annule nulle part, les cocycles $e_\gamma(z)$ et $e'_\gamma(z) = \frac{q(z+\gamma)}{q(z)} e_\gamma(z)$ définissent des fibrés isomorphes, et l'application

$$H^1(X, \mathcal{O}_X^*) \to H^1(\Gamma, H^0(V, \mathcal{O}_V^*))$$

ainsi construite est un isomorphisme[1]. Le terme de gauche

$$H^1(X, \mathcal{O}_X^*) = Pic(X)$$

est le groupe des classes d'isomorphismes de fibrés en droite sur X, appelé groupe de Picard $Pic(X)$ de X. Sous l'hypothèse (automatiquement vérifiée pour les variétés abéliennes) que tout fibré admet une section méromorphe non nulle, il s'identifie au groupe

$$H^0(X, \mathcal{M}_X^*/\mathcal{O}_X^*) = \frac{Div(X)}{Div_\ell(X)}$$

des classes d'équivalence rationnelle de diviseurs sur X, où $D \sim_\ell D'$ si $D - D'$ est le diviseur d'une fonction méromorphe sur X, i.e. $Div_\ell(X)$ est le groupe des diviseurs principaux. On note $\mathcal{O}_X(D)$ le fibré en droites associé à un diviseur D, de sorte que $H^0(X, \mathcal{O}_X(D)) \simeq \{f \text{ mérom. sur } X, div(f) \geq -D\}$.

Pour tout fibré $\mathcal{L}$, on appelle *première classe de Chern* de $\mathcal{L}$ son image $c_1(\mathcal{L})$ par l'application $H^1(X, \mathcal{O}_X^*) \to H^2(X, \mathbb{Z})$ donnée[2] par la suite exacte exponentielle $0 \to \underline{\mathbb{Z}} \to \mathcal{O}_X \to \mathcal{O}_X^* \to 0$. Si X est une courbe (pas forcément elliptique), $H^2(X, \mathbb{Z}) \simeq \mathbb{Z}$, et si $\mathcal{L} = \mathcal{O}_X(D)$, $c_1(\mathcal{L})$ s'identifie au degré du diviseur D. De façon générale, le noyau

$$Pic_0(X) = \{\mathcal{L} \in Pic(X), c_1(\mathcal{L}) = 0\}$$

est formé des classes d'isomorphismes de fibrés topologiquement triviaux. En termes de diviseurs, il s'identifie à $Div_a(X)/Div_\ell(X)$, où (lorsque X est une variété abélienne) $Div_a(X)$ désigne l'ensemble des diviseurs algébriquement équivalents à 0. Le quotient

$$NS(X) = \frac{Pic(X)}{Pic_0(X)} \simeq \frac{Div(X)}{Div_a(X)}$$

[1] Voici une description de la flèche inverse : on prend un recouvrement ouvert de X avec des $\{U_i\}$ assez petits, qu'on relève arbitrairement en des ouverts connexes V_i de V. Si z_i, z_j désignent les relevés dans V_i, V_j d'un point x de U_i, U_j, il existe un unique $\gamma_{ji} \in \Gamma$ tel que $z_j = z_i + \gamma_{ji}$. Alors, les $\{F_{ji}(x) := e_{\gamma_{ji}}(z_i), x \in U_i \cap U_j\}$ définissent un cocycle de Čech dont la classe dans $H^1(X, \mathcal{O}_X^*)$ ne dépend que de la classe de $e_\gamma(z)$ dans $H^1(\Gamma, H^0(V, \mathcal{O}_V^*))$.

[2] Si $\mathcal{L}$ est donnée par un 1-cocyle de Čech $F_{ij} = e^{2i\pi g_{ij}} \in \mathcal{O}_X^*(U_i \cap U_j)$, les $n_{ijk} = g_{ij} - g_{ik} + g_{jk}$ définissent un 2-cocycle de Čech sur X, à valeurs dans $\mathbb{Z}$, dont $c_1(\mathcal{L})$ est la classe dans $H^2(X, \underline{\mathbb{Z}}) \simeq H^2(X, \mathbb{Z})$.

s'appelle le groupe de Néron-Severi de X. Il s'injecte dans $H^2(X,\mathbb{Z})$, et est donc de type fini, puisque $H^2(X,\mathbb{Z}) \simeq \wedge^2 H^1(X,\mathbb{Z}) \simeq \wedge^2(Hom(\Gamma,\mathbb{Z}))$ l'est.

Normalisation des facteurs d'automorphie

Soit $\mathcal{L} \to X$ un fibré en droites, décrit par des 1-cocycles $e_\gamma(z)$. Comme V est simplement connexe, il existe des fonctions holomorphes $f_\gamma(z)$ sur V telles que $e_\gamma(z) = e^{2i\pi f_\gamma(z)}$, et $F(\gamma_1,\gamma_2) = f_{\gamma_2}(z+\gamma_1) - f_{\gamma_1+\gamma_2}(z) + f_{\gamma_1}(z)$ est un 2-cocycle de Γ à valeurs dans $\mathbb{Z}$. Mais alors,

$$E(\gamma_1,\gamma_2) = F(\gamma_1,\gamma_2) - F(\gamma_2,\gamma_1) = f_{\gamma_2}(z+\gamma_1) + f_{\gamma_1}(z) - f_{\gamma_1}(z+\gamma_2) - f_{\gamma_2}(z)$$

est une forme bilinéaire alternée sur Γ, qui ne dépend que de la classe de $e_\gamma(z)$ dans $H^1(\Gamma, H^0(V,\mathcal{O}_V^*))$. Elle représente la classe de Chern de $\mathcal{L}$ (voir Mumford, p. 18, [LB], II.1.2 et II.1.6) et son l'extension $\mathbb{R}$-linéaire à V vérifie $E(iu,iv) = E(u,v)$.

Vérifions cette dernière assertion en admettant que, comme on le verra au paragraphe suivant, on peut "linéariser les exposants des facteurs d'automorphie" de $\mathcal{L}$, autrement dit qu'il existe $q \in H^0(V,\mathcal{O}_V^*)$ tel que le cocycle $\frac{q(z+\gamma)}{q(z)}e_\gamma(z)$ prenne la forme

$$e_\gamma(z) = e^{2i\pi(L(\gamma,z)+J(\gamma))}, \text{ avec } \forall\gamma\in\Gamma, L(\gamma,.) \in Hom_{\mathbb{C}-lin}(V,\mathbb{C}), J(\gamma)\in\mathbb{C}.$$

Alors, les conditions de 1-cocyle de e_γ entraînent que

$$(**)\quad \begin{array}{l} L(\gamma_1+\gamma_2,z) = L(\gamma_1,z)+L(\gamma_2,z), \text{ d'où par } \mathbb{R}\text{-lin} : L : V\times V \to \mathbb{C}; \\ J(\gamma_1+\gamma_2) - J(\gamma_1) - J(\gamma_2) \equiv L(\gamma_1,\gamma_2)\ mod.\mathbb{Z}; \\ E(\gamma_1,\gamma_2) := L(\gamma_1,\gamma_2) - L(\gamma_2,\gamma_1) \in \mathbb{Z}, \text{ d'où par } \mathbb{R}\text{-lin} : E \in Hom(\wedge^2_{\mathbb{R}}V,\mathbb{R}). \end{array}$$

Ainsi, E est bien une forme $\mathbb{R}$-linéaire alternée sur V prenant des valeurs entières sur $\Gamma\times\Gamma$, donc à valeurs réelles, et $E(iu,iv) = E(u,v)$ puisque la différence est à la fois réelle, et imaginaire pure (par $\mathbb{C}$-linéarité de L en la deuxième variable).

Pour toute telle E, notons comme d'habitude $H(u,v) = E(u,iv)+iE(u,v)$ l'unique forme hermitienne sur V associée à E. Pour vérifier que notre fibré $j^*\mathcal{O}(1)$ impose des conditions de Riemann à Γ, une seconde normalisation des facteurs d'automorphie sera utile :

- l'expression $Q(u,z) = L(u,z) - \frac{1}{2i}H(u,z)$ est symétrique en (u,z), donc on peut tordre $e_\gamma(z)$ par $q(z) := e^{-i\pi Q(z,z)}$ pour imposer $L(\gamma,z) = \frac{1}{2i}H(\gamma,z)$;

- dans ces conditions, $J(\gamma_1+\gamma_2) - J(\gamma_1) - J(\gamma_2) \equiv \frac{1}{2i}H(\gamma_1,\gamma_2)\ mod.\mathbb{Z}$, donc $ImJ(\gamma) + \frac{1}{4}H(\gamma,\gamma) := \lambda(\gamma)$ s'étend en une forme $\lambda \in Hom_{\mathbb{R}-lin}(V,\mathbb{R})$, partie réelle d'une unique forme $\ell(z) = \lambda(z) - i\lambda(iz) \in Hom_{\mathbb{C}-lin}(V, \mathbb{C})$. En tordant $e_\gamma(z)$ par $q(z) = e^{2\pi\ell(z)}$, on obtient un nouveau facteur J tel que $ImJ(\gamma) = -\frac{1}{4}H(\gamma, \gamma)$.

En conclusion, le 1-cocyle $e_\gamma(z)$ est équivalent à un cocycle de la forme

$$e_\gamma(z) = \alpha(\gamma) e^{\pi H(\gamma,z) + \frac{\pi}{2} H(\gamma,\gamma)},$$

où α est un "quasi-caractère" de Γ pour E, i.e. une application $\alpha : \Gamma \to \mathbf{U}_1(\mathbb{C})$ telle que

$$\alpha(\gamma_1 + \gamma_2) = \alpha(\gamma_1)\alpha(\gamma_2) e^{i\pi E(\gamma_1, \gamma_2)}\ ,\ \gamma_1, \gamma_2 \in \Gamma.$$

On notera $\mathcal{L}(H, \alpha)$ tout représentant de la classe d'isomorphisme des fibrés attachés à un tel 1-cocyle.

Fonction theta

Revenons enfin au fibré $\mathcal{L} := j^*\mathcal{O}(1)$ fourni par le plongement projectif de X, et notons (H, α) des "caractéristiques" le représentant, i.e. $\mathcal{L} \simeq \mathcal{L}(H, \alpha)$. Nous allons montrer que la forme hermitienne H est nécessairement définie positive. En d'autre terme, le réseau Γ, muni de $E = Im(H)$, vérifie bien les conditions de Riemann.

Le système linéaire $|\mathcal{O}(1)|$ induit sur X un système linéaire $|\mathcal{L}|$ sans point de base : pour tout point x de X, il existe une section globale $s \in H^0(X, \mathcal{L})$ telle que $s(x) \neq 0$, autrement dit $\mathcal{L}$ est engendré par ses sections globales. Déduisons-en que H est ≥ 0, puis, du fait que j est injectif, qu'elle est non dégénérée, donc bien définie positive.

Les sections globales $\neq 0$ de $\mathcal{L}$ sont représentées par des fonctions holomorphes θ (dites *fonctions theta de caractéristiques* (H, α)), vérifiant pour tout $\gamma \in \Gamma$:

$$\theta(z + \gamma) = \alpha(\gamma) e^{\pi H(z,\gamma) + \frac{\pi}{2} H(\gamma,\gamma)} \theta(z),$$

de sorte que la fonction $\phi(z) = e^{-\frac{\pi}{2} H(z,z)} |\theta(z)|$ est Γ-périodique, donc borné, et $|\theta(z)| \leq c^{te} e^{\frac{\pi}{2} H(z,z)}$ pour tout $z \in V$. Supposons maintenant qu'il existe $u \in V$ non nul tel que $H(u, u) < 0$. Alors, la fonction $\theta(z)$ est nulle sur la droite $\mathbb{C}.u$. Ainsi, toutes les sections de $\mathcal{L}$ s'annulent aux points correspondant de X, contradiction. Soit par ailleurs N le noyau de H. Pour tout $z_0 \in V, u \in N$, $|\theta(z_0 + u)| \leq c^{te} e^{\frac{\pi}{2} H(z_0,z_0)}$, donc l'application holomorphe $u \to \theta(z_0 + u)$ est constante sur N, et les images par j des points de X correspondant à z_0 et $z_0 + u$ coïncident. Donc $N = 0$. (On peut en fait montrer que $\Gamma' = N \cap \Gamma$ est un réseau de N, de sorte que j se factorise à travers le tore quotient X/X', où $X' = N/\Gamma'$, et H induit une forme de Riemann sur ce quotient.)

Plus généralement, on appelle fonction theta pour le réseau Γ de V toute fonction holomorphe $\theta \neq 0$ vérifiant $\frac{\theta(z+\gamma)}{\theta(z)} = e_\gamma(z)$, où $e_\gamma(z) = e^{2i\pi(L(\gamma,z)+J(\gamma))}$ est un cocycle linéarisé, appelé type de θ. Elles représentent les sections du fibré correspondant à ce cocyle. Une fonction theta nulle part nulle est dite triviale, et s'écrit nécessairement sous la forme $e^{P(z)}$, où P est un polynôme de degré ≤ 2.

II.3 Variétés abéliennes

Nous montrons maintenant que les conditions de Riemann sur Γ entraînent que le tore $X = V/\Gamma$ admet un plongement j dans un espace projectif, et est donc une variété abélienne.

3.1 Le théorème de Riemann-Roch

Rappelons qu'une matrice antisymétrique de $Mat_{2g,2g}(\mathbb{Z})$ est conjuguée sous $GL_{2g}(\mathbb{Z})$ à une matrice de la forme $\begin{pmatrix} 0 & \Delta \\ -\Delta & 0 \end{pmatrix}$, où Δ est une matrice diagonale à coefficients entiers $d_1|d_2|...|d_g$. En particulier, son déterminant est le carré de l'entier $d_1...d_g$, qu'on appelle son pfaffien.

Théorème II.3.1. - *Soit H une forme de Riemann pour Γ, et $Pf(E)$ le pfaffien de la forme alternée $E = Im(H)$. Pour tout quasi-caractère α relatif à E, l'ensemble des fonctions theta de caractéristiques (H, α), joint à la fonction nulle, forme un $\mathbb{C}$-espace vectoriel $H^0(X, \mathcal{L}(H, \alpha))$ de dimension $|Pf(E)|$.*

Comme H est non-dégénérée, ce pfaffien est non nul. Il existe donc une telle fonction theta, soit θ. L'espace vectoriel ci-dessus, formé de 0 et des fonctions θ' de mêmes facteurs d'automorphie $e_\gamma(z) = \alpha(\gamma)e^{\pi H(\gamma,z)+\frac{\pi}{2}H(\gamma,\gamma)}$ que θ, s'identifie à l'espace des sections holomorphes du fibré $\mathcal{L}(\theta) := \mathcal{L}(H, \alpha)$. En particulier, chaque θ'/θ induit une fonction méromorphe sur X, et une base de $H^0(X, \mathcal{L}(\theta))$ fournit une application $\phi_\theta : X \cdots \to \mathbb{P}_N(\mathbb{C})$, où $N = |Pf(E)| - 1$.

Corollaire II.3.2. (Lefschetz) - $\mathcal{L}(\theta)$ *est ample. Plus précisément,*
pour $n \geq 2$, $\mathcal{L}(\theta^n)$ est sans point de base, i.e. ϕ_{θ^2} est un morphisme.
Pour $n \geq 3$, $\mathcal{L}(\theta^n)$ est très ample, i.e. ϕ_{θ^3} est un plongement.

Preuve du corollaire : Pour tout u dans V, $\theta_u(z) := \theta(z-u)$ vérifie

$$\frac{\theta_u(z+\gamma)}{\theta_u(z)} = e^{\pi H(\gamma,z)+\frac{\pi}{2}H(\gamma,\gamma)}\alpha(\gamma)e^{-\pi H(\gamma,u)}$$

de sorte que :

$$\theta_u\theta_{-u} \in H^0(\mathcal{L}(\theta^2)), \theta_u\theta_v\theta_{-u-v} \in H^0(\mathcal{L}(\theta^3)).$$

(De façon générale, $\Pi_{i=1,\ldots,m}\theta_{u_i}(z) \in H^0(\mathcal{L}(\theta^m))$ si $\Sigma_{i=1,..,m}u_i = 0$.)

Comme θ n'est pas identiquement nul, il n'existe pas de point $z_0 \in V$ où $\theta_u\theta_{-u}$ s'annule pour tout $u \in V$, donc $\mathcal{L}(\theta^2)$ est sans point de base, et idem pour les puissances suivantes. Montrons maintenant que le morphisme $\phi = \phi_{\theta^3}$ est un plongement.

$*$ ϕ est injectif : soient $z_1, z_2 \in V$ tels que $\phi(z_1) = \phi(z_2)$. Alors, il existe $a \in \mathbb{C}^*$ tel que $\theta_u\theta_v\theta_{-u-v}(z_1) = a\theta_u\theta_v\theta_{-u-v}(z_2)$ pour tous $u, v \in V$. Par conséquent, la fonction $u \mapsto \phi(u) := \frac{\theta(z_1-u)}{\theta(z_2-u)}$ est une fonction theta triviale, donc de la forme $\phi(0)e^{2i\pi(Q(u,u)+R(u))}$. Clairement, $Q = 0$ et la forme $\mathbb{C}$-linéaire R vérifie $R(\gamma)-\frac{1}{2i}H(\gamma, z_1-z_2) \in \mathbb{Z}$, d'où $\theta(z_1-u) = \theta(z_2-u)\phi(0)e^{\pi H(z_1-z_2,u)}$. Ainsi, θ est une fonction theta pour $\Gamma' := \Gamma + \mathbb{Z}\zeta$, où $\zeta = z_2 - z_1$, admettant des caractéristiques de la forme (H, α'), pour un quasi-caractère α' relatif à E. Nécessairement, Γ' est d'indice fini d dans Γ, et chaque élément de $H^0(\mathcal{L}(\theta))$ est, de même, de type (H, α'') relativement à Γ' et à l'un des quasi-caractères α'', en nombre fini, étendant α à Γ'. Si $d > 1$, le pfaffien $Pf'(E)$ de E, vue comme forme alternée sur Γ', est strictement inférieur à $Pf(E)$; il découle alors du théorème 3.1 que la plupart des éléments de $H^0(\mathcal{L}(\theta))$ ne peuvent vérifier cette propriété. Donc $d = 1$, et $z_2 \equiv z_1$ mod. Γ.

$*$ ϕ est une immersion : sinon, il existe $z_0 \in V$ et un vecteur tangent $D = \Sigma_{i=1,\ldots,g}\alpha_i\frac{\partial}{\partial z_i}$ non nul que $d_{z_0}\phi$ envoie sur 0 dans $T_{\phi(z_0)}\mathbb{P}_N$. Il existe alors $\alpha_0 \in \mathbb{C}$ tel que

$$\forall\vartheta \in H^0(\mathcal{L}(\theta^3),\ \alpha_0\vartheta(z_0) + \Sigma_{i=1,\ldots,g}\alpha_i\frac{\partial\vartheta}{\partial z_i}(z_0) = 0.$$

Considérant les éléments ϑ de $H^0(\mathcal{L}(\theta^3)$ de la forme $\theta_u\theta_v\theta_{-u-v}$ comme plus haut, et posant $\psi = \frac{D\vartheta}{\vartheta}$, on obtient :

$$\forall u, v \in V\ ,\ \psi(z_0-u) + \psi(z_0-v) + \psi(z_0+u+v) = -\alpha_0.$$

Par conséquent, ψ est holomorphe sur V. Mais $\psi(z+\gamma) = \pi H(\gamma, D) + \psi(z)$, où $D = (\alpha_1, \ldots, \alpha_g) \in V$, donc ψ est une forme affine et l'extension $\mathbb{R}$-linéaire de $\gamma \mapsto \psi(\gamma) - \psi(0) = \pi H(\gamma, D)$ à V, à fois $\mathbb{C}$-lin. et $\mathbb{C}$-antilin., est nulle. Donc D appartient au noyau de H, contradiction.

Preuve du théorème : fixons une base symplectique $\{\gamma_1, ..., \gamma_g, \gamma'_1, ..., \gamma'_g\}$ de Γ pour E, i.e. $E(\gamma_i, \gamma_j) = E(\gamma'_i, \gamma'_j) = 0, E(\gamma_i, \gamma'_i) = d_i$, pour tout $1 \leq i, j \leq g$, et $E(\gamma_i, \gamma'_j) = 0$ pour $i \neq j$. Alors, $\Gamma_1 = \mathbb{Z}\gamma_1 \oplus ... \oplus \mathbb{Z}\gamma_g$ engendre V sur $\mathbb{C}$, sans quoi $V_1 := \Gamma_1 \otimes \mathbb{R}$ contiendrait un vecteur non nul v, ainsi que iv, et $H(v, v) = E(v, iv) \in E(V_1, V_1)$ serait nul. On fixera $\{e_1 = \frac{1}{d_1}\gamma_1, ..., e_g = \frac{1}{d_g}\gamma_g\}$ comme base de V sur $\mathbb{C}$.

Lemme II.3.3. *Soit H une forme de Riemann pour Γ. Relativement à la base $\{\frac{1}{d_1}\gamma_1, ..., \frac{1}{d_g}\gamma_g\}$ de V sur $\mathbb{C}$, le réseau Γ est représenté par $\Delta\mathbb{Z}^g \oplus \tau\mathbb{Z}^g$, où $\tau \in Mat_{g,g}(\mathbb{C})$ est une matrice symétrique dont la partie imaginaire $Im(\tau)$ est définie positive, et H est représentée par $(Im(\tau))^{-1}$.*

Preuve Par définition, les colonnes de $\tau := R + iT$ représentent $\gamma'_1, ..., \gamma'_g$, et E est représentée dans la base réelle $\{e_1, ..., e_g, ie_1, ...ie_g\}$ par

$$ {}^t\begin{pmatrix} \Delta & R \\ 0 & T \end{pmatrix}^{-1} \begin{pmatrix} 0 & \Delta \\ -\Delta & 0 \end{pmatrix} \begin{pmatrix} \Delta & R \\ 0 & T \end{pmatrix}^{-1} = \begin{pmatrix} 0 & T^{-1} \\ -{}^tT^{-1} & {}^tT^{-1}(R - {}^tR)T^{-1} \end{pmatrix} $$

De $E(iu, v) = -E(u, iv)$, on tire : ${}^tT^{-1} = T^{-1}$ et $R - {}^tR = 0$. Donc τ est symétrique, et H est représentée dans la base $\{e_1, ..., e_g\}$ par T^{-1}.

Comme deux fibrés isomorphes ont des espaces de sections globales isomorphes, on peut, pour établir le théorème 3.1, tordre les facteurs d'automorphie $e_\gamma(z) = e^{\pi H(\gamma,z)+\frac{\pi}{2}H(\gamma,\gamma)}\alpha(\gamma)$ par une fonction theta $e^{-\frac{\pi}{2}Q(z,z)-2i\pi\ell(z)}$ triviale. Choisissons la forme $\mathbb{C}$-bilinéaire symétrique Q de sorte que $H - Q$ s'annule sur $V_1 \times V_1$. Alors, $(H-Q)(u, v) = 0$ sur $V_1 \times V$ (par $\mathbb{C}$-linéarité en v), et pour $v \in V_1$, $(H - Q)(u, v) = (\overline{H} - Q)(v, u) = (\overline{H} - H)(v, u) = 2iE(u, v)$. Choisissons par ailleurs la forme linéaire ℓ de sorte que la restriction de α à Γ_1 (qui y induit un vrai caractère) soit égale à $e^{2i\pi\ell}$. Alors $\theta \in H^0(\mathcal{L}(H, \alpha))$ si et seulement si la fonction $\tilde{\theta}(z) := \theta(z)e^{-\frac{\pi}{2}Q(z,z)-2i\pi\ell(z)}$ vérifie :

$$\forall i = 1, ..., g, \ \tilde{\theta}(z + \gamma_i) = \tilde{\theta}(z)$$
$$\forall i = 1, ..., g, \ \tilde{\theta}(z + \gamma'_i) = c_i e^{-2i\pi d_i z_i}\tilde{\theta}(z),$$

où on a posé $z = z_1\gamma_1 + ... + z_g\gamma_g$ et où les c_i sont des constantes ne dépendant que de α et de γ'_i. Ces propriétés reviennent à demander que $\tilde{\theta}$ soit Γ_1-périodique, i.e. admette un développement de Fourier

$$\tilde{\theta}(z) = \Sigma_{k\in\mathbb{Z}^g} a_k e^{2i\pi(k_1z_1+...+k_gz_g)},$$

dont les coefficients vérifient

$$\forall k \in \mathbb{Z}^g, i = 1, ..., g : \; a_k \; e^{2i\pi\Sigma_{j=1,\dots,g} \frac{k_j}{d_j}\tau_{ji}} = c_i \; a_{k+d_i\epsilon_i}.$$

Par conséquent, ces fonctions $\tilde{\theta}$ sont entièrement déterminées par leurs coefficients d'indices $k_i = 0, ..., d_i - 1, i = 1, ..., g$, et forment un espace vectoriel $H^0(X, \mathcal{L}(\tilde{\theta}))$ de dimension $\leq d_1 ... d_g$. Inversement, les familles a_k définies par ces relations et ces conditions initiales vérifient

$$|a_k| \leq e^{2i\pi\Sigma_{i,j} \frac{k_i}{d_i}\frac{k_j}{d_j}\tau_{ij} + O(||k||)}.$$

Comme $Im(\tau)$ est définie positive, les séries de Fourier associées convergent sur tout compact, et $dim H^0(X, \mathcal{L}(\tilde{\theta})) = Pf(E)$.

Fonction theta de Riemann : pour $\Delta = \mathbf{I}_g$, et $a_0 = 1$, on appelle fonction theta de Riemann la fonction theta relative au réseau $\Gamma_\tau := \mathbb{Z}^g \oplus \tau\mathbb{Z}^g$ et à la forme de Riemann $(Im(\tau))^{-1}$

$$\theta(\tau, z) = \Sigma_{k \in \mathbb{Z}^g} e^{i\pi^t k\tau k + 2i\pi^t k.z}.$$

Pour tout $p, q \in \mathbb{Z}^g$, elle vérifie : $\theta(\tau, z+p+\tau q) = e^{-2i\pi^t q.z - i\pi^t q\tau q} \; \theta(\tau, z)$. Pour $a, b \in \mathbb{R}^g$, les fonctions $\theta \begin{bmatrix} a \\ b \end{bmatrix} (\tau, z) := \Sigma_{k \in \mathbb{Z}^g} e^{i\pi^t(k+a)\tau(k+a) + 2i\pi^t(k+a).(z+b)}$ sont aussi des fonctions theta pour ce réseau, mais elle ne sont Γ_1-périodiques que si $a \equiv 0$ mod. $\mathbb{Z}^g$

3.2 Le théorème d'Appell-Humbert

Soit $\mathcal{L}$ un fibré en droite sur un tore complexe $X = V/\Gamma$. En admettant que ses facteurs d'automorphie sont linéarisables, on a vu au paragraphe 2.2 que $\mathcal{L}$ est isomorphe à un fibré de la forme $\mathcal{L}(H, \alpha)$, où H est la forme hermitienne associée à la classe de Chern $c_1(\mathcal{L}) = E$ de $\mathcal{L}$, et α est un quasi-caractère relatif à E. Plus précisément, on a :

Théorème II.3.4. (Appell-Humbert) *pour tout fibré en droites $\mathcal{L}$ sur X, il existe un unique couple (H, α) formé d'une forme hermitienne H sur V pour laquelle $E = Im(H)$ prend des valeurs entières sur Γ, et d'un quasi-caractère α pour E, tel que $\mathcal{L}$ soit isomorphe à $\mathcal{L}(H, \alpha)$.*

Cette description de $Pic(X)$ par les "caractéristiques" $\{H, \alpha\}$ est compatible à sa structure de groupe, en ce sens que

$$\mathcal{L}(H, \alpha) \otimes \mathcal{L}(H', \alpha') \simeq \mathcal{L}(H + H', \alpha\alpha').$$

Si $\mathcal{L}$, représenté par (H, α), est dans $Pic_0(X)$, alors $E = 0$ (par définition), donc $H = 0$ et $\alpha = \chi$ est un vrai caractère de Γ. Vérifions que l'application

$$Hom(\Gamma, \mathbb{U}_1) \to Pic_0(X) : \chi \mapsto \mathcal{L}(0, \chi)$$

est bien un isomorphisme :

$*$ injectivité : si $\mathcal{L}(0, \chi)$ est trivial, il existe $q \in H^0(V, \mathcal{O}_V^*)$ telle que $\chi(\gamma) = \frac{q(z+\gamma)}{q(z)}$ pour tout γ, de sorte que $|q|$ est bornée sur V, et q est constante, donc $\chi = 1$.

$*$ surjectivité : puisque $H^1(X, \underline{\mathbb{C}})$ s'envoie surjectivement sur $H^1(X, \mathcal{O}_X) = Ker(c_1)$, un fibré topologiquement trivial $\mathcal{L}$ admet des facteurs d'automorphie e_γ constants, qui sont donc des homomorphismes de Γ dans $\mathbb{C}^*$. En remplaçant e_γ par son produit par $\frac{e^{\ell(z+\gamma)}}{e^{\ell(z)}} = e^{\ell(\gamma)}$, où ℓ est une forme $\mathbb{C}$-linéaire, on peut de plus imposer que $e_\gamma \in \mathbb{U}_1$, et $\chi : \gamma \mapsto e_\gamma$ vérifie bien $\mathcal{L}(0, \chi) \simeq \mathcal{L}$.

Plus généralement, soit H une forme hermitienne sur V de partie imaginaire E entière sur $\Gamma \times \Gamma$. En considérant le groupe fini $\Gamma/2\Gamma$, on peut construire une application $\alpha : \Gamma \to \mathbb{U}_1$ qui soit un quasi-caractère pour E. Des remarques précédentes, on déduit donc que l'application

$$Pic(X) \to \{\text{couples } (H, \alpha)\}$$

construite au §2.2 est injective, ce qui justifie l'assertion d'unicité du théorème 3.4, et que c'est un *isomorphisme* de groupes.

Dans cet isomorphisme, la classe de Chern[3] d'un fibré $\mathcal{L}$ est donné par $E = Im(H)$, et d'après le paragraphe précédent, $\mathcal{L}$ est ample si et seulement si H est définie positive.

[3] La classe de Chern de $\mathcal{L}$ peut aussi se calculer en fixant une métrique hermitienne $||\cdot||$ sur $\mathcal{L}$: pour toute section locale holomorphe s non nulle de $\mathcal{L}$, l'expression $\frac{1}{2i\pi}\partial\overline{\partial}\log||s(x)||^2$ ne dépend pas de s, et définit une forme réelle de type $(1,1)$, dont l'image dans $H^2_{dR}(X)$ s'identifie à $c_1(\mathcal{L})$ (voir [D], p. 58). Pour $\mathcal{L} = \mathcal{L}(H, \alpha)$, l'expression $||(z,t)|| = e^{-\frac{\pi}{2}H(z,z)}|t|$ est invariante sous l'action de Γ, et définit une métrique sur $\mathcal{L}$. La condition $t = 1$ fournit une section locale de $\mathcal{L}$, pour laquelle $\frac{1}{2i\pi}\partial\overline{\partial}\log e^{-\pi H(z,z)} = \frac{i}{2}\partial\overline{\partial}H(z,z)$, de sorte que $c_1(\mathcal{L})$ est bien représentée par $Im(H)$. De même, sur $\mathbb{P}_N(\mathbb{C})$, la forme de Fubini-Study représente la classe de Chern du fibré $\mathcal{O}(1)$. Enfin, pour $\mathcal{L} = \mathcal{O}_X(D)$, le diviseur D définit une forme linéaire sur $H^{2g-2}_{dR}(X) \simeq H^{2g-2}(X, \mathbb{C})$, dont le dual de Poincaré $\eta_D \in H^2(X, \mathbb{C})$ représente également $c_1(\mathcal{L})$.

Linéarisation des exposants des facteurs d'automorphie

Pour terminer la preuve du théorème 3.4, il reste à justifier que tout cocycle $e_\gamma(z)$ représentant un fibré $\mathcal{L}$ est équivalent à un cocycle de la forme $e^{2i\pi(L(\gamma,z)+J(\gamma))}$, où L est $\mathbb{C}$-linéaire en z. Nous allons le faire en supposant que $\mathcal{L}$ admet une section méromorphe, autrement dit, est de la forme $\mathcal{O}_X(D)$ pour un diviseur D sur X. D'après le théorème de préparation de Weierstrass, les anneaux locaux des variétés analytiques complexes sont factoriels, de sorte que tout diviseur D est différence de deux diviseurs effectifs. On peut donc supposer que D est effectif, i.e. donné, dans un recouvrement ouvert $\{U_\alpha\}$ suffisamment fin de X, par une collection de fonctions holomorphes $h_\alpha \in \mathcal{O}_X(U_\alpha)$ telles que $h_\alpha/h_\beta \in \mathcal{O}_X^*(U_\alpha \cap U_\beta)$ pour tout α, β. Noter que lorsque Γ admet une forme de Riemann H^+, ces réductions se déduisent plus simplement du fait que pour toute forme H de partie imaginaire $c_1(\mathcal{L})$ entière sur Γ et tout entier n suffisamment grand, $H = (H + nH^+) - nH^+$ est la différence de deux formes de Riemann, ce qui, joint au théorème 3.1, montre que tout diviseur est différence de deux diviseurs très amples.

On peut interpréter les facteurs $e_\gamma(z)$ de la façon suivante. L'image inverse de D sous $p : V \to X$ est un diviseur positif sur $\mathbb{C}^g$, donc c'est le diviseur d'une fonction holomorphe $\underline{\theta}$ sur $\mathbb{C}^g$. Alors, $\underline{\theta}$ relève une section holomorphe de $\mathcal{L}$, donc vérifie : $\underline{\theta}(z+\gamma) = e_\gamma(z)\underline{\theta}(z)$ pour tout $\gamma \in \Gamma$. Il s'agit donc de trouver une fonction $q = e^Q \in H^0(V, \mathcal{O}_V^*)$ telle que $\theta(z) = \frac{q(z+\gamma)}{q(z)}\underline{\theta}(z)$ soit une fonction theta.

Partons de la description (U_α, h_α) de D. Les formes $\omega_\alpha = d\log(\frac{h_\alpha}{h_\beta})$ définissent par partition C^∞ de l'unité des formes $\omega_\alpha = \Sigma_\gamma \varphi_\gamma \omega_{\alpha\gamma}$ de type $(1,0)$ telles que $\omega_{\alpha\beta} = \omega_\alpha - \omega_\beta$. Les $d\omega_\alpha$ se recollent alors en une 2-forme fermée sans terme de type $(0,2)$, et le raisonnement du §2.1 montre qu'elle est cohomologue à une forme constante η sans terme de type $(0,2)$: il existe une 1-forme ω_0 sur X, qu'on peut supposer de type $(1,0)$, telle que $d\omega_\alpha = \eta + d\omega_0$. Comme $p^*\eta$ est constante, il existe une $(1,0)$-forme ω_1 de la forme $\omega_1 = \Sigma_{j=1,\dots,g}\lambda_j(z)dz_j$, où les $\lambda_j \in Hom_{\mathbb{R}-lin}(V, \mathbb{C})$, telle que $p^*\eta = d\omega_1$. La forme $p^*(\omega_\alpha - \omega_0) - \omega_1$ est fermée sur U_α, donc de la forme df_α pour une fonction f_α C^∞ sur $p^{-1}(U_\alpha)$; et comme les trois formes sont de type $(1,0)$, f_α est en fait holomorphe. De plus, $df_\alpha - df_\beta = d\log(\frac{h_\alpha}{h_\beta} \circ p)$, et quitte à multiplier f_α par des constantes dans les composantes connexes de $p^{-1}(U_\alpha)$ les fonction $e^{-f_\alpha}h_\alpha \circ p$ se recollent en une fonction holomorphe θ sur V. Celle-ci vérifie $\log\frac{\theta(z+\gamma)}{\theta(z)} = f_\alpha(z) - f_\alpha(z+\gamma)$, et

$$d\log\frac{\theta(z+\gamma)}{\theta(z)} = \omega_1(z+\gamma) - \omega_1(z) = \Sigma_j\lambda_j(\gamma)dz_j$$

(car $p^*(\omega_\alpha - \omega_0)$ est Γ-périodique), donc θ, qui vérifie $div(\theta) = p^*(D)$, a les facteurs d'automorphie de la forme voulue, avec $L(\gamma, z) = \frac{1}{2i\pi}\Sigma_j\lambda_j(\gamma)z_j$: c'est bien une fonction theta !

NB : en dimension 1, $\frac{1}{2i\pi}\int_{\mathcal{P}(\Gamma)}\frac{\theta'(z)}{\theta(z)}dz = E(\gamma_1, \gamma_1')$ est le degré de $div(\theta)$ (nombre de zéros moins nombre de pôles) à l'intérieur d'un parallèlogramme fondamental $\mathcal{P}(\Gamma)$ des périodes, i.e. $c_1 = deg$.

Chapitre III

Polarisations, endomorphismes, torsion

CHAPITRE III

POLARISATIONS, ENDOMORPHISMES, TORSION

III.1 Endomorphismes.

Soient $X = V/\Gamma, X' = V'/\Gamma'$ deux tores complexes, avec $\dim X = g$. Le groupe additif $Hom(X, X')$ admet via le théorème 1.1 du chap. II deux représentations

$$\rho_a : Hom(X, X') \to Hom_{\mathbb{C}}(V, V') \; , \rho_B : Hom(X, X') \to Hom_{\mathbb{Z}}(\Gamma, \Gamma')$$

envoyant un homomorphisme f sur sa différentielle $\rho_a(f) = d_0 f$ en 0, et sur $\rho_B(f) = (d_0 f)_{|\Gamma}$. Pour $X' = X$, il s'agit de représentations de l'anneau $End(X)$, et si $\overline{\rho}_a(f)$ désigne l'image de $\rho_a(f)$ sous la conjugaison complexe de $End(W)^{(0,0)}$, les représentations ρ_B et $\rho_a \oplus \overline{\rho}_a$ sont équivalentes.

L'image $Im(f)$ de f est un sous-tore V_2/Γ_2 de X, où $V_2 := \rho_a(f)(V) \subset V'$ et $\Gamma_2 := V_2 \cap \Gamma' \subset \Gamma'$ est un réseau de V_2 (puisqu'il est discret et engendre V_2 sur $\mathbb{R}$). Le noyau $Ker(f)$ a un nombre fini de composantes connexes (puisqu'il est compact) et sa composante neutre $Ker(f)^0$ est le sous-tore V_1/Γ_1 de X, où $V_1 = Ker(d_0 f)$, et $\Gamma_1 = V_1 \cap \Gamma$ est un réseau de V_1 (car discret à quotient compact). On a : $dim(Ker(f)^0) + dim(Im(f)) = dim(X)$.

Si $Ker(f)^0 = 0$, le noyau $Ker(f)$ est un groupe fini, et son ordre

$$|Ker(f)| = [(\rho_B(f))^{-1}(\Gamma') : \Gamma] := \deg(f)$$

s'appelle le degré de f. On pose $\deg(f) = 0$ si f n'est pas injectif. Par exemple, pour tout $n \in \mathbb{Z}$, l'endomorphisme $[n]_X : X \to X; x \mapsto nx$ est de degré $\deg([n]_X) = n^{2g}$, puisque pour $n \neq 0$,

$$X[n] := Ker([n]_X) = (\frac{1}{n}\Gamma)/\Gamma \simeq \Gamma/n\Gamma \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}.$$

Proposition III.1.1. *i) Soit $f : X \to X'$ un homomorphisme de tores complexes. On suppose que deux des trois propriétés suivantes sont satisfaites :*

a) $\dim X = \dim X'$ *;*

b) f *est surjective ;*

c) $Ker(f)$ *est un groupe fini.*

La troisième l'est alors aussi, et on dit que f *est une* isogénie*.*

ii) Soit $f : X \to X'$ *une isogénie, et* n *un entier* > 0 *tel que* $Ker(f) \subset X[n]$*. Il existe une unique isogénie* $g : X' \to X$ *telle que* $g \circ f = [n]_X$*. Elle vérifie* $f \circ g = [n]_{X'}$*. Pour* $X' = X$*, les isogénies de* X *s'identifient donc aux unités de l'anneau* $End_{\mathbb{Q}}(X) := End(X) \otimes \mathbb{Q}$*.*

Nous allons maintenant étudier une propriété spécifique aux tores polarisables, i.e. aux variétés abéliennes. Notons qu'une forme de Riemann H sur un tore complexe X en induit une sur tous ses sous-tores, donc tout sous-tore d'une variété abélienne est une sous-variété abélienne. De même, pour les tores quotients de X. On dit qu'une variété abélienne est *simple* si elle n'admet pas de sous-variété abélienne distincte de $\{0\}$ et de A.

Proposition III.1.2. (Poincaré) *: i) soit* A *une variété abélienne, et* A_1 *une sous-variété abélienne de* A*. Il existe une sous-variété abélienne* A_2 *de* A *telle que l'homomorphisme* $s : A_1 \times A_2 \to A : s(x_1, x_2) = x_1 + x_2$ *soit une isogénie.*

ii) Toute variété abélienne A *est isogène à un produit* $A_1^{n_1} \times ... \times A_k^{n_k}$ *de puissances de variétés abéliennes deux à deux non isogènes, et une telle décomposition est unique à isogénie près.*

L'unicité de la décomposition résulte de ce qu'un endomorphisme non nul d'une variété abélienne simple est une isogénie. Autrement dit, chacune des $\mathbb{Q}$-algèbre $End_{\mathbb{Q}}(A_i)$ est un corps gauche D_i, et $End(A)$ est un ordre de la $\mathbb{Q}$-algèbre $\Pi_{i=1,...,k} Mat_{n_i,n_i}(D_i)$.

Représentations ℓ-adiques : les modules de Tate

On se place ici sur un corps de base k quelconque, dont on fixe une clôture séparable k^{sep}. Soit A une variété abélienne définie sur k, de dimension g. Pour tout entier n premier à la caractéristique p de k, le sous-groupe $A[n]$ des points de $A(k^{sep})$ d'ordre divisant n est encore isomorphe à $(\mathbb{Z}/n\mathbb{Z})^{2g}$. Fixons un nombre premier $\ell \neq p$. Alors,

$$T_\ell(A) := \varprojlim A[\ell^n] \simeq \varprojlim (\mathbb{Z}/\ell^n\mathbb{Z})^{2g} = \varprojlim \mathbb{Z}_\ell^{2g}$$

est un $\mathbb{Z}_\ell$-module libre de rang $2g$. On l'appelle le module de Tate ℓ-adique de A. On note $V_\ell(A)$ le $\mathbb{Q}_\ell$-espace vectoriel $T_\ell(A) \otimes \mathbb{Q}_\ell$. .

Soit $f : A \to A'$ un homomorphisme de variétés abéliennes de dimensions g, g'. Il induit un homomorphisme sur les points de ℓ^n-torsion, d'où en passant à la limite projective, une représentation

$$\rho_\ell : Hom(A, A') \to Hom_{\mathbb{Z}_\ell}(T_\ell(A), T_\ell(A')).$$

Cette représentation est fidèle (= injective : se ramener à $A = A'$ simple, et noter qu'une isogénie ne peut tuer tous les points de ℓ^n-torsion pour n assez grand). On montre que son extension $\mathbb{Z}_\ell$-linéaire à $Hom(A, A') \otimes \mathbb{Z}_\ell$ l'est encore, de sorte que comme dans le cas $k = \mathbb{C}$, $Hom(A, A')$ est un $\mathbb{Z}$-module libre de rang $\leq 4gg'$.

Pour $f \in End(A)$, on appelle *polynôme caractéristique de* f le polynôme de degré $2g$

$$P_f(T) = det\big(\rho_\ell(f) - T id_{T_\ell(A)}\big),$$

et trace $Tr(f)$ de f l'opposé du coefficient de son terme de degré $2g-1$. Par ailleurs, si f est une isogénie, $deg(f)$ désigne dans ce cadre général le degré de l'extension $[f^*(k(A)) : k(A)]$.

Proposition III.1.3. *Soit f un endomorphisme de A/k et ℓ un nombre premier $\neq car(k)$. Le polynôme caractéristique $P_f(T)$ de f a des coefficients entiers rationnels indépendants de ℓ, et vérifie pour tout entier $n \in \mathbb{Z}$,*

$$deg(f - n\, id_A) = P_f(n).$$

En particulier, $deg(f) = det(\rho_\ell(f))$.

Preuve (dans le cas $k = \mathbb{C}$, où elle est élémentaire) : identifions A au tore complexe $X = V/\Gamma$. Alors,

$$T_\ell(X) = \varprojlim \frac{1}{\ell^n}\Gamma/\Gamma \simeq \varprojlim \Gamma \otimes (\mathbb{Z}/\ell^n\mathbb{Z}) = \Gamma \otimes \mathbb{Z}_\ell,$$

de sorte $\rho_\ell \simeq \rho_B \otimes 1$, et $P_f(T) = det\big(\rho_B(f) - T id_\Gamma\big) \in \mathbb{Z}[T]$ est bien indépendant de ℓ. De plus, pour tout endomorphisme $g = f - n id_X$ de X, $deg(g) = |Ker(g)| = [(\rho_B(g))^{-1}(\Gamma) : \Gamma] = [\Gamma : \rho_B(g)(\Gamma)] = det(\rho_B(g))$ si g est une isogénie ; sinon, $\rho_B(g)$ n'est pas inversible dans $End(\Gamma \otimes \mathbb{Q})$, et $deg(g) = 0 = det(\rho_B(g))$.

En conclusion, on dispose dans le cas $k = \mathbb{C}$ de 3 types de représentations de $End(A) \otimes \mathbb{Q}$: ρ_a (sur le k-espace vectoriel $V = Lie(A)$), ρ_B (sur le $\mathbb{Q}$-espace vectoriel $\Gamma \otimes \mathbb{Q} = H_1(A(\mathbb{C}), \mathbb{Q})$) et les ρ_ℓ (sur les $\mathbb{Q}_\ell$-espaces vectoriels $V_\ell(A)$). Elles sont liées par les équivalences

$$\rho_a \oplus \overline{\rho}_a \simeq \rho_B \ , \ \rho_B \otimes 1 \simeq \rho_\ell.$$

Pour k quelconque, seules subsistent ρ_a, qui n'est en général plus fidèle (cas des morphismes inséparables), et les ρ_ℓ, qui, elles, le restent. Ces dernières conduisent de plus à des représentations *galoisiennes*, de la façon suivante : pour tout $n \in \mathbb{Z}$, l'endomorphisme $[n]_A$ du groupe algébrique A/k est défini sur k. Par conséquent, tout $\sigma \in Gal(k^{sep}/k)$ induit un automorphisme du groupe abstrait $A[n]$, d'où pour $\ell \neq car(k)$, une représentation ℓ-adique, encore notée

$$\rho_\ell : Gal(k^{sep}/k) \to Aut_{\mathbb{Z}_\ell}(T_\ell(A)) \simeq GL_{2g}(\mathbb{Z}_\ell)$$

de ce groupe de Galois. Pour tout endomorphisme f de A défini sur k, on a $\sigma \circ f = f \circ \sigma$, de sorte que l'image $\rho_\ell(Gal(k^{sep}/k))$ est contenue dans le commutant de $\rho_\ell(End(A/k))$ dans $End(V_\ell(A))$.

Si k est un corps de nombres, et $\tau : k \hookrightarrow \mathbb{C}$ est une place archimédienne de k, on a défini au chapitre I.1 le groupe de Mumford-Tate du tore complexe X_τ attaché à la variété abélienne complexe $A \otimes_\tau \mathbb{C}$. Selon la conjecture de Mumford-Tate, $\rho_\ell(Gal(k^{sep}/k))$ serait un sous-groupe ouvert de $MT(X_\tau)(\mathbb{Q}_\ell)$.

III.2 Dualité

Soit $X = V/\Gamma$ un tore complexe. On a vu au chapitre II. 3.2 que le groupe $Pic_0(X)$ des classes d'isomorphismes de fibrés en droites topologiquement triviaux sur X s'identifie au groupe $Hom(\Gamma, \mathbb{U}_1)$ des caractères unitaires de Γ, par l'isomorphisme $\chi \mapsto \mathcal{L}(0, \chi)$. Ce dernier est naturellement muni de la structure de tore complexe suivante.

Soit $\overline{\Omega}$ le $\mathbb{C}$-espace vectoriel des formes $\mathbb{C}$-antilinéaires sur V ; c'est l'image du $\mathbb{C}$-dual $\Omega = Hom_{\mathbb{C}-lin}(V, \mathbb{C})$ de V par la conjugaison complexe relative à la structure réelle $Hom_{\mathbb{R}-lin}(V, \mathbb{R})$ de $Hom_{\mathbb{R}-lin}(V, \mathbb{C})$. Comme toute forme $\mathbb{R}$-linéaire sur V s'écrit de façon unique comme partie imaginaire d'une forme $\mathbb{C}$-antilinéaire, l'accouplement $\mathbb{R}$-bilinéaire $<,>: \overline{\Omega} \times V \to \mathbb{R} :< \ell, v >= Im(\ell(v))$ est non dégénéré. En particulier,

$$\hat{\Gamma} := \{\ell \in \overline{\Omega}, < \ell, \Gamma > \subset \mathbb{Z}\}$$

est un réseau de $\overline{\Omega}$, dit réseau dual de Γ, et $\hat{X} := \overline{\Omega}/\hat{\Gamma}$ est un tore complexe, que l'application $\overline{\Omega} \rightarrow Hom(\Gamma, \mathbb{U}_1) : \ell \mapsto e^{2i\pi<\ell,.>}$, de noyau $\hat{\Gamma}$, permet d'identifier à $Pic_0(X)$. On l'appelle le *tore dual* de X.

Par double antidualité, V s'identifie à l'antidual de $\overline{\Omega}$, et Γ est le réseau dual de $\hat{\Gamma}$. Par conséquent, X est canoniquement isomorphe à son bidual $\hat{\hat{X}}$.

Soit maintenant $\mathcal{L} = \mathcal{O}(D) = \mathcal{L}(H, \alpha)$ un fibré en droites sur X. Pour tout $a \in X$, on note $\tau_a : x \mapsto x - a$ la translation par $-a$. Alors, $\tau_a^* D = D + a$ et

$$\tau_a^* \mathcal{L}(H, \alpha) \simeq \mathcal{L}(H, \alpha e^{2i\pi E(a,.)}).$$

On en déduit le *théorème du carré* qui suit, et qui reste valable sur les variétés abéliennes sur tout corps k. (Pour la déduction (iii) ci-dessus, remplacer $Pf(E)$ par $dim H^0(X, \mathcal{L})$ si $\mathcal{L}$ est ample, ou plus généralement, par sa caractéristique d'Euler-Poincaré $\chi(\mathcal{L})$, qui coïncide également avec le nombre de self-intersection $\frac{1}{g!}(D^g)$; voir [M], §16.)

Proposition III.2.1. *: i)* $\forall \mathcal{L} = \mathcal{O}_X(D) \in Pic(X)$, $\forall a, b \in X$,

$$\tau_{a+b}^* \mathcal{L} \otimes \mathcal{L} \simeq \tau_a^* \mathcal{L} \otimes \tau_b^* \mathcal{L}, \text{ autrement dit : } \tau_{a+b}^* D + D \sim_\ell \tau_a^* D + \tau_b^* D.$$

En particulier, l'application $\phi_{\mathcal{L}} : a \mapsto \tau_a^* \mathcal{L} \otimes \mathcal{L}^{-1}$ *est un homomorphisme de tores complexes de* X *vers* $\hat{X} = Pic_0(X)$.

ii) $Pic_0(X) = \{\mathcal{L} \in Pic(X), \forall a \in X, \tau_a^* \mathcal{L} \simeq \mathcal{L}\}$.

iii) Si $c_1(\mathcal{L}) = E$ *est non-dégénérée,* $\phi_{\mathcal{L}} : X \rightarrow Pic_0(X)$ *est une isogénie, de degré* $Pf(E)^2$*. Son noyau est noté* $K(\mathcal{L})$.

Toujours avec les notations d'Appell-Humbert, on a pour tout endomorphisme f de X, et tout fibré : $f^*\big(\mathcal{L}(H, \alpha)\big) \simeq \mathcal{L}\big(\rho_a(f)^* H, \rho_B(f)^* \alpha\big)$; par conséquent, le fibré $\mathcal{L} = \mathcal{L}(H, \alpha)$ est symétrique, i.e. $[-1]_X^* \mathcal{L} \simeq \mathcal{L}$, si et slt si $\alpha(\Gamma) \subset \{\pm 1\}$. Un autre corollaire, valable en toute caractéristique, est que

$$\forall \mathcal{L} \in Pic(X), \forall n \in \mathbb{Z}, [n]_X^* \mathcal{L} \simeq \mathcal{L}^{n(n+1)/2} \otimes [-1]_X^* \mathcal{L}^{n(n-1)/2}.$$

En particulier, si $\mathcal{L} = \mathcal{O}_X(D)$ est symétrique, $[n]_X^* \mathcal{L} \simeq \mathcal{L}^{n^2}$, ou encore : $[n]_X^* D \sim_\ell n^2 D$, ce qui précise la formule, facile à établir pour D ample, que $[n]_X^*(D^g) = n^{2g}(D^g)$. Notons que sur un corps k de caractéristique finie p, c'est cette formule qui permet de montrer que $[p]_X$ est une isogénie de degré p^{2g} (degré d'inséparabilité compris), même si le groupe abstrait "$X[p]$" a au plus p^g éléments.

Le fibré de Poincaré

Soit A une variété abélienne sur un corps k algébriquement clos. On peut alors encore construire une variété abélienne duale $\hat{A}$ de A, telle que $\hat{A}(k) \simeq Pic_0(A)$. L'énoncé suivant précise cet isomorphisme. Pour tout $t \in \hat{A}(k)$, on note $\mathcal{L}_t \in Pic_0(A)$ le fibré correspondant.

Proposition III.2.2. *i) il existe un fibré en droites $\mathcal{P}$ sur la variété abélienne $A \times \hat{A}$, unique à isomorphisme près, dont la restriction à $\{0\} \times \hat{A}$ soit un fibré trivial sur $\hat{A}$, et tel que pour tout $t \in \hat{A}$, la restriction $\mathcal{P}_t$ de $\mathcal{P}$ à $A \times \{t\} \simeq A$ soit isomorphe à $\mathcal{L}_t$.*

ii) Ce fibré $\mathcal{P}$, appelé fibré de Poincaré, vérifie la propriété universelle suivante. Pour tout k-schéma pointé (T, t_0), et tout faisceau inversible $\mathcal{L}$ sur $A \times T$, dont les restrictions à $\{0\} \times T$ et à $A \times \{t_0\}$ soient triviales, il existe un unique k-morphisme $j : T \to \hat{A}$ tel que $j(t_0) = 0$ et que $(1 \times j)^*(\mathcal{P}) \simeq \mathcal{L}$.

Preuve. - Indiquons seulement la construction de $\mathcal{P}$ dans le cas $k = \mathbb{C}$, en reprenant les notations $A = X = V/\Gamma, \hat{A} = \hat{X} = \overline{\Omega}/\hat{\Gamma}$ ci-dessus, de sorte que $X \times \hat{X} = (V \times \overline{\Omega})/(\Gamma \times \hat{\Gamma})$. Considérons la forme hermitienne $\mathcal{H}(v, \ell)$ sur $V \times \overline{\Omega}$ définie par

$$\mathcal{H}\big((v_1, \ell_1), (v_2, \ell_2)\big) = \overline{\ell_1(v_2)} + \ell_2(v_1).$$

Par définition de $\hat{\Gamma}$, sa partie imaginaire $\mathcal{E} = Im(\mathcal{H})$ prend des valeurs entières sur $\Gamma \times \hat{\Gamma}$. De plus, l'application $\alpha : \Gamma \times \hat{\Gamma} \to \mathbb{U}_1 : \alpha(\gamma, \ell) = e^{i\pi <\ell, \gamma>}$ est un quasi-caractère relativement à $\mathcal{E}$. La relation $\mathcal{P} := \mathcal{L}(\mathcal{H}, \alpha)$ définit donc un fibré en droites sur $X \times \hat{X}$. Sa restriction à $\{0\} \times \hat{X}$ a des facteurs d'automorphie triviaux, dont est triviale. Pour tout $t =$ classe de ℓ_2 dans $\hat{X}$, représentant le fibré $\mathcal{L}_t = \mathcal{L}(0, e^{2i\pi Im \ell_2(.)})$, sa restriction à $X \times \{t\}$ a une classe de Chern nulle, et admet comme facteurs d'automorphie $\gamma \mapsto e^{\pi \ell_2(\gamma)}$, équivalents au (quasi-)caractère $\gamma \to e^{2i\pi <\ell_2, \gamma>}$, donc $\mathcal{P}|_{X \times \{t\}}$ est isomorphe à $\mathcal{L}_t$.

On dispose sur le groupe $Div(A)$ des diviseurs sur A des relations d'équivalence, de moins en moins fines, suivantes :

- équivalence linéaire : $D \sim_\ell D'$ si $D - D'$ est le diviseur d'une fonction rationnelle f sur A ($= f$ méromorphe sur X). En considérant le graphe de f (et en se ramenant à des diviseurs effectifs), on voit que c'est le cas si et slt s'il existe une famille $\{D_t\}, t \in \mathbb{P}_1$, et deux points $t_0 = 0, t_1 = \infty$ sur $\mathbb{P}_1$ tels que $D = D_{t_0}, D' = D_{t_1}$;

- équivalence algébrique $D \sim_a D'$: même définition, en remplaçant $\mathbb{P}_1$ par une courbe algébrique T ;

- équivalence topologique $c_1(\mathcal{O}_X(D)) = c_1(\mathcal{O}_X(D'))$: même définition, en remplaçant la famille algébrique $\{D_t\}$ par une famille continue, paramétrée par l'intervalle réel $[t_0, t_1]$;

- équivalence numérique $D \sim_n D'$: on demande que pour tout courbe $C \subset A$, les nombres d'intersection $D.C$ et $D'.C$ coïncident.

Pour les variétés abéliennes, les trois dernières équivalences coïncident. Par exemple, si D et D' sont topologiquement équivalents, $\mathcal{O}_X(D-D') \in Pic_0(A)$ s'identifie à un point t_1 de $\hat{A}$, et l'existence de courbes algébriques $T \subset \hat{A}$ passant par $t_0 = 0$ et t_1 entraîne que $D \sim_a D'$. La proposition précédente montre également que toute application rationnelle de $\mathbb{P}_1$ dans $\hat{A}$ est constante : sinon, il existerait deux points distincts de $\hat{A} \simeq Div(A)/Div_\ell(A)$ représentant des fibrés isomorphes. (Pour une démonstration plus naturelle, voir [HS].)

L'involution de Rosati

Pour tout homomorphisme de tores complexes $f : X \to X'$, notons $\hat{f} : Pic_0(X') \to Pic_0(X)$ l'homomorphisme de groupes défini par $\mathcal{L}' \mapsto f^*(\mathcal{L}')$. Via la représentation $\mathbb{C}$-linéaire $\rho_a(f) = F$ de f sur les espaces tangents V, V', il est induit par la transposition ${}^tF : \overline{\Omega}' \to \overline{\Omega} : \ell \mapsto \ell \circ F$, de sorte que $\hat{f}$ est un homomorphisme de tores complexes, appelé le dual de f.

Lemme III.2.3. *i) si $f : X \to X'$ une isogénie, $\hat{f} : Pic_0(X') \to Pic_0(X)$ est une isogénie de même degré que f.*

ii) Soit $\mathcal{L}$ un fibré ample sur X, et $\phi_\mathcal{L} : X \to Pic_0(X)$ l'isogénie associée. Alors, $\hat{\phi}_\mathcal{L} = \phi_\mathcal{L}$.

Preuve : i) sans perte de généralité, on peut supposer que $V = V'$ et que $F = id_V$. Alors, $Ker(f) \simeq \Gamma'/\Gamma$ a le même ordre que $Ker\hat{f} \simeq Hom(\Gamma'/\Gamma, \mathbb{U}_1)$.

ii) Soit H la forme de Riemann attachée à $\mathcal{L}$. Alors, $\Phi := \rho_a(\phi_\mathcal{L})$ envoie un $w \in V$ sur la forme antilinéaire $v \mapsto H(v, w)$ i.e. vérifie $< \Phi w, v >= E(v, w)$, et $\rho_a(\hat{\phi}_\mathcal{L})$ est représentée par la transposée ${}^t\Phi$, qui vérifie $<^t \Phi w, v > = < w, \Phi v >= -E(w, v)$ (car dans l'identification de V avec l'antidual de $\overline{\Omega}$, un vecteur w correspond à la forme antilinéaire $\ell \mapsto \overline{\ell(w)}$ sur $\overline{\Omega}$), donc $<^t \Phi w, v >= E(v, w) =< \Phi w, v >$, et ${}^t\Phi = \Phi$.

Fixons un fibré ample $\mathcal{L}$ sur X. Alors, l'application

$$End_\mathbb{Q}(X) \ni f \;\mapsto\; f^\dagger := \phi_\mathcal{L}^{-1} \circ \hat{f} \circ \phi_\mathcal{L} \in End_\mathbb{Q}(X)$$

est une anti-involution de la $\mathbb{Q}$-algèbre $End_{\mathbb{Q}}(X)$, qu'on appelle l'involution de Rosati associée à $\mathcal{L}$. De même que $\phi_{\mathcal{L}}$, elle ne dépend en fait que de $c_1(\mathcal{L})$, i.e. de la classe de $\mathcal{L}$ dans le groupe $NS(X)$. Si $F, F^\dagger, \Phi$ représentent $f, f^\dagger, \phi_{\mathcal{L}}$ sous ρ_a, on a pour tout $w, v \in V$:

$$H(v, F^\dagger(w)) = \big(\Phi(F^\dagger(w))\big)(v) = ({}^t F\big(\Phi(w)\big)(v) = \big(\Phi(w)\big)(F(v)) = H(F(v), w).$$

Ainsi, $F^\dagger$ est *l'adjoint* de F relativement au produit hermitien défini par H. En choisissant une base orthonormée de V, on en déduit que la trace de $F^\dagger F$ est un nombre *réel* > 0, d'où en passant à $\rho_B \simeq \rho_a \oplus \overline{\rho}_a$:

Théorème III.2.4. *L'application $(f, g) \mapsto Tr(f^\dagger g)$ est une forme $\mathbb{Q}$-bilinéaire symétrique sur $End_{\mathbb{Q}}(X)$ dont l'extension $\mathbb{R}$-linéaire est définie positive.*

Dans cet énoncé, Tr désigne la trace relative à la représentation rationnelle ρ_B de $End_{\mathbb{Q}}(X)$ sur $\Gamma \otimes \mathbb{Q}$, i.e. $Tr(f) = Tr(\rho_B(f))$. Comme on l'a dit au §1, c'est aussi la trace de $\rho_\ell(f)$ pour la représentation ℓ-adique de $End_{\mathbb{Q}}(X)$ sur $T_\ell(X)$. Ainsi interprété, le théorème 2.4 reste valable pour les variétés abéliennes sur un corps k quelconque.

III.3 Hasse-Weil // Espace de Siegel

1. Variétés abéliennes sur les corps finis

En guise d'introduction au chapitre IV, nous donnons ci-dessous un "analogue kählérien des conjectures de Weil" (voir Serre, Ann. Maths, 71, 1960, 392-394, pour un énoncé plus substantiel).

Proposition III.3.1. *soient A une variété abélienne complexe, $\mathcal{L}$ un fibré ample sur A, et f un endomorphisme de A. On note † l'involution de Rosati définie par $\mathcal{L}$, et on suppose qu'il existe un entier q tel que $f^\dagger f = [q]_A$. Alors, les valeurs propres de $\rho_B(f)$ sont des entiers algébriques dont tous les conjugués sur $\mathbb{Q}$ sont de valeurs absolues égales à $\sqrt{q}$.*

Preuve : soient H la forme hermitienne que définit $\mathcal{L}$ sur $V = Lie(A)$. Via ρ_a, la relation $f^\dagger f = q$ (qui impose $q > 0$) s'écrit $qH(v, v) = H(v, F^\dagger F(v)) = H(F(v), F(v))$, de sorte que $\frac{1}{\sqrt{q}} F$ est un opérateur unitaire relativement au produit hermitien H. Toutes ses valeurs propres sont donc des nombres complexes de module 1. Mais les valeurs propres de F, jointes à leurs complexes conjugées, forment l'ensemble des valeurs propres de $\rho_B(f)$, i.e. des racines du polynôme $P_f(T)$. Comme $P_f(T)$ est unitaire à coefficients entiers, elles forment un ensemble d'entiers algébriques stable par conjugaison sur $\mathbb{Q}$.

Si on remplace ρ_B par une des représentations ρ_ℓ, la proposition 4.1 reste valable pour une variété abélienne A sur un corps quelconque k. Supposons ainsi que $k = \mathbb{F}_q$ soit un corps fini, de cardinal $q = p^d$. On dispose alors, parmi les endomorphismes de A définis sur k, de l'endomorphisme de Frobenius $\pi : A \to A$, défini en coordonnées projectives par $(x_0 : ..., : x_N) \to (x_0^q : ... : x_N^q)$ (c'est un morphisme de variétés algébriques, envoyant 0_A sur 0_A, donc bien un endomorphisme de groupes algébriques par l'analogue algébrique du Theorème 1.1 du chap. II). En particulier, pour tout entier $m > 0$, un point $x \in A(\overline{\mathbb{F}_q})$ est défini sur $\mathbb{F}_{q^m}$ si et seulement si $\pi^m(x) = x$, et l'on a :

Théorème III.3.2. (Hasse-Weil). - *Soit A une variété abélienne définie sur $\mathbb{F}_q$. Il existe des entiers algébriques $\omega_1, ..., \omega_{2g}$, dont tous les conjugués sur $\mathbb{Q}$ sont de valeurs absolues $\sqrt{q}$, tels que pour tout entier $m > 0$:*

$$card(A(\mathbb{F}_{q^m})) = \Pi_{i=1,...,2g}(1 - \omega_i^m).$$

Il existe donc une constante C_g telle que $|card(A(\mathbb{F}_{q^m}) - q^{mg}| \leq C_g q^{m(g-\frac{1}{2})}$.

Preuve : Comme on vient de le dire, le groupe $A(\mathbb{F}_{q^m})$ s'identifie au noyau de l'endomorphisme $f = \pi^m - id_A$ de A. Par ailleurs, f est un morphisme séparable, car $d_0\pi^m = 0$, donc $d_0 f = id_{LieA}$ est inversible. Donc l'ordre du groupe abstrait $Ker(f)$ est égal au degré $deg(f)$ de l'extension $f^*k(A)/k(A)$, qui vaut $det(T_\ell(f)) = P_{\pi^m}(1)$ d'après la proposition 1.3. Si on note $P_\pi(T) = \Pi_{i=1,...,2g}(T - \omega_i)$ la décomposition du polynôme caractéristique de l'endomorphisme de Frobenius π, de sorte que les ω_i sont des entiers algébriques stables par conjugaison sur $\mathbb{Q}$, on a donc pour tout $m > 0$: $card(A(\mathbb{F}_{q^m})) = \Pi_{i=1,...,2g}(1 - \omega_i^m)$.

Pour conclure, il reste à montrer que les ω_i ont toutes leurs valeur absolues archimédiennes égales à $\sqrt{q}$. Soit $\mathcal{L} = \mathcal{O}_A(D)$ un fibré ample sur A, défini sur $\mathbb{F}_q$. Si $f_\alpha = 0$ désigne un équation locale du diviseur D, π^*D est localement défini par le diviseur de $f_\alpha \circ \pi(x) = f_\alpha(x^q) = (f_\alpha(x))^q$, donc $\pi^*D \sim_\ell qD$, et $\pi^*\mathcal{L} \simeq \mathcal{L}^{\otimes q}$. Par conséquent,

$$\hat{\pi} \circ \phi_\mathcal{L} \circ \pi(x) = \pi^*(\tau^*_{\pi(x)}\mathcal{L} \otimes \mathcal{L}^{-1}) = \tau^*_x\pi^*\mathcal{L} \otimes (\pi^*\mathcal{L})^{-1} = q\ \phi_\mathcal{L}(x).$$

L'involution de Rosati attachée à $\mathcal{L}$ vérifie donc

$$\pi^\dagger\pi = \phi_\mathcal{L}^{-1} \circ \hat{\pi} \circ \phi_\mathcal{L} \circ \pi = [q]_A.$$

Par l'analogue algébrique de la proposition 3.1, toutes les valeurs absolues des valeurs propres ω_i de $T_\ell(\pi)$ sont donc égales à $\sqrt{q}$.

2. L'espace de Siegel

Une variété abélienne *principalement polarisée* est la donnée d'un couple formé d'une variété abélienne A et d'une classe dans $NS(A)$ de fibrés amples $\mathcal{L}$ tels que $dimH^0(A,\mathcal{L}) = 1$; autrement dit, dans le cas complexe, d'une forme de Riemann H telle que $Pf(E) = 1$ (on dit alors que E est unimodulaire). Il revient au même de demander que l'isogénie $\phi_{\mathcal{L}} : A \to \hat{A}$ soit un isomorphisme.

En guise d'introduction au chapitre VI, nous donnons ci-dessous une description ensembliste de l'"espace" des classes d'isomorphisme de variétés abéliennes complexes principalement polarisées, de dimension g.

Soit $(X = V/\Gamma, H)$ une telle variété abélienne principalement polarisée. Choisissons (voir chap. II, §3.1) une base $\{\gamma_1, ..., \gamma_g, \gamma_{g+1}, ..., \gamma_{2g}\}$ de Γ symplectique pour $E = ImH$, i.e. telle que E soit représentée dans cette base par $\mathbf{J}_{2g} := \begin{pmatrix} 0 & \mathbf{I}_g \\ -\mathbf{I}_g & 0 \end{pmatrix}$. Alors $\{\gamma_1, ..., \gamma_g\}$ est une base de V sur $\mathbb{C}$, et les $\{\gamma_{g+1}, ..., \gamma_{2g}, \ \gamma_1, ..., \gamma_g\}$ sont représentés dans cette base par les vecteurs colonnes d'une matrice $(\tau \ \mathbf{I}_g)$, où $\tau \in GL_g(\mathbb{C})$. D'après le Lemme II.3.3, τ appartient à l'espace de Siegel

$$\mathfrak{H}_g = \{\tau \in GL_n(\mathbb{C}), \ {}^t\tau = \tau, Im(\tau) > 0\}$$

des matrices symétriques dont la partie imaginaire représente une forme hermitienne définie positive, et la polarisation principale H est donnée par $(Im\tau)^{-1}$.

Effectuons la même construction avec une autre v.a.p.p. $(X' = V'/\Gamma', H')$, d'où $\tau' \in \mathfrak{H}_g$, et soit $u : (X', H') \to (X, H)$ un isomorphisme de variétés abéliennes polarisées. Cela signifie

• d'une part, que u est un isomorphisme de X' sur X. Si $U = \rho_a(u) \in GL_n(\mathbb{C}), N = \rho_B(u) \in GL_{2g}(\mathbb{Z})$, on a donc

$$U(\tau' \ \mathbf{I}_g) = (\tau \ \mathbf{I}_g)N.$$

Posons ${}^tN = M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$, où $A, B, C, D \in Mat_{gg}(\mathbb{Z})$. On déduit de la relation précédent que $U = \tau^t C +^t D$, donc sa transposée $C\tau + D$ est inversible, et

$$\tau' = (A\tau + B)(C\tau + D)^{-1}.$$

• d'autre part, que u respecte les polarisations : $u^*H = H$, soit en termes de $\rho_B(u)$ et de la forme symplectique E sur Γ : ${}^tN\mathbf{J}_{2g}N = \mathbf{J}_{2g}$. Par conséquent, N (et donc ${}^tN$) appartiennent au groupe symplectique

$$Sp_{2g}(\mathbb{Z}) = \{M \in GL_{2g}(\mathbb{Z}), {}^tM\mathbf{J}_{2g}M = \mathbf{J}_{2g}\}.$$

Dans l'écriture $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$, cela se traduit par les conditions

$${}^tAC = {}^tCA,\ {}^tBD = {}^tDB,\ {}^tAD - {}^tCB = \mathbf{I}_g,$$

(équivalentes à $A\,{}^tB = B\,{}^tA, C\,{}^tD = D\,{}^tC,\ A\,{}^tD - B\,{}^tC = \mathbf{I}_g$.)

Inversement, pour tout $\tau \in \mathfrak{H}_g$, la partie imaginaire de la forme hermitienne $(Im\tau)^{-1}$ sur $\mathbb{C}^g$ est à valeurs entières sur le réseau $\Gamma_\tau := \tau\mathbb{Z}^g \oplus \mathbb{Z}^g$. Par conséquent, l'application $\tau \mapsto \big(\mathbb{C}^g/\Gamma_\tau, (Im\tau)^{-1}), \{\tau\ \mathbf{I}_g\}\big)$ établit une bijection entre $\mathfrak{H}_g$ et l'ensemble des classes d'isomorphisme de v.a.p.p. munies d'une base symplectique. Dans cette bijection, un changement de base symplectique $\Gamma_\tau \to \Gamma_{\tau'}$ est donné par une matrice $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sp_{2g}(\mathbb{Z})$, où $C\tau + D$ est inversible et vérifie $\tau' = (A\tau + B)(C\tau + D)^{-1}$. On vérifie que l'application

$$Sp_{2g}(\mathbb{Z}) \times \mathfrak{H}_g \to \mathfrak{H}_g : \begin{pmatrix} A & B \\ C & D \end{pmatrix} \mapsto (A\tau + B)(C\tau + D)^{-1}$$

définit une action à gauche du groupe $Sp_{2g}(\mathbb{Z})$ sur l'espace de Siegel $\mathfrak{H}_g$. Par conséquent, l'application $\tau \mapsto \big(\mathbb{C}^g/\Gamma_\tau, (Im\tau)^{-1}\big)$ induit une bijection entre

- l'ensemble $Sp_{2g}(\mathbb{Z})\backslash\mathfrak{H}_g$ des orbites de $\mathfrak{H}_g$ sous l'action de $Sp_{2g}(\mathbb{Z})$.

et

- l'ensemble $\mathcal{A}_g$ des classes d'isomorphismes de variétés abéliennes complexes de dimension g principalement polarisées.

Signalons pour conclure que les “Thetanullwerte” $\{\theta \begin{bmatrix} a \\ 0 \end{bmatrix} (\tau, 0), a \in \frac{1}{4}\mathbb{Z}^g\}$ introduites au chap. II, fin du §3.1, permettent d'identifier (un revêtement fini de) $Sp_{2g}(\mathbb{Z})\backslash\mathfrak{H}_g$ à l'ensemble des points complexes d'une variété algébrique quasiprojective. On obtient ainsi l'exemple le plus basique de *variété de Shimura*. Pour une présentation plus intrinsèque, on se rapportera au cours de M2 spécialisé de C. Cornut.

Chapitre IV

Problème d'examen

VARIÉTÉS ABÉLIENNES

~

Examen (M2) du 22 Février 2011
(Durée : 3 heures)

On demande de traiter deux des trois problèmes proposés.

IV.1 Sujet

I

Les 4 premières questions sont indépendantes.

Soient $X = V/\Gamma$ un tore complexe, muni d'une forme de Riemann H, et f un automorphisme de la variété abélienne polarisée (X, H) (voir $(*)$ pour la définition). Soit par ailleurs ℓ un nombre premier ≥ 3. On se propose de montrer que *si f induit l'identité sur le sous-groupe fini $X[\ell] = Ker([\ell]_X)$ de X, alors, $f = id_X$.*

1^0/ Soit f un automorphisme d'une variété abélienne polarisée $(V/\Gamma, H)$, et $F := \rho_a(f) \in GL(V) \simeq GL_g(\mathbb{C})$ sa représentation sur V. On a donc

$$\forall (u,v) \in V \times V,\ H(Fu, Fv) = H(u,v), \qquad (*)$$

où H est une forme hermitienne définie positive. On se propose de montrer que F *est une matrice d'ordre fini dans* $GL_g(\mathbb{C})$: il existe un entier $k \geq 1$ tel que $F^k = \mathbf{I}_g$.

i) Montrer que dans une base convenable de V sur $\mathbb{C}$, F est représentée par une matrice unitaire (${}^t\overline{F}F = \mathbf{I}_g$), et que les matrices $\{(\rho_a \oplus \overline{\rho}_a)(f^k) := \begin{pmatrix} F^k & 0 \\ 0 & \overline{F}^k \end{pmatrix}, k \in \mathbb{Z}\}$ sont contenues dans le groupe unitaire $\mathbb{U}_{2g} = \{\Phi \in GL_{2g}(\mathbb{C}), {}^t\overline{\Phi}\Phi = \mathbf{I}_{2g}\} \subset Mat_{2g,2g}(\mathbb{C})$.

ii) Rappeler pourquoi $(\rho_a \oplus \overline{\rho}_a)(f)$ est conjugée dans $GL_{2g}(\mathbb{C})$ à une matrice $M \in Mat_{2g,2g}(\mathbb{Z})$ à coefficients entiers, et montrer que $M \in GL_{2g}(\mathbb{Z})$.

iii) Montrer que le sous-groupe $< F >$ de $GL_g(\mathbb{C})$ engendré par F est isomorphe à un sous-groupe discret d'un groupe compact, et conclure.

2^0/ Soit $F \in GL_g(\mathbb{C})$ une matrice d'ordre fini. Montrer que F est diagonalisable, et que ses valeurs propres sont des racines de l'unité.

[Indications pour diagonalisable : considérer le polynôme minimal de F ; ou voir $\mathbb{C}^g$ comme une représentation du groupe fini $G =< F >$.]

3^0/ Soient ℓ un entier > 0, et f un endomorphisme du tore complexe $X = V/\Gamma$. On suppose que f induit l'identité sur $X[\ell]$, autrement dit : $\forall x \in X[\ell]$, $x - f(x) = 0$.

i) Montrer qu'il existe un endomorphisme g de X tel que

$$id_X - f = g \circ [\ell]_X.$$

ii) Soit ζ une valeur propre de la matrice $F = \rho_a(f)$. En considérant le polynôme caractéristique de $\rho_B(g) \in Mat_{2g,2g}(\mathbb{Z})$, montrer que $\frac{1}{\ell}(1-\zeta)$ est un entier algébrique.

4^0/ Soient ℓ un nombre premier ≥ 3, et $\zeta \in \mathbb{C}^*$ une racine de l'unité. On suppose que $\frac{1}{\ell}(1-\zeta)$ est un entier algébrique. Montrer que $\zeta = 1$.

[Indication : se ramener au cas où l'ordre k de la racine de l'unité ζ est un nombre premier p, auquel cas $Norm_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1-\zeta) = p$, puis distinguer les cas $p \neq \ell, p = \ell$.]

5^0/ À l'aide des résultats précédents, établir la propriété énoncée dans l'introduction.

II

Les 2 premières questions sont indépendantes.

1^0/ Dans $V = \mathbb{C}^2$, muni de sa base canonique $\{e_1, e_2\}$, on considère le sous-groupe $\tilde{\Gamma}$ engendré par les vecteurs

$$\gamma_1 = e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \gamma_2 = e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \tilde{\gamma}_3 = \begin{pmatrix} i \\ i\sqrt{3} \end{pmatrix}, \gamma_4 = \begin{pmatrix} i\sqrt{2} \\ i\sqrt{5} \end{pmatrix}.$$

On se propose de montrer que *le tore $\tilde{X} = V/\tilde{\Gamma}$ n'est pas polarisable.* On raisonne par l'absurde en supposant que $\tilde{\Gamma}$ admet une forme de Riemann, donnée dans la base $\{e_1, e_2\}$ par une matrice hermitienne $H = \begin{pmatrix} h_1 & h \\ \bar{h} & h_2 \end{pmatrix}, h_1, h_2 \in \mathbb{R}$. On pose $E(u,v) = Im\big(H(u,v)\big)$, de sorte que $E(\gamma, \gamma') \in \mathbb{Z}$ pour tous $\gamma, \gamma' \in \tilde{\Gamma}$.

i) Vérifier que $\tilde{\Gamma}$ est bien un réseau de V.

ii) Calculer les entiers rationnels $E(\gamma_1, \gamma_2)$ et $E(\tilde{\gamma}_3, \gamma_4)$. En déduire qu'ils sont nuls.

iii) Calculer les entiers rationnels $E(\gamma_1, \tilde{\gamma}_3), E(\gamma_1, \gamma_4), E(\gamma_2, \tilde{\gamma}_3), E(\gamma_2, \gamma_4)$. En déduire que $E = 0$, et conclure.

[Indication : $\{1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}\}$ sont linéairement indépendants sur $\mathbb{Q}$.]

2^0/ Dans $V = \mathbb{C}^2$, muni de sa base canonique $\{e_1, e_2\}$, on considère le sous-groupe Γ engendré par les vecteurs

$$\gamma_1 = e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \gamma_2 = e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \gamma_3 = \begin{pmatrix} i \\ 0 \end{pmatrix}, \gamma_4 = \begin{pmatrix} i\sqrt{2} \\ i\sqrt{5} \end{pmatrix}.$$

On se propose de montrer que *le tore $X = V/\Gamma$ n'est pas polarisable.*

i) Vérifier que Γ est bien un réseau de V.

ii) Pour tout $\lambda \in \mathbb{C}$, on note D_λ la droite de V d'équation $z_2 = \lambda z_1$. Montrer que l'intersection $\Gamma_0 := D_0 \cap \Gamma$ de D_0 avec Γ est un réseau de D_0,

iii) Montrer que D_0 est la seule droite vectorielle de V vérifiant cette propriété.

iv) En déduire que X contient une unique courbe elliptique X_0, et conclure.

[Indications : pour (iii) : $\mathbb{Q}(i\sqrt{5}) \cap \mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}$;
pour (iv) : appliquer le théorème de Poincaré.]

3^0/ On reprend les notations du 2^0/, et on pose $F\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = z_2, F(\Gamma) = \Gamma'$.

i) Montrer que F induit un homorphisme surjectif f de X sur une courbe elliptique X'.

ii) En déduire qu'il existe des fonctions méromorphes sur X non constantes.

4^0/ On considère de nouveau le tore $\tilde{X}$ de la question 1^0/.

i) Soit $\mathcal{L}$ un fibré holomorphe sur $\tilde{X}$, et (H, α) ses caractéristiques. Montrer que $H = 0$.

[Indication : dans les calculs du 1^0/, on n'a pas utilisé la positivité de H.]

ii) En déduire que toute fonction méromorphe sur $\tilde{X}$ est constante.

III

On pourra admettre les résultats d'une question pour traiter les suivantes.

Soient k un corps algébriquement clos de caractéristique nulle, et X une courbe projective lisse irréductible de genre $g \geq 2$, définie sur k . On pourra supposer que $k = \mathbb{C}$. On désigne par $k(X)$ le corps des fonctions rationnelles ($\simeq$ méromorphes) sur X, et par $\{\omega_1, ..., \omega_g\}$ une base du k-espace vectoriel

$\Omega^1(X) := H^0(X, \underline{\Omega}^1_{X/k})$ des formes différentielles régulières ($\simeq$ holomorphes) sur X.

1^0/ Soit P un point de X. Pour tout diviseur D sur X, on note $\ell(D)$ la dimension du k-espace vectoriel $L(D) = \{f \in k(X), div(f) \geq -D\}$.

i) Montrer que $\ell(P) = 1$.

[Rappel : si une fonction non constante $x \in k(X)$ admet au plus n pôles distincts, tous simples, alors $k(X)$ est une extension algébrique de degré $\leq n$ de $k(x)$. Et $k(x) \simeq k(\mathbb{P}_1)$.]

ii) Soit $\mathbf{K} = div(\omega)$ un représentant du diviseur canonique de X. On rappelle que $deg(\mathbf{K}) = 2g - 2$. Montrer que $\ell(\mathbf{K} - P) = g - 1$.

2^0/ Soit P un point de X. On désigne par z un paramètre local de X en P ($\simeq$ un isomorphisme biholomorphe d'un voisinage de P sur un ouvert de $\mathbb{C}$, avec $z(P) = 0$), et on pose pour tout $i = 1, ..., g$: $\omega_i = f_i(z)dz$.

i) Déduire de la question 1^0/ (ii) que l'un au moins des nombres $f_i(0), i = 1, ..., g$, est non nul.

ii) Montrer que la droite δ_P engendrée dans k^g par le vecteur $\big(f_1(0), ..., f_g(0)\big)$ ne dépend pas du choix du paramètre local z.

Cette droite δ_P *définit donc intrinsèquement un point* $\phi(P)$ *de l'espace projectif* $\mathbb{P}_{g-1}$.

3^0/ Montrer que l'image de X par l'application $\phi : X \to \mathbb{P}_{g-1}$ ainsi définie n'est contenue dans aucun hyperplan de $\mathbb{P}_{g-1}$.

4^0/ Soient P, Q deux points distincts de X. Montrer que les conditions suivantes sont équivalentes.

i) $\phi(P) \neq \phi(Q)$;
ii) il existe un hyperplan de $\mathbb{P}_{g-1}$ passant par $\phi(P)$, mais pas par $\phi(Q)$;
iii) il existe une forme différentielle régulière ω qui s'annule en P, mais pas en Q ;
iv) $\ell(\mathbf{K} - P - Q) = g - 2$;
v) $\ell(P + Q) = 1$;
vi) il n'existe pas de fonction $x \in k(X)$ dont le diviseur polaire soit $P + Q$.

5^0/ On dit qu'une courbe X de genre ≥ 2 est hyperelliptique si c'est un revêtement (ramifié) de degré 2 de $\mathbb{P}_1$. Montrer que si X n'est pas hyperelliptique, l'application ϕ est injective.

IV.2 Esquisse de corrigé.

I- 1^o/ i) Choisir une base de V orthonormée pour le produit scalaire H. Alors, F et $\overline{F}$ sont unitaires.
ii) $M = \rho_B(f) \in End_{\mathbb{Z}}(\Gamma)$ répond à la question. Comme f est un automorphisme de X, $\rho_B(f)^{-1} \in End_{\mathbb{Z}}(\Gamma)$. (Plus directement, $|detF|^2 = 1$ pour F unitaire.)
iii) Munissons l'e-v. $\mathcal{E} = Mat_{2g,2g}(\mathbb{C})$ de l'une de ses normes usuelles. L'image de $< F >$ par $\rho_a \oplus \overline{\rho}_a$ est contenue dans $\mathbb{U}_{2g}$, qui est un fermé borné de $\mathcal{E}$, et dans un conjugué du sous-ensemble discret $Mat_{2g,g}(\mathbb{Z})$ de $\mathcal{E}$.

I- 2^o/ 1ère méthode : si F est d'ordre k, son polynôme minimal divise $T^k - 1$, qui n'a que des racines simples. 2ème méthode : a) il existe un produit scalaire sur $\mathbb{C}^g$ invariant sous G, donc F est conjuguée à une matrice unitaire, donc est diagonalisable ; ou b) les représentations complexes irréductibles d'un groupe commutatif fini sont de dimension 1.

I- 3^o/ i) 1ère méthode : si $\alpha, \beta \in End(X)$ vérifient $N := Ker(\alpha) \subset Ker(\beta)$, et si $\pi : X \to X/N$ désigne la projection canonique, alors $\beta = b \circ \pi$ se factorise à travers $b : X/N \to X$, $\alpha = a \circ \pi$ se factorise à travers $a : X/N \xrightarrow{\sim} Im(\alpha)$, et $g := b \circ a^{-1} : Im(\alpha) \to X$ vérifie $\beta = g \circ \alpha$. 2ème méthode : $G := (id_V - \rho_a(f)) \circ [\frac{1}{\ell}]_V$ vérifie $G(\Gamma) \subset \Gamma$, donc est de la forme $\rho_a(g)$.
ii) $1 - \zeta = \ell \times$(une racine du polynôme unitaire $Car_{\rho_B(g)}(T) \in \mathbb{Z}[T]$).

I- 4^o/ Si $k = pk'$, $\frac{1}{\ell}(1 - \zeta^{k'}) = \frac{1}{\ell}(1 - \zeta)(1 + ... + \zeta^{k'-1})$ est encore un entier algébrique. Sa norme p/ℓ^{p-1} ne peut être un entier si $\ell > 2$, donc $k = 1$.

I- 5^o/ D'après 2^o/, F est diagonalisable.

$\sim$

II-1^o/i) Une relation de dépendance $\alpha_1\gamma_1 + ... = 0$ sur $\mathbb{R} \Rightarrow \alpha_1 = \alpha_2 = 0$, puis $\alpha_3 = \alpha_4 = 0$.
ii) $E(u, v) = Im({}^t\overline{u}Hv)$. Alors, $E(\gamma_1, \gamma_2)$ et $E(\tilde{\gamma}_3, \gamma_4) \in \mathbb{Z} \Rightarrow Im(h) \in \mathbb{Z}$ mais aussi $Im(h)(\sqrt{6} - \sqrt{5}) \in \mathbb{Z}$, donc $Imh = 0$ par l'indication. Noter pour la suite que $h \in \mathbb{R}$.
iii) En éliminant h_1 entre les expressions des entiers $E(\gamma_1, \tilde{\gamma}_3) = a$ et $E(\gamma_1, \gamma_4) = b$, on trouve $(\sqrt{6}-\sqrt{5})h = \pm b \pm a\sqrt{2}$. De même, $E(\gamma_2, \tilde{\gamma}_3) = c$ et $E(\gamma_2, \gamma_4) = d$ donnent $(\sqrt{6} - \sqrt{5})h = \pm c\sqrt{5} \pm d\sqrt{3}$. L'indication permet de conclure.

II- 2^o/ ii) γ_1 et γ_3, qui sont $\mathbb{R}$-l.i., appartiennent à D_0.
iii) C'est clair pour la droite $D_\infty : z_1 = 0$. Pour les autres, $\gamma = a\gamma_1 + ... + d\gamma_4$ et $\gamma' = a'\gamma_1 + ... + d'\gamma_4$ $(a, ..., d' \in \mathbb{Z})$ sont sur $D_{\lambda \neq 0}$ si et slt si $b + di\sqrt{5} = 0 =$

$a+i(c+d\sqrt{2})$, ce qui impose $\gamma = 0$ (car $\sqrt{2} \notin \mathbb{Q}$), ou si $\frac{b'+d'i\sqrt{5}}{b+di\sqrt{5}} = \frac{a'+i(c'+d'\sqrt{2})}{a+i(c+d\sqrt{2})}$, qui est alors un nombre rationnel, auquel cas $\gamma' \in \mathbb{Q}.\gamma$. Ainsi, $D_\lambda \cap \Gamma$ ne peut être un réseau de D_λ.
iv) Si X était polarisable, il contiendrait un sous-tore strict X_0', forcément $\neq X_0$, tel que $X_0 + X_0' = X$.

II- 3^o/ i) $F(\Gamma) = \mathbb{Z} \oplus i\sqrt{5}\mathbb{Z}$ est un réseau de $\mathbb{C}$, donc $X' = \mathbb{C}/\Gamma'$ est une courbe elliptique. Considérer alors f : classe de v mod. $\Gamma \mapsto$ classe de $F(v)$ mod. Γ'.
ii) X' admet une telle fonction $\wp(z)$. Considérer $\wp \circ f$.

II- 4^o/ i) Les mêmes calculs donnent $E = 0$, donc $H = 0$.
ii) Soit D le diviseur polaire d'une telle fonction ϕ. Alors, le fibré $\mathcal{L} = \mathcal{O}_{\tilde{X}}(D) := \mathcal{L}(0, \alpha)$ admet une section holomorphe non nulle, représentée par une fonction θ de caractéristique $(0, \alpha)$. Comme $|\theta|$ est bornée, θ est constante, donc ϕ est holomorphe, donc constante.

$\sim$

III-1^o/i) Comme $X \not\simeq \mathbb{P}_1$, le rappel entraîne que $L(P)$ ne contient que des constantes.
ii) $\ell(P) - \ell(\mathbf{K} - P) = deg(P) + 1 - g$.

III-2^o/ i) $L(\mathbf{K} - P) \simeq \{f \in k(X), div(f\omega) \geq P\}$ s'identifie au k-e-v. des formes différentielles régulières s'annulant en P. D'après 1^0/.ii, c'est un hyperplan de $\Omega^1(X)$, donc l'un au moins des ω_i n'y appartient pas.
ii) Si t est un autre paramètre local, $\frac{dt}{dz} = g$ est une fonction régulière (resp. holomorphe) au voisinage de P, non nulle en P, et les coordonnées du vecteur sont multipliées par $g(P)$.

III-3^o/ Dans le cas contraire, il existerait une forme différentielle $\omega = \alpha_1\omega_1 + ... + \alpha_g\omega_g \in \Omega^1(X), \omega \not\equiv 0$, s'annulant sur tout X.

III-4^o/ Pour (iii) $\Leftrightarrow$ (iv) : via un paramètre local en Q, la condition pour un ω de s'annuler en Q s'exprime comme l'annulation d'une forme linéaire ℓ_Q sur $\Omega^1(X)$, donc (iii) $\Leftrightarrow$ la restriction de ℓ_Q à $L(\mathbf{K} - P)$ n'est pas identiquement nulle $\Leftrightarrow \ell(\mathbf{K} - P - Q) = \ell(\mathbf{K} - P) - 1$. Puis appliquer 1^o/ ii).
Pour (v) $\Leftrightarrow$ (vi) : d'après 1^o/ i), une fonction x admet $P + Q$ pour diviseur polaire si et seulement si x est non constante et appartient à $L(P + Q)$.

III-5^o/ Si $X \not\simeq \mathbb{P}_1$ n'est pas hyperelliptique, il n'existe pas de $x \in k(X)$ tel que $[k(X) : k(x)] = 2$. D'après le rappel du 1^o/, (vi) est alors vérifié pour tout couple (P, Q) de points distincts .

$\sim$