REPRÉSENTABILITÉS

Première partie 1. Introduction

Objectif. L'objectif de cette première partie du cours est de construire un espace de module pour les variétés abéliennes polarisées munies de quelques structures additionnelles. C'est dans un avatar de cet espace que nous découperons, dans un second temps, des *variétés de Shimura* (de type PEL, c'est-à-dire classifiant des variétés abéliennes munies de **P**olarisations, d'**E**ndomorphismes, et de structures de niveaux (**L**evel structures en anglais)).

Construction. La construction de cet espace de module est un véritable légo, dont voici les grands acteurs.

- Le foncteur $\mathbf{A}^g_{d,n}$: classifie les variétés abéliennes $f : A \to S$ de dimension g, munies d'une polarisation $\lambda : A \to A^t$ de degré d^2, et d'une structure de niveau $\kappa : (\mathbf{Z}/n\mathbf{Z})^{2g}_S \simeq A[n]$. La polarisation λ permet de construire un faisceau inversible $\mathcal{L}(\lambda)$ sur A qui est S-ample et tel que $\mathcal{E}(\lambda) = f_\star(\mathcal{L}(\lambda)^{\otimes 3})$ est un faisceau localement libre sur S de rang $N+1$ où $N = N(g,d)$ est un entier que l'on explicitera. Le morphisme d'adjonction $f^\star\mathcal{E}(\lambda) \to \mathcal{L}(\lambda)^{\otimes 3}$ est surjectif, et définit un plongement $\iota(\lambda) : A \hookrightarrow \mathbf{P}(\mathcal{E}(\lambda))$.
- Le foncteur $\mathbf{RA}^g_{d,n}$: classifie les quadruplets $(A, \lambda, \kappa, \phi)$ où (A, λ, κ) est comme ci-dessus, et où $\phi : \mathcal{E}(\lambda) \simeq \mathcal{O}_S^{N+1}$ est une rigidification. Cette rigidification nous fournit un isomorphisme $\mathbf{P}(\mathcal{E}(\lambda)) \simeq \mathbf{P}(\mathcal{O}_S^{N+1}) = \mathbf{P}^N_S$, et le triplet (A, λ, ϕ) induit donc un plongement $\iota(\lambda, \phi) : A \hookrightarrow \mathbf{P}^N_S$. L'oubli de ϕ donne un morphisme $\mathbf{RA}^g_{d,n} \to \mathbf{A}^g_{d,n}$.
- Le foncteur $\mathbf{Hilb}^{2g}_N$: classifie les couples formés d'un sous-schéma fermé Z de $\mathbf{P}^N_S$ qui est S-plat et de $2g$ sections $\kappa_i : S \to Z$. Le choix d'une base e_i de $(\mathbf{Z}/n\mathbf{Z})^{2g}$ permet de définir un morphisme $\mathbf{RA}^g_{d,n} \to \mathbf{Hilb}^{2g}_N$ qui à $(A, \lambda, \kappa, \phi)$ associe le sous-schéma fermé S-plat $Z = \iota(\lambda, \phi)(A) \subset \mathbf{P}^N_S$ muni des $2g$-sections $\iota(\lambda, \phi) \circ \kappa(e_i)$.
- Le foncteur $\mathbf{Hilb}_N$: classifie les sous-schémas fermés Z de $\mathbf{P}^N_S$ qui sont plats sur S. L'oubli des $2g$-sections fournit un morphisme $\mathbf{Hilb}^{2g}_N \to \mathbf{Hilb}_N$.
- Les foncteurs $\mathbf{Hilb}^\phi_N$ sont des sous-foncteurs de $\mathbf{Hilb}_N$ qui classifient les sous-schémas fermés S-plats Z de $X = \mathbf{P}^N_S$ dont le polynome de Hilbert ϕ_Z est fixé (égal à ϕ). Pour de tels sous-schémas, on peut démontrer qu'il existe un entier $m(\phi)$ explicite tel que pour tout $m \geq m(\phi)$, la surjection $\mathcal{O}_X(m) \twoheadrightarrow \mathcal{O}_Z(m)$ induit une surjection $\pi_\star\mathcal{O}_X(m) \twoheadrightarrow \pi_\star\mathcal{O}_Z(m)$ entre *faisceaux localement libres sur* S (de rang ... et $\phi(m)$ respectivement).
- Pour $\mathcal{F} = \pi_\star\mathcal{O}_X(m)$ et $r = \phi(m)$ (avec $m \geq m(\phi)$), le foncteur $\mathbf{Grass}(\mathcal{F}, r)$ classifie les quotients $\mathcal{F} \to \mathcal{Q}$ qui sont localement libres de rang r sur S. La construction ci-dessus donne donc un morphisme $\mathbf{Hilb}^\phi_N \to \mathbf{Grass}(\mathcal{F}, r)$.

Pour résumer, on a donc le diagramme suivant :

$$\mathbf{Grass}(\mathcal{F}, r) \leftarrow \mathbf{Hilb}_N^{\phi} \hookrightarrow \mathbf{Hilb}_N \leftarrow \mathbf{Hilb}_N^{2g} \leftarrow \mathbf{RA}_{d,n}^{g} \rightarrow \mathbf{A}_{d,n}^{g}.$$

Nous démontrerons la représentabilité de ces foncteurs "de gauche à droite". En chemin, nous expliquerons un peu les techniques qui permettent de "transférer" la propriété pour un foncteur (sur une catégorie de Schémas) d'être représentable à travers un morphisme de foncteurs $F : \mathbf{X} \to \mathbf{Y}$. Il y a un critère simple pour que $\mathbf{Y}$ représentable implique $\mathbf{X}$ représentable : il faut que F soit relativement représentable, cf. proposition 1.1. Il est beaucoup plus difficile d'aller dans l'autre sens : $\mathbf{X}$ représentable implique $\mathbf{Y}$ représentable. Nous verrons quelques critères pour cette *descente*, et tâcherons de l'appliquer au cas de $\mathbf{RA}_{d,n}^{g} \to \mathbf{A}_{d,n}^{g}$.

Schéma de Picard. Pour la formulation même du problème $\mathbf{A}_{d,n}^{g}$, nous devons savoir définir le "schéma abélien dual" A^t/S de A/S. Il nous faut pour cela étudier encore un autre foncteur, le foncteur de Picard $\mathbf{Pic}_{X/S}$ d'un schéma X/S (dans le cas projectif lisse muni d'une section). Sans entrer dans trop de détails, celui-ci s'obtient par un légo du type suivant :

$$\begin{array}{ccccc} & & D(\phi) & \to & \mathbf{Pic}_{X/S}^{\phi} \\ & & \cap & & \cap \\ \mathbf{Hilb}_{X/S} & \leftarrow & \mathbf{Div}_{X/S} & \to & \mathbf{Pic}_{X/S} \end{array}$$

où $\mathbf{Div}_{X/S}$ classifie les diviseurs effectifs sur X qui sont plats sur S, $\mathbf{Hilb}_{X/S}$ tous les sous-schémas fermés Z de X plats sur S, et où $\mathbf{Pic}_{X/S} = \coprod \mathbf{Pic}_{X/S}^{\phi}$ est un découpage par des polynomes de Hilbert associés au choix d'un plongement $X \hookrightarrow \mathbf{P}(\mathcal{E})$. Comme dans le cas précédent, la partie la plus difficile de la preuve est la descente $D(\phi) \to \mathbf{Pic}_{X/S}^{\phi}$.

Deuxième partie 2. Critères et Exemples

1. Critères de Représentabilité

1.1. **Morphismes relativement représentables.** Soit $\alpha : \mathcal{F} \to \mathcal{G}$ un morphisme de foncteur $\mathcal{F}, \mathcal{G} : (\mathbf{Sch}/S)^0 \to \mathbf{Ens}$. Pour tout T/S et $g \in \mathcal{G}(T)$, on note $\mathcal{F}_g : (\mathbf{Sch}/T)^0 \to \mathbf{Ens}$ le sous-foncteur de $\mathcal{F}|T$ défini par

$$\mathcal{F}_g(T') = \{f \in \mathcal{F}(T') : \alpha(f) = g|T'\}.$$

On dit que α est relativement représentable si et seulement si pour tout T/S et tout $g \in \mathcal{G}(T)$, $\mathcal{F}_g$ est représentable (par un T-schéma).

Proposition 1.1. *Supposons que $\mathcal{G}$ est représentable. Alors $\mathcal{F}$ est représentable si et seulement si α est relativement représentable.*

Démonstration. Supposons que $\mathcal{F}$ et $\mathcal{G}$ sont représentables par des S-schémas F et G, et soit $F \to G$ le morphisme correspondant à α. Soit T/S et $g \in \mathcal{G}(T)$, correspondant à un morphisme $T \to G$. Alors $\mathcal{F}_g$ est représentable par $F \times_G T$, donc α est relativement représentable. Supposons ensuite que $\mathcal{G}$ est représentable par un S-schéma G. Soit $g \in \mathcal{G}(G)$ l'élément universel. Si $\mathcal{F}_g$ est représentable par un G-schéma F, alors F représente $\mathcal{F}$ et α correspond au morphisme structural $F \to G$. □

1.2. **Faisceaux et Représentabilité, I.** Soit $\mathcal{F} : (\mathbf{Sch}/S)^0 \to \mathbf{Ens}$ un foncteur. On dit que $\mathcal{F}$ est un faisceau (pour la topologie de Zariski) si et seulement si pour tout S-schéma T sur S et pour tout recouvrement ouvert T_i de T,

$$\mathcal{F}(T) = \ker\left(\prod_i \mathcal{F}(T_i) \rightrightarrows \prod_{i,j} \mathcal{F}(T_{i,j})\right) \quad \text{où } T_{i,j} = T_i \cap T_j = T_i \times_T T_j.$$

Si $T' = \coprod T_i$, on a donc $\mathcal{F}(T') = \prod \mathcal{F}(T_i)$, $\mathcal{F}(T' \times_T T') = \prod_{i,j} \mathcal{F}(T_{i,j})$ et

$$\mathcal{F}(T) = \ker\left(\mathcal{F}(T') \rightrightarrows \mathcal{F}(T' \times_T T')\right) \tag{1.1}$$

On vérifie facilement que *tout foncteur représentable est un faisceau.* Inversement :

Proposition 1.2. *Soit $\mathcal{F} : (\mathbf{Sch}/S)^0 \to \mathbf{Ens}$ un foncteur, (S_i) un recouvrement ouvert de S et $S' = \coprod S_i$. Si $\mathcal{F}$ est un faisceau (pour Zar), les conditions suivantes sont équivalentes.*

(1) *$\mathcal{F}$ est représentable,*
(2) *Pour tout i, $\mathcal{F}_i = \mathcal{F}|S_i : (\mathbf{Sch}/S_i)^0 \to \mathbf{Ens}$ est représentable,*
(3) *$\mathcal{F}' = \mathcal{F}|S' : (\mathbf{Sch}/S')^0 \to \mathbf{Ens}$ est représentable.*

Démonstration. (1) $\Rightarrow$ (2) $\iff$ (3) est facile. Pour (2) $\Rightarrow$ (1) : soit X_i/S_i représentant $\mathcal{F}_i$, $f_i : X_i \to S_i$ le morphisme structural, $S_{ij} = S_i \cap S_j$ et $X_{ij} = f_i^{-1}(S_{ij})$. Alors X_{ij}/S_{ij} et X_{ji}/S_{ij} représentent $\mathcal{F}_i|S_{ij} = \mathcal{F}|S_{ij} = \mathcal{F}_j|S_{ij}$, ce qui nous fournit une *donnée de recollement* $\phi_{ij} : X_{ij} \simeq X_{ji}$. En considérant de même des intersections de trois ouverts, on voit que ces données de recollement vérifient une condition naturelle de compatibilité qui permette de recoller tous les X_i/S_i en un schéma X/S. Soit $\mathcal{G}$ le foncteur représenté par ce schéma, de sorte que $\mathcal{F}|S_i \simeq \mathcal{G}|S_i$ pour tout i. Pour tout $T \to S$, soit T_i et T_{ij} les images inverses de S_i et S_{ij}. Puisque $\mathcal{F}$ et $\mathcal{G}$ sont des faisceaux, on a

$$\mathcal{F}(T) = \ker\left(\prod \mathcal{F}(T_i) \to \prod \mathcal{F}(T_{ij})\right) = \ker\left(\prod \mathcal{G}(T_i) \to \prod \mathcal{G}(T_{ij})\right) = \mathcal{G}(T)$$

donc $\mathcal{F} \simeq \mathcal{G}$, i.e. X représente $\mathcal{F}$. □

Remark 1.3. On ne dit pas "$\mathcal{F}$ est un faisceau (pour la topologie de Zariski) sur $\mathbf{Sch}/S$", mais "le foncteur est (Zariski-)local sur S".

Definition 1.4. On dit d'une famille de sous-foncteurs $\mathcal{F}_i$ de $\mathcal{F}$ que c'est un recouvrement ouvert de $\mathcal{F}$ ssi (1) $\mathcal{F}_i \hookrightarrow \mathcal{F}$ est relativement représentable par des immersions ouvertes, et (2) $\mathcal{F}(x) = \cup \mathcal{F}_i(x)$ pour tout S-schéma ponctuel x.

Proposition 1.5. *Si $\mathcal{F}$ est un faisceau, alors $\mathcal{F}$ est représentable si et seulement si tous les $\mathcal{F}_i$ le sont.*

Démonstration. Soit X_i représentant $\mathcal{F}_i$, $\alpha_i \in \mathcal{F}_i(X_i) \subset \mathcal{F}(X_i)$ l'élément universel, $X_{i,j}$ l'ouvert de X_i représentant $(\mathcal{F}_j)_{\alpha_i}$ et $\alpha_{i,j} \in \mathcal{F}_j(X_{i,j}) \subset \mathcal{F}(X_{i,j})$ l'élément universel. Alors $\alpha_{i,j} = \alpha_i|X_{i,j}$ et $(X_{i,j}, \alpha_{i,j})$ représente $\mathcal{F}_i \cap \mathcal{F}_j$. Il existe donc un (unique) isomorphisme $\phi_{i,j} : X_{i,j} \to X_{j,i}$ qui envoie $\alpha_{i,j}$ sur $\alpha_{j,i}$. Ces isomorphismes vérifient la condition de cocycle, et les X_i se recollent en un S-schéma X. Puisque $\mathcal{F}$ est un faisceau, les α_i se recollent aussi en une section α de $\mathcal{F}$ sur X. Vérifions que (X, α) représente $\mathcal{F}$. Soit donc T/S et $\gamma \in \mathcal{F}(T)$. Soient T_i les ouverts qui représentent $(\mathcal{F}_i)_\gamma$, et $\gamma_i = \gamma|T_i$. Alors γ_i correspond à un morphisme $f_i : T_i \to X_i$ tel que $\gamma_i = f^\star \alpha_i$ et $f_i^{-1}(X_{i,j}) = T_i \cap T_j$ et $f_i = f_j$ sur $T_i \cap T_j$: les morphismes f_i

se recollent en un morphisme $f : \cup T_i \to X$. Puisque les $\mathcal{F}_i$ recouvrent $\mathcal{F}$, $\cup T_i = T$. Enfin $f^\star \alpha = \gamma$ car $\mathcal{F}$ est un faisceau et $f^\star \alpha | T_i = f_i^\star \alpha_i = \gamma_i = \gamma | T_i$. Le morphisme f est unique car ses restrictions aux T_i le sont. □

2. Exemples

2.1. Morphismes.

Lemma 2.1. *Soit $f, g : S \to X$ deux sections d'un S-schéma X. La condition $f = g$ est représentable par le sous-schéma $S(f = g) = (f, g)^{-1}(\Delta_X)$, où $\Delta_X : X \to X \times_S X$ est la diagonale. Si X/S est séparé, $S(f = g)$ est un sous-schéma fermé de S.*

Démonstration. C'est essentiellement une tautologie. □

Lemma 2.2. *Soient S un schéma, X et Y deux S-schémas propres et plats sur S et $f : X \to Y$ un S-morphisme. Les conditions suivantes sont représentables par des ouverts de S : (1) f est plat, (2) f est fini, (3) f est un isomorphisme.*

Démonstration. (1) Soit $S' = S - \pi_X(X - X')$ où $X' = \{x \in X | f \text{ est plat en } x\}$. D'après [1, IV, 11.3.1], X' est ouvert, donc $X - X'$ est fermé, $\pi_X(X - X')$ aussi puisque π_X est propre donc fermé, donc S' est ouvert. Par construction, pour tout $s \in S'$, $X_s \subset X'$ donc $f_s : X_s \to Y_s$ est plat. D'après [1, IV, 11.3.10], f est alors plat au-dessus de S'. Soit maintenant $T \to S$ tel que $f_T : X_T \to Y_T$ est plat. Pour $t \in T \mapsto s \in S$, $f_t : X_t \to Y_t$ est plat, donc $f_s : X_s \to Y_s$ est plat d'après [1, IV, 2.5.1]. Une nouvelle application de [1, IV, 11.3.10] montre alors que f est plat en tout point de X_s (puisque π_X est plat), i.e. $X_s \subset X'$ et $s \in S'$. Donc T se factorise par S'.

(2) Soit $S' = S - \pi_X(X - X')$ où $X' = \{x \in X | x \text{ est isolé dans } f^{-1}f(x)\}$. Puisque X et Y sont propres sur S, $f : X \to Y$ est propre d'après [1, II, 5.4.3]. Donc X' est ouvert dans X, $X - X'$ est fermé, $\pi_X(X - X')$ aussi puisque π_X est propre donc fermé et S' est ouvert. Par construction, pour tout $s \in S'$, $X_s \subset X'$ donc $f_s : X_s \to Y_s$ est quasi-fini. Puisque $f : X \to Y$ est propre, f est propre et quasi-fini au-dessus de S', donc fini d'après [1, IV, 8.11.1]. Soit maintenant $T \to S$ tel que $f_T : X_T \to Y_T$ soit fini. Pour $t \in T \mapsto s \in S$, $f_t : X_t \to Y_t$ est fini, donc $f_s : X_s \to Y_s$ est fini d'après [1, IV, 2.7.1, xv]. Ainsi $X_s \subset X'$ et $s \in S'$, i.e. $T \to S$ se factorise par S'.

(3) On peut déjà supposer que f est plat et fini. Soit $S' = S - \pi_Y(Y - Y')$ où $Y' = \{y \in Y : f^{-1}(y) \simeq y\}$. C'est l'ouvert de Y où $f_\star \mathcal{O}_X$ est de rang 1 sur $\mathcal{O}_Y$. Puisque π_Y est propre donc fermé, S' est ouvert dans S. Par construction, $\pi^{-1}(S') \subset Y'$, donc $f : X \to Y$ est de rang 1 au-dessus de S', i.e. c'est un isomorphisme. Soit maintenant $T \to S$ tel que $f_T : X_T \to Y_T$ soit un isomorphisme. Pour $t \in T \mapsto s \in S$, $f_t : X_t \to Y_t$ est un isomorphisme, donc $f_s : X_s \to Y_s$ est un isomorphisme d'après [1, IV, 2.7.1, viii]. En particulier, $Y_s \subset Y'$, donc $s \in S'$ et $T \to S$ se factorise par S', CQFD. □

2.2. Schémas Affines.

Proposition 2.3. *Soit $\mathcal{B}$ une $\mathcal{O}_S$-algèbre quasi-cohérente. Alors*

$$(\mathbf{Sch}/S)^0 \to Ens : \qquad T \mapsto \mathrm{Hom}_{\mathcal{O}_T-alg}(\mathcal{B}_T, \mathcal{O}_T) = \mathrm{Hom}_{\mathcal{O}_S-alg}(\mathcal{B}, \pi_\star \mathcal{O}_T)$$

est représentable par un S-schéma affine que l'on note Spec$\mathcal{B}$.

Démonstration. Le problème est local sur S, on peut donc supposer que $S = \mathrm{Spec}A$ et $\mathcal{B} = \widetilde{B}$ où B est une A-algèbre, et le résultat résulte alors du lemme suivant. □

Lemma 2.4. *Pour tout S-schéma T, on a*

$$\mathrm{Hom}_{\mathcal{O}_S-alg}(\widetilde{B}, \pi_\star \mathcal{O}_T) = \mathrm{Hom}_{A-alg}(B, \Gamma(T, \mathcal{O}_T)) = \mathrm{Hom}_S(T, \mathrm{Spec}B).$$

Démonstration. Ce problème là est local sur T, que l'on peut donc supposer affine, et le lemme résulte alors de l'anti-équivalence de catégorie entre anneaux et schémas affines, où plus précisément entre A-algèbres et S-schémas affines. □

2.3. **Fibrés vectoriels.**

Proposition 2.5. *Soit $\mathcal{F}$ un $\mathcal{O}_S$-module quasi-cohérent. Alors*

$$(\mathbf{Sch}/S)^0 \to Ab : \qquad T \mapsto \Gamma(T, \mathcal{F}_T^\vee) = \mathrm{Hom}_{\mathcal{O}_T}(\mathcal{F}_T, \mathcal{O}_T)$$

est représentable par un S-schéma affine $\mathbf{V}(\mathcal{F}) = \mathrm{Spec}(\mathcal{S}(\mathcal{F}))$.

Démonstration. En effet, soit $\mathcal{S}(\mathcal{F}) = \oplus_{n\geq 0}\mathcal{F}^{\otimes n}$, qui est quasi-cohérente sur S et de formation compatible au changement de base. Alors

$$\mathrm{Hom}_{\mathcal{O}_T}(\mathcal{F}_T, \mathcal{O}_T) = \mathrm{Hom}_{\mathcal{O}_T-alg}(\mathcal{S}(\mathcal{F}_T), \mathcal{O}_T) = \mathrm{Hom}_{\mathcal{O}_T-alg}(\mathcal{S}(\mathcal{F})_T, \mathcal{O}_T)$$

Donc $\mathbf{V}(\mathcal{F}) = \mathrm{Spec}\mathcal{S}(\mathcal{F})$ convient. □

Corollary. *Soient $\mathcal{F}, \mathcal{G}$ deux $\mathcal{O}_S$-modules localement libres. Alors*

$$(\mathbf{Sch}/S)^0 \to Ab : \qquad T \mapsto \mathrm{Hom}_{\mathcal{O}_T}(\mathcal{F}_T, \mathcal{G}_T)$$

est représentable par un S-schéma affine $\underline{\mathrm{Hom}}(\mathcal{F}, \mathcal{G}) = \mathbf{V}(\mathcal{F} \otimes \mathcal{G}^\vee)$.

Démonstration. En effet, $\mathrm{Hom}(\mathcal{F}, \mathcal{G}) = \mathcal{F}^\vee \otimes \mathcal{G} = \mathrm{Hom}(\mathcal{F} \otimes \mathcal{G}^\vee, \mathcal{O})$. □

Corollary 2.6. *Soit $\mathcal{F}$ un $\mathcal{O}_S$-module localement libre. Alors*

$$(\mathbf{Sch}/S)^0 \to Ab : \qquad T \mapsto \Gamma(T, \mathcal{F}_T)$$

est représentable par $\Gamma(\mathcal{F}) = \mathbf{V}(\mathcal{F}^\vee)$.

Démonstration. En effet, $\Gamma(T, \mathcal{F}_T) = \mathrm{Hom}_{\mathcal{O}_T}(\mathcal{O}_T, \mathcal{F}_T)$. □

Corollary 2.7. *Soit $f, g : \mathcal{F} \to \mathcal{G}$ deux morphismes, avec $\mathcal{F}$ et $\mathcal{G}$ localement libres. La condition $f = g$ définit un sous-schéma fermé de S que l'on note $S(f = g)$. Soit $f \in \Gamma(S, \mathcal{F})$. La condition $f = 0$ définit un sous-schéma fermé de S que l'on note $S(f = 0)$.*

Démonstration. Les morphismes $f, g : \mathcal{F} \to \mathcal{G}$ définissent des sections f, g du S-schéma $\underline{\mathrm{Hom}}(\mathcal{F}, \mathcal{G})$, lequel est séparé sur S, et on applique le lemme 2.1. Idem pour $f \in \Gamma(S, \mathcal{F})$ avec $\Gamma(\mathcal{F})$. □

Mentionnons également :

Lemma 2.8. *Soit $f : \mathcal{F} \to \mathcal{G}$ un morphisme. La condition f est un isomorphisme définit un sous-schéma ouvert de S que l'on note $S(f)$.*

Démonstration. C'est local sur S, on peut donc supposer que $\mathcal{F}$ et $\mathcal{G}$ sont libres sur S affine, alors f a un déterminant, et on veut que ce déterminant soit inversible. □

2.4. Fibrés projectifs et Grassmaniennes.

Proposition 2.9. *Soit $\mathcal{E}$ un $\mathcal{O}_S$-module localement libre et r un entier. Alors*

$$(\mathbf{Sch}/S)^0 \to Ens : \qquad T \mapsto \{\text{quotients } \mathcal{E}_T \twoheadrightarrow \mathcal{Q} \text{ de } \mathcal{E}_T \text{ localement libres de rang } r\}$$

est représentable par un S-schéma que l'on note $\mathbf{Grass}(\mathcal{E}, r)$.

Démonstration. On commence par réécrire ce foncteur

$$T \mapsto \mathcal{P}(T) = \{\mathcal{G} \subset \mathcal{E}_T | \mathcal{E}_T/\mathcal{G} \text{ localement libre de rang } r\}.$$

Le foncteur est local sur S, et l'on peut donc supposer que S est affine et $\mathcal{E}$ libre, disons $\mathcal{E} = \mathcal{O}_S^m$. Soit $\mathcal{J}$ l'ensemble des parties de $I = \{1, \cdots, m\}$ de cardinal r, et pour tout $J \in \mathcal{J}$, soit

$$\mathcal{P}_J(T) = \left\{\mathcal{G} \subset \mathcal{O}_T^m | \mathcal{G} \oplus \mathcal{O}_T^J = \mathcal{O}_T^m\right\}.$$

C'est un sous-foncteur de $\mathcal{P}$. On a

$$\mathcal{P}_J(T) \simeq \mathrm{Hom}_{\mathcal{O}_T}(\mathcal{O}_T^{I-J}, \mathcal{O}_T^J)$$

via $\mathcal{G} \mapsto \pi_{\mathcal{G}} | \mathcal{O}_T^{I-J}$ où $\pi_{\mathcal{G}} : \mathcal{O}_T^I = \mathcal{G} \oplus \mathcal{O}_T^J \to \mathcal{O}_T^J$ est la deuxième projection. La bijection inverse est $(\phi : \mathcal{O}_T^{I-J} \to \mathcal{O}_T^J) \mapsto \mathcal{G} = \ker(\phi + \mathrm{Id} : \mathcal{O}_T^{I-J} \oplus \mathcal{O}_T^J \to \mathcal{O}_T^J)$. On voit donc que ce sous-foncteur est représentable : par $V(\mathcal{O}_S^{J \times I-J}) = \mathbf{A}_S^{r\cdot(m-r)}$. On conclut d'après la proposition 1.5 avec le lemme suivant. $\square$

Lemma 2.10. *Les $\mathcal{P}_J \hookrightarrow \mathcal{P}$ forment un recouvrement ouvert de $\mathcal{P}$.*

Démonstration. Soit $\mathcal{G} \in \mathcal{P}(T)$, i.e. $\mathcal{G} \subset \mathcal{O}_T^m$ et $\mathcal{O}_T^m/\mathcal{G}$ est localement libre de rang r. Soit $T_J \subset T$ le lieu où $\mathcal{G} \in \mathcal{P}_J$: c'est le lieu où $\mathcal{O}_T^J \to \mathcal{O}_T^m/\mathcal{G}$ est un isomorphisme, et c'est donc un ouvert de T d'après le lemme 2.8. De plus, pour tout point t de T, $t \in T_J$ pour au moins un J. CQFD. $\square$

Example 2.11. On note $\mathbf{P}(\mathcal{E}) = \mathbf{Grass}(\mathcal{E}, 1)$ et $\mathbf{P}_S^n = \mathbf{P}(\mathcal{O}_S^{n+1})$. Si $\mathcal{E}$ est localement libre de rang 1, $\mathbf{P}(\mathcal{E}) = S$. En général, il y a sur $\mathbf{P} = \mathbf{P}(\mathcal{E})$ un faisceau inversible universel quotient de $\mathcal{E}_P$: on le note $\mathcal{E}_P \twoheadrightarrow \mathcal{O}_{\mathbf{P}}(1)$. Se donner un morphisme $f : X \to \mathbf{P}$ revient à se donner un quotient $\mathcal{E}_X \twoheadrightarrow \mathcal{L}$, et ce quotient est alors le pull-back de $\mathcal{E}_P \twoheadrightarrow \mathcal{O}_{\mathbf{P}}(1)$. En particulier, $\mathcal{L} = f^\star \mathcal{O}_{\mathbf{P}}(1)$.

Troisième partie 3. Le schéma de Hilbert

3. L'énoncé et ses corollaires

Theorem 3.1. *Soient S un schéma, $\mathcal{E}$ un $\mathcal{O}_S$-module localement libre, et X un sous-schéma fermé de $\mathbf{P}(\mathcal{E})$ qui est plat et de présentation finie sur S. Le foncteur*

$$(\mathbf{Sch}/S)^0 \to Ens : \qquad T \mapsto \left\{ Z | \begin{array}{c} Z \text{ sous-schéma fermé de } X_T \\ \text{plat de présentation finie sur } T \end{array} \right\}$$

est représentable par un S-schéma que l'on note $\mathbf{Hilb}_{X/S}$.

Corollary 3.2. *Soient X et Y des S-schémas projectifs et plats. Le foncteur*

$$(\mathbf{Sch}/S)^0 \to Ens : \qquad T \mapsto \mathbf{Hom}_T(X_T, Y_T)$$

est représentable par un S-schéma que l'on note $\mathbf{Hom}_S(X, Y)$.

Démonstration. L'application qui à un morphisme associe son graphe induit une bijection entre $\mathbf{Hom}_T(X_T, Y_T)$ et l'ensemble des sous-schémas fermés (car $Y_T \to T$ est séparée) Z de $X_T \times_T Y_T = (X \times_S Y)_T$ tels que la projection $X_T \times_T Y_T \to X_T$ induise un isomorphisme de Z sur X_T. Puisque X_T est plat sur T, de tels sous-schémas le sont également. On obtient ainsi un plongement $\mathbf{Hom}_S(X,Y) \hookrightarrow \mathbf{Hilb}_{X\times_S Y/S}$. Le lemme 2.2 montre que ce morphisme est représentable par des immersions ouvertes. $\square$

4. Preuve du Théorème

4.1. **Réduction à $X \subset \mathbf{P}^N_S$, $S = \mathrm{Spec}A$, A noethérien.** Le problème est local sur S, et l'on peut donc supposer que $S = \mathrm{Spec}A$ et $\mathcal{E} \simeq \mathcal{O}_S^{N+1}$, i.e. $\mathbf{P}(\mathcal{E}) \simeq \mathbf{P}^N_A$. Comme X est de présentation finie sur A, tout est déjà défini sur un sous-anneau de A qui est de type fini sur $\mathbf{Z}$, donc noethérien : on remplace A par ce sous-anneau.

4.2. **Polynomes de Hilbert.** Pour tout faisceau coherent $\mathcal{F}$ sur X et tout point $s \in S$, on pose

$$\chi(\mathcal{F}_s) = \sum_i (-1)^i \dim_{k(s)} H^i(X_s, \mathcal{F}_s).$$

Lemma 4.1. *C'est bien défini, et la fonction*

$$n \mapsto \phi(\mathcal{F}_s)(n) = \chi(\mathcal{F}_s(n)) = \sum_i (-1)^i \dim_{k(s)} H^i(X_s, \mathcal{F}_s)$$

est polynomiale de degré inférieur ou égal à la dimension du support de $\mathcal{F}_s$.

Démonstration. Voir plus bas. $\square$

Lemma 4.2. *Si $\mathcal{F}$ est S-plat, les fonctions*

$$s \mapsto \chi(\mathcal{F})(s) = \chi(\mathcal{F}_s) \quad \textit{et} \quad s \mapsto \phi(\mathcal{F})(s) = \phi(\mathcal{F}_s)$$

sont continues, i.e. localement constantes sur S.

Démonstration. Voir plus bas. $\square$

Pour tout sous-schéma fermé Z de X qui est de présentation finie sur S, le $\mathcal{O}_X$-faisceau $\mathcal{O}_Z$ est cohérent, et plat sur S ssi Z l'est. On pose $\phi(Z) = \phi(\mathcal{O}_Z)$. Pour tout polynome $\phi \in \mathbf{Q}[x]$, on définit un sous-foncteur de $\mathbf{Hilb}_{X/S}$ par

$$\mathbf{Hilb}^{\phi}_{X/S}(T) = \left\{ Z \in \mathbf{Hilb}_{X/S}(T) : \phi(Z) \equiv \phi \text{ sur } T \right\}.$$

Il résulte alors immédiatement du lemme précédent que :

Proposition 4.3. *Les $\mathbf{Hilb}^{\phi}_{X/S}$ forment un recouvrement ouvert de $\mathbf{Hilb}_{X/S}$.*

Il suffit donc de montrer que chacun des $\mathbf{Hilb}^{\phi}_{X/S}$ est représentable.

4.3. **Caractère borné de $\mathbf{Hilb}^{\phi}_{X/S}$.** On fixe un polynome de Hilbert $\phi \in \mathbf{Q}[X]$.

Lemma 4.4. *Il existe un entier $m(\phi) \geq 0$ tel que pour tout $m \geq m(\phi)$, pour tout $Z \in \mathbf{Hilb}^{\phi}_{X/S}(T)$ correspondant à une suite exacte de $\mathcal{O}_{X_T}$-modules*

$$0 \to \mathcal{I}_Z \to \mathcal{O}_{X_T} \to \mathcal{O}_Z \to 0,$$

les propriétés suivantes sont vérifiées :

(1) *la suite de $\mathcal{O}_T$-modules*

$$0 \to f_\star \mathcal{I}_Z(m) \to f_\star \mathcal{O}_{X_T}(m) \to f_\star \mathcal{O}_Z(m) \to 0$$

est exacte,

(2) $f_\star \mathcal{O}_X(m)$ *est localement libre et* $f_\star \mathcal{O}_{X_T}(m) = f_\star \mathcal{O}_X(m)_T$,

(3) $f_\star \mathcal{O}_Z(m)$ *est localement libre de rang* $\phi(m)$, *et*

(4) $f^\star f_\star \mathcal{I}_Z(m) \to \mathcal{I}_Z(m)$ *est surjective.*

Démonstration. Voir plus bas. □

4.4. **Fin de la preuve.** Soit $m \geq m(\phi)$ comme ci-dessus et $r = \phi(m)$. Alors $\mathcal{E} = f_\star \mathcal{O}_X(m)$ est localement libre. D'après $(1-3)$ ci-dessus, tout $Z \in \mathbf{Hilb}^\phi_{X/S}(T)$ définit une suite exacte

$$0 \to f_\star \mathcal{I}_Z(m) \to f_\star \mathcal{O}_{X_T}(m) \simeq \mathcal{E}_T \to f_\star \mathcal{O}_Z(m) \to 0$$

où le quotient $\mathcal{Q}(Z) = f_\star \mathcal{O}_Z(m)$ de $\mathcal{E}_T$ est localement libre de rang r. On obtient donc ainsi un point $\mathcal{Q}(Z)$ de $\mathbf{Grass}(\mathcal{E}, r)(T)$. Cette construction est fonctorielle : on en déduit un morphisme

$$\mathbf{Hilb}^\phi_{X/S} \to \mathbf{Grass}(\mathcal{E}, r).$$

D'après (4), ce morphisme est injectif : la connaissance de $\mathcal{Q}(Z)$ permet de reconstruire $f_\star \mathcal{I}_Z(m) \to f_\star \mathcal{O}_{X_T}(m)$, donc aussi

$$f^\star f_\star \mathcal{I}_Z(m) \to f^\star f_\star \mathcal{O}_{X_T}(m) \to \mathcal{O}_{X_T}(m)$$

et (4) nous dit que l'image de ce morphisme n'est autre que $\mathcal{I}_Z(m)$. Il ne reste plus qu'à tordre par $(-m)$ pour obtenir $\mathcal{I}_Z$, donc le point Z de $\mathbf{Hilb}^\phi_{X/S}(T)$. Soit d'autre part $\mathcal{Q}$ un élément quelconque de $\mathbf{Grass}(\mathcal{E}, r)(T)$, correspondant à une suite exacte

$$0 \to \mathcal{K} \to \mathcal{E}_T = f_\star \mathcal{O}_{X_T}(m) \to \mathcal{Q} \to 0.$$

Définissons un idéal cohérent $\mathcal{I}(\mathcal{Q})$ de $\mathcal{O}_{X_T}$ par la formule

$$\mathcal{I}(\mathcal{Q})(m) = \text{image de } f^\star f_\star \mathcal{K} \to f^\star f_\star \mathcal{O}_{X_T}(m) \to \mathcal{O}_{X_T}(m).$$

Soit $Z(\mathcal{Q})$ le sous-schéma fermé de X_T défini par cet idéal. Alors $\mathcal{Q}$ appartient à l'image de $\mathbf{Hilb}^\phi_{X/S}(T)$ si et seulement si (1) $Z(\mathcal{Q})$ est plat sur T et (2) $\phi(Z(\mathcal{Q})) \equiv \phi$.

La première condition définit un ouvert T_1 de T d'après [1, IV, 11.3.1] et la seconde un ouvert T_2 de T_1 par continuité du polynome de Hilbert : notre morphisme serait-il donc relativement représentable par des immersions ouvertes ? Non : il y a une subtilité. L'ouvert T_1 ci-dessus est

$$T_1 = T - f(Z(\mathcal{Q}) - Z(\mathcal{Q})_1) \quad \text{où } Z(\mathcal{Q})_1 = \{z \in Z(\mathcal{Q}) : Z(\mathcal{Q}) \text{ est plat sur } S \text{ en } z\}.$$

C'est bien le plus gros ouvert de T au-dessus duquel $Z(\mathcal{Q})$ est plat, mais cet ouvert ne *représente pas* la condition "$Z(\mathcal{Q})$ est plat sur T" : si $t \in T - T_1$, $Z(\mathcal{Q})_t$ est plat sur $t = \mathrm{Spec} k(t)$ puisque tout est plat sur un corps ! La vraie preuve repose sur une étude plus explicite de ces conditions, voir Grothendieck dans [5, IV].

5. Vérifications Cohomologiques

On se propose ici de vérifier ce que nous avons admis plus haut concernant la cohomologie des schémas propres ou projectifs. On commence par quelques rappels.

5.1. **Cohomologie des Schémas affines et applications.**

Proposition 5.1. *Soit X un schéma affine et $\mathcal{F}$ un $\mathcal{O}_X$-module quasi-cohérent. Alors $H^i(X,\mathcal{F})=0$ pour tout $i>0$.*

Démonstration. Voir [6, III.3] pour $X=\mathrm{Spec}A$ avec A noethérien, et [1, IIII, 1.3.1] dans le cas général. Il suffit de montrer que si I est un A-module injectif, alors $\widetilde{I}$ est acyclique. En effet : si $\mathcal{F}=\widetilde{M}$, on choisit une résolution injective $0\to M\to I^\bullet$ du A-module M, alors $0\to\widetilde{M}\to\widetilde{I^\bullet}$ est une résolution acyclique du faisceau $\widetilde{M}$, donc

$$H^\star(X,\mathcal{F})=H^\star\Gamma(X,\widetilde{I^\bullet})=H^\star(I^\bullet)=[M,0,\cdots].$$

Dans le cas Noethérien, Hartshorne montre que $\widetilde{I}$ est flasque. □

Corollary 5.2. *Soit $f:X\to Y$ un morphisme affine et $\mathcal{F}$ un $\mathcal{O}_X$-module quasi-cohérent. Alors $R^qf_\star\mathcal{F}=0$ pour $q>0$.*

Démonstration. C'est le faisceau associé au préfaisceau $U\mapsto H^q(f^{-1}(U),\mathcal{F})$, lequel est trivial sur les ouverts affines pour $q>0$. □

Corollary 5.3. *Soit $f:X\to Y$ un morphisme affine et $\mathcal{F}$ un $\mathcal{O}_X$-module quasi-cohérent. Alors $H^q(X,\mathcal{F})=H^q(Y,f_\star\mathcal{F})$ pour tout $q\geq 0$.*

Démonstration. La suite spectrale $E_2^{p,q}=H^p(Y,R^qf_\star\mathcal{F})\Rightarrow H^{p+q}(X,\mathcal{F})$ dégénère. □

Proposition 5.4. *Soit X un schéma séparé quasi-compact et $\mathcal{F}$ un $\mathcal{O}_X$-module quasi-cohérent. Alors $H^q(X,\mathcal{F})$ se calcule par la cohomologie de Cech d'un recouvrement ouvert affine fini.*

Démonstration. Le complexe de Cech faisceautisé est une résolution de $\mathcal{F}$ par des faisceaux de la forme $\iota_\star(\mathcal{F}|U)$ pour des ouverts $\iota:U\hookrightarrow X$. Ces ouverts sont des intersections finies des ouverts affines du recouvrement, et ils sont donc affines puisque X est séparé. Cette même hypothèse garantit que $\iota:U\hookrightarrow X$ est un morphisme affine, donc $H^j(X,\iota_\star\mathcal{F}|U)=H^j(U,\mathcal{F})=0$ pour $j>0$ d'après le corollaire ci-dessus et la proposition. □

5.2. **Cohomologie des schémas projectifs et applications.**

Proposition 5.5. *Soit A un anneau noethérien et $X=\mathbf{P}^N_A$. Alors*

1. $H^i(X,\mathcal{O}_X(j))=0$ *si* $i\neq 0,N$,
2. $H^0(X,\mathcal{O}_X(j))\simeq\{P\in A[s_0,\cdots,s_N]:\deg P=j\}$,
3. $H^N(X,\mathcal{O}_X(j))\simeq\{P\in(s_0\cdots s_N)^{-1}A[s_0^{-1},\cdots,s_N^{-1}]:\deg P=j\}$.

Démonstration. On calcule la cohomologie du faisceau quasi-cohérent $\mathcal{F}=\oplus_{j\in\mathbf{Z}}\mathcal{O}_X(j)$ sur X, en utilisant la résolution de Cech du recouvrement ouvert standard de X par les $X(s_i)\simeq\mathrm{Spec}A[\frac{s_0}{s_i},\cdots,\frac{s_N}{s_i}]$. Ce qui nous ramène à un calcul explicite d'algèbre linéaire, pour lequel on renvoie à [6, III.5] (ou à [1, III, 2.1]). □

Corollary 5.6. *Soit $\mathcal{F}$ un faisceau cohérent sur $X\subset\mathbf{P}^N_A$. Alors $H^i(X,\mathcal{F})$ est un A-module de type fini, $H^i(X,\mathcal{F})=0$ pour tout $i>N$ et $H^i(X,\mathcal{F}(j))=0$ pour tout $i>0$ et $j\gg 0$.*

Démonstration. Puisque $H^i(X,\mathcal{F}) = H^i(\mathbf{P}^N_A, \iota_\star\mathcal{F})$ d'après le corollaire 5.3, on peut supposer que $X = \mathbf{P}^N_A$. En calculant la cohomologie de $H^i(X,\mathcal{F})$ à la Cech comme ci-dessus, on voit que $H^i(X,\mathcal{F}) = 0$ pour tout $i > N$. D'après la lemme suivant, il existe une suite exacte de $\mathcal{O}_X$-module cohérent

$$0 \to \mathcal{G} \to \mathcal{O}_X(n)^R \to \mathcal{F} \to 0 \tag{5.1}$$

qui donne pour tout $j \in \mathbf{Z}$ une suite exacte longue

$$\cdots \to H^i(X, \mathcal{O}_X(n+j))^R \to H^i(X,\mathcal{F}(j)) \to H^{i+1}(X,\mathcal{G}(j)) \to \cdots$$

On conclut facilement par récurrence. □

Lemma 5.7. *Soit $\mathcal{F}$ un faisceau cohérent sur $X \subset \mathbf{P}^N_A$. Il existe alors un entier n tel que $\mathcal{F}(n)$ est engendré par ces sections globales.*

Démonstration. C'est un résultat dû à Serre, cf. [6, II, 5.17]. On se ramène immédiatement à $X = \mathbf{P}^N_A$, on recouvre X par les $X(s_i)$, on écrit $\mathcal{F}|X_i = \widetilde{M_i}$ pour un module M_i de type fini sur $A[\frac{s_0}{s_i}, \cdots, \frac{s_N}{s_i}]$, on choisit des générateurs $m_{i,j}$ de M_i. Le point clé est : il existe un entier n tel que la section $s_i^n \otimes m_{i,j}$ de $\mathcal{O}_X(n) \otimes \mathcal{F} = \mathcal{F}(n)$ sur X_i s'étend en une section globale (pour tout i,j). L'ensemble de ces sections globales permet alors de définir un morphisme $\mathcal{O}_X^R \to \mathcal{F}(n)$. La restriction de ce morphisme à $X(s_i)$ est trivialement surjective. □

Corollary 5.8. *La caractéristique d'Euler-Poincaré $\chi(\mathcal{F})$ est bien définie et additive sur les suites exactes courtes de faisceaux cohérents.*

Dans la suite de ce numéro, on suppose que k est un corps, X un sous-schéma fermé de $\mathbf{P}^N_k$ et $\mathcal{F}$ un faisceau cohérent sur X. Pour toute fonction $\phi : \mathbf{Z} \to \mathbf{Z}$, on pose $\Delta\phi(n) = \phi(n) - \phi(n-1)$. On a donc $\phi \in \mathbf{Q}[X] \iff \Delta\phi \in \mathbf{Q}[X]$ et alors $\deg\phi = \deg\Delta\phi + 1$, avec la convention $\deg 0 = -1$.

Proposition 5.9. *La fonction $\phi(\mathcal{F})(j) = \chi(\mathcal{F}(j))$ est polynomiale en j de degré $d(\mathcal{F})$ inférieur ou égal à la dimension $\dim(\mathcal{F})$ du support de $\mathcal{F}$.*

Démonstration. On peut supposer k algébriquement clos, puisque cohomologie et dimension du support commutent aux changements de bases $k \to k^{alg}$. On raisonne alors par récurrence sur la dimension du support de $\mathcal{F}$. Si $\mathcal{F} = 0$, la proposition est trivialement vraie. Sinon, il existe d'après le lemme suivant une suite exacte $0 \to \mathcal{F}(-1) \to \mathcal{F} \to \mathcal{G} \to 0$ avec $\dim\mathcal{G} < \dim\mathcal{F}$. Par récurrence, on sait donc que $\phi(\mathcal{G})$ est un polynome de degré $d(\mathcal{G}) \leq \dim\mathcal{G}$ (en convenant encore que $\dim 0 = -1$). Mais l'additivité de χ sur les suites exactes courtes de faisceaux cohérents montre par ailleurs que $\Delta(\phi(\mathcal{F})) = \phi(\mathcal{G})$, donc $\phi(\mathcal{F})$ est un polynome de degré $d(\mathcal{F}) = d(\mathcal{G}) + 1 \leq \dim\mathcal{G} + 1 \leq \dim\mathcal{F}$, cqfd. □

Lemma 5.10. *Soit k un corps algébriquement clos, $X \subset \mathbf{P}^N_k$ et $\mathcal{F} \neq 0$ un faisceau cohérent sur X. Alors il existe une section s de $\mathcal{O}_X(1)$ induisant une suite exacte $0 \to \mathcal{F}(-1) \to \mathcal{F} \to \mathcal{G} \to 0$ avec $\dim\mathcal{G} < \dim\mathcal{F}$.*

Démonstration. On peut supposer $X = \mathbf{P}^N_k$. Il suffit de choisir s tel que l'hyperplan $H(s) = X - X(s)$ de $\mathbf{P}^N_k$ ne contienne aucun des points associés de $\mathcal{F}$. Pour chaque point associé x de $\mathcal{F}$, choisissons un point fermé $y(x)$ dans $\overline{x}$, et soit $0 \to W(x) \to k^{N+1} \to Q(x) \to 0$ la suite exacte associée à $y(x)$. La réunion des hyperplans $W(x)$ est distincte de k^{N+1} (car k est infini). Tout élément s de $k^{N+1} = \Gamma(X, \mathcal{O}_X(1))$ qui n'est pas dans la réunion de ces $W(x)$ convient. En effet, $y(x) \notin H(s)$ par construction, donc a fortiori $x \notin H(s)$ pour tout point associé x de $\mathcal{F}$. □

Le polynome de Hilbert $\phi(\mathcal{F})$ est déterminé par les dimensions de tous les groupes de cohomologie $H^i(X, \mathcal{F}(j))$. A l'inverse, nous verrons que la connaissance de $\phi = \phi(\mathcal{F})$ permet de borner ces dimensions. D'ores et déjà, notons que :

Proposition 5.11. *On a $H^i(X, \mathcal{F}(j)) = 0$ pour tout $i > d(\mathcal{F})$.*

Démonstration. On peut derechef supposer k algébriquement clos. On raisonne par récurrence sur $d(\mathcal{F})$. Si $d(\mathcal{F}) = -1$, i.e $\phi(\mathcal{F}) = 0$, alors $\mathcal{F} = 0$. En effet, $\phi(\mathcal{F})(j) = \dim H^0(X, \mathcal{F}(j))$ pour tout $j \gg 0$ d'après le corollaire 5.6, et pour l'un quelconque de ces j, il existe $k \in \mathbf{N}$ tel que $\mathcal{F}(j+k)$ soit engendré par ses sections globales : ces dernières étant nulles, $\mathcal{F}(j+k) = 0$ donc $\mathcal{F} = 0$. Si $d(\mathcal{F}) \geq 0$, $\mathcal{F} \neq 0$ et l'on peut utiliser le lemme précédent pour obtenir une suite exacte $0 \to \mathcal{F}(-1) \to \mathcal{F} \to \mathcal{G} \to 0$ avec $d(\mathcal{G}) = d(\mathcal{F}) - 1$. Cette suite exacte donne donc

$$\cdots \to H^{i-1}(X, \mathcal{G}(j+1)) \to H^i(X, \mathcal{F}(j)) \to H^i(X, \mathcal{F}(j+1)) \to H^i(X, \mathcal{G}(j+1)) \to \cdots .$$

Pour $i > d(\mathcal{F})$, $i-1 > d(\mathcal{G})$ et les deux termes extrêmes sont triviaux par récurrence, donc $H^i(X, \mathcal{F}(j))$ ne dépend pas de j. Mais on a déjà vu que c'est trivial pour $j \gg 0$: c'est donc trivial pour tout j. □

5.3. **Faisceaux m-réguliers et applications.** On dit d'un faisceau $\mathcal{F}$ qu'il est m-régulier si et seulement si $\dim_k H^i(X, \mathcal{F}(j)) = 0$ pour tout $i + j = m$ avec $i > 0$. Tout $\mathcal{F}$ est donc m-régulier pour tout $m \gg 0$. Si $d(\mathcal{F}) = 0$, $\mathcal{F}$ est m-régulier pour tout $m \in \mathbf{Z}$. D'après 5.5, $\mathcal{O}_X$ est m-régulier pour tout $m \geq 0$ lorsque $X = \mathbf{P}^N$.

Lemma 5.12. *Si $\mathcal{F}$ est m-régulier, alors*

(1) *$\mathcal{F}$ est n-régulier pour tout $n \geq m$,*

(2) *$H^0(X, \mathcal{F}(n)) \otimes H^0(X, \mathcal{O}(1)) \to H^0(X, \mathcal{F}(n+1))$ est surjectif, et*

(3) *$\mathcal{F}(n)$ est engendré par ses sections globales.*

Démonstration. Comme ci-dessus, on peut suppose k algébriquement clos et raisonner par récurrence sur $\dim \mathcal{F}$, le cas $\mathcal{F} = 0$ ou $\dim \mathcal{F} = 0$ étant trivial. Si $\mathcal{F} \neq 0$, on fixe une suite exacte $0 \to \mathcal{F}(-1) \to \mathcal{F} \to \mathcal{G} \to 0$ comme ci-dessus, avec $\dim \mathcal{G} < \dim \mathcal{F}$. Considérant

$$\cdots \to H^i(X, \mathcal{F}(j)) \to H^i(X, \mathcal{G}(j)) \to H^{i+1}(X, \mathcal{F}(j-1)) \to \cdots$$

on voit que $\mathcal{G}$ est m-régulier, et vérifie donc $(1-3)$ d'après l'hypothèse de récurrence. Considérant alors

$$\cdots \to H^{i-1}(X, \mathcal{G}(j+1)) \to H^i(X, \mathcal{F}(j)) \to H^i(X, \mathcal{F}(j+1)) \to H^i(X, \mathcal{G}(j+1)) \to \cdots$$

on voit par récurrence sur n que $\mathcal{F}$ est bien n-régulier pour tout $n \geq m$, i.e. (1). Pour (2), on utilise le diagramme commutatif suivant, avec toujours $n \geq m$:

$$\begin{array}{ccccccc}
 & & & & H^0(X,\mathcal{F}(n)) \otimes H^0(X,\mathcal{O}(1)) & \to & H^0(X,\mathcal{G}(n)) \otimes H^0(X,\mathcal{O}(1)) \\
 & & & \nearrow & \downarrow & & \downarrow \\
0 & \to & H^0(X,\mathcal{F}(n)) & \to & H^0(X,\mathcal{F}(n+1)) & \to & H^0(X,\mathcal{G}(n+1))
\end{array}$$

Dans le carré, la première flèche horizontale est surjective car $H^1(X, \mathcal{F}(n-1)) = 0$, la deuxième flèche verticale est surjective par l'hypothèse de récurrence, et il en résulte facilement que la première flèche verticale est également surjective, i.e. (2). Enfin pour (3), il s'agit de vérifier que $H^0(X, \mathcal{F}(n)) \otimes \mathcal{O}_X \to \mathcal{F}(n)$ est surjective, ou encore en tensorisant par $\mathcal{O}_X(1)$, que la dernière flèche verticale du diagramme suivant est surjective :

$$\begin{array}{ccc} H^0(X,\mathcal{F}(n))\otimes H^0(X,\mathcal{O}_X(1))\otimes\mathcal{O}_X & \to & H^0(X,\mathcal{F}(n))\otimes\mathcal{O}_X(1) \\ \downarrow & & \downarrow \\ H^0(X,\mathcal{F}(n+1))\otimes\mathcal{O}_X & \to & \mathcal{F}(n+1) \end{array}$$

Mais la première flèche verticale l'est d'après (2), donc $(3)_{n+1} \iff (3)_n$ lorsque $n \geq m$. Or on sait qu'existe $k \in \mathbf{N}$ tel que $\mathcal{F}(n)(k) = \mathcal{F}(n+k)$ est engendré par ses sections globales, et on conclut par une récurrence descendante de $n+k$ à n. □

5.4. **Bornes.** Le but de cette sous-section est de montrer le résultat suivant :

Lemma 5.13. *Il existe une fonction $(\phi_1,\phi_2) \mapsto m(\phi_1,\phi_2)$ telle que pour tout corps k, pour tout N et tout couple de sous-schémas fermés $Z \subset X \subset \mathbf{P}^N_k$, les trois faisceaux de la suite exacte $0 \to \mathcal{I}_Z \to \mathcal{O}_X \to \mathcal{O}_Z \to 0$ sont m-réguliers pour tout $m \geq m(\phi(Z),\phi(X))$ où $\phi(Z) = \phi(\mathcal{O}_Z)$ et $\phi(X) = \phi(\mathcal{O}_X)$.*

Démonstration. Puisque $\mathcal{O}_\mathbf{P}$ est 0-régulier d'après 5.5, le diagramme

$$\begin{array}{ccccccccc} 0 & \to & \mathcal{I}^0_X & \to & \mathcal{O}_\mathbf{P} & \to & \mathcal{O}_X & \to & 0 \\ & & \downarrow & & \| & & \downarrow & & \\ 0 & \to & \mathcal{I}^0_Z & \to & \mathcal{O}_\mathbf{P} & \to & \mathcal{O}_Z & \to & 0 \end{array}$$

(qui donne $\mathcal{I}_Z \simeq \mathcal{I}^0_Z/\mathcal{I}^0_X$) montre qu'il suffit de prouver le lemme suivant. □

Lemma 5.14. *Il existe une fonction $\phi \mapsto m(\phi)$ telle que pour tout corps k, pour tout N et tout sous-schéma fermé X de $\mathbf{P} = \mathbf{P}^N_k$, le faisceau $\mathcal{I}_X \subset \mathcal{O}_\mathbf{P}$ est m-régulier pour tout $m \geq m(\phi(X))$.*

Démonstration. On peut supposer k-algébriquement clos, $X \neq \emptyset$, et raisonner par récurrence sur $d(X) = \deg\phi(X)$. Soit donc X avec $\Phi = \phi(X)$ non constant. Appliquant le lemme 5.10 au $\mathcal{O}_P$-faisceau cohérent $\mathcal{O}_X$, on obtient une section s de $\Gamma(\mathbf{P},\mathcal{O}_\mathbf{P}(1))$ qui donne un diagramme à ligne et colonne exacte

$$\begin{array}{ccccc} \mathcal{I}(-1) & \to & \mathcal{O}_\mathbf{P}(-1) & \to & \mathcal{O}_X(-1) \\ \downarrow & & \downarrow & & \downarrow \\ \mathcal{I} & \to & \mathcal{O}_\mathbf{P} & \to & \mathcal{O}_X \\ \downarrow & & \downarrow & & \downarrow \\ \mathcal{I}' & \to & \mathcal{O}_{\mathbf{P}'} & \to & \mathcal{O}_{X'} \end{array}$$

où $\mathbf{P}' \simeq \mathbf{P}^{N-1}_k$, $\mathcal{I} = \mathcal{I}_X$ et $\mathcal{I}' = \mathcal{I}_{X'}$. D'après ce diagramme, $\phi(X') = \Delta\Phi$, et on peut donc appliquer l'hypothèse de récurrence à X'. Soit $m \geq \max(m(\Delta\Phi),1)$. Puisque $\mathcal{I}'$ est m-régulier, l'exactitude de la première colonne donne immédiatement $H^i(\mathbf{P},\mathcal{I}(j)) = H^i(\mathbf{P},\mathcal{I}(j+1)) = \cdots = 0$ pour $i+j \geq m$ et $i \geq 2$, ainsi que

$$0 \to H^0(\mathbf{P},\mathcal{I}(j-1)) \to H^0(\mathbf{P},\mathcal{I}(j)) \xrightarrow{\alpha(j)} H^0(\mathbf{P},\mathcal{I}'(j)) \to H^1(\mathbf{P},\mathcal{I}(j-1)) \to H^1(\mathbf{P},\mathcal{I}(j)) \to 0$$

pour $1+j \geq m$. Or d'après 5.12, la flèche $\beta(j)$ du diagramme commutatif

$$\begin{array}{ccc} H^0(\mathbf{P},\mathcal{I}(j))\otimes H^0(\mathbf{P},\mathcal{O}_\mathbf{P}(1)) & \xrightarrow{\alpha(j)\otimes Id} & H^0(\mathbf{P},\mathcal{I}'(j))\otimes H^0(\mathbf{P},\mathcal{O}_X(1)) \\ \downarrow & & \downarrow \beta(j) \\ H^0(\mathbf{P},\mathcal{I}(j+1)) & \xrightarrow{\alpha(j+1)} & H^0(\mathbf{P},\mathcal{I}'(j+1)) \end{array}$$

est alors surjective, d'où l'on tire que $\alpha(j)$ surjective implique $\alpha(j+1)$ surjective. Par conséquent, la dimension de $H^1(\mathbf{P},\mathcal{I}(j-1))$ est, pour $j+1 \geq m$, strictement décroissante puis stationnaire égale à 0. En particulier, $H^1(\mathbf{P}, \mathcal{I}(j-1)) = 0$ dès que $j \geq m + \dim_k H^1(\mathbf{P}, \mathcal{I}(m-1))$. Comme $H^i(\mathbf{P}, \mathcal{F}(m-1)) = 0$ pour $i \geq 2$,

$$\phi(\mathcal{I})(m-1) = \dim_k H^0(\mathbf{P}, \mathcal{I}(m-1)) - \dim_k H^1(\mathbf{P}, \mathcal{I}(m-1))$$

avec $H^0(\mathbf{P}, \mathcal{I}(m-1)) \subset H^0(\mathbf{P}, \mathcal{O}_{\mathbf{P}}(m-1))$ de dimension $\leq \phi(\mathcal{O}_{\mathbf{P}})(m-1)$, donc

$$\dim_k H^1(\mathbf{P}, \mathcal{F}(m-1)) \leq \phi(\mathcal{O}_{\mathbf{P}})(m-1) - \phi(\mathcal{I})(m-1) = \Phi(m-1).$$

Finalement, $\mathcal{I}$ est $m+k$-régulier pour tout $k \geq \Phi(m-1)$. On peut donc prendre

$$m(\Phi) = m(\Delta\Phi) + \phi(m(\Delta\Phi) - 1)$$

en initialisant par $m(\mathrm{cst}) = 1$. $\square$

5.5. **Cohomologie et changement de base.** D'après Mumford [8, §5], qui résume merveilleusement bien les résultats les plus utiles de [1, III, 2].

Lemma 5.15. *Soit A un anneau noethérien, $S = \mathrm{Spec} A$ et X un S-schéma propre. Pour tout $\mathcal{O}_X$-faisceau cohérent $\mathcal{F}$ plat sur S, il existe un complexe fini de A-modules localement libres de rang fini*

$$C^0 \to C^1 \to \cdots \to C^r$$

tel que pour toute A-algèbre B,

$$H^\star(X, \mathcal{F} \otimes B) = H^\star(C^\star \otimes B).$$

Démonstration. On part du complexe de Cech de $\mathcal{F}$ lié à un recouvrement de X par des ouverts affines. C'est un complexe fini et plat $\mathcal{C}^0 \to \mathcal{C}^1 \to \cdots \to \mathcal{C}^r$, et par construction, $H^\star(\mathcal{C}^\star \otimes B) = H^\star(X, \mathcal{F} \otimes B)$ pour toute A-algèbre B. Il s'agit de trouver un complexe homotopes $C^\bullet \to \mathcal{C}^\bullet$ vérifiant les conditions de l'énoncé. C'est là un résultat de pure algèbre homologique, pour lequel on renvoie à la preuve de Mumford, cf [8, §5]. $\square$

Corollary 5.16. *Soit S un schéma, X un S-schéma propre et de présentation finie, $\mathcal{F}$ un $\mathcal{O}_X$-module cohérent et plat sur S. Alors*

$$s \mapsto \chi(\mathcal{F}_s) = \sum (-1)^i \dim_{k(s)} H^i(X_s, \mathcal{F}_s)$$

est localement constante sur S.

Démonstration. C'est local sur S et ça descend au cas noethérien, i.e. on peut supposer que $S = \mathrm{Spec} A$ est noethérien, appliquer le lemme précédent pour obtenir un complexe fini $C^\star$ de A-modules localement libres de rangs finis calculant la cohomologie de $\mathcal{F}$, et alors $\chi(\mathcal{F}_s) = \sum (-1)^i \mathrm{rang} C^\star_s$, qui est localement constant parce que chacun des termes l'est. $\square$

Corollary 5.17. *Soit S un schéma, X un S-schéma propre et de présentation finie, $\mathcal{F}$ un $\mathcal{O}_X$ -module cohérent et plat sur S. Soit $i \in \mathbf{N}$ tel que pour tout $s \in S$,*

$$\forall j > i : \qquad H^j(X_s, \mathcal{F}_s) = 0.$$

Alors $R^j f_\star \mathcal{F} = 0$ pour tout $j > i$ et $R^j f_\star \mathcal{F}$ est de formation compatible au changement de base pour tout $j \geq i$. Si de plus $i = 0$, alors $f_\star \mathcal{F}$ est localement libre.

Démonstration. Le problème est local sur S et descend au cas noethérien, donc on peut supposer que $S = \mathrm{Spec}A$ avec A noethérien. On applique alors le lemme, qui fournit un complexe fini $C^\bullet$ de A-modules localement libres de rangs finis (que l'on peut si l'on veut supposer libres en passant à un S plus petit), calculant la cohomologie de $\mathcal{F} \otimes B$ sur $X \otimes B$ pour toute A-algèbre B. On choisit ce complexe de longueur minimale, disons r. L'hypothèse de la proposition devient : pour tout $s \in S$ et tout $j > i$, $H^j(C^\bullet \otimes k(s)) = 0$. Si $r > i$, cette hypothèse implique que $C^{r-1} \to C^r$ est surjectif (d'après Nakayama). On peut donc en choisir un scindage, $C^{r-1} = D^{r-1} \oplus C^r$, et le complexe $C^0 \to C^1 \to \cdots \to C^{r-2} \to D^{r-1}$ est alors homotope à $C^\star$: cela contredit la minimalité de r, donc $r \leq i$.

Soit T un S-schéma. Alors $R^j f_{T,\star}\mathcal{F}_T$ est le faisceau associé au préfaisceau

$$U \mapsto H^j(f_T^{-1}(U), \mathcal{F}_T).$$

Pour $U = \mathrm{Spec}B$, on a $H^j(f_T^{-1}(U), \mathcal{F}_T) = H^j(X_B, \mathcal{F}_B) = H^j(C^\star \otimes B)$, qui est nul si $j > i$. Si $j = i$,

$$H^i(C^\star \otimes B) = \mathrm{coker}\left(C^{i-1} \otimes B \to C^i \otimes B\right) = \mathrm{coker}\left(C^{i-1} \to C^i\right) \otimes B = H^i(C^\star) \otimes B$$

d'où l'on déduit aisément que $R^i f_{T,\star}\mathcal{F}_T = R^i f_\star \mathcal{F}_T = \widetilde{H^i(C^\star)}_T$. Si $i = 0$, $C^\star = C^0$ est libre de rang fini et $f_\star\mathcal{F}$ est le $\mathcal{O}_S$-module libre associé a C^0. □

5.6. **Preuve du lemme 4.4.** Soit $S = \mathrm{Spec}A$ avec A noethérien et X un sous-schéma fermé et S-plat de $\mathbf{P}_S^N$.

Lemma 5.18. *Il existe un entier $m(\phi) \geq 0$ tel que pour tout $m \geq m(\phi)$, pour tout S-schéma T et tout $Z \in \mathbf{Hilb}^\phi_{X/S}(T)$ correspondant à une suite exacte de $\mathcal{O}_{X_T}$-modules*

$$0 \to \mathcal{I}_Z \to \mathcal{O}_{X_T} \to \mathcal{O}_Z \to 0,$$

les propriétés suivantes sont vérifiées :

(1) *la suite de $\mathcal{O}_T$-modules*

$$0 \to f_\star\mathcal{I}_Z(m) \to f_\star\mathcal{O}_{X_T}(m) \to f_\star\mathcal{O}_Z(m) \to 0$$

est exacte,

(2) *$f_\star\mathcal{O}_X(m)$ est localement libre et $f_\star\mathcal{O}_{X_T}(m) = f_\star\mathcal{O}_X(m)_T$,*

(3) *$f_\star\mathcal{O}_Z(m)$ est localement libre de rang $\phi(m)$, et*

(4) *$f^\star f_\star\mathcal{I}_Z(m) \to \mathcal{I}_Z(m)$ est surjective.*

Démonstration. D'après le lemme 5.13, il existe une constante $m(\phi)$ ne dépendant que du polynome ϕ tel que dans la situation de l'énoncé, pour tout $i > 0$, tout $\mathcal{G} \in \{\mathcal{I}_Z, \mathcal{O}_X, \mathcal{O}_Z\}$, tout $m \geq m(\phi)$ et tout $t \in T$, $\mathcal{G}_t$ est m-régulier, et en particulier $H^i(X_s, \mathcal{G}_s(m)) = 0$. Alors $R^i f_\star\mathcal{G}(m) = 0$ pour tout $i > 0$, et chacun des $f_\star\mathcal{G}(m)$ est localement libre sur T, de formation compatible au changement de base. De plus,

$$\phi(m) = \chi(\mathcal{O}_Z(m)_t) = \dim_{k(t)} H^0(Z_t, \mathcal{O}_{Z_t}(m)) = \mathrm{rang} f_\star\mathcal{O}_Z(m).$$

Enfin, (4) peut se vérifier localement sur T, où cela résulte par Nakayama de l'énoncé analogue du lemme 5.12. □

Quatrième partie 4. Le schéma de Picard

6. Le foncteur $\mathbf{Pic}_{X/S}$

Pour tout schéma X, on note $\mathrm{Pic}(X)$ le groupe des classes d'isomorphismes de faisceaux inversibles $\mathcal{L}$ sur X. Pour X/S, on définit un foncteur contravariant

$$P_{X/S} : (\mathbf{Sch}/S)^0 \to \mathbf{Ens} \qquad P_{X/S}(T) = \mathrm{Pic}(X \times_S T).$$

Ce foncteur n'a aucune chance d'être représentable : ce n'est pas un faisceau (pour la topologie de Zariski sur $\mathbf{Sch}/S$). Par exemple, un faisceau inversible de la forme $f^\star\mathcal{L} \in \mathrm{Pic}(X)$ pour $\mathcal{L} \in \mathrm{Pic}(S)$ n'est pas nécessairement trivial, mais il le devient après passage à un recouvrement ouvert suffisamment fin de S. Cela nous condurait à étudier plutôt

$$\mathrm{Pic}^?_{X/S} : (\mathbf{Sch}/S)^0 \to \mathbf{Ens} \qquad \mathrm{Pic}^?_{X/S}(T) = \mathrm{Pic}(X \times_S T)/f_T^\star\mathrm{Pic}(T),$$

mais est-ce vraiment le bon choix ? La réponse est oui, sous certaines hypothèses.

En fait, le bon choix serait bien sûr, et en toute circonstance, de considérer le ***faisceau associé au préfaisceau*** $P_{X/S}$, un faisceau que l'on notera $\mathrm{Pic}_{X/S}$. De l'isomorphisme (classique) $\mathrm{Pic}(X \times_S T) \simeq H^1(X \times_S T, \mathbf{G}_m)$, on déduit une formule aussi compacte que difficile à exploiter, à savoir $\mathrm{Pic}_{X/S}(T) = H^0(T, R^1 f_{T\star}\mathbf{G}_m)$. Pour aller plus loin, on considère la suite spectrale de Leray

$$H^i(T, R^j f_\star \mathbf{G}_m) \Rightarrow H^{i+j}(X \times_S T, \mathbf{G}_m)$$

qui marche si X/S est quasi-compact et quasi-séparé, et donne

$$0 \to H^1(T, f_\star\mathbf{G}_m) \to H^1(X \times_S T, \mathbf{G}_m) \simeq \mathrm{Pic}(X \times_S T) \to \mathrm{Pic}_{X/S}(T) \to H^2(T, f_\star\mathbf{G}_m) \to H^2(X \times_S T, \mathbf{G}_m).$$

Le groupe $H^1(T, f_\star\mathbf{G}_m)$ est en général plus gros que $f^\star\mathrm{Pic}(T) \simeq f^\star H^1(T, \mathbf{G}_m)$. La suite exacte ci-dessus montre donc que le morphisme $\mathrm{Pic}^?_{X/S}(T) \to \mathrm{Pic}_{X/S}(T)$ n'est en général ni injectif ni surjectif, mais nous permet de donner des critères pour qu'il le soit : si $f_\star\mathcal{O}_X = \mathcal{O}_S$ universellement (i.e. $f_{T\star}\mathcal{O}_{X\times_S T} = \mathcal{O}_T$) cette suite exacte se raccourcit en

$$0 \to \mathrm{Pic}^?_{X/S}(T) \to \mathrm{Pic}_{X/S}(T) \to H^2(T, \mathbf{G}_m) \to H^2(X \times_S T, \mathbf{G}_m).$$

Si de plus $f : X \to S$ a une section $e : S \to X$, la dernière flèche est un isomorphisme donc $\mathrm{Pic}^?_{X/S} = \mathrm{Pic}_{X/S}$. En ce qui concerne la première propriété : elle est vraie pour $X = \mathbf{P}^N_S$, et plus généralement dans le cadre suivant.

Lemma 6.1. *Si $f : X \to S$ est propre, plat, de présentation finie, à fibre géométriquement intègre, alors $f_\star\mathcal{O}_X = \mathcal{O}_S$ universellement.*

Démonstration. Le problème est local sur S : on se ramène d'abord au cas où $S = \mathrm{Spec}A$ avec A noethérien. On utilise le lemme 5.15 pour obtenir un complexe fini de A-module localement libre de rang fini $C^\star$ qui calcule la cohomologie de $\mathcal{O}_X$. Quitte à restreindre encore S, on peut même supposer que chacun des C^i est libre. Soit $B = \ker(C^0 \to C^1) = H^0(X, \mathcal{O}_X)$. Pour tout point géométrique s de S, X_s est géométriquement intègre, donc $H^0(X_s, \mathcal{O}_{X_s}) = \ker(C^0 \otimes k(s) \to C^1 \otimes k(s))$ est une $k(s)$-algèbre intègre, et de dimension finie puisque X est propre, donc c'est $k(s)$. En particulier, le rang de $C^0 \to C^1$ est constant : quitte à restreindre encore S, on peut supposer qu'un mineur fixé de la matrice de ce morphisme est partout non-nul, ce qui fournit une décomposition $C^0 = B \oplus D$ et $C^1 = D \oplus C'^1$. En particulier, B est projectif, et localement libre de rang 1 sur A, donc isomorphe à A. $\square$

Nous allons montrer :

Theorem 6.2. *Soit S un schéma, $X \subset \mathbf{P}(\mathcal{E})$ un sous-schéma fermé qui est plat, de présentation finie, à fibre géométriquement intègre sur S, et qui admet une section $e : S \hookrightarrow X$. Alors le foncteur*

$$\mathrm{Pic}_{X/S} : (\mathbf{Sch}/S)^0 \to \mathbf{Ab} : \qquad T \mapsto \mathrm{Pic}(X \times_S T)/f^\star \mathrm{Pic}(T)$$

est représentable par un S-schéma que l'on note encore $\mathrm{Pic}_{X/S}$.

7. Le foncteur $\mathbf{Div}_{X/S}$

7.1. **Définition.** Soit X un S-schéma. Un *diviseur de Cartier effectif relatif* (dCer) sur X/S est un sous-schéma fermé D de X qui est plat sur S et dont l'idéal $\mathcal{I}_D \subset \mathcal{O}_X$ est un $\mathcal{O}_X$-faisceau inversible. On note

$$\mathbf{Div}_{X/S} : (\mathbf{Sch}/S)^0 \to \mathbf{Ens}$$

le foncteur qui à T associe l'ensemble des dCer sur $X \times_S T/T$. Il n'est d'ailleurs pas tout à fait clair que c'est un foncteur : il faut pour cela utiliser la platitude de $\mathcal{O}_D$ sur S, qui implique que la formation de $\mathcal{I}_D$ commute au changement de base. L'intérêt pour nous de ce foncteur est qu'il est muni de deux morphismes

$$\mathbf{Pic}_{X/S} \leftarrow \mathbf{Div}_{X/S} \hookrightarrow \mathbf{Hilb}_{X/S}$$

qui à D sur X_T/T associent respectivement l'image de $\mathcal{O}_X(D) = \mathcal{I}_D^{-1}$ dans $\mathbf{Pic}_{X/S}(T)$ et le sous-schéma fermé $D \subset X$. Ce dernier est en effet plat sur T par définition, et de présentation finie puisque $\mathcal{I}_D$ est inversible (et donc localement sur X engendré par un élément).

7.2. Le morphisme $\mathbf{Div}_{X/S} \hookrightarrow \mathbf{Hilb}_{X/S}$.

Proposition 7.1. *Pour X propre, de présentation finie et plat sur S, le morphisme $\mathbf{Div}_{X/S} \to \mathbf{Hilb}_{X/S}$ est relativement représentable par des immersions ouvertes.*

Démonstration. Soit $Z \subset X$ plat et de présentation finie sur S, $\mathcal{I} \subset \mathcal{O}_X$ l'idéal de Z, $\phi : \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{I}, \mathcal{O}_X) \otimes \mathcal{I} \to \mathcal{O}_X$ le morphisme canonique et Y la réunion des supports du noyau et conoyau de ϕ. Alors Y est fermé dans X, donc $U = S - f(Y)$ est ouvert dans S puisque $f : X \to S$ est propre. Sur U, ϕ est un isomorphisme donc $\mathcal{I}$ est inversible, et H est un diviseur de Cartier effectif relatif. Si maintenant $T \to S$ est un morphisme quelconque tel que $H_T \subset X_T$ est effectif relatif sur T, alors $H_t \subset X_t$ est effectif pour tout $t \in T$, donc $\mathcal{I}_t \subset \mathcal{O}_{X_t}$ est inversible, donc ϕ_t est un isomorphisme, $Y_t = \emptyset$ (ce n'est pas évident), et $T \to S$ se factorise par U. $\square$

Corollary 7.2. *Soit S un schéma, $X \subset \mathbf{P}(\mathcal{E})$ un sous-schéma fermé et plat de présentation finie sur S. Alors $\mathbf{Div}_{X/S}$ est représentable par un S-schéma.*

7.3. **Le morphisme $\mathbf{Div}_{X/S} \to \mathbf{Pic}_{X/S}$.** On reprend les hypothèses et notations du théorème. Soit $\mathcal{L}$ un faisceau inversible sur S et $D_{\mathcal{L}} \subset \mathbf{Div}_{X/S}$ le sous-foncteur de $\mathbf{Div}_{X/S}$ qui à T/S associe l'ensemble des diviseurs de Cartier effectifs relatifs D de $X \times_S T/T$ tels que $\mathcal{O}_X(D) = \mathcal{L}_T$ dans $\mathbf{Pic}_{X/S}(T)$, i.e. $\mathcal{O}_X(D) \simeq \mathcal{L}_T \otimes f_T^\star \mathcal{M}$ sur $X \times_S T$ pour un faisceau inversible $\mathcal{M}$ sur T.

L'inclusion $\mathcal{I}_D \hookrightarrow \mathcal{O}_X$ induit par tensorisation par $\mathcal{I}_D^{-1} = \mathcal{O}_X(D)$ une inclusion $\mathcal{O}_X \hookrightarrow \mathcal{O}_X(D)$, qui elle-même correspond à une section globale régulière s_D de $\mathcal{O}_X(D)$. Puisque D est plat sur S, cette section est même T-régulière. Choisissons un recouvrement ouvert T_i de T qui trivialise $\mathcal{M}$, puis un isomorphisme $\phi_i : \mathcal{O}_X(D) \simeq$

$\mathcal{L}_T$ au-dessus de T_i, de sorte que $\phi_i(s_D|X \times_S T_i)$ est une section T-régulière de $\mathcal{L}_T$ sur $X \times_S T_i$, i.e. un élément de $\Gamma(T_i, f_\star \mathcal{L}^\times)$ où $\mathcal{L}^\times \subset \mathcal{L}$ est le sous-faisceau formé des sections S-régulières de $\mathcal{L}$. Ces sections sont, comme les ϕ_i, bien déterminées modulo les sections inversibles de $\mathcal{O}_{X_T}$ sur $X \times_S T_i$, i.e. modulo $\Gamma(T_i, f_\star \mathcal{O}_X^\times) = \Gamma(T_i, \mathcal{O}_S^\times)$. Elles se recollent en une section globale bien définie $s(D) \in \Gamma(T, f_\star \mathcal{L}^\times / \mathcal{O}_S^\times)$ du *faisceau quotient* $f_\star \mathcal{L}^\times / \mathcal{O}_S^\times$ sur T.

Inversement, une telle section globale s se relève sur un recouvrement ouvert convenable T_i de T en des sections de $f_\star \mathcal{L}^\times$ sur T_i, qui fournissent à leur tour des inclusions $\mathcal{O}_{X \times_S T_i} \hookrightarrow \mathcal{L}_{T_i}$ puis $\mathcal{L}_{T_i}^{-1} \hookrightarrow \mathcal{O}_{X \times_S T_i}$, dont les images se recollent en un idéal inversible bien défini $\mathcal{I}(s)$ de $\mathcal{O}_{X \times_S T}$, lequel donne enfin un diviseur $D \subset X \times_S T$, qui est plat sur T puisque les sections de départ sont T-régulières. En résumé, on a donc :

$$D_{\mathcal{L}}(T) \simeq \Gamma(T, f_\star \mathcal{L}^\times / \mathcal{O}_S^\times).$$

Pour aller plus loin, on peut utiliser ceci :

Proposition 7.3. *Soit $f : X \to S$ propre et de présentation finie, $\mathcal{F}$ sur X cohérent et S-plat. Il existe un $\mathcal{O}_S$-faisceau cohérent $\mathcal{Q}$ tel que $f_\star \mathcal{F} \simeq \mathcal{Q}^\vee$ sur* $\mathbf{Sch}/S$.

Démonstration. C'est local sur S, et l'on suppose derechef $S = \mathrm{Spec} A$ avec A noethérien. On applique le lemme 5.15, qui nous donne un complexe fini $C^\star$ de A-modules localement libres de rangs finis (et même libres si l'on restreint encore S) calculant la cohomologie de $\mathcal{F}$. En particulier pour toute A-algèbre B,

$$(f_B)_\star \mathcal{F}_B = \ker(C^0 \otimes \widetilde{B \to} C^1 \otimes B).$$

Définissons $Q = \mathrm{coker}\big(\mathrm{Hom}_A(C^1, A) \to \mathrm{Hom}_A(C^0, A)\big)$. Donc

$$\mathrm{Hom}_A(C^1, A) \otimes B \to \mathrm{Hom}_A(C^0, A) \otimes B \to Q \otimes_A B \to 0.$$

Mais $\mathrm{Hom}_A(C^\star, A) \otimes B = \mathrm{Hom}_B(C^\star \otimes B, B)$ puisque $C^\star$ est libre de rang fini, donc

$$\mathrm{Hom}_B(C^1 \otimes B, B) \to \mathrm{Hom}_B(C^0 \otimes B, B) \to Q \otimes_A B \to 0.$$

En appliquant encore $\mathrm{Hom}_B(\bullet, B)$, on trouve donc

$$0 \to \mathrm{Hom}_B(Q \otimes_A B, B) \to C^0 \otimes B \to C^1 \otimes B$$

et $(f_B)_\star \mathcal{F}_B = \mathrm{Hom}_B(\widetilde{Q \otimes_A} B, B) = \Gamma(\mathrm{Spec} B, \mathcal{Q}^\vee)$ où $\mathcal{Q} = \widetilde{Q}$. □

Revenons à nos moutons, et soit $\mathcal{Q}^\vee \simeq f_\star \mathcal{L}$. En examinant la preuve ci-dessus, on voit que

$$\Gamma(T, f_\star \mathcal{L}^\times) \subset \Gamma(T, f_\star \mathcal{L}) \simeq \mathrm{Hom}_{\mathcal{O}_T}(\mathcal{Q}_T, \mathcal{O}_T)$$

correspond aux morphismes surjectifs par fibres (donc surjectifs par Nakayama), i.e.

$$\Gamma(T, f_\star \mathcal{L}^\times) \simeq \mathrm{Hom}_{\mathcal{O}_T}^{\mathrm{surj}}(\mathcal{Q}_T, \mathcal{O}_T).$$

L'action de $\Gamma(T, \mathcal{O}_T^\times)$ là-dessus est l'action évidente, d'où l'on déduit que

$$D_{\mathcal{L}}(T) = \Gamma(T, f_\star \mathcal{L}^\times / \mathcal{O}_S^\times) = \mathbf{Grass}(\mathcal{Q}, 1)(T) = \mathbf{P}(\mathcal{Q})(T).$$

Remark 7.4. On retrouve en fait un résultat familier : pour une variété projective lisse X sur un corps algébriquement clos k, munie d'un faisceau inversible $\mathcal{L}$, l'ensemble des diviseurs de Cartier D qui sont linéairement équivalents à $\mathcal{L}$ (i.e. tel que $\mathcal{O}(D) \simeq \mathcal{L}$) est en bijection avec l'espace projectif $\Gamma(X, \mathcal{L}) - \{0\}/k^\times$ des droites de $\Gamma(X, \mathcal{L})$, par l'application qui à une section $s \in \Gamma(X, \mathcal{L})$ associe $D(s) = \{x \in X | \mathcal{L}_x / \mathcal{O}_{X,x} \cdot s_x \neq 0\}$. Noter que l'ensemble des droites de $\Gamma(X, \mathcal{L})$

est bien en bijection avec l'ensemble des quotients de dimension 1 du dual Q de $\Gamma(X,\mathcal{L}) = \Gamma(k, f_\star\mathcal{L})$.

Modulo une petite généralisation de la proposition 2.9, on a donc :

Proposition 7.5. *Le morphisme* $\mathbf{Div}_{X/S} \to \mathbf{Pic}_{X/S}$ *est relativement représentable.*

8. Fin de la Preuve du Théorème 6.2

8.1. **Analyse.** On ne sait toujours pas que $\mathbf{Pic}_{X/S}$ est représentable, mais on sait maintenant que les trois autres foncteurs du diagramme cartésien

$$\begin{array}{ccc} \mathbf{Div}_{X/S} \times_{\mathbf{Pic}_{X/S}} \mathbf{Div}_{X/S} & \to & \mathbf{Div}_{X/S} \\ \downarrow & & \downarrow \\ \mathbf{Div}_{X/S} & \to & \mathbf{Pic}_{X/S} \end{array}$$

le sont. Peut-on reconstruire $\mathbf{Pic}_{X/S}$ à partir des trois autres termes ?

Example 8.1. Considérons une situation analogue dans la catégorie des ensembles. On se donne donc une application $f : D \to P$ et on forme le produit fibré

$$\begin{array}{ccc} D \times_P D & \to & D \\ \downarrow & & \downarrow \\ D & \to & P \end{array}$$

Le sous-ensemble $R = D \times_P D$ de $D \times D$ définit sur D une relation d'équivalence, l'application $f : D \to P$ se factorise en une injection $D/R \hookrightarrow P$ et le diagramme

$$\begin{array}{ccc} R & \to & D \\ \downarrow & & \downarrow \\ D & \to & D/R \end{array}$$

est cartésien et cocartésien. Le diagramme d'origine est donc co-cartésien si et seulement si $f : D \to P$ est surjective.

8.2. **Surjectivité.** On voudrait donc que $\mathbf{Div}_{X/S} \to \mathbf{Pic}_{X/S}$ soit surjectif dans un certain sens. Il y a d'abord une obstruction élémentaire à cette surjectivité. Si l'on prend par exemple $X = \mathbf{P}^1$ sur $S = \mathrm{Spec} k$, le faisceau inversible $\mathcal{O}_X(-1)$ est de degré -1, et il n'est donc linéairement équivalent à aucun diviseur *effectif*. Plus généralement, les faisceaux $\mathcal{O}_X(D)$ ont au moins une section globale, ce qui n'est pas le cas de tous les faisceaux inversibles $\mathcal{L}$ sur X ! Avec les notations de la section précédente, il se peut que $\mathcal{Q} = 0$, i.e. $D_{\mathcal{L}} = \mathbf{P}(\mathcal{Q}) = \emptyset$!

On remédie à cette obstruction en utilisant la structure de groupe sur $\mathbf{Pic}_{X/S}$. Soit $\xi \in \mathbf{Pic}_{X/S}$ l'élément qui correspond au faisceau inversible $\mathcal{O}_X(1)$ provenant du plongement $X \subset \mathbf{P}(\mathcal{E})$. Découpons $\mathbf{Pic}_{X/S}$ en fonction du polynome de Hilbert $\phi = \phi(\mathcal{L})$, calculé relativement au plongement $X \hookrightarrow \mathbf{P}(\mathcal{E})$ (ce polynome ne change pas si l'on remplace $\mathcal{L}$ par $f^\star\mathcal{M}$, puisqu'il se calcule de toute façon sur les fibres). On obtient comme précédemment pour le schéma de Hilbert un recouvrement ouvert et fermé $\mathbf{Pic}_{X/S} = \coprod \mathbf{Pic}^\phi_{X/S}$: pour notre problème de départ, il suffit maintenant de vérifier que chacun des $\mathbf{Pic}^\phi_{X/S}$ est représentable. Or

$$\mathbf{Pic}^\phi_{X/S} + m \cdot \xi = \mathbf{Pic}^{\phi[m]}_{X/S} \quad \text{où} \quad \phi[m](x) = \phi(m+x)$$

et il suffit donc de montrer que $\mathbf{Pic}^{\phi[n]}_{X/S}$ est représentable pour $n \gg 0$. Mais pour un polynome de Hilbert ϕ fixé, on montre comme dans la section 5.6 le lemme suivant.

Lemma 8.2. *Il existe un entier $m(\phi)$ tel que pour tout $m \geq m(\phi)$, les faisceaux inversibles $\mathcal{L}$ qui apparaissent dans (les points géométriques de) $\mathbf{Pic}^{\phi}_{X/S}$ sont tous m-réguliers.*

Démonstration. Cf [2, 6, Exp. XIII, Lemma 2.11]. Si l'on survole la preuve que l'on a donnée pour le schéma de Hilbert, on voit qu'il y a été fait usage - en plus des techniques applicables à tous les faisceaux cohérents - de deux hypothèses : les polynomes de Hilbert étaient fixés, et les faisceaux cohérents concernés étaient des *sous-faisceaux* d'un faisceau fixé (à savoir $\mathcal{O}_X$). Ici, on relâche la seconde hypothèse, mais on restreint notre attention aux faisceaux *inversibles*. Des techniques de dualité sont alors applicables, qui permettent de mieux contrôler les polynomes de Hilbert qui apparaissent dans les récurrences ! □

Remplaçant ϕ par $\phi[m]$ avec $m \gg m(\phi)$, on peut donc supposer que tous les faisceaux inversibles $\mathcal{L}$ qui apparaissent dans les $\mathbf{Pic}^{\phi}_{X/S}(T)$ vérifient : $R^i f_\star \mathcal{L} = 0$ pour $i > 0$ et $f_\star \mathcal{L}$ est localement libre sur T de rang $\phi(0) > 0$, de formation compatible au changement de base. Le faisceau $\mathcal{Q}$ de la section précédente est alors $\mathcal{Q} = f_\star \mathcal{L}^\vee$ et la fibre $D_{\mathcal{L}} \simeq \mathbf{P}(\mathcal{Q}) \neq \emptyset$ est projective lisse sur T.

Soit $D(\phi) \subset \mathbf{Div}_{X/S}$ l'image inverse de $\mathbf{Pic}^{\phi}_{X/S}$. Le morphisme $\ell : D(\phi) \to \mathbf{Pic}^{\phi}_{X/S}$ est alors surjectif dans le sens habituel pour les faisceaux (pour la topologie de Zariski), à savoir : pour tout T sur S et $\mathcal{L} \in \mathbf{Pic}^{\phi}_{X/S}(T)$, il existe un recouvrement ouvert T_i de T tel que $\mathcal{L}|T_i \in \mathbf{Pic}^{\phi}_{X/S}(T_i)$ se relève dans $D(\phi)(T_i)$: il suffit avec les notations précédentes de choisir un recouvrement ouvert T_i qui trivialise le faisceau localement libre $\mathcal{Q}$ sur T, puis de choisir une section de $\mathbf{P}(\mathcal{Q})|T_i \simeq \mathbf{P}^{\phi(0)-1}_{T_i}$ au-dessus de T_i. On en déduit aisément que le diagramme cartésien

$$\begin{array}{ccc} D(\phi) \times_{\mathbf{Pic}^{\phi}_{X/S}} D(\phi) & \to & D(\phi) \\ \downarrow & & \downarrow \\ D(\phi) & \to & \mathbf{Pic}^{\phi}_{X/S} \end{array}$$

est maintenant aussi co-cartésien dans la catégorie des faisceaux (pour la topologie de Zariski) sur $\mathbf{Sch}/S$: en particulier, le faisceau $\mathbf{Pic}^{\phi}_{X/S}$ y est maintenant uniquement déterminé par les deux autres, ce qui est de bon augure pour sa représentabilité.

8.3. **Quotients.**

Theorem 8.3. *Soit S un schéma noethérien, X un S-schéma quasi-projectif, $R \subset X \times_S X$ une relation d'équivalence dans X tel que $p_1 : R \to X$ soit propre et plat. Alors* (1) *le S-schéma quotient X/R existe et il est quasi-projectif sur S,* (2) *$f : X \to X/R$ est surjectif propre et plat, et* (3) *$R = X \times_{X/R} X$.*

C'est un théorème de Grothendieck [5, III, Théorème 6.1], dont voici la preuve in extenso : *on se ramène au cas fini par des quasi-sections convenables de X pour R, la démonstration étant analogue à la construction des groupes algébriques dans le Séminaire Chevalley.* Le cas fini est effectivement assez élémentaire, puisqu'alors tout est affine : les constructions de conoyaux pour des morphismes affines sont équivalentes à des constructions de noyaux pour des morphismes d'anneaux ! Mais l'explication de Grothendieck me semble bien courte ! Heureusement, il y a une autre preuve, décrite dans [4, §8, Théorème 12] qui provient de [3, Theorem 2.9]. L'idée sous-jacente provient de la remarque suivante :

Remark 8.4. Soit X un ensemble, $H = \mathcal{P}(X)$ l'ensemble des sous-ensembles de X, et $Z \subset X \times H$ le sous-ensemble universel de X, c'est-à-dire $Z = \cup_{P \in H} P \times \{P\}$: pour tout ensemble T, pour tout sous-ensemble Q de $X \times T$, il existe une unique application $f : T \to H$ tel que $Q = (Id, f)^{-1}(Z)$, à savoir $f(t) = \{x : (x,t) \in \mathcal{Q}\}$. Soit maintenant $R \subset X \times X$ une relation d'équivalence sur X et $f : X \to H$ l'unique morphisme tel que $R = (Id, f)^{-1}(Z)$. Alors $X/R = f(X) \subset H$ et l'image inverse de $f(X) \subset H$ par $X \times H \to H$ est le graphe $\Gamma_f \subset Z$ de f.

Ceci suggère la construction suivante. Soit $H = \mathbf{Hilb}_{X/S}$, soit Z le sous-schéma universel fermé de $X \times_S H$ (Z est propre et plat sur H), et soit $f : X \to H$ l'unique morphisme tel que $(Id, f)^{-1}(H) = R \subset X \times_S X$, qui est bien un sous-schéma fermé de $X \times_S X$ qui est propre et plat sur X. Le graphe de f est un sous-schéma fermé de $X \times_S H$, et même de Z, et on voudrait construire le quotient X/R comme l'image de f dans H, ou encore comme un sous-schéma fermé $X/R \subset H$ dont l'image inverse via $Z \to H$ serait ce graphe de f, ce qui nous ramène à un problème de descente déjà plus abordable. Mais de toute façon : il faut pour mener à bien ce programme déjà connaître l'existence de $\mathbf{Hilb}_{X/S}$ dans le cas où X/S est seulement *quasi*-projectif (et plus nécessairement plat), ce que font Altman et Kleinman dans [3].

8.4. **Conclusion.** En appliquant le théorème ci-dessus à $D(\phi)/S$ et $R = D(\phi) \times_{\mathrm{Pic}^{\phi}_{X/S}} D(\phi)$, on trouve un S-morphisme propre surjectif et plat $\ell' : D(\phi) \to P'$ qui fait de P' le conoyau de la double flèche $R \rightrightarrows D(\phi)$ dans la catégorie $\mathbf{Sch}/S$ des S-schémas. Or nous avons vu que $\ell : D(\phi) \to P$ faisait de même de $P = \mathrm{Pic}^{\phi}_{X/S}$ le conoyau de cette même double flèche, mais dans la catégorie beaucoup plus grosse $\mathbf{Fais}/S_{Zar}$ des faisceaux sur $\mathbf{Sch}/S$ pour la topologie de Zariski. Dans cette catégorie, on a donc un morphisme $P \to P'$, mais on ignore encore s'il s'agit d'un isomorphisme.

Pour conclure, il faut travailler dans une catégorie intermédiaire :

$$\mathbf{Sch}/S \subset \mathbf{Fais}/S_{fppf} \subset \mathbf{Fais}/S_{Zar}$$

C'est la catégorie des faisceaux fppf, i.e. les faisceaux $\mathcal{F}$ (pour la topologie de Zariski) qui vérifient en outre la propriété suivante : pour tout morphisme $T' \to T$ qui est **f**idèlement **p**lat et de **p**résentation **f**inie, $\mathcal{F}(T)$ est le noyau de la double flèche $\mathcal{F}(T') \rightrightarrows \mathcal{F}(T' \times_T T')$. C'est une sous-catégorie pleine de $\mathbf{Fais}/S_{Zar}$. Il n'est ni trivial, ni trop difficile de démontrer que tous les foncteurs représentables sont effectivement des faisceaux fppf.

On montre alors que (1) P est un faisceau fppf, et (2) tout morphisme fppf (dans $\mathbf{Sch}/S$) est un épimorphisme (dans $\mathbf{Fais}/S_{fppf}$). On en déduit que $\ell : D(\phi) \to P$ et $\ell' : D(\phi) \to P'$ sont des épimorphismes dans $\mathbf{Fais}/S_{fppf}$, puis que ℓ et ℓ' sont toutes deux égales au conoyau de la double flèche $R \rightrightarrows D(\phi)$. En particulier, $P = P'$ est représentable.

9. Propriétés du schémas de Picard

Proposition 9.1. *Si $X \to S$ est propre,* lisse, *à fibres géométriquement connexes (et admet une section), alors $\mathbf{Pic}_{X/S}$ vérifie les critères valuatifs de* séparation *et de* propreté.

Démonstration. Il s'agit de voir que si S est le spectre d'un anneau de valuation discrète R de corps des fractions K, alors $\mathbf{Pic}_{X/S}(R) \to \mathbf{Pic}_{X/S}(K)$ est bijective, ou encore puisque $\mathbf{Pic}(R) = \mathbf{Pic}(K) = 0$, de voir que $\mathbf{Pic}(X) \to \mathbf{Pic}(X_K)$ est bijective. Soit $\mathcal{L}$ un faisceau inversible sur X tel que $\mathcal{L}|X_K$ est trivial. Il existe donc dans $H^0(X_K, \mathcal{L}|X_K) = H^0(X, \mathcal{L}) \otimes_R K$ une section s qui engendre $\mathcal{L}|X_K$ en tous les points de X_K, et on peut supposer que cette section est dans le R-module $H^0(X, \mathcal{L})$. Soit η le point générique de la fibre spéciale (laquelle est lisse et connexe, donc bien irréductible) ; l'anneau local $\mathcal{O}_{X,\eta}$ est un anneau de valuation discrète, une extension non-ramifiée $R \hookrightarrow \mathcal{O}_{X,\eta}$ de R, et $\mathcal{L}_\eta$ est un $\mathcal{O}_{X,\eta}$-module libre de rang 1, et $\mathcal{L}_\eta \otimes_R K$ est engendré par s_η sur $\mathcal{O}_{X,\eta} \otimes_R K$: on peut donc aussi supposer que s engendre $\mathcal{L}$ en η : elle engendre alors $\mathcal{L}$ en *tous les points de codimension* 1 dans X, ce qui est suffisant pour vérifier qu'elle engendre $\mathcal{L}$ partout. Donc $\mathcal{O}_X \to \mathcal{L}$ est surjective, puis bijective, et $\mathcal{L}$ est trivial. Dans l'autre sens : les groupes $\mathbf{Pic}(X)$ et $\mathbf{Pic}(X_K)$ sont tous les deux engendrés par les diviseurs de Weil, et tout diviseur de Weil sur X_K s'étend bien sûr en un diviseur de Weil sur X, donc $\mathbf{Pic}(X) \to \mathbf{Pic}(X_K)$ est également surjective. □

Lemma 9.2. *Avec les mêmes hypothèses,* $\mathbf{Lie}(\mathbf{Pic}_{X/S}) \simeq R^1 f_\star \mathcal{O}_X$.

Démonstration. Par définition,

$$\mathbf{Lie}(\mathbf{Pic}_{X/S})(T) = \ker\left(\mathbf{Pic}_{X/S}(T[\epsilon]) \to \mathbf{Pic}_{X/S}(T)\right)$$

où $T[\epsilon]$ est le T-schéma $\mathrm{Spec}\mathcal{O}_T[\epsilon]$ et $\mathcal{O}_T[\epsilon] = \mathcal{O}_T \oplus \mathcal{O}_T\epsilon$ avec $\epsilon^2 = 0$. Donc

$$\mathbf{Lie}(\mathbf{Pic}_{X/S}) = \ker\left(R^1 f_\star(\mathcal{O}_X[\epsilon]^\times) \to R^1 f_\star(\mathcal{O}_X^\times)\right).$$

Mais on a une suite exacte $0 \to \mathcal{O}_X \to \mathcal{O}_X[\epsilon]^\times \to \mathcal{O}_X^\times \to 1$, qui donne

$$0 \to f_\star\mathcal{O}_X \to f_\star\mathcal{O}_X[\epsilon]^\times \to f_\star\mathcal{O}_X^\times \to R^1 f_\star\mathcal{O}_X \to \mathbf{Lie}(\mathbf{Pic}_{X/S}) \to 0$$

Les trois premiers termes sont

$$0 \to \mathcal{O}_S \to \mathcal{O}_S[\epsilon]^\times \to \mathcal{O}_S^\times \to 0$$

puisque $f_\star\mathcal{O}_X = \mathcal{O}_S$, cqfd. □

Cinquième partie 5. Schémas abéliens

10. Schémas Abéliens

Un schéma abélien sur S est un schéma en groupes A/S qui est propre de présentation finie, lisse, à fibres géométriquement connexes.

10.1. Rigidité et applications.

Proposition 10.1. *Soient S un schéma connexe noethérien, et $\alpha : X \to Y$ un morphisme de S-schéma. On suppose que $\pi_X : X \to S$ est propre, plat, vérifie $\pi_{X\star}\mathcal{O}_X = \mathcal{O}_S$ universellement, admet une section $e : S \to X$. On suppose aussi que $Y \to S$ est séparé. Si α est constant sur une fibre, i.e. $\alpha(X_s)$ est un singleton pour un point s de S, alors α est constant, i.e. $\alpha = \eta \circ \pi_X$ pour la section $\eta = \alpha \circ e$ de $\pi_Y : Y \to S$.*

Démonstration. Soit Z le schéma des coincidences de α et $\beta = \eta \circ \pi_X : X \to Y$. C'est un sous-schéma fermé de X, puisque Y est séparé. Soit $t \in S$ tel que $X_t \subset Z$ ensemblistement, $U = \mathrm{Spec}A$ un voisinage ouvert de t dans S, P l'idéal premier de A correspondant à t, $t(n) = \mathrm{Spec}A_P/P^nA_P$, $\alpha(n), \beta(n) : X_{t(n)} \to Y_{t(n)}$ les morphismes induits par α et β. Par hypothèse, les applications sous-jacentes à $\alpha(n)$ et $\beta(n)$ sont identiques, notons $\gamma(n)$ cette application commune. D'autre part, les sections e et η définissent des suites

$$0 \to \mathcal{I}_\eta \to \mathcal{O}_{Y_{t(n)}} \to \mathcal{O}_{\eta_{t(n)}} \to 0 \quad \text{et} \quad 0 \to \mathcal{I}_e \to \mathcal{O}_{X_{t(n)}} \to \mathcal{O}_{e_{t(n)}} \to 0$$

Les morphismes $\mathcal{O}_{Y_{t(n)}} \to \gamma(n)_\star \mathcal{O}_{X_{t(n)}}$ sont tous les deux compatibles avec ces suites exactes et le morphisme induit $\mathcal{O}_{\eta_{t(n)}} \to \gamma(n)_\star \mathcal{O}_{e_{t(n)}}$ est le même dans les deux cas. Mais puisque $\gamma(n)_\star \mathcal{O}_{X_{t(n)}} = \eta_\star \pi_{X_{t(n)}\star} \mathcal{O}_{X_{t(n)}}$ et $\pi_{X_{t(n)}\star} \mathcal{O}_{X_{t(n)}} = \mathcal{O}_{t(n)}$, $\gamma(n)_\star \mathcal{I}_e = 0$. Donc $\alpha_{t(n)} = \beta_{t(n)}$. Choisissons un voisinage $V = \mathrm{Spec} B$ d'un point de X_t dans $\pi_X^{-1}(U)$ et soit I l'idéal définissant $Z \cap V$. Puisque $X_{t(n)} \cap V \subset Z \cap V$, on a donc $IB_P \subset P^n B_P$. Ceci étant vrai pour tout n, il en résulte que $IB_P = 0$. Mais alors Z contient un voisinage ouvert de la fibre X_t de π_X dans X, voisinage que l'on peut supposer tubulaire puisque π_X est propre donc fermé. Soit alors S' le plus grand ouvert de S tel que $\pi_X^{-1}(S') \subset Z$. C'est non-vide puisque cela contient s d'après ce qui précède. Et d'autre part $t \in S' \iff X_t \subset Z \iff t \in S - \pi_X(X - Z)$ qui est fermé puisque π_X est fidèlement plat donc ouvert : S' est donc un ouvert fermé non-vide du connexe S, donc $S' = S$, $Z = X$ et $\alpha = \beta$. □

Corollary 10.2. *Soient S un schéma, A/S un schéma abélien, G/S un schéma en groupes séparé et de présentation finie, $f : A \to G$ un S-morphisme qui envoie le neutre de A sur celui de G. Alors f est un morphisme de S-schémas en groupes.*

Démonstration. La question est locale sur S, que l'on peut supposer affine connexe et noethérien. Alors A est aussi connexe, puisque $\pi_\star \mathcal{O}_A = \mathcal{O}_S$. On considère le A-morphisme $\alpha : A \times_S A \to G \times_S A$ défini par $(x, y) \mapsto (f(xy)f(y)^{-1}f(x)^{-1}, y)$, qui est constant égal à (e_G, e_A) sur $A \times \{e_A\}$. On applique la proposition précédente à ce A-morphisme, avec la section $A \to A \times_S A$ défini par $y \mapsto (e_A, y)$: on obtient $\alpha(x, y) = (e_G, y)$, donc $f(xy) = f(x)f(y)$ pour tout x, y. □

Corollary 10.3. *Tout schéma abélien A/S est commutatif.*

Démonstration. On applique le corollaire précédent à $f : A \to A$, $f(x) = x^{-1}$. □

Corollary 10.4. *La structure de groupe sur A/S est uniquement déterminée par sa section neutre $e_A : S \to A$.*

Démonstration. On applique le même corollaire à $f : (A, m) \to (A, m')$, $f(x) = x$. □

Proposition 10.5. *Soient A et B deux S-schémas abéliens. Le foncteur*

$$\underline{\mathrm{Hom}}_{Gr}(A, B) : (\mathbf{Sch}/S)^0 \to \mathbf{Ens} \qquad T \mapsto \mathrm{Hom}_{T-gr}(A_T, B_T)$$

est représentable par un S-schéma en groupes commutatifs discrets sans torsion que l'on note $\underline{\mathrm{Hom}}_{Gr}(A, B)$.

Démonstration. Pour la représentabilité, il suffit de montrer que le morphisme

$$\underline{\mathrm{Hom}}_{Gr}(A, B) \to \underline{\mathrm{Hom}}(A, B)$$

est relativement représentable, d'après la proposition 1.1 et le corollaire 3.2. Soit donc $f : A \to B$ un morphisme de S-schéma. Pour tout T/S, $f_T : A_T \to B_T$ est un morphisme de T-schéma en groupe si et seulement si $f_T(e_A) = e_B$, d'après le corollaire 10.2, i.e. si et seulement si $T \to S$ se factorise à travers le sous-schéma (fermé) des coincidences de $f \circ e_A$ et $e_B : S \to B$. Donc $\underline{\mathrm{Hom}}_{Gr}(A,B)$ est un S-schéma en groupes (commutatifs), notons le H et soit $F : A_H \to B_H$ le morphisme universel. Montrons que H/S est discret, i.e. la section triviale $e_H : S \to H$ est une immersion ouverte et fermée. Pour tout point s de $e_H(S)$, $F_s : A_s \to B_s$ est trivial, donc $F : A_H \to B_H$ est trivial au-dessus de toute la composante connexe de s dans H, laquelle est donc contenue dans $e_H(s)$, qui est donc bien une réunion de composantes connexes de H. Montrons enfin que $\underline{\mathrm{Hom}}_{Gr}(A,B)(T)$ est sans torsion : il s'agit de montrer que si $f : A_T \to B_T$ est un T-morphisme (de T-schémas en groupes) tel que $[n]f = 0$ pour un entier $n \geq 1$, alors $f = 0$. Or sur un point géométrique quelconque s de S, $[n]f_s = 0$, donc $f_s(A_s) \subset B_s[n]$ qui est fini, donc $f_s(A_s) = 0$ car A_s est connexe, donc $f_s = 0$. Alors $f = 0$ sur toute la composante connexe de s, et finalement $f = 0$. □

10.2. **Le morphisme Λ.** Soit $\mathcal{L}$ un faisceau inversible sur A, et

$$\mathcal{M} = m^\star(\mathcal{L}) \otimes p_1^\star(\mathcal{L})^{-1} \otimes p_2^\star(\mathcal{L})^{-1} \quad \text{sur } A \times_S A$$

où $m, p_1, p_2 : A \times_S A \to A$ sont la multiplication, la première et la seconde projections, donc

$$\mathcal{M}|e_A(S) \times_S A \simeq [0]^\star \mathcal{L} \simeq \mathcal{M}|A \times_S e_A(S)$$

où $[0] = e \circ f : A \to A$. Posons, pour y voir plus clair, $T = A$ et considérons $A \times_S A = A \times_S T = A_T$ comme un T-schéma abélien, en particulier comme un T-schéma, sur lequel on a donc un faisceau inversible $\mathcal{M}$ qui donne un élément de $\mathbf{Pic}_{A/S}(T)$. Soit P le S-schéma qui représente $\mathbf{Pic}_{A/S}$ et $\mathcal{P} \in \mathbf{Pic}_{A/S}(P)$ l'élément universel. Il existe alors un unique S-morphisme $\Lambda(\mathcal{L}) : T \to P$ tel que $\Lambda(\mathcal{L})^\star(\mathcal{P}) = \mathcal{M}$ dans $\mathbf{Pic}_{A/S}(T)$. Revenant à $T = A$ et $P = \mathbf{Pic}_{A/S}$, on a ainsi obtenu un S-morphisme $\Lambda(\mathcal{L}) : A \to \mathbf{Pic}_{A/S}$.

C'est un morphisme de S-schémas en groupes : puisque $\mathbf{Pic}_{A/S}$ est séparé d'après la proposition 9.1, il suffit de vérifier que $\Lambda(\mathcal{L})$ envoie la section neutre $e_A : S \to A$ sur la section neutre de $\mathbf{Pic}_{A/S}$, ce qui résulte de la seconde des deux formules ci-dessus. Pour tout point $s \in A(S)$, $\Lambda(\mathcal{L})(s) \in \mathbf{Pic}_{A/S}(S)$ est le pull-back de $\mathcal{Q}$ par le morphisme

$$(Id, \Lambda(\mathcal{L})) \circ (Id, s) : A \to A \times_S A \to A \times_S H$$

ou encore le pull-back de $\mathcal{M}$ par $(Id, s) : A \to A \times_S A$. Or $m \circ (Id, s) : A \to A$ est la translation $x \mapsto \mathcal{T}_s(x) = x + s$, $p_1 \circ (Id, s) : A \to A$ est l'identité et $p_2 \circ (Id, s) : A \to A$ est le compose $s \circ f : A \to S \to A$, donc $\Lambda(\mathcal{L})(s) = \mathcal{T}_s^\star \mathcal{L} \otimes \mathcal{L}^{-1}$ dans $\mathbf{Pic}_{A/S}(S)$. Plus généralement, pour tout T/S et $t \in A(T)$, on obtient :

$$\Lambda(\mathcal{L})(t) = \mathcal{T}_t^\star(\mathcal{L}_T) \otimes \mathcal{L}_T^{-1} \quad \text{dans} \quad \mathbf{Pic}_{A/S}(T).$$

On déduit immédiatement de cette formule d'une part que pour tout $x, y \in A(T)$,

$$\mathcal{T}_{x+y}^\star \mathcal{L} \otimes \mathcal{L}^{-1} \sim \mathcal{T}_x^\star \mathcal{L} \otimes \mathcal{L}^{-1} \otimes \mathcal{T}_y^\star \mathcal{L} \otimes \mathcal{L}^{-1} \quad \text{dans} \quad \mathbf{Pic}_{A/S}(T)$$

(c'est le théorème du carré), et d'autre part que l'application qui à $\mathcal{L}$ associe $\Lambda(\mathcal{L})$ est *un morphisme de groupes*,

$$\Lambda : \mathbf{Pic}(A) \to \mathrm{Hom}_{S-Gr}(A, \mathbf{Pic}_{A/S}).$$

En faisceautisant ce dernier, on obtient finalement un morphisme

$$\Lambda : \mathbf{Pic}_{A/S} \to \underline{\mathrm{Hom}}_{Gr}(A, \mathbf{Pic}_{A/S}).$$

10.3. **Les théorèmes.** Soit G un S-schéma en groupes qui est *localement de présentation finie.* Pour tout $s \in S$, on obtient donc un $k(s)$-schéma en groupes G_s qui est localement de type fini, et en particulier localement noethérien : ces composantes connexes sont donc ouvertes (et fermées), i.e. des sous-schémas ouverts et fermés de G_s. L'élément neutre $1_s \in G_s(k(s))$ est un point $k(s)$-rationnel, donc fermé. On note G_s^0 la composante neutre de G_s : c'est un sous-schéma en groupe ouvert et fermé de G_s, connexe et même géométriquement connexe puisqu'il contient un point $k(s)$-rationnel. On note enfin $G^0 = \cup_s G_s^0$, qui n'est à priori... qu'une partie de l'ensemble sous-jacent au schéma G.

Soit A un S-schéma abélien projectif. La discussion ci-dessus s'applique au S-schéma en groupe $G = \mathbf{Pic}_{A/S}$: on a construit ce dernier en le recouvrant par des ouverts fermés $\mathbf{Pic}^{\phi}_{A/S}$ dont on vérifie - en reprenant toutes les démonstrations, que ce sont bien des schémas de présentation finie sur S. On obtient ainsi un sous-ensemble $\mathbf{Pic}^0_{A/S}$ de $\mathbf{Pic}_{A/S}$.

A ce stade, on ignore encore si le foncteur $\underline{\mathrm{Hom}}_{Gr}(A, \mathbf{Pic}_{A/S})$ est représentable (il l'est). Cependant, on sait que $\mathbf{Pic}_{A/S}$ est séparé (d'après la proposition 9.1), et on montre alors facilement, comme dans la proposition 10.5, que le morphisme $S \to \underline{\mathrm{Hom}}_{Gr}(A, \mathbf{Pic}_{A/S})$ qui correspond à la section neutre est relativement représentable par des immersions ouvertes et fermées. Il en est donc de même du pull-back de ce morphisme par Λ, qui n'est autre que l'inclusion $\ker \Lambda \hookrightarrow \mathbf{Pic}_{A/S}$. Par conséquent, le noyau $\ker \Lambda$ est un sous-schéma en groupes ouvert et fermé de $\mathbf{Pic}_{A/S}$. On a donc une inclusion $\mathbf{Pic}^0_{A/S} \subset \ker \Lambda$. Nous allons montrer simultanément les résultats suivants.

Theorem 10.6. (1) $\mathbf{Pic}^0_{A/S} = \ker \Lambda$, (2) $\mathbf{Pic}^0_{A/S}$ *est un S-schéma abélien.*

Definition 10.7. On note $A^t = \mathbf{Pic}^0_{A/S}$: c'est le schéma abélien dual de A/S.

Puisque A/S est à fibre géométriquement connexe, tout morphisme $A \to \mathbf{Pic}_{A/S}$ se factorise par $A^t = \mathbf{Pic}^0_{A/S}$. Compte-tenu de ce qui précède, notre morphisme Λ induit donc un monomorphisme

$$\mathbf{NS}_{A/S} \hookrightarrow \underline{\mathrm{Hom}}_{Gr}(A, A^t)$$

où $\mathbf{NS}_{A/S} = \mathbf{Pic}_{A/S}/\mathbf{Pic}^0_{A/S}$ est le (S-schéma en) groupe de Néron-Séveri. Nous verrons que ce morphisme est relativement représentable. La preuve du théorème ci-dessus repose en définitive sur la construction d'éléments non-triviaux de $\mathbf{NS}_{A/S}$, les *polarisations*, qui joueront un rôle essentiel dans la suite. Ces éléments sont fournis par la théorie des faisceaux inversibles S-amples sur A, via le troisième point du théorème suivant.

Theorem 10.8. *Si $\mathcal{L}$ est S-ample,*

(1) $R^i f_\star \mathcal{L} = 0$ *pour tout* $i > 0$,

(2) $f_\star \mathcal{L}$ *est localement libre de formation compatible au changement de base, et*

(3) $\Lambda(\mathcal{L}) : A \to A^t$ *est une isogénie de degré* $(\mathrm{rang} f_\star \mathcal{L})^2$.

(4) *Pour tout* $n \geq 3$, $f^\star f_\star \mathcal{L}^{\otimes n} \to \mathcal{L}^{\otimes n}$ *est surjectif et induit une immersion fermée* $\iota(\mathcal{L}^{\otimes n}) : A \hookrightarrow \mathbf{P}(f_\star \mathcal{L}^{\otimes n})$ *(i.e.* $\mathcal{L}^{\otimes n}$ *est très S-ample).*

Identifions $\mathbf{Pic}_{A/S}(T) = \mathbf{Pic}(A \times_S T)/p_2^\star \mathbf{Pic}(T)$ au sous-groupe de $\mathbf{Pic}(A \times_S T)$ formé des éléments $\mathcal{L}$ qui sont normalisés par la condition $\mathcal{L}|e_A(S) \times_S T \simeq \mathcal{O}_T$.

Soit $\mathcal{P}$ le faisceau inversible ainsi rigidifié sur $A \times_S A^t$ qui correspond à l'inclusion $A^t \hookrightarrow \mathbf{Pic}_{A/S}$. On a donc $\mathcal{P}|e_A(S) \times_S A^t \simeq \mathcal{O}_{A^t}$ (par la normalisation choisie) et $\mathcal{P}|A \times_S e_{A^t}(S) \in f^\star \mathbf{Pic} S$ (puisque $A^t \hookrightarrow \mathbf{Pic}_{A/S}$ est un morphisme de S-schémas en groupes), d'où l'on déduit facilement que $\mathcal{P}|A \times_S e_{A^t}(S) \simeq \mathcal{O}_A$. Ce faisceau inversible s'appelle le faisceau de Poincarré. On peut le voir aussi comme un faisceau inversible... sur le A-schéma abélien $A \times_S A^t$, ce qui nous donne un morphisme de S-schéma $A \to \mathbf{Pic}_{A^t/S}$. Ce dernier est compatible avec les sections neutres par construction, et c'est donc un morphisme de S-schémas en groupes. Il se factorise nécessairement à travers le sous-schéma en groupe ouvert $A^{tt} = \mathbf{Pic}^0_{A^t/S}$: on obtient donc ainsi un morphisme canonique $\delta : A \to A^{tt}$.

Theorem 10.9. *C'est un isomorphisme $\delta : A \to A^t$.*

10.4. **Le cas d'un corps.** On suppose ici que $S = \mathrm{Spec} k$ où k est algébriquement clos. Soit A/k une variété abélienne de dimension g.

10.4.1. *Cohomologie de $\mathcal{M} \neq 0 \in \ker \Lambda$ et applications.* Soit d'abord $\mathcal{M}$ un faisceau inversible sur A tel que $\Lambda(\mathcal{M}) = 0$, i.e.

$$m^\star \mathcal{M} = p_1^\star \mathcal{M} \otimes p_2^\star \mathcal{M} \quad \text{dans } \mathbf{Pic}(A \times A)/p_2^\star \mathbf{Pic}(A).$$

ou encore : $m^\star \mathcal{M} \simeq p_1^\star \mathcal{M} \otimes p_2^\star \mathcal{M} \otimes p_2^\star \mathcal{L}$ pour un faisceau inversible $\mathcal{L}$ sur A. Alors $m^\star \mathcal{M}|\{0\} \times A = \mathcal{M} \simeq \mathcal{M} \otimes \mathcal{L}$ donc $\mathcal{L} = 0$ et l'égalité ci-dessus est déjà valable dans $\mathbf{Pic}(A \times A)$. En faisant le pull-back par $([n],[1]) : A \to A \times A$, on obtient $[n+1]^\star \mathcal{M} \simeq [n]^\star \mathcal{M} \otimes \mathcal{M}$, d'où l'on déduit immédiatement par récurrence que $[n]^\star \mathcal{M} \simeq \mathcal{M}^n$.

Lemma 10.10. *Si $\mathcal{M} \neq 0$, $H^i(A, \mathcal{M}) = 0$ pour tout $i \geq 0$.*

Démonstration. Par récurrence sur i. Supposons d'abord qu'il existe $s \in H^0(A, \mathcal{M})$ avec $s \neq 0$. Alors s définit un morphisme $\mathcal{O}_A \to \mathcal{M}$ qui est injectif (car $\mathcal{M}$ est localement libre et A intègre), non-surjectif (car $\mathcal{M} \neq 0$), donc $\mathcal{M} \simeq \mathcal{O}(D)$ pour un diviseur effectif D sur A. Mais alors

$$\mathcal{I}_D \simeq \mathcal{M}^{-1} \simeq [-1]^\star \mathcal{M} \simeq \mathcal{O}(-D)$$

admet aussi une section non-nulle, ce qui contredit l'hypothèse $\mathcal{M} \neq 0$. Supposons ensuite démontré : $H^j(X, \mathcal{M}) = 0$ pour tout $j < i \neq 0$. Puisque $m^\star \mathcal{M} \simeq p_1^\star \mathcal{M} \otimes p_2^\star \mathcal{M}$, la formule de Kunneth donne

$$H^i(A \times A, m^\star \mathcal{M}) = \oplus_{j_1+j_2=r} H^{j_1}(A, \mathcal{M}) \otimes H^{j_2}(A, \mathcal{M}) = 0.$$

Mais $A \hookrightarrow A \times A \twoheadrightarrow A$ donnée par $a \mapsto (a, 0)$ et $(a, b) \mapsto a + b$ induit l'identité

$$H^i(A, \mathcal{M}) \to H^i(A \times A, m^\star \mathcal{M}) \to H^i(A, \mathcal{M})$$

donc $H^i(A, \mathcal{M}) = 0$. □

Corollary 10.11. *Si $\mathcal{L}$ est ample, alors*

(1) *Le noyau de $\Lambda(\mathcal{L}) : A \to \mathbf{Pic}_{A/S}$ est fini.*
(2) *L'image de $\Lambda(\mathcal{L})$ est le noyau de $\Lambda : \mathbf{Pic}_{A/S} \to \underline{\mathrm{Hom}}_{Gr}(A, \mathbf{Pic}_{A/S})$.*

Démonstration. (1) Soit $B = \ker \Lambda(\mathcal{L})^0_{red}$ la composante connexe réduite de $\ker \Lambda(\mathcal{L})$. C'est un sous-schéma en groupe de A qui est fermé donc propre sur k, connexe, et réduit donc génériquement lisse donc lisse : bref, c'est une sous-variété abélienne de A. Pour tout $b \in B$, $\mathcal{T}_b^\star \mathcal{L} \simeq \mathcal{L}$ sur A, donc à fortiori $\mathcal{T}_b^\star(\mathcal{L}|B) \simeq \mathcal{L}|B$ sur B, i.e. $\mathcal{L}|B$

est dans le noyau de Λ, ainsi que $(\mathcal{L}|B)^{\otimes n}$ pour tout $n \geq 0$. Puisque $\mathcal{L}$ est ample, $\mathcal{L}|B$ l'est encore et $H^0(B, (\mathcal{L}|B)^{\otimes n}) \neq 0$ pour $n \gg 0$ d'après 5.12, donc $(\mathcal{L}|B)^{\otimes n}$ est trivial pour $n \gg 0$ d'après le lemme précédent. Donc $\mathcal{O}_B$ est un faisceau ample, ce qui ne peut se produire que si B est fini : donc $B = 0$ et $\ker \Lambda(\mathcal{L})$ est fini.

(2) Soit $\mathcal{M} \in \mathbf{Pic}(A)$ tel que $\Lambda(\mathcal{M}) = 0$. On considère sur $A \times A$ le faisceau inversible $\mathcal{K} = m^\star \mathcal{L} \otimes p_1^\star \mathcal{L}^{-1} \otimes p_2^\star(\mathcal{L}^{-1} \otimes \mathcal{M}^{-1})$. On a donc $\mathcal{K}|\{a\} \times A = \mathcal{T}_a\mathcal{L} \otimes \mathcal{L}^{-1} \otimes \mathcal{M}^{-1}$ et $\mathcal{K}|A \times \{a\} = \mathcal{T}_a\mathcal{L} \otimes \mathcal{L}^{-1}$, qui sont encore dans le noyau de Λ (puisque A est connexe, donc $\Lambda(\mathcal{L})(a) = \mathcal{T}_a\mathcal{L} \otimes \mathcal{L}^{-1} \in \mathbf{Pic}^0_{A/S} \subset \ker \Lambda$). Supposons que pour tout $a \in A$, $\mathcal{K}|\{a\} \times A \neq \mathcal{O}_A$. D'après le lemme précédent et le yoga du changement de base, on a donc $R^i p_{1\star}\mathcal{K} = 0$ pour tout $i \geq 0$. La suite spectrale de Leray

$$H^i(A, R^j p_{1\star}\mathcal{K}) \Rightarrow H^{i+j}(A \times A, \mathcal{K})$$

nous donne alors $H^i(A \times A, \mathcal{K}) = 0$ pour tout $i \geq 0$. D'autre part, nous avons vu que le noyau de $\Lambda(\mathcal{L})$ était fini. En dehors de ce noyau, on a donc $\mathcal{K}|A \times \{a\}$ non-trivial, de sorte que par le même raisonnement, $R^i p_{2\star}\mathcal{K}|A - K(\mathcal{L}) = 0$. Il en résulte que la deuxième suite spectrale de Leray

$$H^i(A, R^j p_{2\star}\mathcal{K}) \Rightarrow H^{i+j}(A \times A, \mathcal{K})$$

dégénère en $H^0(A, R^i p_{2\star}\mathcal{K}) = H^i(A \times A, \mathcal{K})$, d'où l'on tire $R^i p_{2\star}\mathcal{K} = 0$ pour tout i. Le yoga du changement de base nous donne alors $H^i(A \times \{a\}, \mathcal{K}|A \times \{a\}) = 0$ pour tout i et tout a. On obtient une contradiction en prenant $i = 0$ et $a = 0$. $\square$

Le corollaire montre en particulier que $\mathbf{Pic}^0_{A/S} = \ker \Lambda$. On note A^t ce sous-schéma en groupes (ouvert et fermé) de $\mathbf{Pic}_{A/S}$. C'est un schéma en groupes propre et connexe sur k : il ne lui manque plus que la lissité pour être une variété abélienne. Or, on sait que

$$\mathbf{Lie}(A^t) \simeq H^1(A, \mathcal{O}_A) \quad \text{et} \quad \dim A^t = \dim A.$$

La première assertion vient de 9.2, et la seconde résulte du corollaire ci-dessus. La lissité de A^t résultera donc du calcul de la cohomologie de $\mathcal{O}_A$, l'élément *trivial* du noyau de Λ : il nous faut voir que $\dim_k H^1(A, \mathcal{O}_A) = g$.

10.4.2. *Cohomologie de $\mathcal{O}_A$ et applications.* Plus généralement :

Lemma 10.12. *Pour tout $i \geq 0$, $\dim_k H^i(A, \mathcal{O}_A) = C_g^i$.*

Exercise 10.13. Donner une preuve élémentaire dans le cas des courbes elliptiques.

Démonstration. Soit $\mathcal{P}$ le faisceau de Poincarré sur $A \times A^t$. C'est donc le faisceau inversible normalisé sur $A \times A^t$ qui correspond à l'inclusion $A^t = \mathbf{Pic}^0_{A/S} \to \mathbf{Pic}_{A/S}$. Il vérifie $\mathcal{P}|\{0\} \times A^t = 0$ (par normalisation) et $\mathcal{P}|A \times \{a\} = \mathcal{P}_a$ où $a \mapsto \mathcal{P}_a$ est exactement l'identification $A^t = \mathbf{Pic}^0_{A/S}$.

Puisque $p_2 : A \times A^t \to A^t$ est propre, lisse et surjectif, ce faisceau inversible (donc cohérent) $\mathcal{P}$ de $A \times A^t$ est plat sur A^t, de sorte que l'on peut appliquer à cette situation le yoga du changement de base propre. Le lemme 10.10 montre que $H^\star(A \times \{a\}, \mathcal{P}|A \times \{a\}) = 0$ pour tout $a \in A^t - \{0\}$, donc $R^\star p_{2\star}\mathcal{P}|A^t - \{0\} = 0$, i.e. tous les faisceaux cohérents $R^i p_{2\star}\mathcal{P}$ sur A^t sont concentrés en 0, et la suite spectrale $H^i(A^t, R^j p_{2\star}\mathcal{P}) \Rightarrow H^{i+j}(A \times A^t, \mathcal{P})$ dégénère en

$$H^i(A \times A^t, \mathcal{P}) = H^0(A^t, R^i p_{2\star}\mathcal{P}) = (R^i p_{2\star}\mathcal{P})_x = H^i(A \times \mathrm{Spec} R, \mathcal{P}|A \times \mathrm{Spec} R)$$

où $R = \mathcal{O}_{A^t,0}$ est l'anneau local de A^t en 0, un anneau local noethérien de dimension g et de corps résiduel k. Soit $C^0 \to C^1 \to \cdots \to C^g$ le complexe de R-modules (localement libres donc) libres de rang fini qui calcule la cohomologie de $\mathcal{P}|A\times \mathrm{Spec}R$ (universellement sur R). On a donc

$$\begin{aligned} (10.1) \qquad & H^i(A\times A^t,\mathcal{P}) &=& H^i(A\times \mathrm{Spec}R,\mathcal{P}|A\times \mathrm{Spec}R)=H^i(C^\bullet),\\ (10.2) \quad \text{et} \quad & H^i(A,\mathcal{O}_A) &=& H^i(A\times\{0\},\mathcal{P}|A\times\{0\})=H^i(C^\bullet\otimes_R k). \end{aligned}$$

La première formule nous dit notamment que les $H^i(C^\bullet)$ sont déjà des k-espaces vectoriels, et en particulier, des R-modules artiniens (=de longueur finie). Or :

Lemma 10.14. *Soit R un anneau local régulier de dimension g et $C^\star$ un complexe de R-modules libres de rang fini tel que $H^i(C^\bullet)$ est artinien. Alors*

$$0\to C^0\to C^1\to\cdots\to C^g\to H^g(C^\bullet)\to 0$$

est exacte.

Démonstration. C'est un lemme d'algèbre commutative, cf. [8, Page 127]. □

On ne peut pas appliquer directement ce lemme, parce que l'on ne sait pas (encore) que notre anneau R est régulier. Par contre R_{red} est régulier : c'est l'anneau local en 0 de A^t_{red}, qui est un groupe algébrique réduit, donc (génériquement lisse donc) lisse. D'autre part, on voit facilement que les R_{red}-modules $H^i(C^\bullet\otimes R_{red})$ sont encore artiniens, et même des k-espaces vectoriels (par exemple en reprenant tout l'argument avec A^t remplacé par A^t_{red} !). Donc,

$$0\to C^0\otimes R_{red}\to C^1\otimes R_{red}\to\cdots\to C^g\otimes R_{red}\to H^g(C^\bullet\otimes R_{red})\to 0$$

est exacte. De même, on vérifie que les R_{red}-modules $H^i(\widehat{C}^\bullet\otimes R_{red})$ sont encore artiniens, et même des k-espaces vectoriels (où $\widehat{X}=\mathrm{Hom}_R(X,R)$ est libre de rang fini si X l'est), donc

$$0\to \widehat{C}^g\otimes R_{red}\to \widehat{C}^{g-1}\otimes R_{red}\to\cdots\to \widehat{C}^0\otimes R_{red}\to H_0(\widehat{C}\otimes R_{red})\to 0$$

est exacte. Mais $H_0(\widehat{C}\otimes R_{red})=H_0(\widehat{C}\otimes R_{red})\otimes k=H_0(\widehat{C}\otimes k)$ est le conoyau de

$$\mathrm{Hom}_R(C^1,R)\otimes k\to \mathrm{Hom}_R(C^0,R)\otimes k$$

et c'est donc le k-dual du noyau $H^0(C^\bullet\otimes k)=H^0(A,\mathcal{O}_A)\simeq k$. Bref, $\widehat{C}^\bullet\otimes R_{red}$ est une résolution du corps résiduel k de R_{red} par des R_{red}-modules libres de rangs finis. Ces résolutions sont toutes homotopes, et il y en a une bien connue qui s'appelle la résolution de Koszul $K^\bullet$. On en déduit que $C^\bullet\otimes R_{red}$ est homotope à $\widehat{K}^\bullet$, donc $C^\bullet\otimes k$ à $\widehat{K}^\bullet\otimes k$: ce qui permet de calculer $H^\star(A,\mathcal{O}_A)=H^\star(C^\bullet\otimes k)=H^\star(\widehat{K}^\bullet\otimes k)$. On trouve la bonne formule pour la dimension. En particulier, $\dim_k H^1(A,\mathcal{O}_A)=g$, donc A^t est lisse et $R_{red}=R$ dans tout l'argument ci-dessus. La formule (10.2) démontre le lemme 10.12. □

Lemma 10.15. $H^i(A\times A^t,\mathcal{P})=0$ *si* $i\neq g$ *et* $H^g(A\times A^t,\mathcal{P})=k$.

Démonstration. Cela résulte de la formule (10.1). □

Corollary 10.16. *Le morphisme de bidualité $\delta: A\to A^{tt}$ est un isomorphisme.*

Démonstration. Par définition, $\mathcal{P}$ sur $A\times A^t$ est le pull-back par (δ,Id) de son analogue $\mathcal{Q}$ sur $A^{tt}\times A^t$. Si δ n'est pas une isogénie, son noyau contient des sous-schémas en groupes F de A de degré $d(F)$ arbitrairement grand, $\mathcal{P}$ est le pull-back d'un faisceau inversible par $A\times A^t\to A/F\times A^t$, donc $d(F)\mid\chi(P)=(-1)^g$, une contradiction, donc δ est une isogénie. Le même argument montre que cette isogénie est de degré 1, i.e. un isomorphisme. □

10.4.3. *Cohomologie des faisceaux amples.* On rappelle la formule suivante, qui résulte classiquement du théorème du cube et figure dans le cours de M. Hindry : pour tout $\mathcal{L} \in \mathbf{Pic} A$ et $n \in \mathbf{N}$,

$$[n]^\star \mathcal{L} \simeq \mathcal{L}^{\frac{n^2+n}{2}} \otimes [-1]^\star \mathcal{L}^{\frac{n^2-n}{2}}$$

Or pour tout $x \in A$,

$$\begin{aligned} \mathcal{T}_x^\star \left(\mathcal{L} \otimes [-1]^\star \mathcal{L}^{-1}\right) &\simeq \mathcal{T}_x^\star \mathcal{L} \otimes [-1]^\star \mathcal{T}_{-x}^\star \mathcal{L}^{-1} \\ &\simeq \mathcal{T}_x^\star \mathcal{L} \otimes [-1]^\star (\mathcal{T}_{-x}^\star \mathcal{L}^{-1} \otimes \mathcal{L}) \otimes [-1]^\star \mathcal{L}^{-1} \\ &\simeq \mathcal{T}_x^\star \mathcal{L} \otimes (\mathcal{T}_{-x}^\star \mathcal{L} \otimes \mathcal{L}^{-1}) \otimes [-1]^\star \mathcal{L}^{-1} \\ &\simeq \mathcal{L} \otimes [-1]^\star \mathcal{L}^{-1} \end{aligned}$$

donc $[-1]^\star \mathcal{L} \sim \mathcal{L}$ et $[n]^\star \mathcal{L} \sim \mathcal{L}^{n^2}$, où $\sim$ dénote l'équivalence algébrique, i.e. modulo $\mathbf{Pic}^0_{A/S}$. Si de plus $\Lambda(\mathcal{L}) : A \to A^t$ est surjective, par exemple si $\mathcal{L}$ est ample, on peut donc trouver un $x \in A$ tel que $\Lambda(\mathcal{L}^{n^2})(x) = [n]^\star \mathcal{L} \otimes \mathcal{L}^{-n^2}$, i.e. $\mathcal{T}_x \mathcal{L}^{n^2} \otimes \mathcal{L}^{-n^2} \simeq [n]^\star \mathcal{L} \otimes \mathcal{L}^{-n^2}$, donc $\mathcal{T}_x \mathcal{L}^{n^2} \simeq [n]^\star \mathcal{L}$.

Lemma 10.17. *Si $\mathcal{L}$ est inversible ample sur A, alors $H^i(A, \mathcal{L}) = 0$ si $i > 0$.*

Démonstration. Puisque $\mathcal{L}$ est ample,

$$H^i(A, [n]^\star \mathcal{L}) \simeq H^i(A, \mathcal{T}_x^\star \mathcal{L}^{n^2}) \simeq H^i(A, \mathcal{L}^{n^2}) = 0$$

pour tout $n \gg 0$ et $i > 0$ d'après le corollaire 5.6. Puisque $[n] : A \to A$ est fini,

$$H^i(A, [n]^\star \mathcal{L}) \simeq H^i(A, [n]_\star [n]^\star \mathcal{L}) = 0$$

pour tout $n \gg 0$ et $i > 0$. Mais si n est premier à la caractéristique de k, $\mathcal{L}$ est un facteur direct de $[n]_\star [n]^\star \mathcal{L}$, donc $H^i(A, \mathcal{L}) = 0$ si $i > 0$. ☐

Le calcul du degré de $\Lambda(\mathcal{L})$ pour $\mathcal{L}$ ample résulte alors immédiatement du lemme suivant, valable plus généralement pour tout $\mathcal{L}$ non-dégénéré, i.e. tel que $\Lambda(\mathcal{L}) : A \to A^t$ soit une *isogénie.*

Lemma 10.18. *Si $\mathcal{L}$ est non-dégénéré,* $\deg \Lambda(\mathcal{L}) = (\chi(\mathcal{L}))^2$.

Démonstration. Posons $\alpha = (Id, \Lambda(\mathcal{L})) : A \times A \to A \times A^\perp$. On a donc

$$\alpha^\star \mathcal{P} = m^\star \mathcal{L} \otimes p_1^\star \mathcal{L}^{-1} \otimes p_2^\star \mathcal{L}^{-1}$$

donc puisque α est fini et plat,

$$\chi(\alpha^\star \mathcal{P}) = \deg \alpha \cdot \chi(\mathcal{P}) = \chi(m^\star \mathcal{L} \otimes p_1^\star \mathcal{L}^{-1} \otimes p_2^\star \mathcal{L}^{-1}).$$

On voit comme plus haut que tous les

$$R^i p_{1,\star}(m^\star \mathcal{L} \otimes p_1^\star \mathcal{L}^{-1} \otimes p_2^\star \mathcal{L}^{-1}) = R^i p_{1,\star}(m^\star \mathcal{L} \otimes p_2^\star \mathcal{L}^{-1}) \otimes \mathcal{L}^{-1}$$

sont à support de dimension 0, donc $R^i p_{1,\star}(m^\star \mathcal{L} \otimes p_2^\star \mathcal{L}^{-1})$ aussi, et

$$H^i(A \times A, m^\star \mathcal{L} \otimes p_1^\star \mathcal{L}^{-1} \otimes p_2^\star \mathcal{L}^{-1}) \simeq H^0(A, \bullet) \simeq H^i(A \times A, m^\star \mathcal{L} \otimes p_2^\star \mathcal{L}^{-1}).$$

Mais l'isomorphisme $\theta : A \times A \to A \times A$ donné par $\theta(a, b) = (a + b, b)$ vérifie

$$\theta^\star (p_1^\star \mathcal{L} \otimes p_2^\star \mathcal{L}^{-1}) = m^\star \mathcal{L} \otimes p_2^\star \mathcal{L}^{-1}$$

d'où l'on tire en utilisant la formule de Künneth que

$$H^i(A \times A, m^\star \mathcal{L} \otimes p_1^\star \mathcal{L}^{-1} \otimes p_2^\star \mathcal{L}^{-1}) \simeq \oplus_{j+j'=i} H^j(A, \mathcal{L}) \otimes H^{j'}(A, \mathcal{L}^{-1}).$$

Il en résulte que $\chi(m^\star\mathcal{L}\otimes p_1^\star\mathcal{L}^{-1}\otimes p_2^\star\mathcal{L}^{-1}) = \chi(\mathcal{L})\cdot\chi(\mathcal{L}^{-1})$. On a donc :

$$\chi(\mathcal{L})\cdot\chi(\mathcal{L}^{-1}) = \chi(\mathcal{P})\cdot\deg\Lambda(\mathcal{L}) = (-1)^g\cdot\deg\Lambda(\mathcal{L}).$$

En appliquant ceci à $\mathcal{L}^{\otimes n}$, $n>0$, on trouve

$$\chi(\mathcal{L}^{\otimes n})\cdot\chi(\mathcal{L}^{-\otimes n}) = (-1)^g n^{2g}\cdot\deg\Lambda(\mathcal{L}).$$

Pour $\mathcal{L}$ ample, on a vu que $n\mapsto\chi(\mathcal{L}^{\otimes n})$ est un polynome, et la formule ci-dessus montre qu'il est homogène de degré g. En particulier $\chi(\mathcal{L}^{-1}) = (-1)^g\chi(\mathcal{L})$, donc $\deg\Lambda(\mathcal{L}) = \chi(\mathcal{L})^2$. Pour le cas général, il faut savoir que $n\mapsto\chi(\mathcal{L}^{\otimes n})$ est encore un polynome. □

Remark 10.19. On a vu dans la preuve ci-dessus que pour $\mathcal{L}$ ample et $n>0$

$$\chi(\mathcal{L}^{\otimes n}) = \dim_k H^0(A,\mathcal{L}^{\otimes n}) = n^g\chi(\mathcal{L}).$$

10.4.4. *Rappels.* Soit X/k une variété propre et lisse, $\mathcal{L}$ un faisceau inversible sur X et $E = H^0(X,\mathcal{L})$. Le support du conoyau du morphisme $E\otimes\mathcal{O}_X\to\mathcal{L}$ est un fermé de X. On note $X(\mathcal{L})$ l'ouvert complémentaire. Par construction, le morphisme canonique $E\otimes\mathcal{O}_{X(\mathcal{L})}\to\mathcal{L}|X(\mathcal{L})$ est surjectif : on obtient donc un morphisme $\iota(\mathcal{L}) : X(\mathcal{L})\to\mathbf{P}(E)$ tel que $\mathcal{L}\simeq\iota(\mathcal{L})^\star\mathcal{O}_{\mathbf{P}}(1)$. D'autre part, nous avons vu que l'ensemble $|\mathcal{L}|$ des diviseurs effectifs D qui sont linéairement équivalents à $\mathcal{L}$ (i.e. tels que $\mathcal{L}\simeq\mathcal{O}_X(D)$) est en bijection avec l'ensemble (l'espace projectif) des *droites* de E, via l'application qui à $s\in E$ associe le diviseur $D(s)$ de s, à savoir le lieu (fermé) de X où le morphisme $\mathcal{O}_X\to\mathcal{L}$ n'est pas surjectif. Cette bijection permet de décrire diverses propriétés de $\iota(\mathcal{L})$. On dit que $|\mathcal{L}|$ est (1) sans point base, (2) sépare les points, (3) sépare les vecteurs tangents ssi (1) pour tout $x\in X$, il existe $D\in|\mathcal{L}|$ tel que $x\notin D$, (2) pour tout $x,y\in X$, il existe $D\in|\mathcal{L}|$ tel que $x\in D$ mais $y\notin D$ ou l'inverse, et (3) pour tout $x\in X$ et $t\in T_xX$, il existe $D\in|\mathcal{L}|$ tel que $x\in D$ mais $t\notin T_xD$. Alors (1) $\iff X(\mathcal{L}) = X$, $(1+2)\iff X(\mathcal{L}) = X$ et $\iota(\mathcal{L})$ est injective, et $(1-3)\iff X(\mathcal{L}) = X$ et $\iota(\mathcal{L})$ est une immersion fermée. Cf. [6, Chap III, Prop. 7.3].

10.4.5. *Application.* On revient au cas qui nous intéresse : $X/k = A/k$ est une variété abélienne. Pour appliquer les résultats ci-dessus, il faut savoir construire des éléments dans $|\mathcal{L}|$: on utilise pour cela le lemme suivant.

Lemma 10.20. *Soit $D\in|\mathcal{L}|$ et $x_1,\cdots,x_r\in A$. Alors*

$$\sum_{i=1}^r x_i = 0 \text{ dans } A \quad\Longrightarrow\quad \sum_{i=1}^r T_{x_i}^\star D\in|\mathcal{L}^{\otimes r}|.$$

Démonstration. Cela résulte de $\Lambda(\mathcal{L})(x_1+\cdots+x_r) = 0$, puisque

$$\Lambda(\mathcal{L})(x)\simeq\mathcal{T}_x^\star\mathcal{L}\otimes\mathcal{L}^{-1}\simeq T_x^\star\mathcal{O}(D)\otimes\mathcal{O}(D)^{-1} = \mathcal{O}(\mathcal{T}_x^\star D)\otimes\mathcal{O}(D)^{-1}$$

donc $\sum_{i=1}^r\mathcal{T}_{x_i}^\star D\sim rD\in|\mathcal{L}^{\otimes r}|$. □

En voici une première application :

Proposition 10.21. *Soit $\mathcal{L}$ un faisceau inversible. Les conditions suivantes sont équivalentes :* (1) *$\mathcal{L}$ est ample,* (2) *$\Lambda(\mathcal{L})$ est une isogénie et $H^0(A,\mathcal{L})\neq 0$,* (3) *$|\mathcal{L}^{\otimes 2}|$ est sans point base et $\iota(\mathcal{L}^{\otimes 2}) : A\to\mathbf{P}(H^0(A,\mathcal{L}^{\otimes 2}))$ est un morphisme fini.*

Démonstration. (3) $\Rightarrow$ (1) est un résultat général de géométrie algébrique, cf. [1, III 2.6.1 ou 4.4.2]. Pour (1) $\Rightarrow$ (2), supposons que $\mathcal{L}$ est ample. On sait alors que $\Lambda(\mathcal{L})$ est une isogénie (corollaire 10.11), que $\chi(\mathcal{L}^{\otimes n}) = n^g\chi(\mathcal{L}) = \dim_k H^0(A, \mathcal{L}^{\otimes n})$ (remarque 10.19), et que $\chi(\mathcal{L}^{\otimes n}) > 0$ pour $n \gg 0$ (lemme 5.7), donc $\dim_k H^0(A, \mathcal{L}) \neq 0$. Pour (2) $\Rightarrow$ (3), on choisit $D \in |\mathcal{L}|$, qui existe d'après (2). Alors pour tout $x \in A$, $\mathcal{T}_x^\star D + \mathcal{T}_{-x}^\star D \in |\mathcal{L}^{\otimes 2}|$ d'après le lemme précédent. Soit alors $y \in A$. En comparant simplement les dimensions, on voit que le support de $[\pm 1](D - y)$ est distinct de A. Si $x \in A$ n'est pas dans ce support, alors y n'est pas dans celui de $\mathcal{T}_x^\star D + \mathcal{T}_{-x}^\star D$, donc $|\mathcal{L}^{\otimes 2}|$ est sans point base. Soit ensuite $H = H^0(A, \mathcal{L}^{\otimes 2})$, $\iota : A \to \mathbf{P}(H)$ le morphisme $\iota(\mathcal{L}^{\otimes 2})$. Pour tout $x \in A$, notons $C(x)$ la composante connexe de x dans $\iota^{-1}\iota(x)$. Le lemme de rigidité appliqué au A-morphisme $C(x) \times A \to \mathbf{P} \times A$ défini par $(y, a) \mapsto (\iota(y + a), a))$ montre que $\iota(y + a) = \iota(x + a)$ pour tout $a \in A$ et $y \in C(x)$. Donc ι est invariant par $\mathcal{T}_{x-y}$, donc $\mathcal{L}^{\otimes 2}$ aussi, et $x - y \in \ker \Lambda(\mathcal{L}^{\otimes 2})$ pour tout $x \in A, y \in C(x)$. En particulier, tous les $C(x)$ sont finis (donc $C(x) = \{x\}$) puisque $\ker \Lambda(\mathcal{L}^{\otimes 2})$ l'est. Donc $\iota(\mathcal{L}^2)$ est quasi-fini (et propre) donc fini. $\square$

Les mêmes techniques permettent de montrer que toute variété abélienne sur un corps algébriquement clos est projective. En travaillant encore plus, on montre même que

Proposition 10.22. *Pour tout $\mathcal{L}$ ample sur A et tout $n \geq 3$, $|\mathcal{L}^{\otimes n}|$ sépare les points et les vecteurs tangents, de sorte que $\iota(\mathcal{L}^{\otimes n}) : A \hookrightarrow \mathbf{P}(H^0(A, \mathcal{L}^{\otimes n}))$ est une immersion fermée.*

Démonstration. Cf. [8, §17]. $\square$

Exercise 10.23. Prouver cette proposition lorsque $\Lambda(\mathcal{L})$ est un isomorphisme.

Montrons comment cela marche lorsque $A = E$ est une courbe elliptique. On sait que $|2 \cdot 0|$ contient $D_x = (x) + (-x)$ pour tout $x \in A$. Donc si $x, y \in A$ avec $x \neq \pm y$, sont distincts, on a $x \in D_{\pm x}$ et $y \notin D_{\pm y}$: on en déduit que $|2 \cdot 0|$ est sans point base et $\iota(2 \cdot 0) : E \hookrightarrow \mathbf{P}(H^0(E, \mathcal{O}(2 \cdot 0))$ a pour fibre les couples $(x, -x)$, donc 0 est ample. Puisque $\dim_k H^0(E, \mathcal{O}_E(0)) = 1$, l'isogénie $\Lambda(0) : E \to E^t$ est un isomorphisme : E est auto-duale. On sait que $|3 \cdot 0|$ contient $D_{x,y} = (x) + (y) + (-x - y)$. Donc si $x, y \in A$ avec $x \neq y$, on peut choisir $z \neq x, y, -x - y$. Alors $x \in D_{x,z}$ mais $y \notin D_{x,z}$, donc $|3 \cdot 0|$ sépare les points. On montre de même que $|3 \cdot 0|$ sépare les vecteurs tangents, donc $\iota(3 \cdot 0)$ est un plongement projectif. Mais on peut faire mieux : on sait que $\dim_k H^0(E, \mathcal{O}_E(n \cdot 0)) = n$ pour $n > 0$, 1 pour $n = 0$, et ces espaces vectoriels forment une suite croissante. Choisissons

$$X \in H^0(E, \mathcal{O}_E(2 \cdot 0)) - H^0(E, \mathcal{O}_E(0)) \quad \text{et} \quad Y \in H^0(E, \mathcal{O}_E(3 \cdot E)) - H^0(E, \mathcal{O}_E(2 \cdot E)).$$

En considérant l'ordre du pole en 0, on voit donc que

$$\begin{array}{rcl}
H^0(E, \mathcal{O}_E(1)) & = & k \cdot 1 \\
H^0(E, \mathcal{O}_E(2)) & = & k \cdot 1 \oplus k \cdot X \\
H^0(E, \mathcal{O}_E(3)) & = & k \cdot 1 \oplus k \cdot X \oplus k \cdot Y \\
H^0(E, \mathcal{O}_E(4)) & = & k \cdot 1 \oplus k \cdot X \oplus k \cdot Y \oplus k \cdot X^2 \\
H^0(E, \mathcal{O}_E(5)) & = & k \cdot 1 \oplus k \cdot X \oplus k \cdot Y \oplus k \cdot X^2 \oplus k \cdot XY \\
H^0(E, \mathcal{O}_E(6)) & = & k \cdot 1 \oplus k \cdot X \oplus k \cdot Y \oplus k \cdot X^2 \oplus k \cdot XY \oplus k \cdot \begin{cases} X^3 & \text{ou} \\ Y^2 & \end{cases}
\end{array}$$

d'où l'on déduit que $Y^2 = aX^3 + bXY + cX + dY + e$ avec $a, b, c, d, e \in k$, $a \neq 0$. Utilisant la base $(X, Y, 1)$ de $H^0(E, \mathcal{O}_E(3)) = H$ pour identifier $\mathbf{P}(H) \simeq \mathbf{P}^2$, on voit que l'image du plongement $\iota(3 \cdot 0) : E \hookrightarrow \mathbf{P}(H) \simeq \mathbf{P}^2$ est la courbe elliptique (plongée) définie par cette équation de Weierstrass.

Exercise 10.24. Traiter en détail ce cas des courbes elliptiques.

10.5. **Preuves sur S quelconque.** Soit A un schéma abélien sur S. Tous les énoncés sont locaux sur S, que l'on peut donc supposer affine, et même Noethérien, et tel que A se plonge dans un $\mathbf{P}^N_S$. Le théorème 10.8 résulte immédiatement des résultats ci-dessus, d'après le yoga du changement de base. De même, $\mathbf{Pic}^0_{A/S} = \ker \Lambda$: c'est donc un sous-schéma ouvert et fermé de $\mathbf{Pic}_{A/S}$. Pour tout $s \in S$, $(\mathbf{Pic}^0_{A/S})_s = \mathbf{Pic}^0_{A_s/s}$ est connexe, donc contenu dans un unique sous-schéma ouvert et fermé $\mathbf{Pic}^{\phi}_{A_s/s}$ de $\mathbf{Pic}_{A_s/s}$, à savoir celui pour $\phi = \phi(A_s)$. Puisque $s \mapsto \phi(A_s)$ est localement constant sur S qui est quasi-compact, $\mathbf{Pic}^0_{A/S}$ est donc entièrement contenu dans la réunion (disjointe) d'un nombre fini de certains $\mathbf{Pic}^{\phi}_{A/S}$. Ces derniers étant de type fini sur S, il en est de même de $\mathbf{Pic}^0_{A/S}$. Puisque $\mathbf{Pic}^0_{A/S}$ est fermé dans $\mathbf{Pic}_{A/S}$, $\mathbf{Pic}^0_{A/S}$ vérifie le critère valuatif de propreté local : c'est donc un S-schéma en groupes propre sur S, dont on sait déjà que les fibres sont lisses et géométriquement connexes. Choisissons un faisceau inversible et S-ample sur A, par exemple $\mathcal{L} = \mathcal{O}_A(1)$. Alors $\Lambda(\mathcal{L}) : A \to \mathbf{Pic}_{A/S}$ induit un morphisme surjectif $\Lambda(\mathcal{L}) : A \to \mathbf{Pic}^0_{A/S}$ qui est une isogénie fibre à fibre, et en particulier plat par fibres. Il résulte alors de [1, IV, 11.3.11] que $\mathbf{Pic}^0_{A/S}$ est plat sur S, donc aussi lisse d'après [1, IV, 17.5.1] : c'est donc bien un S-schéma abélien.

Sixième partie 6. Le schéma de Siegel/Mumford

11. Le théorème de Mumford

Soit A/S un schéma abélien. Une *structure de niveau* n sur A est un isomorphisme κ du S-schéma en groupes constant $(\mathbf{Z}/N\mathbf{Z})^{2g}_S$ sur le S-schéma en groupes $A[n]$. Une *polarisation* de degré d^2 est une isogénie $\lambda : A \to A^t$ de degré d^2 (il faut donc que A^t/S existe) telle que pour tout point géométrique s de S, λ_s est de la forme $\Lambda(\mathcal{L}_s)$ pour un faisceau inversible ample sur $\mathcal{L}_s$.

Theorem 11.1. *Soit $g, d, N > 0$ des entiers. On considère le foncteur $\mathbf{M}^g_{d,n}$*

$$(\mathbf{Sch}/\mathbf{Z})^0 \to Ens : \qquad S \mapsto \left\{ (A, \kappa, \lambda) \;\middle|\; \begin{array}{c} A/S \text{ schéma abélien de dim } g \\ \kappa : (\mathbf{Z}/n\mathbf{Z})^{2g}_S \simeq A[n] \text{ struct. niv. } n \\ \lambda : A \to A^t \text{ polarisation de deg } d^2 \end{array} \right\} / \sim$$

Si $n \geq 3$, ce foncteur est représentable par un $\mathbf{Z}$-schéma que l'on note $\mathbf{M}^g_{d,n}$.

Remark 11.2. Ce schéma n'a pas de points en caractéristique $p \mid n$: le schéma ainsi obtenu est donc en fait un $\mathbf{Z}[\frac{1}{n}]$-schéma !

12. Rigidification

12.1. **Analyse.** Soit S un schéma, A/S un schéma abélien projectif et $\lambda : A \to A^t$ un morphisme de schémas en groupes. Le composé du morphisme $\lambda : A \to A^t$ avec l'inclusion $A^t = \mathbf{Pic}^0_{A/S} \hookrightarrow \mathbf{Pic}_{A/S}$ est un A-point du S-schéma $\mathbf{Pic}_{A/S}$, et correspond donc à un faisceau inversible normalisé $\mathcal{P}(\lambda)$ sur $A = A \times_S A$ (normalisé par $\mathcal{P}(\lambda)|e_A(S) \times_S A \simeq \mathcal{O}_A$). C'est le pull-back du faisceau de Poincarré $\mathcal{P}$ par $(Id, \lambda) : A \times_S A \to A \times_S A^t$. L'image inverse de $\mathcal{P}(\lambda)$ par la diagonale $\Delta : A \to A \times_S A$ est un faisceau inversible $L(\lambda) = \Delta^\star \mathcal{P}(\lambda)$ sur A vérifiant $e_A^\star L(\lambda) \simeq \mathcal{O}_S$. Ce faisceau inversible définit donc un morphisme $\Lambda(L(\lambda)) : A \to A^t$ de S-schéma en groupes. En faisceautisant cette construction, on obtient un diagramme :

$$\underline{\mathrm{Hom}}_{Gr}(A, A^t) \xrightarrow{L} \mathbf{Pic}_{A/S} \xrightarrow{\Lambda} \underline{\mathrm{Hom}}_{Gr}(A, A^t).$$

Proposition 12.1. *On a* $2\Lambda = \Lambda \circ L \circ \Lambda$.

Démonstration. Il faut montrer que $2\Lambda(x) = \Lambda \circ L \circ \Lambda(x)$ pour tout T/S et $x \in \mathbf{Pic}_{A/S}(T)$. Par changement de base, on se ramène au cas où $S = T$, et on peut supposer que x est représenté par un faisceau inversible $\mathcal{L}$ sur A, normalisé par $e_A^\star \mathcal{L} \simeq \mathcal{O}_A$. Soit $\lambda = \Lambda(\mathcal{L})$. Alors $\mathcal{P}(\lambda) = m^\star \mathcal{L} \otimes p_1^\star \mathcal{L}^{-1} \otimes p_2^\star \mathcal{L}^{-1}$, donc $L(\lambda) = [2]^\star \mathcal{L} \otimes \mathcal{L}^{-2}$. On veut voir que $\Lambda(L(\lambda)) = 2\Lambda(\mathcal{L})$ dans $\mathrm{Hom}_{S-Gr}(A, A^t)$, et il suffit par rigidité de le montrer pour un point géométrique de chaque composante connexe de S : ce qui nous ramène au cas où S est le spectre d'un corps algébriquement clos. On veut alors que $L(\lambda) \otimes \mathcal{L}^{-2} \simeq [2]^\star \mathcal{L} \otimes \mathcal{L}^{-4}$ soit dans le noyau $\mathbf{Pic}^0_{A/S}$ de Λ, ou encore que $[2]^\star \mathcal{L} \sim \mathcal{L}^4$: on a vu plus haut que $[n]^\star \mathcal{L} \sim \mathcal{L}^{n^2}$ pour tout n, cqfd. □

Corollary 12.2. *Si* $\lambda : A \to A^t$ *est une polarisation de degré* d^2*, alors* (0) $\Lambda(L(\lambda)) = 2\lambda$*,* (1) $L(\lambda)$ *est* S*-ample,* (2) *le* $\mathcal{O}_S$*-module* $\mathcal{E}(\lambda) = f_\star(L(\lambda)^{\otimes 3})$ *est localement libre de rang* $6^g d$*, et* (3) *le morphisme canonique* $f^\star \mathcal{E}(\lambda) \to L(\lambda)^{\otimes 3}$ *est surjectif et induit une immersion fermée* $\iota(\lambda) : A \hookrightarrow \mathbf{P}(\mathcal{E}(\lambda))$*.*

Démonstration. Pour (0), il suffit (par rigidité) de le vérifier en un point géométrique s de chaque composante connexe de S, ou cela résulte du fait que par hypothèse, $\lambda_s = \Lambda(\mathcal{L}_s)$ pour un faisceau inversible ample $\mathcal{L}_s$ sur A. Donc $2\lambda_s = 2\Lambda(\mathcal{L}_s) = \Lambda \circ L \circ \Lambda(\mathcal{L}_s) = \Lambda(L(\lambda_s))$. Pour (1) : En utilisant [1, IV, 9.6.4] (qui dit que l'amplitude peut se vérifier sur les fibres), et [1, IV, 2.7.2] (qui dit que l'amplitude descend par les morphismes fidèlement plats), on est à nouveau ramené au cas des points géométriques s de S comme ci-dessus, où $\lambda_s = \Lambda(\mathcal{L}_s)$, donc $L(\lambda_s) = [2]^\star \mathcal{L}_s \otimes \mathcal{L}_s^{-2}$, avec $[2]^\star \mathcal{L}_s \sim \mathcal{L}_s^4$. Or on sait aussi que $\Lambda(\mathcal{L}_s^2)$ est surjective, de sorte qu'il existe $x \in A_s$ (ou plutôt $A(s)$) tel que $\mathcal{T}_x^\star \mathcal{L}_s^2 \otimes \mathcal{L}_s^{-2} \simeq [2]^\star \mathcal{L}_s \otimes \mathcal{L}_s^{-4}$, donc $L(\lambda_s) \simeq \mathcal{T}_x^\star \mathcal{L}_s^2$, qui est bien ample. Donc $L(\lambda)^{\otimes n}$ est ample pour tout $n \geq 1$, $R^i f_\star(L(\lambda)^{\otimes n}) = 0$ pour tout $i, n \geq 1$, $f_\star(L(\lambda)^{\otimes n})$ est localement libre de formation compatible avec le changement de base. Soit d_n son degré. Alors $\Lambda(L(\lambda)^{\otimes n}) = n\Lambda(L(\lambda)) = 2n\lambda$ est de degré $(2n)^{2g} d^2 = d_n^2$, donc $d_n = (2n)^g d$. De plus, $L(\lambda)^{\otimes n}$ est très ample si $n \geq 3$, i.e. est engendré par ses sections globales et induit une immersion fermée $\iota(L(\lambda)^{\otimes n}) : A \hookrightarrow \mathbf{P}(f_\star(L(\lambda))^{\otimes n})$. QED, avec $n = 3$. □

Definition 12.3. Une rigidification de (A, λ) est un S-isomorphisme

$$\theta : \mathbf{P}(\mathcal{E}(\lambda)) \simeq \mathbf{P}_S^N$$

où $N = 6^g d - 1$. On note $\iota(\lambda, \theta) = \theta \circ \iota(\lambda)$ le plongement correspondant :

$$\iota(\lambda, \theta) : A \hookrightarrow \mathbf{P}_S^N.$$

On obtient ainsi un sous-schéma fermé de $\mathbf{P}_S^N$ qui est plat sur S, i.e. un S-point $\iota(A,\lambda,\phi)$ du S-schéma de Hilbert $\mathbf{Hilb}_{\mathbf{P}_S^N/S}$. Son polynome de Hilbert est

$$\phi(s,r) = \sum_{i=0}^{g} (-1)^i \dim H^i\left(A_s, \iota(\lambda,\theta)^\star \mathcal{O}_{\mathbf{P}_s^N}(r)\right).$$

Notons que sur $\mathbf{P}(\mathcal{E}(\lambda))$, on a maintenant deux quotients remarquables :

$$f^\star\mathcal{E}(\lambda) \twoheadrightarrow \mathcal{O}_{\mathbf{P}(\mathcal{E}(\lambda))}(1) \quad \text{et} \quad \mathcal{O}_{\mathbf{P}(\mathcal{E}(\lambda))}^{N+1} \twoheadrightarrow \theta^\star(\mathcal{O}_{\mathbf{P}_S^N}(1)).$$

On sait d'autre part que : si S est connexe, tous les faisceaux inversibles sur $\mathbf{P}_S^N$ sont de la forme $\mathcal{O}_{\mathbf{P}_S^N}(r)\otimes f^\star\mathcal{L}$ pour un faisceau inversible $\mathcal{L}$ sur S, cf. [9, Lecture 13]. Cet énoncé est d'ailleurs équivalent à $\mathbf{Pic}_{\mathbf{P}_S^N/S} \simeq \mathbf{Z}_S$, et on peut déjà noter avec les techniques dont on dispose qu'effectivement $\mathbf{LiePic}_{\mathbf{P}_S^N/S} = R^1 f_\star\mathcal{O}_S = 0$ d'après 9.2 et 5.5. On en déduit facilement que $\theta^\star(\mathcal{O}_{\mathbf{P}_S^N}(1)) \simeq \mathcal{O}_{\mathbf{P}(\mathcal{E})}(1)\otimes f^\star\mathcal{L}$. En prenant le pull-back par $\iota(\lambda) : A \to \mathbf{P}(\mathcal{E})$, on trouve

$$\iota(\lambda,\theta)^\star(\mathcal{O}_{\mathbf{P}_S^N}(1)) \simeq L(\lambda)^{\otimes 3}\otimes f^\star\mathcal{L}$$

et en prenant le pull-back par la section $e_A : S \to A$, on trouve finalement

$$e(\lambda,\theta)^\star(\mathcal{O}_{\mathbf{P}_S^N}(1)) \simeq \mathcal{L}$$

où $e(\lambda,\theta) = \iota(\lambda,\theta)\circ e_A$. Dans tous les cas, on a donc (pour $r \geq 1$)

$$\phi(s,r) = \sum_{i=0}^{g}(-1)^i \dim_{k(s)} H^i\left(A_s, L(\lambda_s)^{\otimes 3r}\right) = \dim_{k(s)} H^0\left(A_s, L(\lambda_s)^{\otimes 3r}\right)$$

Mais $(\dim_{k(s)} H^0(A_s, L(\lambda_s)^{\otimes 3r}))^2 = \deg \Lambda(L(\lambda_s)^{\otimes 3r}) = \deg 6r\lambda = (6r)^{2g} d^2$, donc

$$\phi(s,r) \equiv \phi(r) \quad \text{où} \quad \phi(X) = 6^g d\cdot X^g.$$

Donc $\iota(A,\lambda,\theta)\in \mathbf{Hilb}^{\phi}_{\mathbf{P}_S^N/S}(S)$.

12.2. **Le foncteur de Mumford rigidifié.** Les considérations précédentes permettent de définir, pour tout $g,d,n\geq 1$, un foncteur de Mumford *rigidifié*,

$$\mathbf{RM}^g_{d,n} : \mathbf{Sch}^0 \to \mathbf{Ens} : \qquad S \mapsto \left\{ (A,\kappa,\lambda,\theta) \;\middle|\; \begin{array}{c} A/S \text{ schéma abélien de dim } g \\ \kappa : (\mathbf{Z}/n\mathbf{Z})_S^{2g} \simeq A[n] \text{ struct. niv. } n \\ \lambda : A\to A^t \text{ polarisation de deg } d^2 \\ \theta : \mathbf{P}(\mathcal{E}(\lambda)) \simeq \mathbf{P}_S^N \text{ rigidification} \end{array} \right\} / \sim$$

avec $N = 6^g d - 1$. Posant $\phi(X) = 6^g d\cdot X^g$, on dispose alors de morphismes

$$\mathbf{M}^g_{d,n} \longleftarrow \mathbf{RM}^g_{d,n} \longrightarrow \mathbf{RM}^g_{d,1} = \mathbf{RM}^g_d \xrightarrow{\iota} \mathbf{Hilb}^{\phi}_{\mathbf{P}^N}$$

où les flèches sont respectivement l'oubli de la rigidification θ, l'oubli de la structure de niveau κ, et la dernière $(A,\lambda,\theta)\mapsto \iota(A,\lambda,\theta) = \iota(\lambda,\theta)(A)\subset \mathbf{P}_S^N$.

Lemma 12.4. $\mathbf{RM}^g_d \to \mathbf{Hilb}^{\phi}_{\mathbf{P}^N}$ *est relativement représentable.*

Corollary 12.5. $\mathbf{RM}^g_d$ *est représentable.*

Démonstration. (du lemme) Il est utile de décomposer ce morphisme en deux, en introduisant

$$\mathbf{Hilb}^{\phi,1}_{\mathbf{P}^N} : \mathbf{Sch}^0 \to \mathbf{Ens} \qquad S \mapsto \left\{ (Z,e) : Z \in \mathbf{Hilb}^{\phi}_{\mathbf{P}^N}(S) \text{ et } e : S\to Z \text{ section}\right\}$$

et les morphisme $\iota'(A,\lambda,\theta)=\iota(\lambda,\theta)(A,e_A)$, $(Z,e)\mapsto Z$, de sorte que

$$\left(\mathbf{RM}_d^g \xrightarrow{\iota} \mathbf{Hilb}^{\phi}_{\mathbf{P}^N}\right)=\left(\mathbf{RM}_d^g \xrightarrow{\iota'} \mathbf{Hilb}^{\phi,1}_{\mathbf{P}^N}\to \mathbf{Hilb}^{\phi}_{\mathbf{P}^N}\right)$$

Le morphisme $\mathbf{Hilb}^{\phi,1}_{\mathbf{P}^N}\to \mathbf{Hilb}^{\phi}_{\mathbf{P}^N}$ est relativement représentable : c'est une tautologie. Plus précisément, $\mathbf{Hilb}^{\phi,1}_{\mathbf{P}^N}$ est représentable par le sous-schéma fermé plat universel de $\mathbf{P}^N\times\mathbf{Hilb}^{\phi}_{\mathbf{P}^N}$. Pour $\mathbf{RM}_d^g\to\mathbf{Hilb}^{\phi,1}_{\mathbf{P}^N}$, j'affirme tout d'abord que c'est un monomorphisme. En effet, (pour tout schéma S), si l'on connaît (1) le plongement $\iota : A\hookrightarrow \mathbf{P}^N_S$ et (2) la section neutre $e_A : S\to A$, on peut successivement reconstruire : (a) la structure de S-schéma en groupes sur A, puisqu'elle est déterminée uniquement par e_A, (b) le faisceau inversible

$$L(\lambda)^{\otimes 3}=\iota^\star\mathcal{O}_{\mathbf{P}^N_S}(1)\otimes f^\star\mathcal{L}\qquad \mathcal{L}=e^\star\mathcal{O}_{\mathbf{P}^N_S}(-1)$$

donc aussi (c) le morphisme $6\lambda=\Lambda(L(\lambda)^{\otimes 3})$ et le morphisme $\lambda : A\to A^t$, puisque $\mathrm{Hom}_{S-Gr}(A,A^t)$ est sans torsion et (d) le faisceau inversible $\mathcal{E}(\lambda)=f_\star(L(\lambda)^{\otimes 3})$ sur S. Mais on a aussi : (e) l'épimorphisme $\mathcal{O}_A^{N+1}\twoheadrightarrow \iota^\star\mathcal{O}_{\mathbf{P}^N_S}(1)$, que l'on peut tordre par $f^\star\mathcal{L}$ pour obtenir $f^\star\mathcal{L}^{N+1}\twoheadrightarrow L(\lambda)^{\otimes 3}$, puis pousser sur S pour obtenir

$$\mathcal{L}^{N+1}\to f_\star f^\star\mathcal{L}^{N+1}\to\mathcal{E}(\lambda)=f_\star L(\lambda)$$

Enfin, on obtient (f) $\theta : \mathbf{P}(\mathcal{E}(\lambda))\to\mathbf{P}(\mathcal{L}^{N+1})\simeq\mathbf{P}^N$ en applique $\mathbf{P}$ à ce dernier morphisme.

On va maintenant définir des sous-foncteurs intermédiaires

$$\mathbf{RM}_d^g=\mathbf{H}_5\hookrightarrow\mathbf{H}_4\hookrightarrow\cdots\hookrightarrow\mathbf{H}_1\hookrightarrow\mathbf{H}_0=\mathbf{Hilb}^{\phi}_{\mathbf{P}^N}$$

et montrer que chaque étape est relativement représentable.

– $\mathbf{H}_1(S)=\{(X,e)\in\mathbf{H}_0(S)|f : X\to S$ est propre et **lisse**$\}$.

Soit $(X,e)\in\mathbf{H}_0(S)$ et $S'=S-f(X-U)$ où U est l'ouvert de X des points où f est lisse. Alors S' est ouvert dans S car f est propre donc fermé et f est lisse sur S'.Si $T\to S$ et $f_T : X_T\to T$ est lisse, alors pour tout point t de T sur s de S, $f_t : X_t\to t$ est lisse, donc $f_s : X_s\to s$ est lisse (d'après [1, IV, 17.7.1] pour faire court), donc $f : X\to S$ est lisse aux points de X_s (d'après [1, IV, 17.5.1]), donc $X_s\subset U$, $s\in S'$ et $T\to S$ se factorise par S'. Le morphisme $\mathbf{H}_1\hookrightarrow\mathbf{H}_0$ est donc représentable par des immersions ouvertes.

– $\mathbf{H}_2(S)=\{(X,e)\in\mathbf{H}_1(S)|f : X\to S$ est propre, lisse et **géo. connexe**$\}$.

Soit $(X,e)\in\mathbf{H}_1(S)$. La fonction $s\mapsto c(s)=\dim_{k(s)}H^0(X_s,\mathcal{O}_{X_s})$ est semi-continue du bon côté d'après le yoga du changement de base, donc $S'=c^{-1}(1)$ est ouvert dans S. Les fibres de f sont connexes (et lisses) donc géométriquement connexes au-dessus de S'. Si $T\to S$ et $f_T : X_T\to T$ est à fibres géométriquement connexes, alors $c(t)=1$ pour tout t de T, donc $c(s)=1$ pour tout s dans l'image de $T\to S$, i.e. $T\to S$ se factorise par S'. Le morphisme $\mathbf{H}_2\hookrightarrow\mathbf{H}_1$ est donc représentable par des immersions ouvertes.

– $\mathbf{H}_3(S)=\{(X,e)\in\mathbf{H}_2(S)|X/S$ est un **schéma abélien** de neutre $e\}$.

Soit $(X,e)\in\mathbf{H}_2(S)$. Soit H le S-schéma universel pour l'existence de morphismes $m : X\times_S X\to X$ et $i : X\to X$ et $m_H : X_H\times_H X_H\to X_H$, $i_H : X_H\to X_H$ les morphismes universels. Les conditions qui expriment le fait que m_H est une loi de groupe sur X_H de neutre e_H et d'inverse i_H s'expriment par la commutativité de certains diagrammes de morphismes de S-schémas propres et plats construits à partir de m_H, i_H et e_H, et sont donc représentables par des sous-schémas de coincidences de sections des H-schémas qui représentent ces types de morphismes.

Par exemple : soit H' le H-schéma universel pour l'existence de morphismes $X_H \to X_H$. Les deux morphismes $x \mapsto m(x, i(x))$ et $x \mapsto e$ définissent des sections $H \to H'$, et le sous-schéma des coincidences de ces deux sections représente la condition i est un inverse à droite pour m. Le morphisme $\mathbf{H}_3 \to \mathbf{H}_2$ est donc relativement représentable.

Pour $(\iota : A \hookrightarrow \mathbf{P}^N_S) \in \mathbf{H}_3(S)$, on pose $\mathcal{M} = \iota^\star \mathcal{O}_{\mathbf{P}^N_S}(1)$ et $\mathcal{L} = e^\star \mathcal{O}_{\mathbf{P}^N_S}(-1)$.

– $\mathbf{H}_4(S) = \{(A, \lambda : A \to A^t) | A \in \mathbf{H}_3(S) \text{ et } L(\lambda)^{\otimes 3} \simeq \mathcal{M} \otimes \mathcal{L}\}$.

Soit $A \in \mathbf{H}_3(S)$. Soit H le schéma universel pour les morphismes $\lambda : A \to A^t$. Sur A_H, on a maintenant deux faisceaux inversibles normalisés, à savoir $L(\lambda)^{\otimes 3}$ et $\mathcal{M} \otimes \mathcal{L}$. Ils donnent deux sections $H \to \mathbf{Pic}_{A/S}$. Le sous-schéma des coincidences de ces deux sections représente la fibre de $\mathbf{H}_4 \to \mathbf{H}_3$ sur A.

– $\mathbf{H}_5(S) = \{(A, \lambda, \theta) | (A, \lambda) \in \mathbf{H}_4(S),\ \theta : \mathbf{P}(\mathcal{E}(\lambda)) \simeq \mathbf{P}^N_S \text{ t.q. } \iota(\lambda, \theta) = \iota\}$

Soit $(A, \lambda) \in \mathbf{H}_4(S)$. Soit H le schéma universel pour $\theta : \mathbf{P}(\mathcal{E}(\lambda)) \to \mathbf{P}^N_S$ et $\theta' : \mathbf{P}^N_S \to \mathbf{P}(\mathcal{E}(\lambda))$. Soit H' le sous-schéma de H où $\theta \circ \theta' = Id$ et $\theta' \circ \theta = Id$ (c'est un schéma de coincidence). Soit H'' le sous-schéma de H' où $\theta \circ \iota(\lambda) : A \to \mathbf{P}^N_{H'}$ est le plongement de départ (c'est encore un schéma de coincidence). Alors H'' représente la fibre de $\mathbf{H}_5 \to \mathbf{H}_4$ sur (A, λ). CQFD. □

Lemma 12.6. *Le morphisme* $\mathbf{RM}^g_{d,n} \to \mathbf{RM}^g_d$ *est relativement représentable.*

Corollary 12.7. $\mathbf{RM}^g_{d,n}$ *est représentable.*

Démonstration. (du lemme) Soit $(A, \lambda, \theta) \in \mathbf{RM}^g_d(S)$, H le schéma universel pour les morphismes $\kappa : (\mathbf{Z}/n\mathbf{Z})^{2g} \to A_H[n]$ et κ' dans l'autre sens, H' le sous-schéma de H ou $\theta\theta' = Id$ et $\theta'\theta = Id$. Alors H' représente la fibre de $\mathbf{RM}^g_{d,n} \to \mathbf{RM}^g_d$ sur (A, λ, θ). On peut aussi partir de $H = A[n]^{2g}$ et découper dedans l'ouvert $A[n]^{2g\star}$ des $\mathbf{Z}/n\mathbf{Z}$-générateurs. □

13. Le morphisme $\mathbf{RM}^g_{d,n} \to \mathbf{M}^g_{d,n}$

C'est la partie la plus difficile de la construction : on sait que $\mathbf{RM}^g_{d,n}$ est représentable (pour tout n), et il faut maintenant descendre cette représentabilité à $\mathbf{M}^g_{d,n}$ (pour $n \geq 3$). Il faut donc se débarrasser du choix de l'isomorphisme $\theta : \mathbf{P}(\mathcal{E}(\lambda)) \to \mathbf{P}^N_S$: on le fait en divisant par le groupe des automorphismes $\mathbf{PGL}_{N+1,S}$ de $\mathbf{P}^N_S$. Les notes ci-dessus donnent quelques informations rudimentaires sur cette construction de Mumford, qui lui valut la médaille Fields. Pour plus de détails, il faut lire [10] !

13.1. **Fibrés principaux.** Soit S un schéma que l'on supposera noethérien, G un S-schéma en groupe plat et de type fini sur S, X un S-schéma sur lequel G agit par $\rho : G \times_S X \to X$. On dit que X est un G-fibré principal de base $\overline{X}$ si et seulement si $p : X \to \overline{X}$ est un S-morphisme fidèlement plat et quasi-compact tel que $(g, x) \mapsto (g \cdot x, x)$ induit un S-isomorphisme $G \times_S X \simeq X \times_{\overline{X}} X$.

Prenons pour G le groupe des automorphismes $G = PGL(V)$ des automorphismes de $\mathbf{P}(V)$ où V est un $\mathcal{O}_S$-module libre de rang $N+1$ (donc $\mathbf{P}(V) \simeq \mathbf{P}^{N+1}_S$ et $G = PGL_{N+1,S}$), et faisons agir G diagonalement sur $X = (\mathbf{P}(V))^r$. Si r est trop petit, tous les points de X ont un stabilisateur non-trivial dans G, donc X n'est pas un G-fibré principal. Si r est suffisamment grand, en revanche, il y a un ouvert X_{reg} de X qui est essentiellement défini par la condition suivante : $(D_1, \cdots, D_r) \in X_{reg}(T)$ si et seulement si pour toute décomposition $V_1 \oplus V_2 = V_T$

telle que pour tout i, $D_i \subset V_1$ ou $D_i \subset V_2$, alors $V_1 = 0$ ou $V_2 = 0$. Les points géométriques de X_{reg} sont les points dont le stabilisateur dans G est trivial, ce qui signifie que X_{reg} est le plus gros sous-espace de X qui a quelque chance d'être un G-fibré principal. En utilisant la définition ci-dessus, Mumford parvient à recouvrir X_{reg} par des ouverts affines stables sous G dont il montre que ce sont bien des G-fibrés principaux (de base affine). On en déduit par recollement que X_{reg} est bien un G-fibré principal, mais la base $\overline{X}_{reg}$ de ce fibré n'est pas séparée ! Mumford définit alors un ouvert X_{st} de X_{reg}, dont il montre qu'il est G-stable, et un G-fibré principal *de base quasi-projective sur* S [10, Chapter 3]. La définition de la *condition de stabilité* qui définit cet ouvert stable est l'un des apports essentiels de Mumford.

13.2. **La technique de Mumford.** La technique de Mumford pour démontrer la représentabilité de $\mathbf{RM}^g_{d,n}$ lorsque $n \gg 0$ repose sur les deux propositions suivantes.

Proposition 13.1. *S'il existe un morphisme de schémas* $\pi : \mathbf{RM}^g_{d,n} \to X$ *qui fait de* $\mathbf{RM}^g_{d,n}$ *un* $\mathbf{PGL}_{N+1}$*-fibré principal, avec* X *quasi-projectif sur* $\mathbf{Spec}\mathbf{Z}$*. Alors*

(1) *les données universelles* $(RA_u, R\lambda_u, R\kappa_u)$ *sur* $\mathbf{RM}^g_{d,n}$ *descendent à* X *et*

(2) *les données descendues* $(A_u, \lambda_u, \kappa_u)$ *font de* X *un schéma qui représente* $\mathbf{M}^g_{d,n}$.

Démonstration. Admettons (1), qui relève des techniques de descente : on veut descendre les données universelles $(RA_u, R\lambda_u, R\kappa_u)$ le long du morphisme fidèlement plat et quasi-compact $\mathbf{RM}^g_{d,n} \to X$. Les données de recollement proviennent de l'action de $G = \mathbf{PGL}_{N+1}$ sur $\mathbf{RM}^g_{d,n}$, RA_u etc, cf. [10, Proposition 7.6]... Montrons (2). On commence par :

(2*a*) Si $(A, \lambda, \kappa, \theta) \in \mathbf{RM}^g_{d,n}(S)$, alors $\mathbf{Aut}_S(A, \lambda, \kappa, \theta) = \{1\}$. En effet, de tels automorphismes sont dans $\mathbf{Aut}_S(A)$ et doivent préserver le *plongement* $\iota(\lambda, \theta)$: $A \hookrightarrow \mathbf{P}^N_S$.

(2*b*) Si $(A, \lambda, \kappa, \theta) \in \mathbf{RM}^g_{d,n}(S)$, alors $\mathbf{Aut}_S(A, \lambda, \kappa) = \{1\}$. En effet, soit γ un tel automorphisme. Alors $\gamma(A, \lambda, \kappa, \theta) = (A, \lambda, \kappa, g\theta)$ pour un automorphisme $g \in \mathbf{PGL}_{N+1}(S)$ de $\mathbf{P}^N_S$. Donc $(A, \lambda, \kappa, g\theta) \simeq (A, \lambda, \kappa, \theta)$ dans $\mathbf{RM}^g_{d,n}(S)$, i.e. $g \cdot (A, \lambda, \kappa, \theta) = (A, \lambda, \kappa, \theta)$ pour l'action de $\mathbf{PGL}_{N+1}(S)$ sur $\mathbf{RM}^g_{d,n}(S)$. Mais alors $g = 1$ (puisque l'action est libre par hypothèse) donc $g\theta = \theta$ et $\gamma \in \mathbf{Aut}_S(A, \lambda, \kappa, \theta)$, donc $\gamma = 1$.

(2*c*) Si $(A, \lambda, \kappa) \in \mathbf{M}^g_{d,n}(S)$, il existe au plus un morphisme $f : S \to X$ et au plus un isomorphisme $F : (A, \lambda, \kappa) \to f^\star(A_u, \lambda_u, \kappa_u)$. En effet, soit (f_1, F_1) et (f_2, F_2) deux telles paires. Supposons d'abord que les f_i se factorisent par $g_i : S \to \mathbf{RM}^g_{d,n}$. Alors les deux $g_i^\star(RA_u, R\lambda_u, R\kappa_u, R\theta_u)$ sont isomorphes au θ-près, i.e. les deux g_i sont conjugués par un élément de $\mathbf{PGL}_{N+1}(S)$, donc les deux $f_i = \pi \circ g_i$ sont égaux, disons à f, et $F_1 = F_2 : (A, \lambda, \kappa) \to f^\star(A_u, \lambda_u, \kappa_u)$ par 2*c*. Dans le cas général, on note que $\pi : \mathbf{RM}^g_{d,n} \to X$ admet des sections après un changement de base fidèlement plat et quasi-compact, par exemple par π lui-même. Donc $(f_1, F_1) = (f_2, F_2)$ après un tel changement de base, et $(f_1, F_1) = (f_2, F_2)$ par descente.

(2*d*) Si $(A, \lambda, \kappa) \in \mathbf{M}^g_{d,n}(S)$, il existe un unique morphisme $f : S \to X$ et un unique isomorphisme $F : (A, \lambda, \kappa) \to f^\star(A_u, \lambda_u, \kappa_u)$. En effet, on montre l'existence localement en recouvrant S par des ouverts S_i qui trivialisent $\mathcal{E}(\lambda)$, et le choix sur chaque S_i d'une telle trivialisation $\mathcal{E}(\lambda)|S_i \simeq \mathcal{O}^{N+1}_{S_i}$ fournit un relèvement local

$(A|S_i, \lambda|S_i, \kappa|S_i, \theta_i) \in \mathbf{RM}^g_{d,n}(S_i)$, donc un g_i, F_i puis un $(f_i = \pi \circ g_i, F_i)$ comme ci-dessus. L'unicité de (2c) permet de tout recoller.

A fortiori : si $(A, \lambda, \kappa) \in \mathbf{M}^g_{d,n}(S)$, il existe un unique morphisme $f : S \to X$ tel que $(A, \lambda, \kappa) \simeq f^\star(A_u, \lambda_u, \kappa_u)$, i.e. X représente $\mathbf{M}^g_{d,n}$. □

Proposition 13.2. *Soient S un schéma noethérien, X, Y des S-schémas de type fini muni d'une action d'un même S-schéma en groupe G, plat et de type fini sur S, $\phi : X \to Y$ un G-morphisme de S-schémas. On suppose que :* (1) *Y est un G-fibré principal de base $\overline{Y}$ quasi-projective sur S,* (2) *X admet un faisceau inversible $\mathcal{L} \in \mathbf{Pic}^G X$ qui est ample sur Y. Alors X est un G-fibré principal de base $\overline{X}$ quasi-projective sur S.*

Démonstration. [10, Proposition 7.1] On veut descendre le Y schéma X en un $\overline{Y}$-schéma $\overline{X}$, i.e. on veut faire de la descente relativement au morphisme fpqc $Y \to \overline{Y}$. Il nous faut pour cela une donnée de recollement sur ce Y-schéma X, c'est-à-dire un isomorphisme entre $p_1^\star X$ et $p_2^\star X$, où $p_i : Y \times_{\overline{Y}} Y \to Y$ sont les deux projections. Or le diagramme commutatif

$$\begin{array}{ccccc} G \times_S X & \Rightarrow & X & \cdots & ?\overline{X}? \\ \downarrow & & \downarrow & & \vdots \\ G \times_S Y & \Rightarrow & Y & \to & \overline{Y} \end{array}$$

où les flèches $\Rightarrow$ sont l'action et la seconde projection *est* une telle donnée de recollement, puisque $G \times_S Y \simeq Y \times_{\overline{Y}} Y$ et que les deux carrés donnés par les flèches doubles sont cartésiens. On vérifie que cette donnée de recollement est une donnée de descente. L'hypothèse (2) permet alors de descendre simultanément la paire $(X, \mathcal{L})$ en une paire $(\overline{X}, \overline{\mathcal{L}})$ qui vérifie toutes les propriétés requises. □

On veut appliquer cette proposition à $G = \mathbf{PGL}_{N+1} = \mathbf{Aut}(\mathbf{P}^N)$ agissant sur $X = \mathbf{RM}^g_{d,n}$. On prend d'abord $Y = (\mathbf{P}^N)^{n^{2g}}$ avec l'action diagonale de G, et pour ϕ le morphisme défini par les n^{2g}-sections de la structure de niveau :

$$(A, \lambda, \kappa, \theta) \in \mathbf{RM}^g_{d,n}(S) \longmapsto \prod_{x \in (\mathbf{Z}/n\mathbf{Z})^{2g}} \iota(\lambda, \theta)(\kappa(x)) \in Y_1(S) = (\mathbf{P}^N)^{n^{2g}}(S).$$

Ce morphisme est évidemment G-linéaire. Mumford montre que *pour* $n \gg 0$ ce morphisme atterrit dans l'ouvert ouvert $Y_{st} \subset Y_{reg}$ de Y [10, Proposition 7.7], qui vérifie bien les hypothèses de l'énoncé (il faut encore dire ce que l'on prend pour faisceau inversible $\mathcal{L}$ sur $\mathbf{RM}^g_{d,n}$, et comment on définit dessus des données de recollement, cf. [10, Proposition 7.4]).

13.3. **Conclusion.** Au final, les techniques ci-dessus permettent de montrer que $\mathbf{M}^g_{d,n}$ est représentable pour $n \gg 0$, plus précisément pour $n > 6^g d\sqrt{g!}$, cf. [10, Theorem 7.9]. Pour conclure, il faut choisir des entiers k auxiliaires et travailler avec le morphisme $\mathbf{M}^g_{d,nk} \to \mathbf{M}^g_{d,n}$ au-dessus de $\mathbf{Z}[\frac{1}{nk}]$. Pour $k \gg 0$, $\mathbf{M}^g_{d,nk}$ est représentable, et la représentabilité de $\mathbf{M}^g_{d,n}$ s'en déduit en quotient par l'action du groupe fini, constant

$$\ker \mathbf{GL}(2g, \mathbf{Z}/nk\mathbf{Z}) \to \mathbf{GL}_{2g}(\mathbf{Z}/n\mathbf{Z}).$$

(Ce passage au quotient n'est pas trop difficile à analyser). On obtient ainsi la représentabilité de $\mathbf{M}^g_{d,n}$ pour $n \geq 3$, mais seulement au dessus de $\mathbf{Z}[\frac{1}{nk}]$. Il reste à recoller ces modèles en choisissant $k_1, k_2 \gg 0$ avec $(k_1, k_2) = 1$!

Septième partie 7. Compléments

14. Faisceaux amples

Un faisceau inversible $\mathcal{L}$ sur un schéma X est ample ssi (1) X est quasi-compact et quasi-séparé, et (2) pour un $n > 0$, il y a des sections globales $\ell_1, \cdots, \ell_r$ de $\mathcal{L}^{\otimes n}$ qui engendrent $\mathcal{L}^{\otimes n}$ et sont telles que $X(\ell_i)$ est quasi-affine. Il est alors vrai que pour tout $n > 0$ et toute section ℓ de $\mathcal{L}^{\otimes n}$, $X(\ell)$ est quasi-affine. Il est en revanche faux que pour tout $n > 0$, $\mathcal{L}^{\otimes n}$ engendre X, mais c'est tout de même vrai pour tout $n \gg 0$.

Si X est maintenant un S-schéma, un faisceau inversible $\mathcal{L}$ sur X est S-ample si et seulement si il existe un recouvrement ouvert *affine* S_i de S tel que $\mathcal{L}|S_i$ est ample. Les deux notions (absolues et S-relatives) coincident lorsque S est affine. Dans tous les cas, X doit être quasi-séparé !

Partons de $f : X \to S$ quasi-compact et quasi-séparé. Soit $\mathcal{L}$ un faisceau inversible sur X. Alors $f_\star(\mathcal{L}^{\otimes n})$ est quasi-cohérent pour tout n et $\mathcal{M} = \oplus f_\star(\mathcal{L}^{\otimes n})$ est gradué, ce qui nous donne donc un S-schéma $\mathbf{P}(\mathcal{L}) = \mathbf{Proj}(\mathcal{M})$ (attention : conflit de notation avec $\mathbf{P}(\mathcal{E})$ pour $\mathcal{E}$ sur S !). Supposons d'abord S affine. Pour toute section ℓ de $\mathcal{L}^{\otimes n}$ sur X, vu comme une section de $\mathcal{O}_{\mathbf{P}}(n)$ sur $\mathbf{P}(\mathcal{L})$, on a

$$\Gamma(X(\ell), \mathcal{O}_X) = \Gamma(\mathbf{P}(\mathcal{L})(\ell), \mathcal{O}_{\mathbf{P}}).$$

Mais par construction $\mathbf{P}(\mathcal{L})(\ell)$ est affine. On obtient donc

$$X(\ell) \to \mathrm{Spec}\Gamma(X(\ell), \mathcal{O}_X) = \mathbf{P}(\mathcal{L})(\ell) \hookrightarrow \mathbf{P}(\mathcal{L}).$$

Revenant au cas général, notons $U(\mathcal{L}) = \cup U_n$ où U_n est l'ouvert de X où $f^\star f_\star(\mathcal{L}^{\otimes n}) \to \mathcal{L}^{\otimes n}$ est surjective. Alors $\mathcal{L}$ nous fournit un S-morphisme $U(\mathcal{L}) \to \mathbf{P}(\mathcal{L})$ et : $\mathcal{L}$ est S-ample si et seulement si $U(\mathcal{L}) = X$ et $X \to \mathbf{P}(\mathcal{L})$ est une immersion ouverte.

15. Descente

Une bonne référence : [4, Chapter 6]. Pour un formalisme plus avancé (catégories fibrés, gerbes et champs/stacks), il faut SGA !

15.1. **Abstract nonsense.** Etant donné un morphisme $f : S' \to S$, il y a de nombreux contextes dans lesquels on a une notion de changement de base : à un objet X sur S, on peut associer un objet $X' = f^\star X$ sur S'. Par exemple, X pourrait être un faisceau sur S, un morphisme de faisceaux sur S, un schéma sur S, un morphisme de schémas sur S, ou même une structure beaucoup plus complexe, tel que : une classe d'isomorphismes de variétés abéliennes polarisées munies d'endomorphismes et/ou de structures de niveau... Il y a une première gamme de questions récurrentes pour le changement de base : si X/S a une propriété P, est-ce que X'/S' a aussi cette même propriété ? Est-ce que telle ou telle construction commute à ce changement de base ? La descente envisage typiquement les questions inverses, par exemple : si X'/S' à une propriété P, est-ce que X/S a aussi cette même propriété ? Et pour commencer : si l'on dispose seulement de l'objet X'/S', existe-t-il un objet X/S tel que $X' \simeq f^\star X$. Autrement dit : quelle est l'image essentielle du foncteur $X \mapsto f^\star X$?

On voit tout de suite que cette question est mal posée. Soit en effet $S" = S' \times_S S'$ et $p_i : S" \to S'$ les deux projections. Alors pour tout objet $X' = f^\star X$ sur S', les deux objets $p_1^\star X'$ et $p_2^\star X'$ sur $S"$ sont canoniquement isomorphes. On introduit alors la catégorie des objets X' sur S' qui sont munis d'une *donnée de recollement*, i.e. d'un isomorphisme $\phi : p_1^\star X' \simeq p_2^\star X'$. Notre question devient : quelle est l'image essentielle de $X \mapsto f^\star X$ dans cette nouvelle catégorie ?

On voit aussi tout de suite qu'il y a une condition nécessaire pour que (X', ϕ) appartienne à cette image. En effet pour X' sur S' et $\phi : p_1^\star X' \simeq p_2^\star X'$ une donnée de recollement, on peut encore faire le pull-back de ϕ par les trois projections $p_{12}, p_{13}, p_{23} : S''' \to S$", où $S''' = S' \times_S S' \times_S S'$. On obtient des isomorphismes $p_{12}^\star \phi : q_1^\star X' \to q_2^\star X'$, $p_{13}^\star \phi : q_1^\star X' \to q_3^\star X'$ et $p_{23}^\star \phi : q_2^\star \phi \to q_3^\star \phi$ où $q_1, q_2, q_3 : S''' \to S'$ sont les trois projections. Lorsque $X' = f^\star X$ et ϕ est la donnée de recollement canonique, la *condition de cocycle* $p_{13}^\star \phi = p_{23}^\star \phi \circ p_{12}^\star \phi : q_1^\star \phi \to q_3^\star \phi$ est vérifiée. En général, on dit que ϕ est une *donnée de descente* si et seulement si cette condition de cocycle est vérifiée. La catégorie qui nous intéresse sera donc plutôt la catégorie des objets sur X' munie d'une donnée de descente (c'est une sous-catégorie pleine de la précédente). Notre question devient : quelle est l'image essentielle de $X \mapsto f^\star X$ dans cette nouvelle catégorie ? On dit que la descente est effective si $X \to f^\star X$ est essentiellement surjectif. Dans tous les cas intéressants, ce sera même une équivalence de catégorie (je ne connais pas de terminologie adaptée à ce cas).

Example 15.1. Soit S un espace topologique, S_i un recouvrement ouvert de S, $S' = \coprod S_i$, $f : S' \to S$ et pour objets : les faisceaux d'ensembles. Un faisceau $\mathcal{F}'$ sur S' est une famille de faisceaux $(\mathcal{F}'_i)$, où $\mathcal{F}'_i$ est un faisceau sur S_i. Le foncteur $\mathcal{F} \mapsto f^\star \mathcal{F} = \mathcal{F}'$ associe à $\mathcal{F}$ la famille de ces restrictions $\mathcal{F}'_i = \mathcal{F}|S_i$. On a $S" = \coprod S_{i,j}$, où $S_{i,j} = S_i \cap S_j$, et les deux projections sont $p_1 : S_{i,j} \hookrightarrow S_i$ et $p_2 : S_{i,h} \hookrightarrow S_j$. Une donnée de recollement sur $\mathcal{F}' = (\mathcal{F}'_i)$ est donc une collection d'isomorphismes $\phi_{i,j} : \mathcal{F}'_i|S_{i,j} \simeq \mathcal{F}'_j|S_{i,j}$, et la condition de cocycle est $\phi_{j,k}|S_{i,j,k} \circ \phi_{i,j}|S_{i,j,k} = \phi_{i,k}|S_{i,j,k}$, où $S_{i,j,k} = S_i \cap S_j \cap S_k$. Si $\mathcal{F}' = f^\star \mathcal{F}$, la donnée de descente canonique est l'identité $\mathcal{F}|S_{i,j} = \mathcal{F}|S_{i,j}$. Dans ce cas, il est bien connu que $\mathcal{F} \mapsto f^\star \mathcal{F}$ est une équivalence de catégorie : la descente des faisceaux pour $S' \to S$ est effective.

15.2. **Descente fpqc.**

Theorem 15.2. *Soit $f : S' \to S$ un morphisme* fidèlement plat *et* quasi-compact. *Alors*

(1) *Pour les faisceaux quasi-cohérents : $\mathcal{F} \mapsto f^\star \mathcal{F}$ est une équivalence de catégorie.*

(2) *Pour les schémas relativement affines : $X \mapsto f^\star X$ est une équivalence de catégorie.*

(3) *Pour les schémas relativement quasi-affines : $X \mapsto f^\star X$ est une équivalence de catégorie.*

(4) *Pour les schémas généraux : $X \mapsto f^\star X$ est pleinement fidèle.*

(5) *(Pour S' et S affines) Une donnée de descente $\phi : p_1^\star X' \simeq p_2^\star X'$ est effective si et seulement si X' admet un recouvrement par des ouverts affines stabilisés par ϕ.*

(6) *(Pour S' et S affines) Une donnée de descente $\phi : p_1^\star X' \simeq p_2^\star X'$ est effective si et seulement si X' admet un recouvrement par des ouverts quasi-affines stabilisés par ϕ.*

Démonstration. On se borne ici à considérer le cas où S' et S sont affines : le cas général s'en déduit *grosso modo* en considérant un recouvrement ouvert affine S_i

de S et pour chaque i un recouvrement ouvert affine fini $S'_{i,j}$ du quasi-compact $f^{-1}(S_i)$; les techniques élémentaires de recollement sur des recouvrements ouverts (comme dans l'exemple ci-dessus) permettent de passer de S à $\coprod S_i$, de S' à $\coprod S'_{i,j}$, et le cas affine s'applique à $\coprod S'_{i,j} \to S_i$ (c'est là que l'on se sert de l'hypothèse de quasi-compactité : pour que $\coprod S'_{i,j}$ soit affine). Soit donc $S = \mathbf{Spec}A$ et $S' = \mathbf{Spec}B$. Les hypothèses sont alors : B est une A-algèbre fidèlement plate.

Montrons que $\mathcal{F} \mapsto f^\star\mathcal{F}$ est pleinement fidèle. Il faut donc voir que pour $\mathcal{F}$ et $\mathcal{G}$ quasi-cohérent sur S, si $\phi' : f^\star\mathcal{F} \to f^\star\mathcal{G}$ est un morphisme compatible avec les données canoniques de recollement, alors $\phi' = f^\star\phi$ pour un unique morphisme $\phi : \mathcal{F} \to \mathcal{G}$, ce qui se traduit par l'exactitude de

$$\mathbf{Hom}_S(\mathcal{F},\mathcal{G}) \to \mathbf{Hom}_{S'}(f^\star\mathcal{F}, f^\star\mathcal{G}) \rightrightarrows \mathbf{Hom}_{S"}(g^\star\mathcal{F}, g^\star\mathcal{G})$$

où $S" = S' \times_S S' = \mathbf{Spec}B \otimes_A B$ et $g : S" \to S$ est le morphisme structural. Posant $\mathcal{F} = \widetilde{M}$, $\mathcal{G} = \widetilde{N}$, il faut donc montrer l'exactitude de

$$\mathbf{Hom}_A(N, M) \to \mathbf{Hom}_B(N \otimes_A B, M \otimes_A B) \rightrightarrows \mathbf{Hom}_{B\otimes_A B}(N \otimes_A B \otimes_A B, M \otimes_A B \otimes_A B)$$

Il suffit pour cela de montrer l'exactitude, pour tout A-module M, de

$$M \to M \otimes_A B \rightrightarrows M \otimes_A B \otimes_A B.$$

Puisque $A \to B$ est fidèlement plat, il suffit de vérifier l'exactitude de

$$(M \otimes_A B) \to (M \otimes_A B) \otimes_A B \rightrightarrows (M \otimes_A B \otimes_A B) \otimes_A B.$$

Posons $\mathcal{A} = B$, $\mathcal{B} = B \otimes_A B$ vu comme $\mathcal{A}$-algèbre par $b \mapsto 1 \otimes b$, et $\mathcal{M} = M \otimes_A B$ vu comme $\mathcal{A}$-module par $b \cdot m = m \otimes b$. Le diagramme ci-dessus est alors

$$\mathcal{M} \to \mathcal{M} \otimes_{\mathcal{A}} \mathcal{B} \rightrightarrows \mathcal{M} \otimes_{\mathcal{A}} \mathcal{B} \otimes_{\mathcal{A}} \mathcal{B}$$

qui est donc du même type que précédemment. On a pourtant avancé, puisqu'on sait maintenant que $\mathcal{A} \to \mathcal{B}$ admet une *section*, à savoir le produit $\mathcal{B} = B \otimes_A B \to B = \mathcal{A}$ (qui correspond bien sur à la diagonale $\Delta : S' \to S' \times_S S'$ du diagramme de départ). Notant $\mathcal{I}$ le noyau de cette section, notre diagramme est maintenant

$$\mathcal{M} \to \mathcal{M} \oplus \mathcal{M} \otimes_{\mathcal{A}} \mathcal{I} \rightrightarrows \mathcal{M} \oplus \mathcal{M} \otimes_{\mathcal{A}} \mathcal{I} \oplus \mathcal{M} \otimes_{\mathcal{A}} \mathcal{I} \oplus \mathcal{M} \otimes_{\mathcal{A}} \mathcal{I}^{\otimes 2}$$

où les flèches sont $m \mapsto (m, 0)$ et $(m_1, m_2 \otimes i) \mapsto (m_1, m_2 \otimes i, 0, 0)$ ou $(m_1, 0, m_2 \otimes i, 0)$: c'est trivialement exact.

Exercise 15.3. Formaliser l'argument final ci-dessus en montrant que si $f : S' \to S$ admet une section $e : S \to S'$, alors $X' \mapsto e^\star X'$ est un quasi-inverse de $X \mapsto f^\star X$, qui est donc une équivalence de catégorie (entre "objets sur X" et "objets sur X' munis d'une donnée de descente relative à $S' \to S$")!

Montrons ensuite que $\mathcal{F} \mapsto f^\star\mathcal{F}$ est essentiellement surjectif. Il faut donc voir que si M est un B-module muni d'une donnée de descente $\phi : M \otimes_{B,p_1} (B \otimes_A B) \simeq M \otimes_{B,p_2} (B \otimes_A B)$, i.e. d'un isomorphisme $B \otimes_A B$-linéaire ϕ entre $M \otimes_A B$ et $B \otimes_A M$ qui vérifie une certaine condition de cocycle, alors $M \simeq N \otimes_A B$ pour un A-module N. Vu le calcul précédent, il est clair qu'il faut poser

$$N = \ker\left((\phi \circ \iota_1, \iota_2) : M \rightrightarrows B \otimes_A M\right)$$

où $\iota_1 : M \to M \otimes_A B$ et $\iota_2 : M \to B \otimes_A M$ sont les morphismes évidents. Il faut vérifier que l'application canonique $N \otimes_A B \to M$ est un isomorphisme de B-modules (ce morphisme étant compatible avec les données de descente par construction même de N) . Il suffit à nouveau de le vérifier après le changement de base fidèlement plat $A \to B$, i.e. on peut supposer que $A \to B$ admet une section. Toute donnée de descente étant alors effective, on peut donc aussi supposer que M est déjà de la forme $M = N' \otimes_A B$, et que ϕ est l'identité de $N' \otimes_A B \otimes_A B$. Alors

$$N = \ker\left((\iota_1, \iota_2) : N' \otimes_A B \rightrightarrows N' \otimes_A B \otimes_A B\right) = N'$$

donc $M = N \otimes_A B$!

On a donc montré le (1) de la proposition. On en déduit le (2) en utilisant (l'anti)-équivalence de catégorie $\mathcal{A} \to \mathbf{Spec}\mathcal{A}$ entre les faisceaux quasi-cohérents de $\mathcal{O}_S$-algèbres et les S-schémas affines (et bien sûr, idem sur S'). Le (4) et le (5) en résultent assez facilement. Pour le (3), on note que X' est quasi-affine sur S' ssi $X' \to X'_{aff} = \mathbf{Spec} f_\star \mathcal{O}_{X'}$ est une immersion ouverte quasi-compacte : une donnée de descente sur X' induit une donnée de descente sur X'_{aff}, qui descend donc en un schéma affine X_{aff} sur S d'après (2). Le morphisme $q : X'_{aff} \to X_{aff}$ vérifie $q^{-1}q(X') = X'$ (cela résulte formellement de la compatibilité des données de recollement sur X' et X'_{aff}), et $q(X')$ est ouvert puisque $q : X'_{aff} \to X_{aff}$ est fidèlement plat. Le (6) résulte de (3) comme le (5) de (2). $\square$

Remark 15.4. La forme la plus utilisée du (6) est la suivante : supposons toujours que $S' \to S$ est fidèlement plat et quasi-compact. On considère les paires $(X, \mathcal{L})$ formées d'un S-schéma quasi-compact et d'un faisceau inversible S-ample $\mathcal{L}$ sur X. Alors $(X, \mathcal{L}) \mapsto (f^\star X, f^\star \mathcal{L})$ est une équivalence de catégorie. Partant d'une paire $(X', \mathcal{L}')$ munie d'une donnée de descente, l'idée est *grosso modo* d'utiliser la donnée de descente sur $\mathcal{L}'$ pour découper dans X' des ouverts quasi-affines stables par la donnée de descente sur X'.

Références

[1] A. Grothendieck et J. Dieudonné, *Eléments de géométrie algébrique.* Publications Mathématiques de l'IHES n°**4**, **8**, **11**, **17**, **20**, **24**, **28** et **32**.

[2] A. Grothendieck et Coll. Séminaires de géométrie algébrique.

[3] A. Altman et S. Kleiman, *Compactifying the Picard Scheme.* Adv. Math **35** (1980).

[4] S. Bosh, W. Lutkebohmert, M. Raynaud, *Néron Models.* Ergebenisse der Mathematik und ihrer Grenzgebiete, **3**. Folge, Band **21**.

[5] A. Grothendieck, *Techniques de descentes et théorèmes d'existence en géométrie algébrique. I, II, III, IV, V et VI.* (Séminaire Bourbaki).

[6] R. Hartshorne, *Algebraic Geometry.* GTM **52**.

[7] Haruzo Hida, *p-adic Automorphic Forms on Shimura Varieties.* Springer Monographs in Mathematics.

[8] D. Mumford, *Abelian Varieties.*

[9] D. Mumford, *Lectures on curves on an algebraic surface.* Annals of Math. Studies **59** (1966)

[10] D. Mumford, *Geometric Invariant Theory.* Ergebnisse der Mathematik **34** (1965)

STRUCTURES

Dans cette seconde partie du cours, nous allons envisager diverses structures supplémentaires que l'on peut rajouter à nos problèmes de modules. Cela aboutira à la définition des problèmes de modules de type **PEL.**

Première partie 1. Endomorphismes

1. Endomorphismes

Soit $\mathcal{O}$ une $\mathbf{Z}$-algèbre qui est un $\mathcal{O}$-module libre de rang fini. Une action de $\mathcal{O}$ sur un S-schéma abélien A est un morphisme d'anneau $\iota : \mathcal{O} \to \mathrm{End}_S(A)$. On dit aussi que A/S est un $\mathcal{O}$-schéma abélien. La proposition suivante nous permettra d'ajouter de telles structures sur nos problèmes de modules.

Proposition 1.1. *Soit A/S un schéma abélien. Le foncteur $\mathcal{F} : (\mathbf{Sch}/S)^0 \to \mathbf{Ens}$ qui à un S-schéma T associe $\mathrm{Hom}_{Ann}(\mathcal{O}, \mathrm{End}_T(A_T))$ est représentable.*

Démonstration. Soient $e_1, \cdots, e_r$ une $\mathbf{Z}$-base de $\mathcal{O}$, $e_ie_j = \sum \alpha_{ijk}e_k$ la table de multiplication de $\mathcal{O}$, S_0 le schéma qui représente $T \mapsto \mathrm{End}_T(A_T)$, $S_1 = S_0^r$ le schéma qui représente $T \mapsto \mathrm{Hom}_{Gr}(\mathcal{O}, \mathrm{End}_T(A_T))$, $\iota_u : \mathcal{O} \to \mathrm{End}_{S_1}(A_{S_1})$ le morphisme de groupe universel, $E_{i,j} = \iota_u(e_ie_j)$ et $F_{i,j} = \sum_k \alpha_{ijk}\iota_u(e_k)$. Ce sont des endomorphismes $A_{S_1} \to A_{S_1}$. Soit S_2 le sous-schéma ouvert et fermé de S_1 où $E_{i,j} = F_{i,j}$ pour tout i, j. Alors S_2 représente $T \mapsto \mathrm{Hom}_{Ann}(\mathcal{O}, \mathrm{End}_T(A_T))$. □

Remark 1.2. Si A/S est un $\mathcal{O}$-schéma abélien projectif, A^t est naturellement muni d'une action de l'anneau opposé $\mathcal{O}^{opp}$. Si $\star$ est une involution de $\mathcal{O}$, on peut donc à nouveau considérer A^t/S comme un $\mathcal{O}$-schéma abélien. Dans ce contexte, on dira d'un morphisme $\lambda : A \to A^t$ qu'il est $(\mathcal{O}, \star)$-linéaire s'il est compatible avec ces structures, i.e. $\lambda(ox) = o^{\star t}\lambda(x)$. Dans les problèmes de modules où apparaissent à la fois des $\mathcal{O}$-structures et des polarisations, on demandera toujours que la polarisation soit ainsi $(\mathcal{O}, \star)$-linéaire.

Deuxième partie 2. Modules de Tate

Si A est une variété abélienne de dimension g sur un corps de caractéristique $\neq p$, son module de Tate $T_pA = \varprojlim A[p^n]$ est un $\mathbf{Z}_p$-module libre de rang $2g$ muni d'une action de Gal_k. Cet énoncé n'est pas très précis : il faut fixer d'abord une clotûre séparable k^{sep}/k pour définir $T_p(A, k^{sep}) = \varprojlim A[p^n](k^{sep})$ et l'action de $\mathrm{Gal}(k^{sep}/k)$ sur $T_p(A, k^{sep})$: la classe d'isomorphisme du couple $(T_p(A, k^{sep}), \mathrm{Gal}(k^{sep}/k))$ ne dépend pas du choix de la clotûre algébrique.

Si maintenant A est un schéma abélien sur une base S plus générale, on peut de même choisir un point géométrique s de S et former $T_p(A, s) = \varprojlim A[p^n](s)$: si $p \neq \mathbf{car}(k(s))$, c'est encore un $\mathbf{Z}_p$-module libre de rang $2g$, et l'on peut faire agir dessus le groupe des automorphismes de $k(s)/k(s_0)$, où $s_0 \in S$ est le point base de s. Mais il est évident que ce groupe d'automorphismes dépend fortement du choix de s. Par exemple, supposons que S est le spectre d'un anneau de valuation discrète $\mathcal{O}$ de corps des fractions K et de corps résiduel k (avec $\mathbf{car}k \neq p$). Le groupe d'automorphismes ci-dessus peut alors être Gal_K ou Gal_k, selon que l'on prend $s = K^{sep}$ ou $s = k^{sep}$ au-dessus respectivement du point générique et du point fermé de $S = \mathrm{Spec}\mathcal{O}$. Cependant, on sait dans cette situation que la réduction définit un *isomorphisme* $T_p(A, K^{sep}) \to T_p(A, k^{sep})$ qui est compatible avec le morphisme de groupe $\mathrm{Gal}(K^{sep}/K) \to \mathrm{Gal}(k^{sep}/k)$ induit par l'isomorphisme $\mathrm{Gal}(K^{nr}/K) \simeq \mathrm{Gal}(k^{sep}/k)$, où K^{nr} est l'extension maximale non-ramifiée de K dans K^{sep}. Ceci suggère que le bon couple serait plutot $(T_p(A, K^{nr}), \mathrm{Gal}(K^{nr}/K))$.

Et en effet, sur n'importe quelle base S connexe où p est inversible, il existe un *groupe fondamental* $\pi(S, s)$ qui agit sur T_pA_s, tel que la classe d'isomorphisme de la paire $(T_pA_s, \pi(S, s))$ est bien définie. Dans les deux exemples précédents, le groupe $\pi(S, s)$ est exactement celui que l'on veut, à savoir $\mathrm{Gal}(k^{sep}/k)$ si $S = \mathrm{Spec}k$, ou $\mathrm{Gal}(K^{nr}/K)$ si $S = \mathrm{Spec}\mathcal{O}$.

2. Le groupe fondamental

Definition 2.1. Soit S un schéma connexe, $\mathbf{REt}/S$ la catégorie des revêtements étales de S, s un point géométrique de S, et $\mathcal{F}(s) : (\mathbf{REt}/S) \to \mathbf{Ens}$ le foncteur (covariant, pour une fois) qui à E/S associe $E(s)$. Le *groupe fondamental* de S de point base s est le groupe des automorphismes de ce foncteur : $\pi(S, s) = \mathrm{Aut}\mathcal{F}(s)$.

Un élément $\sigma \in \pi(S, s)$ est donc donné par une collection $(\sigma_E)_E$ ou pour chaque revêtement étale $E \to S$, σ_E est un automorphisme de l'ensemble fini $E(s)$, ces automorphismes étant compatibles avec les flèches de $\mathbf{REt}/S$. En particulier : pour tout $E \in \mathbf{REt}/S$, l'application $\sigma \mapsto \sigma_E$ munit $E(s)$ d'une structure de $\pi(S, s)$ ensemble. On obtient ainsi une factorisation $\mathcal{F}(s) = \mathcal{O} \circ \mathcal{G}(s)$ où

$$\mathcal{G}(s) : (\mathbf{REt}/S) \to \pi(S, s) - \mathbf{EnsFini}$$

et $\mathcal{O}$ est le foncteur d'oubli de la $\pi(S, s)$-structure.

Proposition 2.2. *C'est une équivalence de catégorie.*

Pour construire le quasi-inverse, nous avons besoin de la notion d'objet Galoisien :

Lemma 2.3. *Soit E/S un revêtement étale* connexe *et $G = \mathrm{Aut}_S E$. On dit que E/S est Galoisien ssi les conditions équivalentes qui suivent sont vérifiées.*

1. $|G| = [E : S]$
2. $|G| = |E(s)|$
3. *L'application $E \times G \to E \times_S E$ définie par $(e, g) \mapsto (e, ge)$ est un isomorphisme.*
4. *L'application $E(s) \times G \to E(s) \times E(s)$ définie par $(e, g) \mapsto (e, ge)$ est un isomorphisme.*
5. *L'action de G sur $E(s)$ est simplement transitive.*

Démonstration. On a (1) $\iff$ (2) puisque $[E : S] = |E(s)|$, et (3) $\Rightarrow$ (4) $\Rightarrow$ (2) est évident. Pour (1) $\Rightarrow$ (3), on note que le morphisme est (a) toujours étale, et (b) toujours géométriquement injectif, car si $(e, ge) = (e', g'e')$, alors $e = e'$ et $ge = g'e$, donc le schéma des coïncidences de (g, g') sur E est non-vide (il contient le point géométrique e). Puisque ce schéma est aussi ouvert et fermé dans E (comme la diagonale dans $E \times_S E$ dont il est le pull-back par (g, g'), cf. [1, IV, 17.4.2]), c'est donc E tout entier, puisque E est connexe, donc $g = g'$. On conclut : un morphisme étale injectif est une immersion ouverte [1, IV, 17.9.1]. Donc par comparaison des rangs sur S, c'est un isomorphisme. □

Lemma 2.4. *Tout revêtement étale connexe est dominé par un revêtement étale connexe Galoisien.*

Démonstration. Soit $E \to S$, $F = E(s)$, $D = E^F$, donc $D(s) = \mathcal{F}(F,F)$. Soit C la composante connexe de D qui contient $Id_F \in D(s)$. C'est inclus dans le complémentaire dans D de l'ensemble $\{(d_f)_{f\in F} | \exists f_1 \neq f_2 | d_{f_1} = d_{f_2}\}$ puisque ce complémentaire, ouvert et fermé, est une réunion de composantes connexes et contient $\mathbf{Id}_{E(s)}$. Tout élément σ de $C(s)$ induit donc une permutation de $F = E(s)$, qui à son tour induit un automorphisme σ de $D = E^F$, lequel envoie $Id_F \in C(s) \subset D(s)$ sur $\sigma \in C(s) \subset D(s)$, donc C sur C. On obtient ainsi une application $C(s) \to \mathrm{Aut}_S C$ qui est une section de l'application $\mathrm{Aut}_S C \to C(s)$ qui à σ associe $\sigma \cdot Id_F$. Puisque cette dernière est toujours injective, on en conclut bien que C/S est Galoisien. Il reste à choisir $f \in F = E(s)$ pour projeter C sur E via la "f-ieme projection" $E^F \to E$. □

Si $E \to S$ est Galoisien, deux groupes agissent sur $E(s)$: $\pi(S,s)$ via $\sigma \mapsto \sigma_E$ et $\mathrm{Gal}(E/S)$, ce dernier simplement transitivement. Par définition même de $\pi(S,s)$, ces deux actions commutent. Le choix d'un point de $E(s)$ induit donc un morphisme $\pi(S,s) \to \mathrm{Gal}(E/S)^o$. On déduit du lemme qu'il existe une famille filtrante de revêtements Galoisiens connexes qui est cofinale dans la catégorie des revêtements étales connexes (cela pose toutefois des problèmes d'univers qu'il faut résoudre). Le choix de points géométriques compatibles dans cette famille fournit alors une identification de $\pi(S,s)$ avec la limite projective des $\mathrm{Gal}(E/S)^o$. Il n'est alors pas très dur de construire le foncteur inverse ci-dessus : au $\pi(S,s)$ ensemble transitif $\mathrm{Gal}(E/S)^o$, on va bien sûr associer le revêtement Galoisien connexe E de S.

Example 2.5. Pour $S = \mathrm{Spec} k$, les revêtements étales connexes Galoisiens de S sont les $E = \mathrm{Spec} k'$, pour k'/k extension Galoisienne finie, et on obtient un système cofinal de tels revêtements en se restreignant aux k' dans une clôture algébrique $\overline{k}$ fixée de k. Prenant $s = \mathrm{Spec}\overline{k}$, on trouve donc

$$\pi(S,s) = \varprojlim \mathrm{Aut}(E/S)^o = \varprojlim \mathrm{Aut}(k'/k) = \mathrm{Gal}(k^{sep}/k)$$

où k^{sep} est la clôture séparable de k dans $\overline{k}$. De même, pour $S = \mathrm{Spec}\mathcal{O}$ le spectre d'un anneau de valuation discrète, ou même d'un anneau de Dedekind, les revêtements étales de S sont les $E = \mathrm{Spec}\mathcal{O}'$ pour $\mathcal{O}'$ l'anneau des entiers d'une extension Galoisienne partout non-ramifiée K' du corps des fractions $K = \mathrm{Frac}\mathcal{O}$. Prenant $s = \mathrm{Spec}\overline{K}$, on trouve donc encore $\pi(S,s) = \mathrm{Gal}(K^{nr}/K)$, où K^{nr} est l'extension non-ramifiée maximale de K dans $\overline{K}$. En particulier, $\pi(\mathrm{Spec}\mathbf{Z}, s) = \{1\}$!

3. Modules de Tate

3.1. **Définition.** Soit A/S un schéma abélien, s un point géometrique de S.

Lemma 3.1. *Si N est inversible sur S, la multiplication par N sur A est un morphisme étale, donc $A[N]$ est un S-schéma étale et $A[N](s)$ un $\pi(S,s)$-module.*

Démonstration. On peut le vérifier sur les fibres géometriques, où on sait déjà que la multiplication par N est un morphisme fini et plat de degré N^{2g}. On applique le critère pour formellement étale : il faut voir que si $x \in A(k[\epsilon])$ vérifie $\overline{x} =$

$N\overline{y} \in A(k)$, il existe un unique $y \in A(k[\epsilon])$ tel que $Nz = x$ et y se réduit sur $\overline{y}$. Commençons par relever arbitrairement $\overline{y}$ en y (puisque A est lisse), et translatons tout par y : cela nous ramène au cas où $\overline{x} = 0$, $\overline{y} = 0$. Il faut alors voir que : pour tout $x \in \mathbf{Lie}A = \ker(A(k[\epsilon]) \to A(k))$, il existe un unique $y \in \mathbf{Lie}A$ tel que $Ny = x$. Mais $\mathbf{Lie}A$ est un k espace vectoriel et N est inversible dans k : cqfd. $\square$

Si p est inversible sur S, on pose

$$\begin{aligned} T_p(A,s) &= \lim A[p^n](s) \\ V_p(A,s) &= T_p(A,s) \otimes \mathbf{Q} \end{aligned}$$

Ce sont donc des $\mathbf{Z}_p$ (resp. $\mathbf{Q}_p$)-modules libres de rang $2g$ munis d'actions continues de $\pi(S,s)$. Si S est un $\mathbf{Q}$-schéma, on pose

$$\begin{aligned} T_f(A,s) &= \lim A[N](s) \\ V_f(A,s) &= T_f(A,s) \otimes \mathbf{Q} \end{aligned}$$

Ce sont donc des $\widehat{\mathbf{Z}}$ (resp. $\mathbf{A}_f$)-modules libres de rang $2g$ munis d'actions continues de $\pi(S,s)$. Si S est un $\mathbf{Z}_{(p)}$-schéma, on pose

$$\begin{aligned} T_f^p(A,s) &= \lim_{(N,p)=1} A[N](s) \\ V_f^p(A,s) &= T_f^p(A,s) \otimes \mathbf{Q} \end{aligned}$$

Ce sont donc des $\widehat{\mathbf{Z}}^p$ (resp. $\mathbf{A}_f^p$)-modules libres de rang $2g$ munis d'actions continues de $\pi(S,s)$.

3.2. **Dualité.** Pour tout S-schéma en groupe G commutatif, fini et plat sur S, on note

$$\mathbf{D}(G) = \underline{\mathrm{Hom}}(G, \mathbf{G}_m).$$

Proposition 3.2. *C'est un S-schéma en groupe commutatif, fini et plat sur S, et l'application canonique $G \to \mathbf{D}(\mathbf{D}(G))$ définie par $g \mapsto (f \mapsto f(g))$ est un isomorphisme de S-schéma en groupes qui préserve le rang.*

Démonstration. Le problème est local sur S, que l'on peut donc supposer affine, disons $S = \mathrm{Spec}A$, et tel que $G \to S$ soit de rang constant, disons n, et même libre de rang n, donc $G = \mathrm{Spec}B$ pour une A-algèbre B qui est un A-module libre de rang n. La structure de A-algèbre commutative sur B se traduit par l'existence de morphismes de A-modules

$$e : A \to B \quad \text{et} \quad \mu : B \otimes_A B \to B$$

vérifiant diverses propriétés, tandis que la structure de S-schéma en groupe commutatif sur G se traduit par l'existence de morphismes de A-modules

$$e^\star : B \to A \quad \text{et} \quad \mu^\star : B \to B \otimes_A B$$

vérifiant des propriétés "opposées". Soit $B' = \mathrm{Hom}_A(B, A)$ le A-dual du A-module B. Les structures ci-dessus induisent donc des morphismes de A-modules

$$e' : B' \to A \quad \text{et} \quad \mu' : B' \to B' \otimes_A B'$$

ainsi que

$$e^{\star\prime} : A \to B' \quad \text{et} \quad \mu^{\star\prime} : B' \otimes_A B' \to B'$$

le tout vérifiant des propriétés duales. On vérifie que le couple $(e^{\star\prime}, \mu^{\star\prime})$ munit B' d'une structure de A-algèbre commutative, et que (e', μ') munit le S-schéma

$\mathbf{D}'(G) = \mathrm{Spec}B'$ d'une structure de S-schéma en groupe. Il est clair que $\mathbf{D}' \circ \mathbf{D}'(G) \simeq G$, et il reste donc à voir que $\mathbf{D}' = \mathbf{D}$. Or un morphisme de S-schéma en groupe $\alpha : G \to \mathbf{G}_{m,S}$ n'est autre qu'un morphisme $\alpha : G \to \mathbf{A}^1_S$ de S-schéma tel que (1) $\alpha(e_G) = 1_G$ et (2) $\alpha(g_1 g_2) = \alpha(g_1)\alpha(g_2)$. Les morphismes de S-schémas $\alpha : G \to \mathbf{A}^1_S$ correspondent aux morphismes de A-algèbres $\alpha^\star : A[T] \to B$, i.e. aux éléments $b = \alpha^\star(T)$ de B, et les conditions (1) et (2) se traduisent respectivement par (1′) $e^\star_G(b) = 1$ dans A et (2′) $\mu^\star_G(b) = b \otimes b$ dans $B \otimes_A B$. On veut donc

$$\{b \in B : e^\star_G(b) = 1 \text{ et } \mu^\star_G(b) = b \otimes b\} = \mathbf{D}'(G)(S) = \mathrm{Hom}_{A-alg}(B', A).$$

Mais $B \simeq \mathrm{Hom}_{A-mod}(B', A)$ par $b \mapsto \delta_b = (f \mapsto f(b))$, et $\delta_b : B' \to A$ est un morphisme de A-algèbres si et seulement si (1′) $\delta_b \circ e^{\star\prime}_G = Id : A \to A$, i.e. $e^\star_G(b) = 1$, et (2′) $\delta_b \circ \mu^{\star\prime}_G(f_1 \otimes f_2) = \delta_b(f_1)\delta_b(f_2)$ pour tout $f_1, f_2 \in B'$, i.e.

$$(f_1 \otimes f_2)(\mu^\star_G(b)) = f_1(b) f_2(b)$$

pour tout $f_1, f_2 \in B'$, condition qui est clairement équivalente à $\mu^\star_G(b) = b \otimes b$, comme on voit en choisissant une A-base de B. □

Remark 3.3. Pour plus d'information sur cette dualité, on peut consulter l'excellent article de Tate [4] dans le livre sur Fermat.

Proposition 3.4. *Soit $\alpha : A \to B$ une isogénie de S-schéma abéliens (projectifs) et $\alpha^t : B^t \to A^t$ l'isogénie duale. Il existe un accouplement $e_\alpha : \ker\alpha \times_S \ker\alpha^t \to \mathbf{G}_{m,S}$ qui induit des isomorphismes*

$$\ker\alpha^t \simeq \mathbf{D}(\ker\alpha) \quad et \quad \ker\alpha \simeq \mathbf{D}(\ker\alpha^t).$$

Démonstration. Pour tout S-schéma T,

$$\begin{array}{rcl} (\ker\alpha^t)(T) & = & \ker\alpha^\star : \mathbf{Pic}^0_{B/S}(T) \to \mathbf{Pic}^0_{A/S}(T) \\ & = & \ker\alpha^\star : \mathbf{Pic}_{B/S}(T) \to \mathbf{Pic}_{A/S}(T) \\ & \simeq & \ker\alpha^\star : \mathbf{Pic}(B \times_S T) \to \mathbf{Pic}(A \times_S T) \end{array}$$

Cela résulte respectivement des diagrammes commutatifs

$$\begin{array}{ccccccc} 0 & \to & \mathbf{Pic}^0_{B/S}(T) & \to & \mathbf{Pic}_{B/S}(T) & \to & \mathrm{Hom}_T(B_T, B^t_T) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \to & \mathbf{Pic}^0_{A/S}(T) & \to & \mathbf{Pic}_{A/S}(T) & \to & \mathrm{Hom}_T(A_T, A^t_T) \end{array}$$

où la dernière flèche verticale est $f \mapsto \alpha^t \circ f \circ \alpha$ (qui est injective : il suffit par rigidité de le vérifier sur les points géométriques de T, où $\alpha^t \circ f \circ \alpha = 0$ implique $f \circ \alpha = 0$ puisque A est connexe et $\ker\alpha^t$ fini, qui implique à son tour $f = 0$ puisque α est surjective), et

$$\begin{array}{ccccccccc} 0 & \to & \mathbf{Pic}(T) & \to & \mathbf{Pic}(B \times_S T) & \to & \mathbf{Pic}_{B/S}(T) & \to & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \to & \mathbf{Pic}(T) & \to & \mathbf{Pic}(A \times_S T) & \to & \mathbf{Pic}_{A/S}(T) & \to & 0 \end{array}$$

On doit donc déterminer le noyau de $\alpha^\star : \mathbf{Pic}(B) \to \mathbf{Pic}(A)$, i.e. l'ensemble des classes d'isomorphismes de faisceau inversible $\mathcal{L}$ sur B tels que $\alpha^\star\mathcal{L} \simeq \mathcal{O}_A$. C'est un problème de descente (de $\mathcal{O}_A$ le long de $\alpha : A \to B$), et le noyau cherché est donc en bijection avec l'ensemble des données de descente sur $\mathcal{O}_A$ relativement à $\alpha : A \to B$, lesquelles correspondent à leur tour (puisque $A \times_B A \simeq \ker\alpha \times_S A$)

aux “actions linéaires de $\ker\alpha$ sur $\mathcal{O}_A$ au-dessus de l'action par translation de $\ker\alpha$ sur A”, i.e. aux actions linéaires

$$\mu_2 : \ker\alpha \times_S (A \times_S \mathbf{A}^1_S) \to (A \times_S \mathbf{A}^1_S)$$

au-dessus de $m : \ker\alpha \times_S A \to A$. Un tel morphisme μ s'écrit donc

$$\mu_2(k, a, x) = (k + a, \mu_1(k, a) \cdot x)$$

pour $k \in \ker\alpha$, $a \in A$ et $x \in \mathbf{A}^1_S$, avec $\mu_1 : \ker\alpha \times_S A \to \mathbf{G}_{m,S}$ qui se factorise nécessairement par $\mu : \ker\alpha \to \mathbf{G}_{m,S}$ puisque $f_{\ker\alpha\star}\mathcal{O}_{\ker\alpha\times_S A} = \mathcal{O}_{\ker\alpha}$. Donc

$$(\ker\alpha^t)(S) = \ker(\alpha^\star : \mathbf{Pic}B \to \mathbf{Pic}A) = \mathrm{Hom}_{S-Gr}(\ker\alpha, \mathbf{G}_{m,S}) = \mathbf{D}(\ker\alpha)(S)$$

et on conclut en remplaçant S par T. □

Exercise 3.5. Montrer que cette définition coïncide avec celle du cours de M. Hindry lorsque S est le spectre d'un corps algébriquement clos. Cf. [3, §20].

Remark 3.6. On peut démontrer que $A^t = \mathbf{Ext}^1(A, \mathbf{G}_{m,S})$ dans une catégorie de faisceau abélien convenable où $0 \to \ker\alpha \to A \to B \to 0$ est exacte. Appliquant $\mathbf{RHom}(\bullet, \mathbf{G}_m)$ à cette suite, on trouve

$$0 \to \mathbf{Hom}(B, \mathbf{G}_m) \to \mathbf{Hom}(A, \mathbf{G}_m) \to \mathbf{Hom}(\ker\alpha, \mathbf{G}_m) \to \mathbf{Ext}^1(B, \mathbf{G}_m) \to \mathbf{Ext}^1(A, \mathbf{G}_m)$$

Les deux premiers termes sont triviaux, et le reste donne

$$0 \to \mathbf{D}(\ker\alpha) \to B^t \to A^t$$

i.e. $\mathbf{D}(\ker\alpha) = \ker\alpha^t$.

En appliquant ceci à l'isogénie $[n] : A \to A$, dont l'isogénie duale $[n]^t$ est encore $[n] : A^t \to A^t$ (il suffit de le vérifier sur les points géométriques par rigidité, où l'on utilise $[n]^\star\mathcal{L} \simeq \mathcal{L}^{\otimes n}$ pour $\mathcal{L} \in \mathbf{Pic}^0_{A/S}$), on trouve *l'accouplement de Weil*

$$e^A_n : A[n] \times_S A^t[n] \to \mu_{n,S}.$$

Ces accouplements sont compatibles lorsque n varie. Si n est inversible dans S, les schémas ci-dessus sont des revêtement étales de S, et l'on obtient donc pour tout point géométrique s de S un accouplement parfait et $\pi(S, s)$-équivariant

$$e^A_n(s) : A[n](s) \times A^t[n](s) \to \mu_n(s).$$

Prenant $n = p^k$ avec p inversible dans S et faisant varier k, on obtient donc finalement un accouplement parfait de $\mathbf{Z}_p[\pi(S, s)]$-modules

$$\langle\bullet,\bullet\rangle^A_p : T_p(A, s) \times T_p(A^t, s) \to T_p(\mu, s).$$

Il résulte assez facilement des définitions que pour tout morphisme de S-schéma abélien $\alpha : A \to B$, le diagramme suivant est commutatif :

$$\begin{array}{cccccc} \langle\bullet,\bullet\rangle^A_p : & T_p(A,s) & \times & T_p(A^t,s) & \to & T_p(\mu,s) \\ & \alpha\downarrow & & \alpha^t\uparrow & & \| \\ \langle\bullet,\bullet\rangle^B_p : & T_p(B,s) & \times & T_p(B^t,s) & \to & T_p(\mu,s) \end{array} \tag{3.1}$$

Pour tout $\lambda : A \to A^t$, on obtient aussi un accouplement de $\mathbf{Z}_p[\pi(S, s)]$-modules

$$\langle\bullet,\bullet\rangle^\lambda_p : T_p(A, s) \times T_p(A, s) \to T_p(\mu, s) \qquad \langle x, y\rangle^\lambda_p = \langle x, T_p(\lambda, s)(y)\rangle^A_p$$

qui est encore parfait si λ est une isogénie et $p \nmid \deg\lambda$. Le cas intéressant est celui où on prend $\lambda = \Lambda(\mathcal{L})$ pour un faisceau inversible $\mathcal{L}$ sur A. On note alors

$\langle \bullet, \bullet \rangle_p^{\mathcal{L}} = \langle \bullet, \bullet \rangle_p^{\Lambda(\mathcal{L})}$. Si $\alpha : A \to B$ est un morphisme de S-schéma abélien et $\mathcal{L}$ un faisceau inversible sur B, le diagramme suivant est commutatif :

$$\begin{array}{rccccccc} & \langle \bullet, \bullet \rangle_p^{\alpha^\star \mathcal{L}} : & T_p(A,s) & \times & T_p(A,s) & \to & T_p(\mu, s) \\ (3.2) & & \downarrow & & \downarrow & & \| \\ & \langle \bullet, \bullet \rangle_p^{\mathcal{L}} : & T_p(B,s) & \times & T_p(B,s) & \to & T_p(\mu, s) \end{array}$$

En effet, on vérifie facilement que $\Lambda(\alpha^\star \mathcal{L}) : A \to A^t$ est $\alpha^t \circ \Lambda(\mathcal{L}) \circ \alpha$, donc

$$\langle \alpha(x), \alpha(y) \rangle_p^{\mathcal{L}} = \langle \alpha(x), \Lambda(\mathcal{L}) \circ \alpha(y) \rangle_p^{B} = \left\langle x, \alpha^t \circ \Lambda(\mathcal{L}) \circ \alpha(y) \right\rangle_p^{A} = \langle x, y \rangle_p^{\alpha^\star \mathcal{L}} .$$

Proposition 3.7. *Pour tout faisceau inversible $\mathcal{L}$ sur A, $\langle \bullet, \bullet \rangle_p^{\mathcal{L}}$ est anti-symétrique.*

Démonstration. On peut supposer $S = s$, et il suffit de montrer que

$$e_n^A(x, \Lambda(\mathcal{L})(x)) = 1$$

pour tout n et tout $x \in A[n]$. Si $\mathcal{L} \simeq \mathcal{O}(D)$ pour un diviseur D sur A, $\Lambda(\mathcal{L})(x) = \mathcal{T}_x^\star \mathcal{L} \otimes \mathcal{L}^{-1} \simeq \mathcal{O}_A(\mathcal{T}_x^{-1} D - D)$ et $[n]^\star \Lambda(\mathcal{L})(x) = \mathcal{O}_A([n]^\star \mathcal{T}_x^\star D - [n]^\star D) \simeq \mathcal{O}_A$. Choisissons $g \in K(A)$ tel que $\mathbf{div}(g) = [n]^\star \mathcal{T}_x^\star D - [n]^\star D$. Alors $e_n^A(x, \Lambda(\mathcal{L})(x)) = \mathcal{T}_x^\star g / g$, et il faut montrer que $T_x^\star g = g$. Posons $E = [n]^\star D$ et choisissons y tel que $ny = x$, de sorte que

$$\mathbf{div}(g) = [n]^\star \mathcal{T}_x^\star D - [n]^\star D = \mathcal{T}_y^\star [n]^\star D - [n]^\star D = \mathcal{T}_y^\star E - E$$

Puisque $nx = 0$, $\mathcal{T}_x^\star E = E$ donc

$$\mathbf{div}(\prod_{i=0}^{n-1} \mathcal{T}_{iy}^\star g) = \sum_{i=0}^{n-1} \mathcal{T}_{(i+1)y}^\star E - \mathcal{T}_{iy}^\star E = \mathcal{T}_x^\star E - E = 0$$

donc $h = \prod_{i=0}^{n-1} \mathcal{T}_{iy}^\star g$ est constant, et en particulier $1 = \mathcal{T}_y^\star h / h = \mathcal{T}_x^\star g / g$. □

Corollary 3.8. *Pour toute polarisation λ, $\langle \bullet, \bullet \rangle_p^{\lambda}$ est anti-symétrique.*

Le lemme suivant montre que l'on peut imposer la $(\mathcal{O}, \star)$-linéarité d'un morphisme $\lambda : A \to A^t$ par une condition au niveau des modules de Tate.

Lemma 3.9. *Soit $\mathcal{O}$ un anneau agissant sur A/S, $\star$ une involution de $\mathcal{O}$ et $\lambda : A \to A^t$. Alors λ est $(\mathcal{O}, \star)$-linéaire si et seulement si $\langle ox, y \rangle_p^{\lambda} = \langle x, o^\star y \rangle_p^{\lambda}$ pour tout $o \in \mathcal{O}$, $x, y \in T_p(A, s)$.*

Démonstration. On a $\langle ox, y \rangle_p^{\lambda} - \langle x, o^\star y \rangle_p^{\lambda} = \langle ox, \lambda y \rangle_p^{A} - \langle x, \lambda o^\star y \rangle_p^{A} = \langle x, (o^t \lambda - \lambda o^\star) y \rangle_p^{\lambda}$, donc

$$\begin{aligned} \forall x, y \in T_p(A,s) : \quad \langle ox, y \rangle_p^{\lambda} = \langle x, o^\star y \rangle_p^{\lambda} \quad &\iff \quad o^t \lambda = \lambda o^\star \text{ sur } T_p(A,s) \\ &\iff \quad o^t \lambda = \lambda o^\star \text{ dans } \mathrm{Hom}(A, A^t) \end{aligned}$$

CQFD. □

3.3. **Compléments.** Calculons l'accouplement $\langle \bullet, \bullet \rangle_p^{\mathcal{P}}$ sur $A \times_S A^t$, où $\mathcal{P}$ est le faisceau de Poincarré. Tout d'abord, appliquant (3.2) à $\alpha : A \to A \times_S A^t$ ou à $\alpha : A \to A \times_S A^t$, on trouve

$$\langle (x, 0), (y, 0) \rangle_p^{\mathcal{P}} = 0 = \left\langle (0, x^t), (0, y^t) \right\rangle_p^{\mathcal{P}}$$

pour tout $x, y \in T_p(A,s)$ et $x^t, y^t \in T_p(A^t, s)$, puisque $\alpha^\star\mathcal{P}$ est trivial dans les deux cas. D'autre part,

$$\Lambda(\mathcal{P}) : A \times_S A^t \to (A \times_S A^t)^t = A^t \times_S A$$

est l'isomorphisme $(a, a^t) \mapsto (a^t, a)$. Donc pour $x, y \in T_p(A,s)$ et $x^t, y^t \in T_p(A^t, s)$,

$$\begin{aligned}
\left\langle (x,x^t),(y,y^t)\right\rangle_p^{\mathcal{P}} &= \left\langle (x,0),(0,y^t)\right\rangle_p^{\mathcal{P}} - \left\langle (y,0),(0,x^t)\right\rangle_p^{\mathcal{P}} \\
&= \left\langle (x,0),(y^t,0)\right\rangle_p^{A\times_S A^t} - \left\langle (y,0),(x^t,0)\right\rangle_p^{A\times_S A^t} \\
&= \left\langle x,y^t\right\rangle_p^{A} - \left\langle y,x^t\right\rangle_p^{A}
\end{aligned}$$

où la dernière égalité résulte de (3.1). Appliquons alors (3.2) à la transposition $\tau(a^t, a) = (a, a^t)$, en notant que $\tau^\star\mathcal{P}$ est le fibré de Poincarré sur $A^t \times_S A$:

$$\left\langle (x,x^t),(y,y^t)\right\rangle_p^{\mathcal{P}} = \left\langle (x^t,x),(y^t,y)\right\rangle_p^{\tau^\star\mathcal{P}} = \left\langle x^t,y\right\rangle_p^{A^t} - \left\langle y^t,x\right\rangle_p^{A^t},$$

d'où l'on déduit en prenant $y = 0$ et $x^t = 0$ que

$$\left\langle x,y^t\right\rangle_p^{A} + \left\langle y^t,x\right\rangle_p^{A^t} = 0.$$

Si $\mathcal{L}$ est un faisceau inversible sur A, $\lambda = \Lambda(\mathcal{L}) : A \to A^t$ et $x, y \in T_p(A,s)$,

$$\left\langle \lambda^t x, y\right\rangle_p^{A^t} = \langle x, \lambda y\rangle_p^{A} = \langle x, y\rangle_p^{\mathcal{L}} = -\langle y, x\rangle_p^{\mathcal{L}} = -\langle y, \lambda x\rangle_p^{A} = \langle \lambda x, y\rangle_p^{A^t}.$$

Puisque $\langle \bullet, \bullet\rangle_p^{A^t}$ est parfait, $\lambda^t = \lambda$ sur $T_p(A,s)$ donc $\lambda^t = \lambda$ sur A_s, et $\lambda^t = \lambda$ sur A par rigidité. On a ainsi démontré que le morphisme $\Lambda : \mathbf{NS}_{A/S} \to \underline{\mathbf{Hom}}_{Gr}(A, A^t)$ atterrit dans la partie symétrique.

4. Structures de niveaux

4.1. **Définition.** Soit $\mathcal{O}$ une $\mathbf{Z}$-algèbre, $\star$ une involution de $\mathcal{O}$, p un nombre premier inversible dans S, Λ_p un $\mathcal{O}_p = \mathcal{O} \otimes \mathbf{Z}_p$-module qui est un $\mathbf{Z}_p$-module libre de rang $2g$, $\psi_p : \Lambda_p \times \Lambda_p \to \mathbf{Z}_p$ une forme symplectique non-dégénérée telle que $\psi_p(ox, y) = \psi_p(x, o^\star y)$ pour tout $o \in \mathcal{O}_p$ et $x, y \in \Lambda_p$, et K un sous-groupe du groupe des similitudes $\mathcal{O}_p$-linéaires de (Λ_p, ψ_p).

Definition 4.1. Soit S un schéma connexe où p est inversible et (A, λ, ι) un S-schéma abélien (projectif) polarisé muni d'une action de $\mathcal{O}$. Une *structure de niveau* K sur (A, λ, ι) est la donnée, pour un point géométrique s de S, d'une K-orbite $[\kappa] = \kappa K$ *d'isomorphismes* de $\mathcal{O}_p$-modules $\kappa : \Lambda_p \xrightarrow{\simeq} T_p(A,s)$ tels que

(I): il existe un isomorphisme $T_p(\mu, s) \simeq \mathbf{Z}_p$ qui fait commuter le diagramme

$$\begin{array}{ccccccc}
\psi_p : & \Lambda_p & \times & \Lambda_p & \to & \mathbf{Z}_p \\
& \downarrow & & \downarrow & & \downarrow \\
\langle \bullet, \bullet\rangle_p^{\lambda} : & T_p(A,s) & \times & T_p(A,s) & \to & T_p(\mu, s)
\end{array}$$

(II): pour tout $\sigma \in \pi(S, s)$, il existe $k(\sigma) \in K$ tel que $\sigma \circ \kappa = \kappa \circ k(\sigma)$.

Remark 4.2. Si la propriété (I) (resp. (II)) est vérifiée pour un isomorphisme $\kappa : \Lambda_p \xrightarrow{\simeq} T_p(A,s)$, elle l'est aussi pour tout $\kappa \circ k$ avec $k \in K$. Dans (II), l'élément $k(\sigma) = \kappa^{-1} \circ \sigma \circ \kappa$ est unique, et l'application $\sigma \to k(\sigma)$ est un morphisme de groupes $\pi(S, s) \to K$. Modulo les automorphismes intérieurs de K, ce morphisme de groupes ne dépend que de $[\kappa] = \kappa K$.

Remark 4.3. Soit s' un autre point géométrique de S. On sait alors qu'il existe des isomorphismes $\theta : \pi(S,s) \to \pi(S,s')$ et $\Theta : T_p(A,s) \to T_p(A,s')$ tels que

$$\Theta(\sigma t) = \theta(\sigma)\Theta(t) \quad \text{et} \quad \langle \Theta(t_1), \Theta(t_2)\rangle_p^\lambda = \langle t_1, t_2\rangle_p^\lambda$$

pour tout $\sigma \in \pi(S,s)$ et $t, t_1, t_2 \in T_p(A,s)$. Soit $[\kappa] = \kappa K$ une structure de niveau K sur $T_p(A,s)$. Alors $[\Theta \circ \kappa] = \Theta\kappa K$ est une structure de niveau K sur $T_p(A,s')$. La paire d'isomorphismes (θ, Θ) n'est cependant bien définie que modulo l'action de $\pi(S,s)$ donnée par $\sigma \cdot (\theta,\Theta) = (\theta \circ \mathrm{Ad}(\sigma), \Theta \circ \sigma)$: puisque $\Theta\sigma\kappa K = \Theta\kappa K$, cela n'affecte nullement la construction de $[\Theta \circ \kappa]$. Une structure de niveau K donnée en un point géometrique s de S détermine donc uniquement une structure de niveau K en tout point géométrique s de S.

Remark 4.4. Si l'on ne suppose plus S connexe, une structure de niveau K sur A/S est une collection $([\kappa_{S'}])_{S'}$ de structures de niveau K sur $A_{S'}/S'$ pour $S' \in \pi^0(S)$.

Remark 4.5. Dans tous les cas, l'existence d'une structure de niveau K implique la $(\mathcal{O},\star)$-linéarité de la polarisation $\lambda : A \to A^t$.

Donnons deux cas particuliers de structure de niveau :

Lemma 4.6. *On suppose S connexe. On note $K(n)$ le groupe des similitudes symplectiques $\mathcal{O}_p$-linéaires de (Λ_p, ψ_p) qui agissent trivialement sur $\Lambda_p/p^n\Lambda_p$.*

1. *Pour $n = 0$, il existe au plus une structure de niveau $K(0)$ sur A/S : c'est l'ensemble des isomorphismes (lorsqu'il y en a !) $\kappa : \Lambda_p \xrightarrow{\simeq} T_p(A,s)$ qui vérifient la condition (I).*
2. *Pour $n > 0$, il revient au même de se donner une structure de niveau $K(n)$ sur A/S ou un isomorphisme $\mathcal{O}_p$-linéaire $\overline{\kappa} : (\Lambda_p/p^n\Lambda_p)_S \xrightarrow{\simeq} A[p^n]$ telle que pour un (resp. pour tout) point géométrique s de S, il existe un isomorphisme $\mathcal{O}_p$-linéaire $\kappa : \Lambda_p \xrightarrow{\simeq} T_p(A,s)$ vérifiant la condition (I) qui relève $\overline{\kappa}(s)$:*

$$\overline{\kappa}(s) = \kappa \bmod p^n : \qquad \Lambda_p/p^n\Lambda_p \xrightarrow{\simeq} A[p^n](s) = T_p(A,s)/p^nT_p(A,s).$$

Démonstration. (1) C'est évident. (2) Soit $[\kappa]$ une structure de niveau $K(n)$ sur A/S. Alors $[\kappa]$ induit un isomorphisme $\mathcal{O}_p$-linéaire de $\pi(S,s)$-modules

$$\kappa \bmod p^n : \Lambda_p/p^n\Lambda_p \to A[p^n](s)$$

qui induit à son tour un isomorphisme $\mathcal{O}_p$-linéaire de S-schémas (en groupes) étales

$$\overline{\kappa} : (\Lambda_p/p^n\Lambda_p)_S \to A[p^n]$$

qui vérifie évidemment les conditions de requises. Inversement, soit $\overline{\kappa}$ un tel isomorphisme. Soit X l'ensemble des relèvements de $\overline{\kappa}(s)$ en un isomorphisme $\mathcal{O}_p$-linéaires $\kappa : \Lambda_p \xrightarrow{\simeq} T_p(A,s)$ vérifiant la condition (I). Alors X est non-vide par hypothèse, c'est une $K(n)$-orbite par définition de $K(n)$, et c'est stable sous $\pi(S,s)$ par construction : c'est donc une structure de niveau $K(n)$ sur A/S. □

4.2. **Représentabilité.**

Proposition 4.7. *Soit K un sous-groupe ouvert (compact) du groupe des similitudes symplectiques $\mathcal{O}_p$-linéaires $K(0)$ de (Λ_p, ψ_p). Pour tout S-schéma abélien (projectif) polarisé (A,ι,λ) muni d'une action de $\mathcal{O}$, le foncteur $\mathcal{F}_K : (\mathbf{Sch}/S)^0 \to$* **Ens** *qui à T/S associe l'ensemble des structures de niveau K sur (A,ι,λ) est représentable par un revêtement étale d'un ouvert de S.*

Démonstration. Pour $K = K(0)$, $\mathcal{F}_K$ est représentable par la réunion des composantes connexes de S où $\Lambda_p \simeq T_p(A,s)$ par un isomorphisme $\mathcal{O}_p$-linéaire vérifiant la condition (I). Pour $K = K(n)$, fixons une $\mathbf{Z}/p^n\mathbf{Z}$-base $(e_1, \cdots, e_{2g})$ de $\Lambda_p/p^n\Lambda_p$. Soit $S_1 = A[p^n] \times_S \cdots \times_S A[p^n]$ ($2g$ facteurs), $\sigma_i : S_1 \to A_{S_1}[p^n] = A[p^n] \times_S S_1$ la i-ème section et $\overline{\kappa}_1 : (\Lambda_p/p^n)_{S_1} \to A_{S_1}[p^n]$ le morphisme qui envoie e_i sur σ_i. C'est un morphisme de groupes entre deux revêtements étales (de même rang constant $(p^n)^{2g}$) de S_1, qui est lui-même un revêtement étale de S (de rang constant $(p^n)^{4g^2}$). Soit S_2 la réunion des composantes connexes de S_1 dans lesquelles pour un (ou tout) point géométrique s les deux conditions suivantes sont vérifiées : (a) $\overline{\kappa}_1(s)$ est un isomorphisme et (b) cet isomorphisme se relève en un isomorphisme $\mathcal{O}_p$-linéaire $\kappa : \Lambda_p \to T_p(A,s)$ vérifiant (I). Alors la restriction $\overline{\kappa}_2$ de $\overline{\kappa}_1$ à S_2 est un isomorphisme $\mathcal{O}_p$-linéaire qui définit, d'après le lemme précédent, une structure de niveau $K(n)$ sur A_{S_2}. Le foncteur $\mathcal{F}_K$ est alors représentable par S_2, qui est bien un revêtement étale d'un ouvert fermé de S.

Traitons enfin le cas général. Les $K(n)$ forment une base de voisinages ouverts de $1 \in K(0)$, il existe donc $n \geq 1$ tel que $K(n) \subset K$. Soit $S(n)$ le représentant de $\mathcal{F}_{K(n)}$ et $[\kappa_u] \in \mathcal{F}_{K(n)}(S(n))$ la structure universelle de niveau $K(n)$. Le groupe fini $\overline{K} = K/K(n)$ agit sur $\mathcal{F}_{K(n)}$, donc sur son représentant $S(n)$. Soit $\overline{S}$ le quotient de $S(n)$ pour cette action.

Exercise 4.8. Montrer que $\overline{S}$ existe dans tous les sens raisonnables du mot quotient, est un revêtement étale d'un ouvert de S (l'image de $S(n)$ dans S), et que $S(n) \to \overline{S}$ est un revêtement étale de groupe $\overline{K}$.

Soit $\overline{s}$ un point géométrique de $\overline{S}$, $s \in S(n)(\overline{s})$ (qui existe puisque $S(n) \to \overline{S}$ est un revêtement), et $\kappa_u : \Lambda_p \to T_p(A,s) = T_p(A,\overline{s})$ un élément de la structure de niveau $K(n)$ correspondant à s. C'est donc un isomorphisme $\mathcal{O}_B$-linéaire qui vérifie (I) et (II) : pour tout $\sigma \in \pi(S(n),s)$, il existe $k(\sigma) \in K(n)$ tel que $\sigma \circ \kappa_u = \kappa_u \circ k(\sigma)$. Le revêtement étale galoisien $S(n) \to \overline{S}$ induit une suite exacte

$$0 \to \pi(S(n),s) \to \pi(\overline{S},\overline{s}) \to \overline{K}^o \to 0$$

Soit $\sigma \in \pi(\overline{S},\overline{s})$ d'image k dans $\overline{K}^o$. Alors $\sigma \circ \kappa_u : \Lambda_p \to T_p(A,\sigma s) = T_p(A,\overline{s})$ est un élément de la structure de niveau $K(n)$ correspondant à ks, donc dans $\kappa_u K(n) k \subset \kappa_u K$. Donc $\kappa_u K$ est stable par $\pi(\overline{S},\overline{s})$, i.e. c'est un élément $[\kappa_u] \in \mathcal{F}_K(\overline{S})$ qui ne dépend évidemment pas du choix de $s \in S(n)(\overline{s})$.

Si deux morphismes $f, g : T \to \overline{S}$ induisent le même élément $f^\star[\kappa_u] = g^\star[\kappa_u] \in \mathcal{F}_K(T)$, ils sont égaux : si ces deux morphismes se factorisent par $S(n) \to \overline{S}$, les morphismes relevés $f', g' : T \to S(n)$ induisent deux éléments de $\mathcal{F}_{K(n)}(T)$ qui ont la même image dans $\mathcal{F}_K(T)$ par hypothèse, donc $f' = kg'$ pour un $k \in \overline{K}$, donc $f = g$; sinon, il existe un revêtement étale T' de T tel que les deux morphismes $f', g' : T' \to T \to S$ se factorisent par $S(n) \to \overline{S}$ (et induisent le même élément de $\mathcal{F}_K(T')$), donc $f' = g'$ et $f = g$. Soit enfin T/S et $[\kappa] \in \mathcal{F}_K(T)$. Soit t un point géométrique de T et $\kappa : \Lambda_p \to T_p(A,t)$ dans κK. L'action de $\pi(T,t)$ sur $\kappa K(n)$ se factorise par un quotient $\pi(T,t)/\pi(T',t)$, donc $[\kappa]|T'$ est dans l'image de $\mathcal{F}_{K(n)}(T') \to \mathcal{F}_K(T')$, il existe donc un morphisme $f' : T' \to S(n) \to \overline{S}$ tel que $[\kappa]|T' = f'^\star[\kappa_u]$. Les deux morphismes $T' \times_T T' \to T' \to \overline{S}$ induisent par pull-back le même élément de $\mathcal{F}_K(T' \times_T T')$: ils sont donc égaux. Par descente des morphismes le long de $T' \to T$ (qui est un revêtement étale et à fortiori plat et quasi-compact), $f' : T' \to \overline{S}$ se factorise en $f : T \to \overline{S}$, et $f^\star[\kappa_u] = [\kappa]$: $\overline{S}$ représente $\mathcal{F}_K$. $\square$

4.3. **Variantes.** On peut aussi définir des structures de niveaux K pour un sous-groupe K du groupe des automorphismes $\mathrm{Aut}(V_p, \psi_p)$, où $V_p = \Lambda_p \otimes \mathbf{Q}_p$. Ce sont alors des K-orbites κK d'isomorphismes $\mathcal{O} \otimes \mathbf{Q}_p$-linéaires $\kappa : V_p \xrightarrow{\simeq} V_p(A,s)$ vérifiant l'analogue de (I) et (II). On montre comme ci-dessus que le foncteur $\mathcal{F}_K$ est relativement représentable lorsque K est un sous-groupe ouvert et *compact*, ou même vu (I) seulement *compact modulo le centre* de $\mathrm{Aut}(V_p, \psi_p)$.

Exercise 4.9. Pourquoi faut-il ajouter ici cette hypothèse de compacité ?

On peut aussi fixer directement un $\mathcal{O}$-module Λ qui est libre de rang $2g$ sur $\mathbf{Z}$, une forme symplectique non-dégénérée $\psi : \Lambda \times \Lambda \to \mathbf{Z}$ induisant $\star$ sur $\mathcal{O}$, et travailler simultanément avec *tous* les modules de Tate (i.e. avec $T_f(A,s)$ ou $V_f(A,s)$). Soit G le $\mathbf{Z}$-schéma en groupe des similitudes symplectiques $\mathcal{O}$-linéaires de (Λ, ψ). Pour un sous-groupe K de $G(\widehat{\mathbf{Z}})$ (resp. de $G(\mathbf{A}_f)$), une structure de niveau K est alors une K-orbite d'isomorphisme $\widehat{\mathcal{O}}$-linéaire (resp. $\widehat{B}$-linéaire)

$$\kappa : \widehat{\Lambda} \xrightarrow{\simeq} T_f(A,s) \qquad (\text{resp. } \kappa : \widehat{V} \xrightarrow{\simeq} V_f(A,s))$$

qui vérifie l'analogue de (I) (compatibilité des accouplements à un facteur près) et (II) (stabilité sous $\pi(S,s)$. On a bien sûr posé $\widehat{\Lambda} = \Lambda \otimes \widehat{\mathbf{Z}}$, $V = \Lambda \otimes \mathbf{Q}$, $B = \mathcal{O} \otimes \mathbf{Q}$ etc... Cependant, il faut alors travailler avec des schémas abéliens sur des schémas S où *tous* les nombres premiers sont inversibles, i.e. avec des $\mathbf{Q}$-schémas. Lorsqu'on veut faire de la réduction modulo p, i.e. travailler avec des $\mathbf{Z}_{(p)}$-schémas, on doit donc plutôt travailler avec $T_f^p(A,s)$ ou $V_f^p(A,s)$, et des sous-groupes K de $G(\widehat{\mathbf{Z}}^p)$ ou $G(\mathbf{A}_f^p)$.

Dans tous les cas, on montre comme ci-dessus que les foncteurs $\mathcal{F}_K$ que l'on obtient sont relativement représentables lorsque K est un *sous-groupe ouvert et compact* (ou seulement *compact modulo le centre)* du groupe d'automorphismes où il vit.

5. Schémas Abéliens à Isogénie Près

5.1. **Définition.**

Definition 5.1. Soit S un schéma. La catégorie $\mathbf{Ab}_S$ des S-schémas abéliens est la sous-catégorie pleine de la catégorie des S-schémas en groupes dont les objets sont les S-schémas abéliens. La catégorie $\mathbf{Ab}_S^0$ des S-schémas abéliens *à isogénie près* est la catégorie dont les objets sont les S-schémas abéliens, mais où l'on modifie les groupes d'homomorphismes comme suit

$$\mathrm{Hom}_{\mathbf{Ab}_S^0}(A,B) = \mathrm{Hom}_{\mathbf{Ab}_S}(A,B) \otimes \mathbf{Q}.$$

Si A et B sont deux S-schémas abéliens, on note en général

$$\mathrm{Hom}_S(A,B) = \mathrm{Hom}_{\mathbf{Ab}_S}(A,B) \qquad \text{et} \qquad \mathrm{Hom}_S^0(A,B) = \mathrm{Hom}_{\mathbf{Ab}_S^0}(A,B).$$

Le nom “à isogénie près” provient du lemme suivant :

Lemma 5.2. *Un morphisme $\alpha : A \to B$ dans $\mathbf{Ab}_S^0$ est un isomorphisme si et seulement si un multiple entier convenable $n\alpha$ de α est une isogénie dans $\mathbf{Ab}_S$.*

Démonstration. Si α est un isomorphisme dans $\mathbf{Ab}_S^0$, il existe un entier n tel que $n\alpha$ est dans $\mathbf{Ab}_S$. C'est encore un isomorphisme dans $\mathbf{Ab}_S^0$, donc $V_f(n\alpha, s)$: $V_f(A,s) \to V_f(B,s)$ est encore un isomorphisme pour tout point géométrique s de S. En particulier, le noyau de $(n\alpha)_s$ est fini, donc $(n\alpha)_s$ est une isogénie et

$n\alpha : A \to B$ est une isogénie. Inversement, il s'agit de montrer que toute isogénie $\alpha : A \to B$ est un isomorphisme dans $\mathbf{Ab}^0_S$. Le problème étant local sur S, on peut supposer que $\ker \alpha \subset A[n]$ pour un $n \geq 1$. Alors $[n]_A$ se factorise par α, i.e. il existe un morphisme $\beta : B \to A$ tel que $[n]_A = \beta \circ \alpha$, et β est alors une isogénie. Il existe donc aussi $m > 0$ et $\gamma : A \to B$ tel que $[m]_B = \gamma \circ \beta$. Mais

$$[n]_A \circ \gamma = \gamma \circ [n]_A = \gamma \circ \beta \circ \alpha = [m]_B \circ \alpha$$

donc $\gamma = \frac{m}{n}\alpha$ dans $\mathrm{Hom}^0_S(A, B)$. Alors $(\frac{1}{n}\beta) \cdot \alpha = \mathbf{1}_A$ dans $\mathrm{End}^0_S(A)$ et

$$\alpha \cdot (\frac{1}{n}\beta) = (\frac{m}{n}\alpha) \cdot (\frac{1}{m}\beta) = \frac{1}{m}\gamma\beta = \mathbf{1}_B$$

dans $\mathrm{End}^0_S(B)$, donc α est inversible dans $\mathbf{Ab}^0_S$. □

5.2. **Sur un corps parfait.** L'intérêt de cette catégorie apparaît clairement lorsqu'on travaille sur le spectre d'un corps parfait k, par exemple un corps de caractéristique 0, ou bien un corps fini, ou bien un corps algébriquement clos. On a alors :

Theorem 5.3. *La catégorie* $\mathbf{Ab}^0_k$ *est abélienne et semi-simple.*

Une variété abélienne A sur k est dite *simple* si elle ne contient pas de sous-variété abélienne $B \neq 0, A$. Si A est simple et $\alpha : A \to B$ est un morphisme non-nul, alors $\ker(\alpha)^0_{red}$ est une sous-variété abélienne propre de A, donc $\ker(\alpha)^0_{red} = 0$ et α est fini. Si de plus B est simple, $A/\ker\alpha$ est une sous-variété abélienne non-nulle de B, donc $A/\ker\alpha = B$ et α est une isogénie, donc un isomorphisme dans $\mathbf{Ab}^0_k$. On en déduit que pour A et B simples, tout élément non-nul de $\mathrm{Hom}^0_k(A, B)$ est un isomorphisme dans $\mathbf{Ab}^0_k$. En particulier, $\mathrm{End}^0_k(A)$ est un corps.

Lemma 5.4. *Toute variété abélienne A sur k est isogène à une somme directe de sous-variétés abéliennes simples.*

Démonstration. Soit $i : B \hookrightarrow A$ une inclusion de variété abélienne sur k, $i^t : A^t \to B^t$ le morphisme dual, $\mathcal{L}$ un faisceau inversible ample sur A, et $j : C \hookrightarrow A$ la composante connexe réduite du noyau de $i^t \circ \Lambda(\mathcal{L}) : A \to B^t$. C'est une sous-variété abélienne de A et $\dim B + \dim C = \dim B^t + \dim C = \dim A$. De plus, $x \in B \cap C$ implique $x \in B$ et $i^t \circ \Lambda(\mathcal{L})(x) = i^\star(\mathcal{T}^\star_x\mathcal{L} \otimes \mathcal{L}^{-1}) = 0$, i.e. $\mathcal{T}^\star_{i(x)}(i^\star\mathcal{L} \otimes i^\star\mathcal{L}^{-1}) = 0$ ou encore $\Lambda(i^\star\mathcal{L})(i(x)) = 0$, donc $i(x) \in \ker \Lambda(i^\star\mathcal{L}) : B \to B^t$, qui est fini puisque $i^\star\mathcal{L}$ est ample sur B. Donc $B \cap C$ est fini et $B \times C \to A$ est une isogénie. On conclut par récurrence. □

Le théorème résulte formellement de ce qui précède. Soit $\mathcal{C} = \mathbf{Ab}^0_k$, $\mathcal{X}$ l'ensemble des classes d'isomorphismes d'objets simples de $\mathcal{C}$. Pour tout $[X] \in \mathcal{X}$, on note $\mathcal{C}(X)$ la sous-catégorie pleine de $\mathcal{C}$ formée des objets isomorphes à une somme directe finie de copies de X. Le foncteur évident $\oplus_{[X]\in\mathcal{X}}\mathcal{C}(X) \to \mathcal{C}$ est essentiellement surjectif d'après le lemme précédent, fidèle par construction, et plein puisque $\mathrm{Hom}^0_k(X, Y) = 0$ si $[X] \neq [Y]$ dans $\mathcal{X}$. C'est donc une équivalence de catégorie, et il suffit de montrer que $\mathcal{C}(X)$ est abélienne semi-simple pour tout $[X] \in \mathcal{X}$. Soit $D_X = \mathrm{End}^0_k X$, qui est un corps gauche d'après la discussion qui précède. Alors $A \mapsto \mathrm{Hom}^0(X, A)$ est un foncteur de $\mathcal{C}(X)$ dans la catégorie $\mathbf{Mod}^{df}_{D_X}$ des D_X-modules à droite de D_X-dimension finie, dont on montre facilement que c'est encore une équivalence de catégorie. En particulier, $\mathcal{C}(X)$ est abélienne semi-simple puisque $\mathbf{Mod}^{df}_{D_X}$ l'est.

5.3. **Variantes.** Pour diverses raisons, on voudrait aussi considérer une catégorie de variétés abéliennes où l'on n'inverse que les isogénies de degré premier à p, pour un nombre premier p fixé. C'est la catégorie $\mathbf{Ab}_S^p$ dont les objets sont encore les S-schémas abéliens, mais où l'on modifie maintenant les homomorphismes en posant

$$\mathrm{Hom}_{\mathbf{Ab}_S^p}(A,B) = \mathrm{Hom}_S^p(A,B) = \mathrm{Hom}_S(A,B) \otimes \mathbf{Z}_{(p)}.$$

6. Probleme de type PEL, I

On définit ici ce qui sera le prototype de problème de modules que l'on sera amené à considérer dans la suite.

6.1. **Le problème de module sur Q.** Soit B une $\mathbf{Q}$-algèbre semi-simple, $\star$ une involution de B, V un B-module de $\mathbf{Q}$-dimension $2g$, $\psi : V \times V \to \mathbf{Q}$ une forme symplectique telle que $\psi(bv,w) = \psi(v, b^\star w)$ pour tout $v,w \in V$ et $b \in B$. On note G le $\mathbf{Q}$-schéma en groupes des similitudes symplectiques B-linéaires de (V,ψ) et K un sous-groupe ouvert et compact de $G(\mathbf{A}_f)$. On considère le foncteur

$$\mathbf{M} : (\mathbf{Sch}/\mathbf{Q})^0 \to \mathbf{Ens}$$

qui à un $\mathbf{Q}$-schéma S associe l'ensemble des classes d'isomorphismes de quadruplet $(A, \iota, [\lambda], [\kappa])$ où

- A/S est un S-schéma abélien *à isogénie près*,
- $\iota : B \to \mathrm{End}_S^0(A)$ est un morphisme de $\mathbf{Q}$-algèbre,
- $[\lambda] = \mathbf{Q}\lambda \subset \mathrm{Hom}_S^0(A, A^t)$ une $\mathbf{Q}$-droite engendrée par une polarisation $\lambda : A \to A^t$,
- $[\kappa]$ une structure de niveau K.

On rappelle que ce dernier élément consiste en la donnée, pour un point géométrique s dans chaque composante connexe de S, d'une K-orbite stable sous $\pi(S,s)$ d'isomorphismes $\widehat{B}$-linéaires $\kappa : \widehat{V} \to V_f(A,s)$ pour lesquels il existe un isomorphisme $\mathbf{A}_f \xrightarrow{\simeq} V_f(\mu, s)$ qui fait commuter le diagramme suivant :

$$\begin{array}{ccccccc}
\widehat{\psi} : & & \widehat{V} & \times & \widehat{V} & \to & \mathbf{A}_f \\
& & \downarrow & & \downarrow & & \downarrow \\
\langle \bullet, \bullet \rangle_f^\lambda : & & V_f(A,s) & \times & V_f(A,s) & \to & V_f(\mu,s)
\end{array}$$

Theorem 6.1. *Si K est assez petit, ce foncteur est représentable par un $\mathbf{Q}$-schéma.*

On fixe dans V un réseau Λ tel que $\widehat{\Lambda}$ est stable par K et $\psi(\Lambda,\Lambda) \subset \mathbf{Z}$. On note d^2 le cardinal de $\widehat{\Lambda}/\Lambda$. On choisit un ordre $\mathcal{O}$ dans B tel que $\mathcal{O} \cdot \Lambda \subset \Lambda$. On note

$$\mathbf{M}' : (\mathbf{Sch}/\mathbf{Q})^0 \to \mathbf{Ens}$$

le foncteur qui à un $\mathbf{Q}$-schéma S associe l'ensemble des classes d'isomorphismes de quadruplets $(A, \iota, \lambda, [\kappa])$ où

- A/S est un S-schéma abélien,
- $\iota : \mathcal{O} \to \mathrm{End}_S(A)$ est un morphisme de $\mathbf{Z}$-algèbre,
- $\lambda : A \to A^t$ est une polarisation,
- $[\kappa]$ est une structure de niveau K,

où cette dernière structure est maintenant la donnée, pour un point géométrique s dans chacune des composantes connexes de S, d'une K-orbite stable sous $\pi(S,s)$

d'isomorphismes $\kappa : \widehat{\Lambda} \to T_f(A,s)$ tels qu'il existe un isomorphisme $\widehat{\mathbf{Z}} \to T_f(\mu,s)$ qui fait commuter le diagramme

$$\begin{array}{ccccccc} \widehat{\psi}: & \widehat{\Lambda} & \times & \widehat{\Lambda} & \to & \widehat{\mathbf{Z}} \\ & \downarrow & & \downarrow & & \downarrow \\ \langle \bullet, \bullet \rangle_f^\lambda : & T_f(A,s) & \times & T_f(A,s) & \to & T_f(\mu,s) \end{array}$$

Cette structure de niveau garantit donc que λ est de degré d^2 et A/S de dimension relative g. Si K est assez petit, disons inclus dans le groupe $K(n)$ des similtudes symplectiques $\mathcal{O}$-linéaires de (Λ,ψ) qui sont l'identité module $n \geq 3$, cette structure de niveau K induit une structure de niveau $K(n)$, donc un isomorphisme

$$\overline{\kappa}(s) : \widehat{\Lambda}/n\widehat{\Lambda} = \Lambda/n\Lambda \simeq T_f(\mu,s)/nT_f(\mu,s) = A[n](s).$$

Choisissant une $\mathbf{Z}/n\mathbf{Z}$-base de $(\Lambda/n\Lambda)$, on obtient donc une structure de niveau n naïve sur A/S. En résumé, on dispose d'un morphisme de foncteur $\mathbf{M}' \to \mathbf{M}^g_{d,n}$. Montrons que ce morphisme est relativement représentable. Cela résulte des deux lemmes suivants : le premier nous dit que les fibres de ce morphisme s'identifient aux foncteurs considérés dans le second.

Lemma 6.2. *Pour tout schéma abélien A/S et $n \geq 3$, tout automorphisme de A/S qui agit trivialement sur $A[n]$ est trivial.*

Démonstration. ... □

Lemma 6.3. *Pour tout $[A,\lambda,\overline{\kappa}] \in \mathbf{M}^g_{d,n}(S)$, le foncteur qui à T associe l'ensemble des structures $(\iota,[\kappa])$ comme ci-dessus sur (A_T,λ_T) telles que $[\kappa]$ relève $\overline{\kappa}_T$ est représentable.*

Démonstration. Soit S_1 le S-schéma qui représente $T \mapsto \mathrm{Hom}_{Ann}(\mathcal{O}, \mathrm{End}_T(A_T))$ (Proposition 1.1) et $\iota_1 : \mathcal{O} \to \mathrm{End}_{S_1}(A_{S_1})$ la structure universelle. Soit S_2 le S_1-schéma qui représente le foncteur qui à T associe l'ensemble des structures de niveau K sur $(A_T, \iota_{1,T}, \lambda_T)$ (sans la condition de relèvement, Proposition 4.7) et $[\kappa_2]$ la structure de niveau K universelle sur $(A_{S_2}, \iota_{1,S_2}, \lambda_{S_2})$. Sur A_{S_2}, on dispose maintenant de deux structures de niveau n naïve : $\overline{\kappa}_{1/2} : (\Lambda/n\Lambda)_{S_2} \to A[n]_{S_2}$, où $\overline{\kappa}_1$ provient de $\overline{\kappa}$ et $\overline{\kappa}_2$ de $[\kappa_2]$. Soit S_3 l'ouvert fermé de S_2 où ces deux structures de niveau coïncident. Alors S_3 représente le foncteur considéré. □

Il en résulte que le foncteur $\mathbf{M}' : (\mathbf{Sch}/\mathbf{Q})^0 \to \mathbf{Ens}$ est représentable. Considérons maintenant le morphisme $\mathbf{M}' \to \mathbf{M}$ qui correspond à l'inclusion des catégories $\mathbf{Ab}_S \to \mathbf{Ab}^0_S$. Nous allons montrer que c'est un *isomorphisme*, ce qui achèvera la preuve du théorème.

Lemma 6.4. *Pour tout $\mathbf{Q}$-schéma S, $\mathbf{M}'(S) \to \mathbf{M}(S)$ est injective.*

Démonstration. Soit $[A_i, \iota_i, \lambda_i, [\kappa_i]]$ deux éléments de $\mathbf{M}'(S)$ ayant la même image de $\mathbf{M}(S)$. Cela signifie qu'il existe un isomorphisme $\alpha : A_1 \xrightarrow{\simeq} A_2$ dans la catégorie $\mathbf{Ab}^0_S$ des S-schémas abéliens à isogénie près qui est B-linéaire, vérifie $\mathbf{Q} \cdot \lambda_2 \circ \alpha = \mathbf{Q} \cdot \alpha \circ \lambda_1$ dans $\mathrm{Hom}^0_S(A_1, A_2^t)$, et

$$\kappa_2 K = V_f(\alpha) \circ \kappa_1 K \quad \text{dans } \mathrm{Hom}_{\widehat{B}}\left(\widehat{V}, V_f(A_2,s)\right).$$

En particulier (puisque $K \cdot \widehat{\Lambda} = \widehat{\Lambda}$),

$$V_f(\alpha)(T_f(A_1,s)) = V_f(\alpha) \circ \kappa_1(\widehat{\Lambda}) = \kappa_2(\widehat{\Lambda}) = T_f(A_2,s).$$

Choisissons $m \geq 1$ tel que $m\alpha$ soit une isogénie $\beta : A_1 \to A_2$. Alors

$$T_f(\beta)(T_f(A_1, s)) = mT_f(A_2, s))$$

donc $\beta|A_1[m] = 0$ et β se factorise en $\alpha' \circ [m]$ pour une isogénie $\alpha' : A_1 \to A_2$. On a

$$T_f(\alpha')(T_f(A_1, s)) = T_f(A_2, s)$$

donc α' est un isomorphisme dans $\mathbf{Ab}_S$. En d'autres termes, l'isomorphisme α (de $\mathbf{Ab}_S^0$) est déjà dans $\mathbf{Ab}_S$ et y est encore un isomorphisme. C'est bien sûr un isomorphisme $\mathcal{O}$-linéaire (par fidélité de $A \to T_f(A, s)$) qui envoie $[\kappa_1]$ sur $[\kappa_2]$ et λ_1 sur... $x\lambda_2 \in \mathrm{Hom}_S(A_2, A_2^t) \cap \mathbf{Q} \cdot \lambda_2$ pour un $x \in \mathbf{Q}$. Choisissons $D \geq 1$ tel que $N = Dx \in \mathbf{Z}$. Alors $Dx\lambda_2 = N\lambda_2$ et $D\lambda_2$ sont des polarisations de même degré $D^{2g}d^2$ sur A_2, donc $N > 0$ et $N = D$, i.e. $x = 1$. Donc $[A_1, \iota_1, \lambda_1, [\kappa_1]] = [A_2, \iota_2, \lambda_2, [\kappa_2]]$ dans $\mathbf{M}'(S)$. CQFD. □

Lemma 6.5. *Pour tout* $\mathbf{Q}$*-schéma* S, $\mathbf{M}'(S) \to \mathbf{M}(S)$ *est surjective.*

Démonstration. Soit $[A, \iota, [\lambda], [\kappa]] \in \mathbf{M}(S)$. Pour tout point géométrique s de S,

$$T(s) = \kappa \cdot \widehat{\Lambda} \subset V_f(A, s)$$

est un réseau de $V_f(A, s)$ stable sous $\widehat{\mathcal{O}}$ (puisque $\widehat{\Lambda}$ l'est et κ est $\widehat{B}$-linéaire), qui ne dépend pas du choix de $\kappa \in [\kappa]$, et qui est donc aussi stable sous l'action de $\pi(S, s)$ sur $V_f(A, s)$. En jonglant un peu avec les définitions de $\mathbf{Ab}_S^0$ et $V_f(A, s)$, on montre qu'il existe un isomorphisme $\alpha : B \to A$ dans $\mathbf{Ab}_S^0$ qui envoie $T_f(B, s)$ sur $T(s)$. En transportant toutes les structures sur A à B via cet isomorphisme, on peut donc supposer que $B = A$, i.e. $T(s) = T_f(A, s)$. Si $o \in \mathcal{O} \subset B$ et $m \geq 1$ est un entier tel que $m\iota(o) \in \mathrm{End}_S(A)$, alors

$$T_f(m\iota(o), s)(T_f(A, s)) = mT_f(\iota(o), s)(T_f(A, s)) \subset mT_f(A, s)$$

donc $m\iota(o) = 0$ sur $A[m]$ et $m\iota(o) = mo'$ pour un $o' \in \mathrm{End}_S(A)$, i.e. $\iota(o) \in \mathrm{End}_S(A)$. Donc $\iota : \mathcal{O} \to \mathrm{End}_S(A)$ est une $\mathcal{O}$-structure sur A. Sur A, on dispose aussi de la droite $\mathbf{Q}\lambda$ où $\lambda : A \to A^t$ est une polarisation. On sait d'autre part qu'il existe un isomorphisme $\mathbf{A}_f \to V_f(\mu, s)$ qui fait commuter le diagramme suivant

$$\begin{array}{ccccccccc} \widehat{\psi}: & \widehat{\Lambda} & \times & \widehat{\Lambda} & \to & \widehat{\mathbf{Z}} & \subset & \mathbf{A}_f \\ & \downarrow & & \downarrow & & & & \downarrow \\ \langle \bullet, \bullet \rangle_f^\lambda : & T_f(A, s) & \times & T_f(A, s) & \to & T_f(\mu, s) & \subset & V_f(\mu, s) \end{array}$$

L'image de $\widehat{\mathbf{Z}}$ par cet isomorphisme est de la forme $\nu^{-1}T_f(\mu, s)$ pour un $\nu \in \mathbf{A}_f^\times = \widehat{\mathbf{Q}}^\times = \mathbf{Q}_>^\times \cdot \widehat{\mathbf{Z}}^\times$, que l'on peut donc supposer dans $\mathbf{Q}_{>0}^\times$. Alors $\nu\lambda$ est un morphisme $A \to A^t$ dans $\mathbf{Ab}_S^0$ et

$$\langle x, V_f(\nu\lambda, s)y \rangle_f^A = \nu \langle x, V_f(\lambda)y \rangle_f^A = \nu \langle x, y \rangle_f^\lambda \in T_f(\mu, s)$$

pour tout $x, y \in T_f(A, s)$, donc $V_f(\nu\lambda, s)$ envoie $T_f(A, s)$ dans $T_f(A^t, s)$. On en déduit comme précédemment que $\nu\lambda$ est un morphisme $A \to A^t$, et puisqu'un multiple entier positif de $\nu\lambda$ est une polarisation, $\nu\lambda$ est encore une polarisation. On peut donc supposer que $\nu\lambda = \lambda$, i.e. $\nu = 1$ et l'on a alors un diagramme commutatif

$$\begin{array}{ccccccc} \widehat{\psi}: & \widehat{\Lambda} & \times & \widehat{\Lambda} & \to & \widehat{\mathbf{Z}} \\ & \downarrow & & \downarrow & & \downarrow \\ \langle \bullet, \bullet \rangle_f^\lambda : & T_f(A, s) & \times & T_f(A, s) & \to & T_f(\mu, s) \end{array}$$

Alors $[A, \iota, \lambda, [\kappa]] \in \mathbf{M}'(S)$ est un relèvement de $[A, \iota, [\lambda], [\kappa]] \in \mathbf{M}(S)$. $\square$

6.2. **Le problème de module sur $\mathbf{Z}_{(p)}$.** L'approche précédente nous contraint à travailler sur $\mathbf{Q}$. Si l'on veut faire de la réduction en p, il nous faut donc "étendre" ce problème de module à $\mathbf{Z}_{(p)}$. Il nous faut alors travailler avec la variante $V_f^p(A, s)$ des modules de Tate. La solution consiste alors à travailler dans les catégories $\mathbf{Ab}_S^p$ des "schémas abéliens à isogénie première à p près".

Conservant les notations de la section précédente, on suppose que $K = K^p K_p$ pour des sous-groupes ouverts compacts K^p de $G(\mathbf{A}_f^p)$ et K_p de $G(\mathbf{Q}_p)$. On fixe en outre un $\mathbf{Z}_{(p)}$-ordre $\mathcal{O}_{(p)}$ dans B et un entier $d_p \in \mathbf{N}$ vérifiant l'hypothèse technique suivante : il existe dans V un $\mathcal{O}_{(p)}$-réseau $\Lambda_{(p)}$ tel que $\psi(\Lambda_{(p)}, \Lambda_{(p)}) \subset \mathbf{Z}_{(p)}$ et $\Lambda_{(p)}^{\perp}/\Lambda_{(p)}$ est de cardinal p^{2d_p}. On considère le foncteur

$$\mathbf{M}^p : (\mathbf{Sch}/\mathbf{Z}_{(p)})^0 \to \mathbf{Ens}$$

qui à un $\mathbf{Z}_{(p)}$-schéma S associe l'ensemble des classes d'isomorphismes de quadruplets $(A, \iota, [\lambda], [\kappa])$ où

- A/S est un objet de $\mathbf{Ab}_S^p$ (un schéma abélien à "isogénie première à p près"),
- $\iota : \mathcal{O}_{(p)} \to \mathrm{End}_S^p(A)$ est un morphisme d'anneau,
- $[\lambda] = \mathbf{Z}_{(p)}\lambda \subset \mathrm{Hom}_S^p(A, A^t)$ est une $\mathbf{Z}_{(p)}$-droite engendrée par une polarisation $\lambda : A \to A^t$ *de degré* $p^{2d_p}x$ *avec* $(x, p) = 1$,
- $[\kappa]$ est une structure de niveau K^p sur $(A, \iota, [\lambda])$

où cette dernière structure est maintenant la donnée, pour un point géométrique s dans chaque composante connexe de S, d'une K^p-orbite stable sous $\pi(S, s)$ d'isomorphismes $\widehat{\mathcal{O}}_{(p)}^p = \mathcal{O}_{(p)} \otimes_{\mathbf{Z}_{(p)}} \mathbf{A}_f^p$-linéaires $\kappa : \widehat{V}^p \xrightarrow{\simeq} V_f^p(A, s)$ tels qu'il existe un isomorphisme $\mathbf{A}_f^p \to V_f^p(\mu, s)$ qui rende commutatif le diagramme suivant :

$$\begin{array}{cccccc}
\widehat{\psi}^{(p)} : & \widehat{V}^p & \times & \widehat{V}^p & \to & \mathbf{A}_f^p \\
& \downarrow & & \downarrow & & \downarrow \\
\langle \bullet, \bullet \rangle_f^{p,\lambda} : & V_f^p(A, s) & \times & V_f^p(A, s) & \to & T_f^p(\mu, s)
\end{array}$$

Theorem 6.6. *Si K^p est assez petit, ce foncteur est représentable par un $\mathbf{Z}_{(p)}$-schéma.*

La preuve est identique à celle du théorème précédent. On choisit dans V un $\mathbf{Z}$-réseau Λ qui étend $\Lambda_{(p)}$, dans B un $\mathbf{Z}$-ordre $\mathcal{O}$ qui étend $\mathcal{O}_{(p)}$, et on montre que $\mathbf{M}^p = \mathbf{M}'^p$ pour un foncteur $\mathbf{M}'^p$ qui classifie les quadruplets $(A, \iota, \lambda, [\kappa])$ où A est un (vrai) S-schéma abélien, ι une action de $\mathcal{O}$ sur A/S, λ une polarisation de degré égal au cardinal de $\Lambda^{\perp}/\Lambda$, et $[\kappa]$ une structure de niveau K^p sur $T_f^p(A, s)$.

6.3. **Comparaison des deux problèmes de module sur Q.** Il reste à répondre à la question suivante : dans quelle mesure le foncteur $\mathbf{M}^p$ est-il une extension de $\mathbf{M}$ (de $\mathbf{Sch}/\mathbf{Q}$ à $\mathbf{Sch}/\mathbf{Z}_{(p)}$) ? On ne peut pas directement comparer les foncteurs $\mathbf{M}^p|\mathbf{Q}$ et $\mathbf{M}$. Pour le faire, il faut introduire encore des variantes, par exemple un foncteur $\widetilde{\mathbf{M}}$ qui classifierait les schémas abéliens à isogénie près munis de polarisation, d'endomorphisme, et de structure de niveau K^p, qui nous donnerait des morphismes $\mathbf{M}^p \to \widetilde{\mathbf{M}}$ (correspondant à $\mathbf{Ab}_S^p \hookrightarrow \mathbf{Ab}_S^0$) et $\mathbf{M}|\mathbf{Q} \to \widetilde{\mathbf{M}}|\mathbf{Q}$ (oubli de la K_p-structure). On peut aussi utiliser ce qui à déjà été fait, et comparer directement les variantes $\mathbf{M}'$ et $\mathbf{M}'^p$ de $\mathbf{M}$ et $\mathbf{M}^p$. Si l'on définit $\mathbf{M}'$ via le choix de $(\Lambda, \mathcal{O}) \subset (V, B)$ et $\mathbf{M}'^p$ par $(\Lambda_{(p)}, \mathcal{O}_{(p)})$, on a alors directement un morphisme $\mathbf{M}' \to \mathbf{M}'^p|\mathbf{Q}$ qui correspond à l'oubli de la K_p-structure $[\kappa_p]$ pour $\kappa_p : \Lambda_p \to T_p(A, s)$. Si K^p est assez petit (donc $\mathrm{Aut}_S(A,[\kappa^p]) = \{1\}$), les fibres de ce morphisme s'identifient exactement aux foncteurs $\mathcal{F}_{K_p}$ de la proposition 4.7. En particulier :

Lemma 6.7. *Si K_p est le groupe des similitudes symplectiques de (Λ_p, ψ_p), alors $\mathbf{M}' \to \mathbf{M}'^p|\mathbf{Q}$ est relativement représentable par des immersions ouvertes et fermées, donc $\mathbf{M}/\mathrm{Spec}\mathbf{Q}$ est un sous-schéma ouvert et fermé de la fibre générique de $\mathbf{M}^p/\mathrm{Spec}\mathbf{Z}_{(p)}$.*

Troisième partie 3. Algèbres de Lie

7. Algèbres de Lie

7.1. **Rappels.** Soit G un S-schéma en groupe. Pour tout S-schéma T, on note

$$\mathrm{Lie}G(T) = \ker\left(G(T[\epsilon]) \to G(T)\right).$$

On obtient ainsi un foncteur en groupe sur la catégorie des S-schémas. C'est en fait réprésentable par un S-schéma en groupes commutatifs, et même en $\mathcal{O}_S$-algèbre de Lie. Pour le voir, on étudie ce qu'est $\alpha \in \mathrm{Lie}G(S)$. Par définition, c'est un morphisme

$$\alpha : S[\epsilon] \to G \quad \text{tel que } \alpha \circ \mathrm{aug} : S \to S[\epsilon] \to G = e : S \to G.$$

Puisque $S \xrightarrow{\mathrm{aug}} S[\epsilon] \xrightarrow{\mathrm{struct}} S$ induisent des homéomorphismes sur les espaces sous-jacents, la composante topologique α_{top} de α n'est pas très mystérieuse : c'est juste e_{top}. Tout est donc dans le morphisme de $f^{-1}\mathcal{O}_S$-algèbre

$$\alpha^{\#} : \mathcal{O}_G \to e_\star \mathcal{O}_{S[\epsilon]} = e_\star \mathcal{O}_S \oplus e_\star \mathcal{O}_S[\epsilon]$$

On a $\alpha^{\#} = e^{\#} + D \cdot \epsilon$ où $e^{\#} : \mathcal{O}_G \to e_\star \mathcal{O}_S$ est le morphisme de faisceaux de $f^{-1}\mathcal{O}_S$-algèbres associé à $e : S \to G$ et où $D : \mathcal{O}_G \to e_\star \mathcal{O}_S$ est un morphisme de $f^{-1}\mathcal{O}_S$-modules tel que

$$\forall a, b \in \mathcal{O}_G : \qquad D(ab) = e^{\#}(a)D(b) + e^{\#}(b)D(a)$$

On dit d'un tel morphisme que c'est une $f^{-1}\mathcal{O}_S$-dérivation. Si $\mathcal{I}$ est le noyau de $e^{\#}$, on a $e^{\#} : \mathcal{O}_G \to e_\star\mathcal{O}_S \simeq \mathcal{O}_G/\mathcal{I}$. Donc $D(\mathcal{I}^2 + f^{-1}\mathcal{O}_S \cdot \mathcal{I}) = 0$ et on peut voir D comme un morphisme de $f^{-1}\mathcal{O}_S$-modules $D : \mathcal{O}_G/\mathcal{I}^2 + f^{-1}\mathcal{O}_S \cdot \mathcal{I} \to e_\star\mathcal{O}_S$. Un tel morphisme est uniquement déterminé par sa restriction à $\mathcal{I}/\mathcal{I}^2 + f^{-1}\mathcal{O}_S \cdot \mathcal{I} \to e_\star\mathcal{O}_S$, laquelle est équivalente à celle du morphisme de $e^{-1}f^{-1}\mathcal{O}_S = \mathcal{O}_S$-module

$$e^{-1}(\mathcal{I}/\mathcal{I}^2 + f^{-1}\mathcal{O}_S \cdot \mathcal{I}) \to \mathcal{O}_S.$$

En considérant e comme le pull-back de $\Delta : G \to G \times_S G$ par (Id, e), on voit que

$$e^{-1}(\mathcal{I}/\mathcal{I}^2 + f^{-1}\mathcal{O}_S \cdot \mathcal{I}) = e^\star(\Delta^{-1}(\mathcal{J}/\mathcal{J}^2)) = e^\star(\Omega^1_{G/S}) = \omega^1_{G/S}$$

où $\mathcal{J}$ est l'idéal de $\mathcal{O}_{G\times_S G}$ correspondant à la diagonale. On a obtenu :

$$\mathrm{Lie}G(S) = \mathrm{Hom}_{\mathcal{O}_S}(\omega^1_{G/S}, \mathcal{O}_S)$$

et plus généralement, $\mathrm{Lie}G = (\omega^1_{G/S})^\vee$. On peut vérifier que la structure de $\mathcal{O}_S$-module ainsi obtenue est donnée par $\gamma \mapsto (\epsilon \mapsto \gamma\epsilon)$, et que la structure de groupe sous-jacente à cette structure de $\mathcal{O}_S$-module coïncide avec celle provenant de la définition initiale de $\mathrm{Lie}G$ comme noyau d'un morphisme de groupe. Si G/S est lisse de dimension relative g, $\Omega^1_{G/S}$ est un $\mathcal{O}_G$-module localement libre de rang g, donc $\omega^1_{G/S}$ itou et $\mathrm{Lie}G = \mathbf{V}(\omega^1_{G/S})$.

La structure de $\mathcal{O}_S$-algèbre de Lie provient de l'interprétation en termes de dérivation : si D_1 et D_2 sont deux dérivations, le produit $D_1D_2 - D_2D_1$ en est une également. Nous n'aurons pas besoin du crochet, mais il faut mentionner que si G est abélien, ce crochet est nul. Cette même interprétation montre que si $S = \mathrm{Spec}\mathbf{C}$, $\mathrm{Lie}G(\mathbf{C}) = T_0G$ est l'espace tangent de G en 0.

7.2. **Modules sur les algèbres d'Azumaya.** Soient $\mathcal{A}$ une $\mathcal{O}_S$-algèbre (pas nécessairement commutative) et $\mathcal{L}$ un $\mathcal{A}$-module. On suppose que $\mathcal{A}$ et $\mathcal{L}$ sont des $\mathcal{O}_S$-modules localement libres de rang fini. Alors l'application

$$a \in \Gamma(T, \mathcal{A}) \mapsto \det(a|\mathcal{L}_T) \in \Gamma(T, \mathcal{O}_T)$$

induit un morphisme $\det(\bullet|\mathcal{L}) : \Gamma(\mathcal{A}) \to \Gamma(\mathcal{O}_S) = \mathbf{A}^1_S$, où $\Gamma(\mathcal{B})$ est le S-schéma (affine, lisse, en groupes commutatifs) qui représente le foncteur $T \mapsto \Gamma(T, \mathcal{B})$. Ce morphisme commute au changement de base : pour tout T/S ,

$$\det(\bullet|\mathcal{L})_T = \det(\bullet|\mathcal{L}_T) : \Gamma(\mathcal{A}_T) = \Gamma(\mathcal{A})_T \to \mathbf{A}^1_T.$$

Si $d : \Gamma(\mathcal{A}) \to \Gamma(\mathcal{O}_S)$ est un S-morphisme fixé, on peut définir un sous-foncteur

$$\mathcal{C}(d, \mathcal{L}) : (\mathbf{Sch}/S)^0 \to \mathbf{Ens}$$

du foncteur constant ponctuel S (qui à T/S associe le singleton $\mathrm{Hom}_S(T, S)$!) défini par la condition $\mathcal{C}(d, \mathcal{L})(T) \neq \emptyset$ si et seulement si $d_T = \det(\bullet|\mathcal{L})_T$. Si le morphisme d lui-même est de la forme $\det(\bullet|\mathcal{L}')$ pour un $\mathcal{A}$-module $\mathcal{L}'$ qui est localement libre sur S, on note $\mathcal{C}(\mathcal{L}', \mathcal{L})$ ce sous-foncteur, qui est donc défini par la condition

$$\mathcal{C}(\mathcal{L}', \mathcal{L})(T) \neq \emptyset \iff \det(\bullet|\mathcal{L}')_T = \det(\bullet|\mathcal{L})_T.$$

En général, j'ignore si ces foncteurs sont représentables, et je ne pense pas que ce soit le cas.

Definition 7.1. On dit que $\mathcal{A}$ est une $\mathcal{O}_S$-algèbre d'Azumaya si et seulement si $\mathcal{A}$ est, localement pour la topologie étale sur S, isomorphe à un produit d'algèbre $M_n(\mathcal{O}_S)$.

Proposition 7.2. *Soient $\mathcal{A}$ une $\mathcal{O}_S$-algèbre d'Azumaya et $\mathcal{L}_1$, $\mathcal{L}_2$ deux $\mathcal{A}$-modules qui sont des $\mathcal{O}_S$-modules localement libres. Alors pour tout T sur S, $\mathcal{C}(\mathcal{L}_1, \mathcal{L}_2)(T) \neq \emptyset$ si et seulement si localement pour la topologie étale sur T, $\mathcal{L}_{1,T} \simeq \mathcal{L}_{2,T}$ comme $\mathcal{A}_T$-modules. De plus, $\mathcal{C}(\mathcal{L}_1, \mathcal{L}_2)$ est alors représentable par un ouvert de S.*

Démonstration. Soit $S' \to S$ un revêtement étale tel que $\mathcal{A}_{S'} \simeq \prod_j M_{n_j}(\mathcal{O}_{S'})$. Pour tout T/S, on note $T' = T \times_S S'$: c'est un revêtement étale de T. Supposons que $\mathcal{C}(\mathcal{L}_1, \mathcal{L}_2)(T) \neq \emptyset$, donc $\mathcal{C}(\mathcal{L}_1, \mathcal{L}_2)(T') \neq \emptyset$. Soit $U = \mathrm{Spec}R$ un ouvert affine de T', donc $\mathcal{A}_U = \widetilde{A}$ avec $A = \prod_j M_{n_j}(R)$ et $\mathcal{L}_i = \widetilde{L_i}$ pour un A-module L_i qui est un R-module localement libre de rang fini, donc de la forme $L_i = \prod L_{i,j}$ où $L_{i,j}$ est un $M_{n_j}(R)$-module qui est un R-module localement libre de rang fini, donc - d'après l'équivalence de Morita - de la forme $R^{n_j} \otimes_R (L^0_{i,j})$ pour un R-module localement libre $L^0_{i,j}$. Quitte à restreindre encore U, on peut supposer que tous ces $L_{i,j}$ sont libres sur R, disons de rang $r_{i,j}$. Puisque $\mathcal{C}(\mathcal{L}_1, \mathcal{L}_2)(U) \neq 0$, $\det(a|L_1) = \det(a|L_2)$ pour tout $a \in A$, d'où l'on déduit facilement que $r_{1,j} = r_{2,j}$ pour tout j, donc $L_1 \simeq L_2$, donc $\mathcal{L}_{1,T'} \simeq \mathcal{L}_{2,T'}$ localement pour la topologie de Zariski sur T', donc $\mathcal{L}_{1,T} \simeq \mathcal{L}_{2,T}$ localement pour la topologie étale sur T. L'inverse est immédiat : si $\mathcal{L}_{1,T} \simeq \mathcal{L}_{2,T}$ après un changement de base fidèlement plat et quasi-compact $T' \to T$, alors $\det(\mathcal{L}_1)_{T'} = \det(\mathcal{L}_2)_{T'}$ donc $\det(\mathcal{L}_1)_T = \det(\mathcal{L}_2)_T$. Enfin, soit $\mathcal{L}_{i,S'} = \prod \mathcal{L}_{i,j}$

la décomposition de $\mathcal{L}_{i,S'}$ correspondant à $\mathcal{A}_{S'} = \prod_j M_{n_j}(\mathcal{O}_{S'})$, et soit $r_{i,j}$ le rang de $\mathcal{L}_{i,j}$. C'est une application continue de $S' \to \mathbf{N}$, donc

$$S'_0 = \{s' \in S' | \forall j : \quad r_{1,j}(s') = r_{2,j}(s')\}$$

est un ouvert de S', $S_0 = S - \pi(S' - S'_0)$ est un ouvert de S (puisque $\pi : S' \to S$ est fini donc fermé), et cet ouvert représente $\mathcal{C}(\mathcal{L}_1, \mathcal{L}_2)$ d'après la discussion précédente. □

Proposition 7.3. *Soient $\mathcal{A}$ une $\mathcal{O}_S$-algèbre d'Azumaya, $\mathcal{L}$ un $\mathcal{A}$-module qui est un $\mathcal{O}_S$-module localement libre et $d : \Gamma(\mathcal{A}) \to \mathbf{A}^1_S$ un S-morphisme qui est de la forme* $\det(\mathcal{L}')$ *localement pour la topologie fpqc. Alors $\mathcal{C}(d, \mathcal{L})$ est représentable par un ouvert de S.*

Démonstration. Exercice. □

7.3. **Rigidification des algèbres de Lie.** On reprend les notations des problèmes de type PEL. On se donne donc une $\mathbf{Q}$-algèbre semi-simple B et un $\mathbf{Z}$-ordre R de B, et on considère des S-schémas abéliens A munis d'une action $\iota : R \to \mathrm{End}(A)$ (il n'y a pas besoin de polarisations dans cette section). Soit $\mathcal{L} = \mathrm{Lie}(A)$: c'est un $\mathcal{O}_S$-module localement libre muni d'une action de la $\mathcal{O}_S$-algèbre localement libre (et même libre) $\mathcal{A} = R \otimes \mathcal{O}_S$. On voudrait rigidifier ce $\mathcal{A}$-module par une condition de déterminant.

Décomposons B en produit d'algèbre simple B_i de centre F_i et soit U l'ouvert de $\mathrm{Spec}\mathbf{Z}$ au-dessus duquel (1) R est maximal et (2) les F_i sont non-ramifiés. On fixe un premier $p \in U$, et on choisit pour chaque i une extension L_i de F_i qui décompose B_i et est non-ramifiée au-dessus de p (il en existe...). Soit L le produit de ces extensions et $\mathcal{O}$ l'anneau des p-entiers dans L. C'est donc une extension fini et *non-ramifiée* de $\mathbf{Z}_{(p)}$. Par construction, $R \otimes_{\mathbf{Z}} \mathcal{O}$ est un R-ordre maximal dans $B \otimes_{\mathbf{Q}} L \simeq \prod M_{n_i}(L)$, donc de la forme $\prod M_{n_i}(\mathcal{O})$. Ceci démontre que pour tout $p \in U$, $R \otimes \mathbf{Z}_{(p)}$ est une $\mathbf{Z}_{(p)}$-algèbre d'Azumaya. En travaillant un peu, on en déduit que $R \otimes \mathcal{O}_U$ est une $\mathcal{O}_U$-algèbre d'Azumaya mais nous n'en aurons pas vraiment besoin.

La proposition ci-dessus permet donc - si besoin est - d'affiner encore nos problèmes de modules, en se restreignant aux schémas abéliens A/S (munis d'une action de R) pour lesquels la structure de $\mathcal{A} = R \otimes \mathcal{O}_S$-module sur $\mathrm{Lie}A$ est essentiellement fixée par avance - mais il faut alors tout de même restreindre les-dits problèmes aux schémas S qui sont au-dessus de l'ouvert $U = U(R)$ de $\mathrm{Spec}\mathbf{Z}$ défini ci-dessus. En outre, il faut bien sûr être capable de *spécifier* le $\mathcal{A}$-module qui servira de modèle pour les algèbres de Lie, ou au moins son déterminant. C'est ce que nous allons faire dans la section suivante.

7.4. **Corps réflexe.** Soit V un B-module de $\mathbf{Q}$-dimension $2g$, G le $\mathbf{Q}$-groupe algébrique des automorphismes B-linéaires de V et $\mathcal{X} = G(\mathbf{R}) \cdot I$ une $G(\mathbf{R})$-orbite de structures complexes I sur $V_{\mathbf{R}}$ (i.e. $I \in G(\mathbf{R})$ et $I^2 = -1$). Pour tout $I \in \mathcal{X}$, on note $V_{\mathbf{R},I}$ le $B \otimes \mathbf{C}$-module défini par $(V_{\mathbf{R}}, I)$. La classe d'isomorphisme de ce module ne dépend pas du choix de I dans $\mathcal{X}$, puisque tout élément $g \in G(\mathbf{R})$ induit un isomorphisme de $B \otimes \mathbf{C}$-module $V_{\mathbf{R},I} \to V_{\mathbf{R},g \cdot I}$.

Fixons un ordre $R \subset B$, soit $\mathcal{A} = R \otimes \mathcal{O}_{\mathbf{Z}}$ et $d(\mathcal{X}) : \Gamma(\mathcal{A})_{\mathbf{C}} \to \mathbf{A}^1_{\mathbf{C}}$ le déterminant du $\mathcal{A}_{\mathbf{C}}$-module $V_{\mathbf{R},I}$ (pour n'importe quel $I \in \mathcal{X}$). Soit $L \subset \mathbf{C}$ un corps de nombre tel que $B \otimes L \simeq \prod M_{n_i}(L)$. Alors $B \otimes \mathbf{C} \simeq \prod M_{n_i}(\mathbf{C})$ donc $V_{\mathbf{R},I} \simeq \prod (\mathbf{C}^{n_i})^{r_i}$ et $V_{\mathbf{R},I} \simeq W \otimes_L \mathbf{C}$ pour $W = \prod (L^{n_i})^{r_i}$: le morphisme $d(\mathcal{X})$ est donc défini sur L.

Definition 7.4. Le corps réflexe $E = E(\mathcal{X})$ est le corps de définition de $d(\mathcal{X})$.

C'est donc un corps de nombre plongé dans $\mathbf{C}$, contenu dans tous les corps de nombres $L \subset \mathbf{C}$ qui décomposent B, mais qui est typiquement plus petit que leur intersection. Concrètement, c'est le sous-corps de $\mathbf{C}$ engendré par les $d(\mathcal{X})(a) = \det_{\mathbf{C}}(a|V_{\mathbf{R},I})$ pour tout $a \in R$. Avec les notations ci-dessus, on peut choisir dans le $B \otimes L$-module W un $\mathcal{O}_L$-réseau stable sous R, ce qui montre que $a \mapsto d(\mathcal{X})(a)$ atterrit en fait dans l'anneau des entiers $\mathcal{O}_E$ de E, i.e.

$$d(\chi) : \Lambda(\mathcal{A})_{\mathrm{Spec}\mathcal{O}_E} \to \mathbf{A}^1_{\mathrm{Spec}\mathcal{O}_E}.$$

Proposition 7.5. *Soit $p \in U(R)$, $\mathcal{O}$ l'anneau des p entiers dans $E(\mathcal{X})$, S un $\mathcal{O}$-schéma et A un S-schéma abélien muni d'une action de R. Alors*

$$\forall a \in R : \qquad \det(a|\mathrm{Lie}(A)) = d(\mathcal{X})(a)$$

est représentable par un ouvert de S.

En résumé, on peut spécifier le déterminant sur les algèbres de Lie, à condition de ne travailler qu'avec des schémas sur $U(R) \times \mathrm{Spec}\mathcal{O}_{E(\mathcal{X})}$: sur $U(R)$ pour que $\mathcal{A} = R \otimes \mathcal{O}_{\mathbf{Z}}$ soit d'Azumaya, sur $\mathcal{O}_{E(\mathcal{X})}$ pour que le "modèle du déterminant" soit bien défini.

Références

[1] J. Dieudonné, A. Grothendieck, *Eléments de Géométrie algébriques*, Publications de L'IHES.

[2] Kottwitz, *Zeta functions of some simple Shimura Varieties*

[3] D. Mumford, *Abelian Varieties.*

[4] J. Tate, *Finite Flat Group Schemes.*

POINTS COMPLEXES & EXEMPLES

Dans cette troisième partie du cours, nous allons étudier les points complexes des différents problèmes de modules que nous avons définis.

Première partie 1. **Exemples**

1. La catégorie des variétés abéliennes sur $\mathbf{C}$

Référence : le cours de M. Hindry, ou celui de Milne, ou [5].

1.1. Soit A une variété abélienne sur $\mathbf{C}$. Alors T_0A est un $\mathbf{C}$-espace vectoriel, et l'exponentielle $\exp : T_0A \to A$ est un morphisme de groupe surjectif dont le noyau est un réseau de T_0A. En particulier, A est un tore complexe V/Λ. On obtient ainsi : la catégorie des variétés abéliennes sur $\mathbf{C}$ est une sous-catégorie pleine de la catégorie des tores complexes.

1.2. Un tore complexe V/Λ est une variété abélienne si et seulement si il existe sur V une forme hermitienne $H : V \times V \to \mathbf{C}$ ($\mathbf{C}$-linéaire à gauche par convention) qui est (1) définie positive et (2) dont la partie imaginaire prend des valeurs entières sur Λ.

1.3. Toute forme sesquilinéaire $H : V \times V \to \mathbf{C}$ se décompose en

$$H(x, y) = \phi(x, y) + i\psi(x, y)$$

avec $\phi, \psi : V \times V \to \mathbf{R}$ bilinéaires, $\phi(x, y) = \psi(ix, y)$ et $\phi(x, y) = -\psi(x, iy)$, donc $\psi(ix, iy) = \psi(x, y)$. Inversement, tout $\psi : V \times V \to \mathbf{R}$ tel que $\psi(ix, iy) = \psi(x, y)$ définit une forme sesquilinéaire

$$H(x, y) = \psi(ix, y) + i\psi(x, y).$$

On a (1) H est non-dégénérée si et seulement si ψ l'est, (2) H est hermitienne (i.e $H(x, y) = \overline{H(y, x)}$) si et seulement si ψ est anti-symétrique, et (3) H est hermitienne définie positive si et seulement si ψ est anti-symétrique et $\psi(ix, y)$ (symétrique et) définie positive.

1.4. Pour un tore complexe $X = V/\Lambda$, on pose $X^t = V^{\iota\star}/\Lambda^\star$ où

$$V^{\iota\star} = \mathrm{Hom}_{\mathbf{C}}(V^\iota, \mathbf{C}) \quad \text{et} \quad \Lambda^\star = \{f \in V^{\iota\star} | \mathrm{im} f(\Lambda) \subset \mathbf{Z}\}.$$

Les morphismes $\lambda : X \to X^t$ correspondent aux morphismes $\mathbf{C}$-linéaires $v \mapsto H(v, \bullet)$ de V dans $V^{\star\iota}$ qui envoie Λ dans $\Lambda^\star$, donc au formes bilinéaires $\psi : \Lambda \times \Lambda \to \mathbf{Z}$ tels que $\psi_{\mathbf{R}}(ix, iy) = \psi_{\mathbf{R}}(x, y)$. On a : (1) λ est une isogénie si et seulement si ψ est non-dégénéré, (2) $\lambda^t = \lambda$ si et seulement si ψ est symplectique, (3) λ est une polarisation si et seulement ψ est simplectique et $\psi_{\mathbf{R},i}(x, y) = \psi_{\mathbf{R},i}(x, y)$ est (symétrique et définie positive).

1.5. La catégorie des tores complexes est équivalente à la catégorie des paires (Λ, I) où Λ est un réseau (i.e. un $\mathbf{Z}$-module libre de rang fini) et I une structure complexe sur le $\mathbf{R}$-espace vectoriel $V = \Lambda \otimes \mathbf{R}$: le tore complexe associé est $X = V_I/\Lambda$, où V_I est le $\mathbf{R}$-espace vectoriel V muni de sa structure complexe I. Une *polarisation* de (Λ, I) est une forme symplectique $\psi : \Lambda \times \Lambda \to \mathbf{R}$ telle que (1) $\psi_{\mathbf{R}}(Ix, Iy) = \psi_{\mathbf{R}}(x, y)$ et (2) $\psi_{\mathbf{R},I}(x, y) = \psi_{\mathbf{R}}(Ix, y)$ est (symétrique et) définie positive. La catégorie des variétés abéliennes sur $\mathbf{C}$ est équivalente à la catégorie des paires (Λ, I) qui sont *polarisables*.

1.6. La catégorie des variétés abéliennes polarisées est équivalentes à la catégorie des triplets (Λ, ψ, I) où Λ est un réseau, $\psi : \Lambda \times \Lambda \to \mathbf{Z}$ une forme symplectique et I une structure complexe sur $V = \Lambda \otimes \mathbf{R}$ telle que (1) $I \in \mathbf{Sp}(V, \psi_{\mathbf{R}})$ et (2) $\psi_{\mathbf{R},I} > 0$. La variété abélienne associée est $A = V_I/\Lambda$, sa variété abélienne duale est $A^t = V_I^{\star\iota}/\Lambda^\star$, la polarisation $\lambda : A \to A^t$ est le morphisme $v \mapsto H(v, \star)$ où $H : V \times V \to \mathbf{C}$ est la forme hermitienne (définie positive) induite par ψ, le module de Tate est

$$T_f A = T_f(A, \mathbf{C}) = \varprojlim n^{-1}\Lambda/\Lambda \simeq \widehat{\Lambda}$$

et l'accouplement de Weil $\langle \bullet, \bullet \rangle_f^\lambda : T_f A \times T_f A \to T_f \mu$ est

$$\forall x, y \in T_f A \simeq \widehat{\Lambda} : \qquad \langle x, y \rangle_f^\lambda = \xi^{\widehat{\psi}(x,y)}$$

où $\xi = \varprojlim \exp(\frac{2i\pi}{n}) \in T_f \mu$.

1.7. De même : la catégorie des tores complexes à isogénie près est équivalente à la catégorie des paires (V, I) où V est un $\mathbf{Q}$-espace vectoriel de dimension finie et I une structure complexe sur $V_{\mathbf{R}} = V \otimes \mathbf{R}$, une polarisation d'une telle structure est une forme symplectique $\psi : V \times V \to \mathbf{Q}$ telle que (1) $I \in \mathbf{Sp}(V_{\mathbf{R}}, \psi_{\mathbf{R}})$ et (2) $\psi_{\mathbf{R},I} > 0$, et la catégorie des variétés abéliennes sur $\mathbf{C}$ à isogénie près est équivalente à celle des paires (V, I) qui sont polarisables.

2. Exemple n°1 : Courbes Modulaires

On veut ici calculer les $\mathbf{C}$-points du schéma $\mathbf{M} = \mathbf{M}^1_{1,n} = Y(n)$. Il nous faut donc classifier les courbes elliptiques E sur $\mathbf{C}$, munies d'une polarisation principale (= de degré 1) et d'une structure de niveau n : $\kappa : (\mathbf{Z}/n\mathbf{Z})^2 \simeq E[n]$. Il revient donc au même de classifier les quadruplets $(\Lambda, \psi, I, \kappa)$ où Λ est un réseau de rang 2, ψ une forme symplectique parfaite sur Λ, I une structure complexe sur $(\Lambda_{\mathbf{R}}, \psi_{\mathbf{R}})$ telle que $\psi_{\mathbf{R},I} > 0$, et κ un isomorphisme $(\mathbf{Z}/n\mathbf{Z})^2 \simeq n^{-1}\Lambda/\Lambda$.

Il n'y a qu'une classe d'isomorphisme de $\mathbf{Z}$-module libre de rang 2 : $\Lambda = \mathbf{Z}^2$. Sur $\mathbf{Z}^2$, il y a exactement 2 formes bilinéaires alternées parfaites, données par $\pm \det$, et ces deux formes sont conjuguées par n'importe quel élément de déterminant -1 dans $GL_2(\mathbf{Z})$. Il n'y a donc qu'une classe d'isomorphisme de couple (Λ, ψ), celle de $(\Lambda, \psi) = (\mathbf{Z}^2, \mathbf{det})$ (où le déterminant est calculé dans la base canonique de $\mathbf{Z}^2$). Le groupe des automorphismes de (Λ, ψ) est $\Gamma = \mathbf{SL}_2(\mathbf{Z})$.

Il est bien connu que $\mathbf{SL}_2(\mathbf{Z}) \to \mathbf{SL}_2(\mathbf{Z}/n\mathbf{Z})$ est surjective. Les Γ-orbites de structure de niveau κ sont donc indexées par le quotient

$$\mathbf{GL}_2(\mathbf{Z}/n\mathbf{Z})/\mathbf{SL}_2(\mathbf{Z}/n\mathbf{Z}) \simeq (\mathbf{Z}/n\mathbf{Z})^\times.$$

Le stabilisateur (commun) des κ est le sous-groupe de congruence $\Gamma(n)$ de $\Gamma(1) = \Gamma$ formé des matrices $g \in \mathbf{SL}_2(\mathbf{Z})$ telles que $g \equiv Id \bmod n$.

Enfin, toutes les structures complexes I sur $\Lambda \otimes \mathbf{R} = \mathbf{R}^2$ induisent sur ce $\mathbf{R}$-espace vectoriel une structure de $\mathbf{C}$-espace vectoriel de dimension 1 : toutes ces structures sont donc conjuguées par un élément de $\mathbf{GL}_2(\mathbf{R})$. Il y a en revanche exactement deux $\mathbf{SL}_2(\mathbf{R})$-orbites, qui correspondent à l'orientation de (x, Ix). Les formes $\psi_{\mathbf{R},I}$ sont donc définies positives sur l'une de ces deux orbites, et définies négatives sur l'autre. Pour $I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$,

$$\psi_{\mathbf{R},I}\left(\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}\right) = \det\begin{pmatrix} x_1 & -y_2 \\ y_1 & x_2 \end{pmatrix} = x_1x_2 + y_1y_2$$

est définie positive, et le stabilisateur K_I de I dans $\mathbf{SL}_2(\mathbf{R})$ est $K_I = \mathbf{SO}_2(\mathbf{R})$. Donc :

$$\mathbf{M}(\mathbf{C}) = \coprod_{(\mathbf{Z}/n\mathbf{Z})^\times} \Gamma(n)\backslash\mathbf{SL}_2(\mathbf{R})/\mathbf{SO}_2(\mathbf{R}).$$

Identifiant $\mathbf{SL}_2(\mathbf{R})/\mathbf{SO}_2(\mathbf{R})$ au demi-plan supérieur $\mathcal{H} = \{\tau \in \mathbf{C} : \mathrm{im}\tau > 0\}$ par $g \mapsto g \cdot i$ (pour l'action usuelle de $\mathbf{GL}_2(\mathbf{R})$ sur $\mathbf{C} - \mathbf{R}$), on voit donc que $\mathbf{M}(\mathbf{C})$ est la réunion disjointe indexée par $(\mathbf{Z}/n\mathbf{Z})^\times$ de copies de $Y(n) = \Gamma(n)\backslash\mathcal{H}$.

Exercise 2.1. Lorsque $n \geq 3$, on sait qu'il existe sur $Y(n)$ une courbe elliptique universelle et une structure de niveau n. Décrire ces objets.

Remark 2.2. On peut interpréter l'ensemble $(\mathbf{Z}/n\mathbf{Z})^\times$ des composantes connexes directement sur le problème de module. Pour tout schéma S et toute courbe elliptique E/S, l'accouplement de Weil $e : E[n] \times_S E^t[n] \to \mu_{n,S}$ est une forme bilinéaire alternée parfaite. Le choix d'une base x_1, x_2 de $(\mathbf{Z}/n\mathbf{Z})^2$, permet donc d'associer à tout élément (E, λ, κ) de $\mathbf{M}(S)$ l'élément $e(x_1, \lambda(x_2))$ de $\mu_n(S)$. On atterrit en fait dans $\mu_n^\star(S)$, où $\mu_n^\star$ est le sous-foncteur des générateurs de μ_n. On obtient un morphisme $\mathbf{M} \to \mu_n^\star$ qui donne en passant aux points complexes une application $\mathbf{M}(\mathbf{C}) \twoheadrightarrow \mu_n^\star(\mathbf{C})$: c'est ce que l'on cherchait, puisque $\mu_n^\star(\mathbf{C})$ est un $(\mathbf{Z}/n\mathbf{Z})^\times$-torseur. Mentionnons que sur $\mathbf{Z}$, le foncteur $\mu_n^\star$ est représentable par $\mathrm{Spec}\mathcal{O}(\mu_n)$ où $\mathcal{O}(\mu_n)$ est l'anneau des entiers de l'extension cyclotomique $\mathbf{Q}(\mu_n)$ de $\mathbf{Q}$. Mentionnons aussi que $Y(n) \to \mu_n^\star$ n'est autre que la restriction à $Y(n)$ de la factorisation de Stein du morphisme structural $X(n) \to \mathrm{Spec}\mathbf{Z}$, où $X(n)$ est la compactification classique de $Y(n)$, construite en rajoutant des cusp à l'infini. Cf. [2].

3. Exemple n°2 : La variété de Siegel $\mathbf{M}_{1,n}^g$

Il s'agit maintenant de classifier les variétés abéliennes sur $\mathbf{C}$ de dimension g munie d'une polarisation principale et d'une structure de niveau n, ou, ce qui revient au même, les quadruplets $(\Lambda, \psi, I, \kappa)$ où Λ est un $\mathbf{Z}$-réseau de dimension $2g$, $\psi : \Lambda \times \Lambda \to \mathbf{Z}$ une forme symplectique parfaite, I une structure complexe sur $(\Lambda \otimes \mathbf{R}, \psi_{\mathbf{R}})$ telle que $\psi_{\mathbf{R},I} > 0$ et $\kappa : (\mathbf{Z}/n\mathbf{Z})^{2g} \xrightarrow{\simeq} n^{-1}\Lambda/\Lambda$.

Tout espace symplectique (Λ, ψ) admet une base de Witt, et il n'y a donc qu'une classe d'isomorphisme. Soit $G = \mathbf{Sp}(\Lambda, \psi)$ le $\mathbf{Z}$-groupe algébrique (lisse) des automorphismes de (Λ, ψ), donc $\mathrm{Aut}(\Lambda, \psi) = G(\mathbf{Z})$. Puisque G est lisse, $G(\mathbf{Z}) \to G(\mathbf{Z}/n\mathbf{Z})$ est surjectif : les classes d'isomorphismes de triplets (Λ, ψ, κ) sont donc indexées par le quotient

$$\mathcal{S} = \mathbf{GL}_{2g}(\mathbf{Z}/n\mathbf{Z})/\mathbf{Sp}_{2g}(\mathbf{Z}/n\mathbf{Z})$$

et $\mathrm{Aut}(\Lambda, \psi, \kappa) = \Gamma(n) = \ker(G(\mathbf{Z}) \to G(\mathbf{Z}/n\mathbf{Z}))$. Toutes les structures complexes I sur $(\Lambda \otimes \mathbf{R}, \psi_{\mathbf{R}})$ telles que $\psi_{\mathbf{R},I} > 0$ sont conjuguées sous $G(\mathbf{R})$. En effet, si I_1

et I_2 sont deux telles structures, elles définissent avec $\psi_{\mathbf{R}}$ deux espaces hermitiens $(\Lambda \otimes \mathbf{R}, I_j, H_j)$ avec $H_j > 0$. Ces deux espaces hermitiens sont alors isomorphes, ce qui signifie qu'il existe un isomorphisme $\mathbf{R}$-linéaire $g : \Lambda \otimes \mathbf{R} \to \Lambda \otimes \mathbf{R}$ tel que $H_2(gx, gy) = H_1(x, y)$ et $gI_1 = I_2 g$. Puisque $\mathrm{im} H_j = \psi_{\mathbf{R}}$, $g \in G(\mathbf{R})$ et $I_2 = gI_1g^{-1}$. Finalement,

$$\mathbf{M}(\mathbf{C}) = \coprod_{\mathcal{S}} \Gamma(n)\backslash\mathcal{X} = \coprod_{\mathcal{S}} \Gamma(n)\backslash G(\mathbf{R})/K_I$$

où $\mathcal{X} = G(\mathbf{R}) \cdot I$ et K_I est le stabilisateur de I.

4. Exemple n°3 : Endomorphismes

On se donne une $\mathbf{Q}$-algèbre semi-simple B avec une involution $\star$, un ordre $\mathcal{O}_B$ dans B stables sous $\star$, et on veut classifier les variétés abéliennes sur $\mathbf{C}$ de dimension g, munies d'une action de $\mathcal{O}_B$, d'une polarisation $(\mathcal{O}_B, \star)$-linéaire de degré d^2, et d'une structure de niveau n naïve. Il revient au même de classifier les quadruplets $(\Lambda, \psi, \kappa, I)$ où Λ est une $\mathcal{O}_B$-module qui est libre de rang $2g$ sur $\mathbf{Z}$, $\psi : \Lambda \times \Lambda \to \mathbf{Z}$ une $(\mathcal{O}_B, \star)$- forme symplectique avec $\left|\Lambda^\perp/\Lambda\right| = d^2$, $\kappa : (\mathbf{Z}/n\mathbf{Z})^{2g} \simeq n^{-1}\Lambda/\Lambda$ est un isomorphisme, et I une structure complexe $B \otimes \mathbf{R}$-linéaire sur $(V_{\mathbf{R}}, \psi_{\mathbf{R}})$ telle que $\psi_{\mathbf{R},I} > 0$ (où $V = \Lambda \otimes \mathbf{Q}$).

4.1. **Décomposition naïve.** Regroupant ces quadruplets en fonction de la classe d'isomorphisme des trois premières composantes, on trouve

$$\mathbf{M}(\mathbf{C}) = \coprod_{(\Lambda,\psi,\kappa)/\sim} \mathbf{M}(\Lambda, \psi, \kappa)$$

où pour chaque (Λ, ψ, κ) vérifiant les trois premières conditions ci-dessus, $\mathbf{M}(\Lambda, \psi, \kappa)$ est l'ensemble des structures complexes I vérifiant la dernière condition, modulo les automorphismes du triplet (Λ, ψ, κ). Soit $G = \mathbf{Aut}(\Lambda, \psi)$ le $\mathbf{Z}$-schéma en groupe des automorphismes ($\mathcal{O}_B$-linéaires) de (Λ, ψ). C'est un schéma en groupe de type fini sur $\mathbf{Z}$, et le groupe des automorphismes de (Λ, ψ) est le sous-groupe discret $\Gamma = G(\mathbf{Z})$ de $G(\mathbf{Q}) \subset G(\mathbf{R})$. Le stabilisateur de κ dans Γ est le groupe de congruence

$$\Gamma(n) = \ker\left(G(\mathbf{Z}) \to G(\mathbf{Z}/n\mathbf{Z})\right)$$

de $\Gamma = \Gamma(1)$. Les structures complexes I recherchées sont les éléments de $G(\mathbf{R})$ (i.e. les automorphismes $B \otimes \mathbf{R}$-linéaires de $(\Lambda_{\mathbf{R}}, \psi_{\mathbf{R}})$) tels que $I^2 = -1$ et $\psi_{\mathbf{R},I} > 0$. Le groupe $G(\mathbf{R})$ agit sur cet ensemble par conjugaison. Regroupant ces structures complexes en fonction de leur classe de $G(\mathbf{R})$-conjugaison, on trouve donc

$$\mathbf{M}(\Lambda, \psi, \kappa) = \coprod_{I/\sim} \Gamma(n)\backslash\mathcal{X}(I) \quad \text{où } \mathcal{X}(I) = \mathrm{Ad}(G(\mathbf{R})) \cdot I = G(\mathbf{R})/K_I$$

où K_I est le commutant de I dans $G(\mathbf{R})$: c'est un sous-groupe fermé de $G(\mathbf{R})$ qui est contenu dans le groupe spécial orthogonal $SO(\Lambda_{\mathbf{R}}, \psi_{\mathbf{R},I})$, et qui est donc compact puisque $\psi_{\mathbf{R},I} > 0$. On a ainsi obtenu une décomposition

$$\mathbf{M}(\mathbf{C}) = \coprod_{(\Lambda,\psi,\kappa)/\sim} \coprod_{I/\sim} \Gamma(n)\backslash\mathcal{X}(I).$$

Remark 4.1. Il se trouve que les $G(\mathbf{R})$ sont *connexes,* et que la décomposition ci-dessus est un homéomorphisme si l'on munit chacun des $\Gamma(n)\backslash\mathcal{X}(I) = \Gamma(n)\backslash G(\mathbf{R})/K_I$ de la topologie quotient de celle de $G(\mathbf{R})$. Cette décomposition est donc la décomposition en composantes connexes de $\mathbf{M}(\mathbf{C})$! Si l'on savait déjà que $\mathbf{M}$ est de type fini sur Spec$\mathbf{Z}$ (c'est vrai, mais nous ne l'avons pas démontré), on obtiendrait comme corollaire du calcul ci-dessus un énoncé de finitude : l'ensemble de classes d'isomorphismes qui indexent la décomposition de $\mathbf{M}(\mathbf{C})$ est fini.

4.2. **Décomposition un peu moins naïve.** On regroupe cette fois-ci nos quadruplets en fonction de la *classe d'isomorphisme* du couple (V,ψ), ce qui nous donne une décomposition

$$\mathbf{M}(\mathbf{C}) = \coprod_{[V,\psi]} \mathbf{M}([V,\psi]).$$

Fixons $[V,\psi]$. Soit $G = \mathbf{Sp}_B(V,\psi)$, c'est un $\mathbf{Q}$-groupe algébrique et $\mathrm{Aut}_B[V,\psi] = G(\mathbf{Q})$. On ajoute ensuite (Λ,κ) et I. Le groupe $G(\mathbf{A}_f)$ agit sur l'ensemble des (Λ,κ) par $g(\Lambda,\kappa) = (g\Lambda, g\kappa)$ où $g\Lambda = g\cdot\widehat{\Lambda}\cap V$ et

$$g\kappa : (g \bmod n)\circ\kappa : (\mathbf{Z}/n\mathbf{Z})^{2g} \to n^{-1}\Lambda/\Lambda = n^{-1}\widehat{\Lambda}/\widehat{\Lambda} \to n^{-1}g\cdot\widehat{\Lambda}/g\cdot\widehat{\Lambda} = n^{-1}g\Lambda/\Lambda.$$

Le groupe $G(\mathbf{R})$ agit sur l'ensemble des I par conjugaison. On regroupe ces structures en fonction de leur $G(\mathbf{A}_f)\times G(\mathbf{R}) = G(\mathbf{A})$-orbites, ce qui nous donne

$$\mathbf{M}([V,\psi]) = \coprod_{\mathcal{X}_f,\mathcal{X}_\infty} G(\mathbf{Q})\backslash(\mathcal{X}_f\times\mathcal{X}_\infty) \quad \text{où} \quad \begin{cases} \mathcal{X}_f = G(\mathbf{A}_f)\cdot(\Lambda,\kappa) & = G(\mathbf{A}_f)/K_f \\ \mathcal{X}_\infty = G(\mathbf{R})\cdot I & = G(\mathbf{R})/K_I \end{cases}$$

où K_f est le stabilisateur (ouvert compact) de (Λ,κ) dans $G(\mathbf{A}_f)$ et K_I le stabilisateur (compact, puisque contenu dans $\mathbf{SO}(\psi_{\mathbf{R},I})$) de I dans $G(\mathbf{R})$. On a donc décomposé $\mathbf{M}(\mathbf{C})$ en un produit de

$$G(\mathbf{Q})\backslash\left(G(\mathbf{A}_f)/K_f\times\mathcal{X}_\infty\right) = G(\mathbf{Q})\backslash G(\mathbf{A})/K_fK_I.$$

4.3. **Conclusion.** On voudrait découper dans $\mathbf{M}$ des sous-foncteurs ouverts et fermés, dont les $\mathbf{C}$-points seraient une réunion d'un petit nombre de composantes connexes de $\mathbf{M}(\mathbf{C})$. Il nous faut pour cela savoir attacher à tout quadruplet (A,ι,λ,κ) de $\mathbf{M}(S)$ (sur une base S beaucoup plus générale que Spec$\mathbf{C}$) des invariants qui, spécialisés à $S = $ Spec$\mathbf{C}$, déterminent au mieux la classe d'isomorphisme des triplets (Λ,ψ,κ) (auxquels il faut si possible adjoindre la classe de $G(\mathbf{R})$-conjugaison de I, où $G = \mathrm{Aut}(\Lambda,\psi)$ n'est à priori défini que lorsqu'on a déjà fixé Λ et ψ).

Le point de départ est $\Lambda = H_1(A,\mathbf{Z})$: la théorie cohomologique correspondant à ce H_1 est la cohomologie de Betti (de la variété topologique sous-jacente à $A(\mathbf{C})$), qui n'a donc aucun sens à priori sur une base S quelconque. Sur une base générale, on dispose cependant de deux théories cohomologiques qui permettent de palier partiellement à l'absence de Betti : la *cohomologie étale* - qui apparaîtra plus bas sous le déguisement des modules de Tate T_pA, et la *cohomologie de de Rham*, qui sera de même avantageusement remplacée par l'algèbre Lie$A$.

5. Exemple n°4 : Variétés de type PEL

Soit B une $\mathbf{Q}$-algèbre semi-simple avec une involution $\star$, V un B-module de type fini, $\psi : V\times V\to\mathbf{Q}$ une forme symplectique induisant $\star$ sur B, $G = \mathbf{GSp}(V,\psi)$ le groupe des similitudes symplectiques B-linéaire de (V,ψ), K un sous-groupe ouvert compact de $G(\mathbf{A}_f)$, et $\mathcal{X}$ une $G(\mathbf{R})$-orbite de structures complexes I sur $(V_{\mathbf{R}},\psi_{\mathbf{R}})$ telle que $\pm\psi_{\mathbf{R},I} > 0$[1]. On veut classifier les variétés abéliennes A sur $\mathbf{C}$ à isogénie près, munies d'une action $\iota : B\to\mathrm{End}^0_{\mathbf{C}}(A)$, d'une droite $\mathbf{Q}\lambda\subset\mathrm{Hom}^0(A,A^t)$ où $\lambda : A\to A^t$ est une polarisation qui est $(B,\star)$-linéaire, et d'une structure de

[1]La condition $\psi_{\mathbf{R},I} > 0$ est stable par $\mathbf{Sp}(V,\psi)$, mais pas par $\mathbf{GSp}(V,\psi)$.

niveau K, i.e. d'une K-orbite d'isomorphismes B-linéaires $\kappa : \widehat{V} \to V_f A = V_f(A, \mathbf{C})$ compatible modulo un isomorphisme $\mathbf{A}_f \simeq V_f \mu$ avec les accouplements $\widehat{\psi} : \widehat{V} \times \widehat{V} \to \mathbf{A}_f$ et $\langle \bullet, \bullet \rangle_f^\lambda : V_f A \times V_f A \to V_f \mu$. On demande en plus que $\mathbf{Lie}(A) \simeq (V_\mathbf{R}, I)$ comme $B \otimes \mathbf{C}$-module.

Il revient au même de classifier les quadruplets $(W, J, \mathbf{Q}\phi, \kappa K)$ où W est un B-module de type fini, J une structure complexe sur le $B_\mathbf{R}$-module $W_\mathbf{R}$ telle que $(V_\mathbf{R}, I) \simeq (W_\mathbf{R}, J)$ comme $B \otimes \mathbf{C}$-modules, $\phi : W \times W \to \mathbf{Q}$ une polarisation de (W, J) (i.e. une forme symplectique induisant $\star$ sur B telle que (1) $\phi_\mathbf{R}(Jx, Jy) = \phi_\mathbf{R}(x, y)$ et (2) $\phi_{\mathbf{R},I} > 0$), et $\kappa : \widehat{V} \to \widehat{W}$ est un isomorphisme E-linéaire qui envoie $\mathbf{A}_f^\times \widehat{\psi}$ sur $\mathbf{A}_f^\times \widehat{\phi}$.

La structure de niveau détermine la classe de $\mathbf{Q}_p$-similitude des B_p-modules symplectiques : $(V_p, \mathbf{Q}_p^\times \psi_p) \simeq (W_p, \mathbf{Q}_p^\times \phi_p)$ pour tout nombre premier p. De même, nous verrons plus bas que l'isomorphisme de $B \otimes \mathbf{C}$-module $(V_\mathbf{R}, I) \simeq (W_\mathbf{R}, J)$ et les conditions $\pm\psi_{\mathbf{R},I} > 0$, $\phi_{\mathbf{R},J} > 0$ déterminent la classe d'isomorphisme des triplets $(V_\mathbf{R}, I, \pm\psi_{\mathbf{R},I}) \simeq (W_\mathbf{R}, J, \phi_{\mathbf{R},J})$, donc aussi la classe d'isomorphisme des triplets $(V_\mathbf{R}, \pm\psi_\mathbf{R}, I) \simeq (W_\mathbf{R}, \phi_\mathbf{R}, J)$, et a fortiori la classe de $\mathbf{R}$-similitude des $B_\mathbf{R}$-modules symplectiques : $(V_\mathbf{R}, \mathbf{R}^\times \psi_\mathbf{R}) \simeq (W_\mathbf{R}, \mathbf{R}^\times \phi_\mathbf{R})$.

Si les $\mathbf{Q}$-similitudes de B-modules symplectiques vérifient *le principe de Hasse*, les données ci-dessus déterminent donc uniquement la classe d'isomorphisme de $(V, \mathbf{Q}^\times \psi) \simeq (W, \mathbf{Q}^\times \phi)$. Il nous reste alors à classifier, modulo $\mathrm{Aut}(V, \mathbf{Q}^\times \psi) = G(\mathbf{Q})$, les données $(\kappa K, J)$ où κ est maintenant un isomorphisme de $(\widehat{V}, \mathbf{A}_f^\times \widehat{\psi})$ (i.e. un élément de $G(\mathbf{A}_f)$) et J une structure complexe sur le $B_\mathbf{R}$-module symplectique $(V_\mathbf{R}, \psi_\mathbf{R})$ telle que $\pm\psi_{\mathbf{R},J} > 0$ et $(V_\mathbf{R}, I) \simeq (V_\mathbf{R}, J)$ comme $B \otimes \mathbf{C}$-module. Mais alors à nouveau $(V_\mathbf{R}, I, \pm\psi_{\mathbf{R},I}) \simeq (V_\mathbf{R}, J, \pm\psi_{\mathbf{R},J})$, donc aussi $(V_\mathbf{R}, I, \pm\psi_\mathbf{R}) \simeq (V_\mathbf{R}, J, \pm\psi_\mathbf{R})$: il existe un automorphisme de $(V_\mathbf{R}, \mathbf{R}^\times \psi_\mathbf{R})$ (i.e. un élément de $G(\mathbf{R})$) qui conjugue I et J, donc $J \in \mathcal{X}$. Finalement :

$$\mathbf{M}(\mathbf{C}) = G(\mathbf{Q}) \backslash \left(G(\mathbf{A}_f)/K \times \mathcal{X} \right).$$

Si le principe de Hasse est en défaut, on obtient une réunion finie de telles composantes, correspondant à des espaces $(W, \mathbf{Q}^\times \phi)$ qui sont partout localement isomorphes à $(V, \mathbf{Q}^\times \psi)$.

Deuxième partie 2. Classification(s)

On se propose ici de décrire, pour $F = \mathbf{Q}$, les ensembles suivants :

$\mathcal{A}(F)$ les classes d'isomorphismes de F-algèbres semi-simples A.

Pour tout $[A] \in \mathcal{A}(F)$,

$\mathcal{I}(A)$ les classes d'isomorphismes d'involution $\star$ sur A.

$\mathcal{P}(A)$ les classes d'isomorphismes de A-modules V de F-dimension finie.

Pour tout $[\star] \in \mathcal{I}(A)$, $[V] \in \mathcal{P}(A)$ et u dans $U = \{u \in Z(A) | u^\star u = 1\}$,

$\mathcal{H}(A, \star, u)(V)$ les classes d'isomorphismes de formes u-hermitiennes ψ sur V.

On en déduira une description de

$\mathcal{A}'(F)$ les classes d'isomorphismes de F-algèbres semi-simples à involution $(A, \star)$,

Et, pour tout $[A, \star] \in \mathcal{A}'(F)$,

$\mathcal{H}(A, \star, u)$ les classes d'isomorphismes de $(A, \star)$-espaces u-hermitiens

On note également

$I(A)$ l'ensemble des involutions de A et

$H(A,\star,u)(V)$ l'ensemble des formes u-hermitiennes ψ sur V.

Les définitions de ces objets et des isomorphismes entre iceux seront données en temps voulu. Dans les énoncés, le corps F sera toujours supposé parfait. Le plus souvent, F sera : un corps fini, un corps local non-archimédien ou archimédien, un corps de nombre, ou un corps algébriquement clos.

Note 5.1. Tout cela ne devrait guère servir dans la suite du cours !

6. Algèbres semi-simples

On ne donne pas de preuve ici, mais une référence : le cours de Milne [4].

6.1. **Décomposition.**

Proposition 6.1. *Toute F-algèbre semi-simple A est un produit fini de F-algèbres simples, et toute F-algèbre simple est isomorphe à une algèbre de matrice sur une F-algèbre à division de dimension finie. Donc*

$$A = A_1 \times \cdots \times A_r \quad \text{avec } A_i \simeq M_{n_i}(D_i)$$

où D_i est un corps gauche de centre C_i, une extension finie de F.

Corollary 6.2. *Il y a une bijection entre* (1) *les composantes simples A_i de A,* (2) *les composantes simples $Z(A_i) \simeq C_i$ du centre $Z(A)$ de A, et* (3) *les idempotents centraux minimaux 1_{A_i} de A.*

6.2. **Classification.** Pour compléter l'étude de $\mathcal{A}(F)$, il reste à classifier les F-algèbres à division, ce qui revient à déterminer l'ensemble $\mathrm{Br}(K)$ des classes d'isomorphismes de corps gauche de centre K pour toute extension K de F. Dans ce qui suit, on prend $K = F$.

On dit que deux F-algèbres centrales simples A_1 et A_2 sont Brauer, ou Morita équivalentes si $A_1 \simeq M_{n_1}(D)$ et $A_2 \simeq M_{n_2}(D)$ pour un même corps gauche D (de centre $Z(D) = F$). Cette relation est compatible avec le produit tensoriel, qui munit donc l'ensemble $\mathrm{Br}(F)$ des classes d'équivalences de F-algèbre centrale simple d'une structure de monoide, et même de groupe puisque $D \otimes D^o \sim F$. Ce groupe admet une interprétation cohomologique

$$\mathrm{Br}(F) \simeq H^2(F, \mathbf{G}_m).$$

On a $\mathrm{Br}(F) = 0$ si F est fini (théorème de Wedderburn) ou si F est algébriquement clos. La proposition qui suit est intimement liée à la théorie du corps de classe.

Theorem 6.3. *Pour les corps qui nous intéressent :*

(1) *Si F est un corps local non-archimédien,*

$$H^2(F, \mathbf{G}_m) \leftarrow H^2_{nr}(F, \mathbf{G}_m) \leftarrow H^1_{nr}(F, \mathbf{Z}) \leftarrow H^0_{nr}(F, \mathbf{Q}/\mathbf{Z})$$

induit un isomorphisme $\mathrm{inv} : \mathrm{Br}(F) \simeq \mathbf{Q}/\mathbf{Z}$. *Si $[D : F] = d^2$, alors*

$$\mathrm{inv} D = \frac{r}{d} \bmod \mathbf{Z} \quad \text{avec } (r, d) = 1.$$

(2) *Si F est un corps local archimédien,*

$$H^2(F, \mathbf{G}_m) = \begin{cases} \{0\} & si\ F \simeq \mathbf{C} \\ \frac{1}{2}\mathbf{Z}/\mathbf{Z} & si\ F \simeq \mathbf{R} \end{cases}$$

qui donne encore un morphisme $\mathrm{inv} : \mathrm{Br}(F) \hookrightarrow \mathbf{Q}/\mathbf{Z}$.

(3) *Si F est un corps global, les morphismes* $\mathrm{Br}(F) \to \mathrm{Br}(F_v)$ *induisent*

$$\mathrm{Br}(F) \simeq \ker \left(\sum_v \mathrm{inv}_v : \oplus \mathrm{Br}(F_v) \to \mathbf{Q}/\mathbf{Z} \right).$$

Corollary 6.4. *Soit $A = M_n(D)$ une F-algèbre centrale simple. Les conditions suivantes sont équivalentes : (1) $A \simeq A^{opp}$ comme F-algèbre, (2) $2[A] = 0$ dans $\mathrm{Br}(F)$, (3) $2[D] = 0$ dans $\mathrm{Br}(F)$, (4) $D \simeq D^{opp}$ comme F-algèbre, (5) $D = F$ ou D est un corps de quaternions sur F.*

Démonstration. Les implications (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) sont évidentes. Supposons donc (4) et soit $d^2 = [D : F]$. Si F est local, $\mathrm{inv}D = \frac{r}{d} \bmod \mathbf{Z}$ avec $(r, d) = 1$ est tué par 2, donc $d = 1$ ou 2, d'où (5). Si F est global, on a de même $\mathrm{inv}_v D \in \{0, \frac{1}{2}\} \bmod \mathbf{Z}$ pour toute place v de F, et l'ensemble S des places ou $\mathrm{inv}_v D = \frac{1}{2}$ est pair. Soit B l'algèbre de quaternion sur F telle que $\mathbf{Ram} B = S$. Alors $[B] = [D]$ dans $\mathrm{Br}(F)$, donc $B \simeq D$ si B est un corps (i.e. $S \neq \emptyset$). Sinon, $[B] = 0 = [D]$, donc $D = F$ car D est un corps, d'où (5). Supposons enfin (5) et notons $\star$ l'identité de D si $[D : F] = 1$, l'involution canonique de D si $[D : F] = 4$. Alors $M \mapsto (M^\star)^t$ est une involution F-linéaire de $A = M_n(D)$, et cette involution induit en particulier un isomorphisme de F-algèbre $A \simeq A^{opp}$, d'où (1). □

7. Modules

On fixe une F-algèbre semi-simple A et on se propose de décrire l'ensemble $\mathcal{P}(A)$ des classes d'isomorphismes de A-modules (à gauche) de F-dimension finie. Si $A = \prod A_i$, on a évidemment $\mathcal{P}(A) = \prod \mathcal{P}(A_i)$. La proposition 6.1 nous ramène donc immédiatement au cas d'une F-algèbre simple, de la forme $A \simeq M_n(D)$ pour un corps gauche D (avec $F \subset Z(D)$). La proposition suivante (un cas particulièrement limpide d'équivalence de Morita) appliquée à $a = n$ et $b = 1$ montre alors que $\mathcal{P}(A) \simeq \mathcal{P}(D)$. La théorie de la dimension montre enfin que $\mathcal{P}(D) \simeq \mathbf{N}$.

Proposition 7.1. *Soit $A = M_a(D)$, $B = M_b(D)$, $X = M_{b,a}(D)$, $Y = M_{a,b}(D)$ et*

$$\mathcal{X} : \mathbf{Mod}(A) \leftrightarrow \mathbf{Mod}(B) : \mathcal{Y}$$

les foncteurs définis par $\mathcal{X}(V) = X \otimes_A V$ et $\mathcal{Y}(W) = Y \otimes_B W$. Alors $\mathcal{X}$ et $\mathcal{Y}$ sont des équivalences de catégories quasi-inverses l'une de l'autre.

Démonstration. Le produit matriciel définit des isomorphismes de (A, A) (resp. (B, B)) bimodules $\alpha : Y \otimes_B X \simeq A$ et $\beta : X \otimes_A Y \simeq B$ qui induisent à leur tour des isomorphismes d'endofoncteurs

$$\alpha : \mathcal{Y} \circ \mathcal{X} \to \mathrm{Id}_{\mathbf{Mod}(A)} \quad \text{et} \quad \beta : \mathcal{X} \otimes \mathcal{Y} \to \mathrm{Id}_{\mathbf{Mod}(B)}$$

respectivement définis par

– $\alpha_V : Y \otimes_B (X \otimes_A V) \simeq (Y \otimes_B X) \otimes_A V \xrightarrow{\alpha} A \otimes_A V \simeq V$ et
– $\beta_W : X \otimes_A (Y \otimes_B W) \simeq (Y \otimes_A X) \otimes_B W \xrightarrow{\beta} B \otimes_B W \simeq W$.

CQFD. □

Conclusion 7.2. Si $A \simeq \prod_{i=1}^{r} M_{n_i}(D_i)$, alors

$$\mathcal{P}(A) \simeq \mathbf{N}^r \quad \text{via} \quad (x_1, \cdots, x_r) \mapsto \oplus_{i=1}^{r} (D_i^{n_i})^{x_i}.$$

8. Involutions

8.1. **Définitions.** Une involution d'un anneau A est un morphisme de groupe $\star$: $A \to A$ tel que $(ab)^\star = b^\star a^\star$ et $a^{\star\star} = a$. On a alors $1_A^\star = 1_A$ et $\psi : A \to A^o$ est un isomorphisme d'anneau. On note $I(A)$ l'ensemble des involutions de A. On définit trois relations d'équivalences sur $I(A)$:

$\star_1 \equiv \star_2$ si et seulement si il existe un automorphisme intérieur $\mathrm{Ad}\alpha : A \to A$ tel que $\mathrm{Ad}\alpha \circ \star_1 = \star_2 \circ \mathrm{Ad}\alpha$.

$\star_1 \simeq \star_2$ si et seulement si il existe un automorphisme intérieur $\mathrm{Ad}a : A \to A$ avec $a \in A^\times$ et $a^{\star_1} = a$ tel que $\star_2 = \mathrm{Ad}a \circ \star_1$.

$\star_1 \sim \star_2$ si et seulement si il existe un automorphisme intérieur $\mathrm{Ad}a : A \to A$ avec $a \in A^\times$ tel que $\star_2 = \mathrm{Ad}a \circ \star_1$.

Dans le premier cas, $\star_2 = \mathrm{Ad}(\alpha\alpha^{\star_1}) \circ \star_1$ donc $\star_1 \simeq \star_2$ et bien sur $\star_1 \sim \star_2$. Dans le troisième cas, $(\mathrm{Ad}a \circ \star_1)^2 = 1$ donc $\mathrm{Ad}(a^{\star_1}) = \mathrm{Ad}(a)$ i.e. $a^{\star_1} = \lambda a$ avec $\lambda \in Z(A^\times)$. Puisque $\lambda = a^{\star_1} a^{-1} = a^{-1} a^{\star_1}$, on a $\lambda^c \lambda = 1$ où c est l'involution de $Z(A^\times)$ induite par $\star_1$ ou $\star_2 = \mathrm{Ad}a \circ \star_1$. La substitution $a \mapsto \frac{1}{\mu} a$ avec $\mu \in Z(A^\times)$ ne change pas $\star_2$, mais modifie λ en $\mu^{1-c}\lambda$. On a donc :

Proposition 8.1. *Pour $\star_1, \star_2 \in I(A)$:*

$$\star_1 \equiv \star_2 \implies \star_1 \simeq \star_2 \implies \star_1 \sim \star_2.$$

De plus :

1. *Dans la classe d'équivalence de $\star$ pour $\simeq$, les classes d'équivalences de $\equiv$ sont en bijection avec le quotient de $\{a \in A^\times | a^\star = a\}$ pour la relation d'équivalence $a \leftrightarrow \mu\alpha^\star a \alpha$, $\alpha \in A^\times$ et $\mu \in Z(A)^\times$, $\mu^\star = \mu$.*
2. *Dans la classe d'équivalence de $\star$ pour $\sim$, les classes d'équivalences de $\simeq$ sont en bijection avec un sous-ensemble de $\{\lambda \in Z(A^\times) | \lambda^c \lambda = 1\} \bmod \{\mu/\mu^c | \mu \in Z(A^\times)\}$, où $c = \star | Z(A)$.*

Classifier les involutions sur A signifie : déterminer les classes d'équivalences pour la plus fine des relations, à savoir $\equiv$. Pour ce faire, on commence par déterminer les classes d'équivalences pour $\sim$, puis $\simeq$.

8.2. **Décomposition et types.** Lorsque A est une F-algèbre semi-simple, tout $Z(A)$-automorphisme de A est intérieur, donc

Lemma 8.2. *$\star_1 \sim \star_2$ si et seulement si $\star_1$ et $\star_2$ induisent la même involution c sur $Z(A)$.*

On note alors $I(A, c)$ l'ensemble des involutions de A qui induisent c sur $Z(A)$: c'est un sous-ensemble de $I(A)$ qui est soit vide, soit une classe d'équivalence pour $\sim$ (selon que c se prolonge ou non en une *involution* de A[2]). Tous les éléments de $I(A, c)$ induisent la même involution c sur l'ensemble des idempotents centraux minimaux, donc la même involution c sur l'ensemble des composantes simples de A. En regroupant ces composantes simples en c-orbites, on voit donc que l'étude de $I(A, c)$ se ramène à l'un des trois cas irréductibles suivants :

[2]Attention : c se prolonge toujours en un automorphisme de A !

8.2.1. *Type D : $A = A_1 \times A_2$ avec A_1 et A_2 simples et échangés par c.* Soit $\star \in I(A,c)$. Alors $\star|A_2$ induit un isomorphisme $A_2 \simeq A_1^o$. Par transport de structure, on peut supposer que $A_2 = A_1^o$ et que cet isomorphisme est l'identité, ce qui nous ramène à $A = A_1 \times A_1^o$ avec $\star(0,a) = (a,0)$ donc $\star(a,0) = (0,a)$ et $\star(a,b) = (b,a)$. On en déduit facilement que les trois relations d'équivalences $\sim, \simeq$ et $\equiv$ coincident sur $I(A,c)$, et qu'il n'y a donc qu'une classe d'équivalence pour chacune de ces relations.

8.2.2. *Type I : A est simple et $c = Id$ sur $C = Z(A)$.* Soit $\star_1, \star_2 \in I(A, Id)$. Soit $a \in A^\times$ tel que $\star_2 = \mathrm{Ad}(a) \circ \star_1$. Alors $a^{\star_1} = \epsilon a$ avec $\epsilon \in \{\pm 1\}$ et

$$A[\star_2 \pm Id] = A[\star_1 \pm \epsilon Id] \cdot a$$

donc $\dim_C A[\star_2 \pm Id] = \dim_C A[\star_1 \pm \epsilon Id]$. Si $A = M_n(C)$ et $\star_1$ est la transposition,

$$\dim_C A[\star_1 - Id] = \frac{n(n+1)}{2} > \dim_C A[\star_1 + Id] = \frac{n(n-1)}{2}.$$

Puisque toute C-algèbre centrale simple devient isomorphe à $M_n(C')$ sur une extension convenable C' de C, les classes d'équivalences de $\simeq$ dans $I(A, Id)$ sont

$$I(A, \pm) = \{\star \in I(A, Id) | \dim_C A[\star \mp Id] > \dim_C A[\star \pm Id]\}.$$

Attention : il se peut toutefois que $I(A, \pm) = \emptyset$!

Proposition 8.3. *Soit $A = M_n(D)$ avec $Z(A) = Z(D) = C$ et $d^2 = [D : C]$.*
- *Si $d = 1$, $I(A,+) \neq \emptyset$ et ($I(A,-) \neq \emptyset \iff n \equiv 0 \bmod 2$).*
- *Si $d = 2$, $I(A,+) \neq \emptyset$ et $I(A,-) \neq \emptyset$. De plus, $I(D,-) = \{can\}$.*
- *Si $d > 2$ et $C \in \{loc, cn\}$, $I(A,+) = I(A,-) = \emptyset$.*

Démonstration. Si $\star \in I(D, \pm)$, alors $(m_{i,j}) \mapsto (m_{j,i}^\star) \in I(A, \pm)$. Si $D = C$, $I(D,+) = \{Id\} \neq \emptyset$, qui donne $\star \in I(A,+) \neq \emptyset$. Les éléments de $I(A,\pm)$ sont alors de la forme $\mathrm{Ad}a \circ t$ avec $a^t = \pm a$, donc

$$I(A,-) \neq 0 \iff \exists a \in GL_n(C) | a^t = -a \iff n \equiv 0 \bmod 2.$$

Si D est un corps de quaternion sur C, l'involution canonique $\star = can$ est dans $I(D,-) \neq \emptyset$. Les éléments de $I(D,\pm)$ sont de la forme $\mathrm{Ad}d \circ \star$ avec $d^\star = \mp d$. Donc $I(D,-) = \{can\}$, $I(D,+) = \mathrm{Ad}(D_0^\times) \cdot \{can\} \neq \emptyset$ où $D_0 = \ker(\mathrm{tr} : D \to C)$ et $D_0^\times = D_0 - \{0\}$, et $I(A,\pm) \neq \emptyset$. Si enfin $d > 2$ et C est un corps local ou un corps de nombre, alors $A \not\simeq A^0$ donc $I(A,\pm) = \emptyset$. □

8.2.3. *Type II : A est simple et $c \neq Id$ sur $C = Z(A)$.* Le théorème de Hilbert 90 montre alors que $\simeq = \sim$ sur $I(A,c)$.

Proposition 8.4. *Soit $A = M_n(D)$ avec $Z(A) = Z(D) = C$ et $d^2 = [D : C]$. Soit $C_0 = \{x \in C | x^c = x\}$.*

(1) *Si $d = 1$, $I(A,c) \neq \emptyset$.*

(2) *Si $d > 1$ et C est local, $I(A,c) = \emptyset$.*

(3) *Si $d > 1$ et C est global,*

$$I(A,c) \neq \emptyset \iff \forall v_0 \text{ de } C_0 : \sum_{v | v_0} \mathrm{inv}_v C = 0.$$

Démonstration. Si $d = 1$, $(m_{i,j}) \mapsto (m^c_{j,i}) \in I(A, c) \neq \emptyset$. En général : si $\star \in I(A, c)$, l'isomorphisme semi-linéaire $\star : A \to A^o$ induit un isomorphisme de C-algèbres $A \otimes_{C,c} C \simeq A^0$, donc $[A] + c[A] = 0$ dans BrC. Si C est local, l'action de c sur BrC est triviale, donc $2[A] = 0$ dans BrC, et $D = C$ ou D est un corps de quaternion. Dans le second cas, can $\circ \star$ fournit une donnée de descente sur D/C relativement à Spec$C \to$ SpecC_0 : il existe donc une C_0-algèbre (de quaternion) D_0 telle que $D_0 \otimes_{C_0} C \simeq D$. Mais alors $D \simeq M_2(C)$ puisque $[C : C_0] = 2$, une contradiction. Supposons enfin que C est global. Soit $v \mid v_0$ une place de c. Si $cv = c$, $\star \in I(A_v, c) \neq \emptyset$ donc inv$_v A = 0$. Sinon, inv$_v A$+inv$_{cv} A = 0$. Pour la preuve de l'implication inverse $\Leftarrow$ dans (3), voir [6], mais nous n'en aurons (presque) pas besoin. □

8.3. **Conclusion.** On connaît maintenant les classes d'équivalences d'involutions sur A pour $\simeq$ (les *types* d'involution, qui sont des produits de *types élémentaires* D, $I(\pm)$ ou $II(c)$). On veut ensuite décomposer chacun de ces *types* en classes d'équivalence pour $\equiv$. Nous verrons plus bas que ce problème est un cas particulier de la classification des formes hermitiennes correspondant à une involution du type donnée.

9. Formes hermitiennes

9.1. **Définitions.** Soit A un anneau, $C = Z(A)$ le centre de A, $\star$ une involution de A, $U = \{u \in C | u^c u = 1\}$ le groupe des unités de (C, c).

Definition 9.1. Soit V un A-module à gauche. Une forme sesquilinéaire sur V est un morphisme biadditif $\psi : V \times V \to A$ tel que

$$\forall a, b \in A, \forall v, w \in V : \qquad \psi(av, bw) = a\psi(v, w)b^\star.$$

On note $S(A, \star)(V)$ l'ensemble des formes sesquilinéaires sur V. C'est un C-module à gauche muni d'une involution semi-linéaire τ définie par

$$(\tau\psi)(v, w) = \psi(w, v)^\star.$$

Definition 9.2. Soit $u \in U$ et V un A-module à gauche. Une forme u-hermitienne sur V est une forme sequilinéaire $\psi : V \times V \to A$ telle que (1) $\tau\psi = u\psi$, i.e.

$$\forall v, w \in V : \qquad \psi(w, v)^\star = u\psi(v, w)$$

et (2) ψ est non-dégénérée, i.e.

$$\forall v \in V : \qquad \psi(v, \bullet) \equiv 0 \iff \psi(\bullet, v) \equiv 0 \iff v = 0.$$

On note $\mathcal{H}(A, \star, u)(V)$ l'ensemble des formes u-hermitiennes sur V et $\mathcal{H}(A, \star, u)$ l'ensemble des classes d'isomorphismes d'espace u-hermitien (V, ψ) où V est de type fini sur A.

9.2. **Variantes.** Supposons que A est une F-algèbre semi-simple, et que $F \subset C$ est stable sous $\star$. On note tr $=$ tr$_{A/F} : A \to F$ le composé de la trace réduite tr$_{A/C} : A \to C$ et de la trace usuelle Tr$_{C/F} : C \to F$.

Lemma 9.3. *C'est une application F-linéaire qui vérifie*

(1) $\mathrm{tr}(ab) = \mathrm{tr}(ba)$,
(2) $\mathrm{tr}(a\bullet) \equiv 0 \iff \mathrm{tr}(\bullet a) \equiv 0 \iff a = 0$,
(3) $\mathrm{tr}(a^\star) = \mathrm{tr}(a)^\star$.

Démonstration. Par définition, si $A = \prod A_i$ est la décomposition de A en facteurs simples A_i de centre C_i, on a $\mathrm{tr}_{A/F} = \sum_i \mathrm{tr}_{A_i/F} = \sum_i \mathrm{Tr}_{C_i/F} \circ \mathrm{tr}_{A_i/C_i}$. Les propriétés (1) et (2) résultent donc des propriétés similaires pour les algèbres centrales simples A_i/C_i, lesquelles se démontrent par passage à une clôture algébrique de C_i. Le même argument montre aussi que $\mathrm{tr}_{A/F}(a) = \mathrm{tr}_{A^{opp}/F}(a)$ pour tout $a \in A$. Si $\sigma : F \to F'$ est un isomorphisme de corps et $\sigma : A \to A'$ un isomorphisme σ-linéaire, on voit de même que $\sigma \circ \mathrm{tr}_{A/F} = \mathrm{tr}_{A'/F'} \circ \sigma : A \to F'$. Appliquant ceci à $\star : A \to A^{opp}$, on en déduit que $\mathrm{tr}_{A/F}(a)^\star = \mathrm{tr}_{A^{opp}/F}(a^\star) = \mathrm{tr}_{A/F}(a^\star)$ pour tout $a \in A$. □

Corollary 9.4. *Pour tout A-module V de F-dimension finie, $\phi \mapsto \mathrm{tr}_{A/F} \circ \phi$ induit un isomorphisme* $\mathrm{Hom}_A(V, A) \to \mathrm{Hom}_F(V, F)$.

Démonstration. C'est F-linéaire et injectif par (2) : il suffit donc de voir que source et but ont même dimension. Or si $A \simeq \oplus A_i$ avec $A_i = M_{n_i}(D_i)$ et $V = \oplus V_i$ avec $V_i = V_{i,0}^{r_i}$ où $V_{i,0} = D_i^{n_i}$, on a

$$\mathrm{Hom}_A(V, A) = \oplus_i \mathrm{Hom}_{A_i}(V_i, A_i) = \oplus_i \mathrm{Hom}_{A_i}(V_{i,0}, A_i)^{r_i}$$

et $\mathrm{Hom}_{A_i}(V_{i,0}, A_i) \simeq \mathrm{Hom}_{D_i}(D_i, D_i^{n_i}) = (D_i^{opp})^{n_i}$ par Morita, donc

$$\dim_F \mathrm{Hom}_A(V, A) = \sum_i r_i n_i \dim_F D_i = \dim_F V = \dim_F \mathrm{Hom}_F(V, F),$$

CQFD. □

Munissons $\mathrm{Hom}_A(V, A)$ de la structure de A-module à gauche définie par

$$\forall a \in A \text{ et } v \in V : \qquad (a\Phi)(v) = \Phi(v)a^\star$$

Puisque $\mathrm{tr}(\Phi(v)a^\star) = \mathrm{tr}(a^\star\Phi(v)) = \mathrm{tr}(\Phi(a^\star v))$, elle correspond sur $\mathrm{Hom}_F(V, F)$ à

$$\forall a \in A \quad \text{et} \quad v \in V : \qquad (a\phi)(v) = \phi(a^\star v).$$

La donnée d'une forme sesquilinéaire $\Psi : V \times V \to A$ est équivalente à la donnée d'un morphisme de A-module $\Phi : V \to \mathrm{Hom}_A(V, A)$, via $\Phi(v)(w) = \Psi(w, v)$, donc à la donnée d'un morphisme de A-module $\phi : V \to \mathrm{Hom}_F(V, F)$, elle même équivalente à la donnée d'une forme bi-additive $\psi : V \times V \to F$, via $\phi(v)(w) = \psi(w, v)$. On obtient ainsi une bijection $\Psi \mapsto \psi = \mathrm{tr} \circ \Psi$ de l'ensemble des formes sesquilinéaires $\Psi : V \times V \to A$ sur l'ensemble des formes $\psi : V \times V \to F$ telles que

$$\forall \lambda_1, \lambda_2 \in F \quad \text{et} \quad v, w \in V : \qquad \psi(\lambda_1 v, \lambda_2 w) = \lambda_1 \lambda_2^\star \psi(v, w)$$

et

$$\forall a \in A \quad \text{et} \quad v, w \in V : \qquad \psi(av, w) = \psi(v, a^\star w).$$

On note $S_F(A, \star)(V)$ l'ensemble de ces formes, que l'on appelle aussi sesquilinéaires.

L'involution $(\tau\Psi)(v, w) = \Psi(w, v)^\star$ de $S(A, \star)(V)$ correspond à l'involution donnée par la même formule $(\tau\psi)(v, w) = \psi(w, v)^\star$ sur $S_F(A, \star)(V)$, tandis que la structure de C-module $(c\Psi)(v, w) = c\Psi(v, w)$ de $S(A, \star)(V)$ correspond à la structure $(c\psi)(v, w) = \psi(cv, w) = \psi(v, c^\star w)$. L'ensemble $\mathcal{H}(A, \star, u)(V)$ des formes u-hermitiennes $\Psi : V \times V \to A$ correspond enfin à l'ensemble $\mathcal{H}_F(A, \star, u)(V)$ des formes sesquilinéaires $\psi : V \times V \to F$ telles que (1) $\psi(w, v)^\star = \psi(uv, w)$ et (2) $\psi(v, \bullet) \equiv 0 \iff \psi(\bullet, v) = 0 \iff v = 0$.

9.3. **Formes et Involutions.** Soit $(A,\star)$ comme ci-dessus et V un A-module à gauche de type fini. Pour tout $\psi \in \mathcal{H}(A,\star,u)(V)$, la formule

$$\forall v,w \in V : \qquad \psi(bv,w) = \psi(v, b^{\star_\psi} w)$$

définit une involution $\star_\psi$ de $B = \mathrm{End}_A V$.

Proposition 9.5. *Si A est simple de centre C, alors B est simple de centre C et*

(1) *Si $\star$ est de type $I(\pm)$, alors $\psi \mapsto \star_\psi$ induit une bijection*

$$\mathcal{H}(A,\star,\epsilon)(V) \bmod C^\times \simeq \mathcal{I}(B,\pm\epsilon).$$

(2) *Si $\star$ est de type $II(c)$, alors $\psi \mapsto \star_\psi$ induit une bijection*

$$\mathcal{H}(A,\star,u)(V) \bmod U \simeq \mathcal{I}(B,c).$$

Dans les deux cas, la relation d'équivalence $\equiv$ sur le terme de droite correspond à la relation $\psi \equiv \psi'$ si et seulement si il existe un A-isomorphisme de V qui envoie ψ sur un C-multiple de ψ' (le facteur multiplicatif est alors un élément inversible du sous-corps C_0 de C fixé par c). Si $A = D$ et $V = D^n$, alors $B = M_n(D)$. On obtient ainsi la classification annoncée des involutions :
- Pour connaître $\mathcal{I}(M_n(D),\pm)$ modulo $\equiv$, il suffit de déterminer $\mathcal{H}(D,\star,\pm\epsilon)$ pour une seule involution $\star \in \mathcal{I}(D,\epsilon)$.
- Pour connaître $\mathcal{I}(M_n(D),c)$ modulo $\equiv$, il suffit de déterminer $\mathcal{H}(D,\star,1)$ pour une seule involution $\star \in \mathcal{I}(D,c)$.

9.4. **Décomposition.**

Lemma 9.6. *Si $(A,\star) = \prod (A_i,\star_i)$, $Z(A) = \prod Z(A_i)$ et $u = (u_i)$, alors*

$$\mathcal{H}(A,\star,u) = \prod_i \mathcal{H}(A_i,\star_i,u_i).$$

Démonstration. C'est immédiat. □

Cela nous ramène immédiatement, dans la classification des espaces u-hermitiens, à l'un des quatre types élémentaires de $(A,\star)$: D (décomposé), $I(\pm)$ (simple de première espèce), ou $II(c)$ (simple de seconde espèce).

9.5. **Le type D.** On suppose que $(A,\star) = (A_1 \times A_1^o, \star)$ avec $(a,b)^\star = (b,a)$ (où A_1 est une F-algèbre simple). Alors $u = (u_1, u_1^{-1})$ avec u_1 dans le centre C_1 de A_1. Soit V un A-module à gauche. Alors $V = V_1 \times V_1^o$ où V_1 et V_1^o sont respectivement des A_1 et A_1^o-modules à gauche. On regarde V_1^0 comme un A_1-module à droite. La donnée d'une forme sesquilinéaire $\psi : V \times V \to A$ est équivalentes à celles de deux applications

$$\psi_1 : V_1 \times V_1^0 \to A_1 \quad \text{et} \quad \psi_1^0 : V_1^0 \times V_1 \to A_1$$

telles que $\psi_1(av,wb) = a\psi_1(v,w)b$ et $\psi_1^0(wb,av) = a\psi_1^0(w,v)a$, via

$$\psi((v,w),(v',w')) = (\psi_1(v,w'), \psi_1^0(w,v')) \in A_1 \times A_1^0$$

On a alors $(\tau\psi)_1(v,w) = \psi_1^0(w,v)$ et $(\tau\psi)_1^0(w,v) = \psi_1(v,w)$. Donc ψ est u-hermitienne si et seulement si $\psi_1^0(w,v) = u_1\psi_1(v,w)$ et

$$\psi_1(v,\bullet) \equiv 0 \iff \psi_1(\bullet,v) \equiv 0 \iff v = 0.$$

Dans ce cas, ψ_1 induit un isomorphisme de A_1-modules à droite[3]

$$v_1^0 \in V_1^0 \mapsto \psi_1(\bullet, v_1^0) \in \mathrm{Hom}_A(V_1, A_1).$$

Par transport de structure, on peut donc supposer que $V_1^0 = \mathrm{Hom}_A(V_1, A_1)$, $\psi_1(v,w) = w(v)$ et alors $\psi_1^0(w,v) = u_1 w(v)$. On en déduit que

Lemma 9.7. *$(V,\psi) \mapsto V_1$ induit une bijection $\mathcal{H}(A,\star,u) \simeq \mathcal{P}(A_1)$.*

9.6. **Les types I et II (Morita).** On fixe $(D,\star)$ et pour tout $x,y \in \mathbf{N}$, on note encore $\star : M_{x,y}(D) \to M_{y,x}(D)$ l'application $(m_{i,j}) \mapsto (m_{j,i}^\star)$. Soient
- $A = M_a(D)$ muni de $\star_A = \mathrm{Ad}u_A \circ \star \sim \star$ avec $u_A^\star = \epsilon_A u_A$, $\epsilon_A \in U$,
- $B = M_b(D)$ muni de $\star_B = \mathrm{Ad}u_B \circ \star \sim \star$ avec $u_B^\star = \epsilon_B u_B$, $\epsilon_B \in U$.

On considère
- $X = M_{ba}(D)$ muni de $[,]_B : X \times X \to B$ où $[x_1,x_2]_B = x_1 u_A x_2^\star u_B^{-1}$,
- $Y = M_{ab}(D)$ muni de $[,]_A : Y \times Y \to B$ où $[y_1,y_2]_A = y_1 u_B y_2^\star u_A^{-1}$.

On peut alors étendre les foncteurs de l'équivalence de Morita

$$\mathcal{X} : \mathbf{Mod}(A) \leftrightarrow \mathbf{Mod}(B) : \mathcal{Y} \qquad \mathcal{X}(V) = X \otimes_A V \quad \text{et} \quad \mathcal{Y}(W) = Y \otimes_B W$$

aux catégories d'espaces sesquilinéaires

$$\mathcal{X} : S(A,\star_A) \leftrightarrow S(B,\star_B) : \mathcal{Y}$$

en posant :
- Pour $V \in \mathbf{Mod}(A)$ et $\phi \in S(A,\star_A)(V)$, $\mathcal{X}(\phi) : \mathcal{X}(V) \times \mathcal{X}(V) \to B$ est
$$\mathcal{X}(\phi)(x_1 \otimes v_1, x_2 \otimes v_2) = [x_1\phi(v_1,v_2), x_2]_B.$$
- Pour $W \in \mathbf{Mod}(B)$ et $\psi \in S(B,\star_B)(W)$, $\mathcal{Y}(\psi) : \mathcal{Y}(V) \times \mathcal{Y}(V) \to A$ est
$$\mathcal{Y}(\phi)(y_1 \otimes w_1, y_2 \otimes w_2) = [y_1\psi(w_1,w_2), y_2]_B.$$

On vérifie aisément que

$$\mathcal{X}(\tau\phi) = \epsilon_A\epsilon_B\tau\mathcal{X}(\phi) \quad \text{et} \quad \mathcal{Y}(\tau\psi) = \epsilon_A\epsilon_B\tau\mathcal{Y}(\psi).$$

On en déduit que pour $V \leftrightarrow \mathcal{W}$, les constructions ci-dessus induisent des bijections

$$\mathcal{H}(A,\star_A,u\epsilon_A) \leftrightarrow \mathcal{H}(B,\star_B,u\epsilon_B)$$

pour tout u dans $U = \{u \in Z(D) | u^c u = 1\}$.

9.7. **Les types I et II (Classification).** D'après les résultats qui précèdent, il ne nous reste plus qu'à étudier les cas suivants (où *loc*=corps local non-archimédien et *cn*=corps de nombre) :
- $\mathcal{Q}(F) = \mathcal{H}(F,1,1)$ pour $F \in \{loc, \mathbf{R}, \mathbf{C}, cn\}$,
- $\mathcal{A}(F) = \mathcal{H}(F,1,1)$ pour $F \in \{loc, \mathbf{R}, \mathbf{C}, cn\}$,
- $\mathcal{Q}(B) = \mathcal{H}(B,can,1)$ pour B/F corps de quaternions, $F \in \{loc, \mathbf{R}, cn\}$,
- $\mathcal{A}(B) = \mathcal{H}(B,can,-1)$ pour B/F corps de quaternions, $F \in \{loc, \mathbf{R}, cn\}$,
- $\mathcal{H}(K) = \mathcal{H}(K,c,1)$ pour K/F quadratique avec $F \in \{loc, \mathbf{R}, cn\}$,
- $\mathcal{H}(D) = \mathcal{H}(D,\star,1)$ pour $D/K/F$ centrale simple avec $F \in \{cn\}$.

Mentionnons quelques principes généraux :

(1) Toutes les formes admettent des décompositions de Witt : hyperbolique + anisotrope. Cela permet de définir l'index de Witt.

[3] C'est le seul endroit où l'on a besoin des hypothèses de finitudes - de A_1 et V sur F- pour ramener cette question à un calcul de F-dimension.

(2) Toutes les formes sont diagonalisables, sauf pour $\mathcal{A}(F)$. Cela permet de calculer/définir le déterminant (ou le discriminant), ainsi que d'autres invariants : signature, invariants de Hasse...

(3) Toutes les formes vérifient le principe de Hasse, *sauf* $\mathcal{A}(D)$.

Donnons enfin la liste des invariants qui permettent de classifier toutes ces formes.

9.7.1. *Pour* $\mathcal{A}(F)$. Le rang suffit. C'est le double de l'index.

9.7.2. *Pour* $\mathcal{Q}(F)$. C'est le cas le plus classique, très lié à la théorie du corps de classe. Les invariants sont

$$\begin{cases} F = \mathbf{R} & \text{rang, signature} \\ F = \mathbf{C} & \text{rang} \\ F = loc & \text{rang, discriminant, Hasse} \\ F = cn & \text{rang, discriminant, Hasse, signatures} \end{cases}$$

9.7.3. *Pour* $\mathcal{H}(K)$. C'est encore très classique, et cela résulte du théorème de Jacobson, qui dit qu'une forme K-hermitienne est déterminée par la forme quadratique sous-jacente. Les invariants sont :

$$\begin{cases} F = \mathbf{R} & \text{rang, signature} \\ F = loc & \text{rang, discriminant} \\ F = cn & \text{rang, discriminant, signatures} \end{cases}$$

9.7.4. *Pour* $\mathcal{Q}(D)$. C'est moins classique. Le théorème de Jacobson dit maintenant qu'une forme D-hermitienne est déterminée par la forme quadratique sous-jacente. Les invariants sont :

$$\begin{cases} F = \mathbf{R} & \text{rang, signature} \\ F = loc & \text{rang} \\ F = cn & \text{rang, signatures} \end{cases}$$

9.7.5. *Pour* $\mathcal{A}(D)$. Le principe de Hasse est en défaut, et la classification sur un corps de nombre est donc plus difficile. Les invariants sont

$$\begin{cases} F = \mathbf{R} & \text{rang} \\ F = loc & \text{rang, discriminant} \\ F = cn & \mathbf{???} \end{cases}$$

9.7.6. *Pour* $\mathcal{H}(D)$. Cela ne fait sens que sur un corps de nombre. Les invariants sont le rang, les signatures aux places où $K/F = \mathbf{C}/\mathbf{R}$, et le discriminant.

10. Conditions de Positivité

10.1. **Les R-algèbres simples.** Il y a $M_n(\mathbf{R})$, $M_n(\mathbf{C})$ et $M_n(\mathbf{H})$ où $\mathbf{H}$ est le corps de quaternions.

10.2. **Les formes hermitiennes élémentaires.** Le tableau suivant liste les classes d'isomorphismes d'espaces hermitiens $(V, \psi) \in \mathcal{H}(D, \star, \pm 1)$ dans les situations élémentaires. Les représentants sont donnés sous la forme V =D-espace vectoriel des vecteurs lignes à n-coefficients dans D et $\psi(X, Y) = XMY^{\star t}$ avec $M \in M_n(D)$.

Nom	$\mathcal{H}(D, \star, u)$	Formes $XMY^{\star t}$	Rang	Invariants
$\mathcal{A}(\mathbf{R})$	$\mathcal{H}(\mathbf{R}, Id, -1)$	$M = J_m$	$n = 2m$	index m
$\mathcal{A}(\mathbf{C})$	$\mathcal{H}(\mathbf{C}, Id, -1)$	$M = J_m$	$n = 2m$	index m
$\mathcal{A}(\mathbf{H})$	$\mathcal{H}(\mathbf{H}, can, -1)$	$M = jI_n$	n	rang n
$\mathcal{Q}(\mathbf{R})$	$\mathcal{H}(\mathbf{R}, Id, 1)$	$M = I_{p,q}$	$n = p + q$	signature (p, q)
$\mathcal{Q}(\mathbf{C})$	$\mathcal{H}(\mathbf{C}, Id, 1)$	$M = I_n$	n	rang n
$\mathcal{Q}(\mathbf{H})$	$\mathcal{H}(\mathbf{H}, can, 1)$	$M = I_{p,q}$	$n = p + q$	signature (p, q)
$\mathcal{H}(\mathbf{C})$	$\mathcal{H}(\mathbf{C}, can, 1)$	$M = I_{p,q}$	$n = p + q$	signature (p, q)

L'élément j de $\mathbf{H}$ vérifie $j^2 = -1$ et les matrices sont

$$J_m = \begin{pmatrix} 0 & -I_m \\ +I_m & 0 \end{pmatrix} \quad I_{p,q} = \begin{pmatrix} +I_p & 0 \\ 0 & -I_q \end{pmatrix}$$

La démonstration se fait comme suit.

Pour $\mathcal{A}(\mathbf{R})$ et $\mathcal{A}(\mathbf{C})$, les espaces considérés admettent des décompositions de Witt, $V = \perp_{k=1}^{n} De_k \oplus De_{-k}$ avec $\psi(e_k, e_{-k}) = 1$. Dans tous les autres cas, ils admettent des décompositions orthogonales : $V = \perp_{k=1}^{n} De_k$. Posons $\alpha_k = \psi(e_k, e_k) \neq 0$. La substitution $e_k \mapsto de_k$ change α_k en $d\alpha_k d^\star$. Dans le cas $\mathcal{A}(H)$, $\alpha_k^\star = -\alpha_k$, donc $\alpha_k^2 = -\mathrm{nr}\alpha_k < 0$ et l'on peut changer chaque α_k en $j \in \mathbf{H}$. Pour les quatre derniers cas, on a $\alpha_k^\star = \alpha_k$, que l'on peut changer en 1 dans le cas $\mathcal{Q}(\mathbf{C})$, et en ± 1 dans les trois autres cas $\mathcal{Q}(\mathbf{R})$, $\mathcal{Q}(\mathbf{H})$ et $\mathcal{H}(\mathbf{C})$.

10.3. **Les classes d'équivalences d'involutions.** On en déduit que les classes d'équivalences de paires élémentaires $(A, \star)$ sont données par (1) les types D, i.e. $(A_1 \times A_1^o, \star)$ pour $A_1 = M_n(\mathbf{R})$, $M_n(\mathbf{C})$ ou $M_n(\mathbf{H})$ et $(a, b)^\star = (b, a)$, et (2) les autres :

nom	A	Type	Involution	Invariants
$\mathcal{A}(\mathbf{R})$	$M_{2m}(\mathbf{R})$	$I(-)$	$\mathrm{Ad}J_m \circ (M \mapsto M^t)$	rang $2m$
$\mathcal{A}(\mathbf{C})$	$M_{2m}(\mathbf{C})$	$I(-)$	$\mathrm{Ad}J_m \circ (M \mapsto M^t)$	rang $2m$
$\mathcal{A}(\mathbf{H})$	$M_n(\mathbf{H})$	$I(+)$	$\mathrm{Ad}jI_n \circ (M \mapsto \overline{M}^t)$	rang n
$\mathcal{Q}(\mathbf{R})$	$M_n(\mathbf{R})$	$I(+)$	$\mathrm{Ad}I_{p,q} \circ (M \mapsto M^t)$	signature $\{p, q\}$
$\mathcal{Q}(\mathbf{C})$	$M_n(\mathbf{C})$	$I(+)$	$M \mapsto M^t$	rang n
$\mathcal{Q}(\mathbf{H})$	$M_n(\mathbf{H})$	$I(-)$	$\mathrm{Ad}I_{p,q} \circ (M \mapsto \overline{M}^t)$	signature $\{p, q\}$
$\mathcal{H}(\mathbf{C})$	$M_n(\mathbf{C})$	$II(c)$	$\mathrm{Ad}I_{p,q} \circ (M \mapsto \overline{M}^t)$	signature $\{p, q\}$

Le nom est $\simeq \mathcal{H}(A, \star)$ par équivalence de Morita.

10.4. **Formes et involutions positives.** Pour tout $(A, \star)$ et $\psi \in \mathcal{H}(A, \star)(V)$, on peut former

$$\psi_{\mathbf{R}} = \mathrm{Tr}_{A/\mathbf{R}} \circ \psi \in \mathcal{H}_{\mathbf{R}}(A, \star)(V)$$

puis oublier la structure de A-module sur V pour obtenir

$$\psi_{\mathbf{R}} \in \mathcal{H}_{\mathbf{R}}(\mathbf{R}, \star)(V) = \mathcal{Q}(\mathbf{R})(V)$$

i.e. une forme quadratique sur V.

Definition 10.1. On dit que $\psi > 0$ ssi cette forme quadratique est définie positive.

D'autre part, $(a,b) \mapsto ab^\star$ est un élément canonique $\psi(\star)$ de $\mathcal{H}(A,\star)(A)$. Ce qui nous conduit à la définition :

Definition 10.2. On dit que $\star > 0$ ssi $\psi(\star) > 0$, i.e. $\mathrm{Tr}_{A/\mathbf{R}}(aa^\star) > 0$ pour tout $a \neq 0$.

On se propose de démontrer :

Proposition 10.3. *Les conditions suivantes sur $(A,\star)$ sont équivalentes :*

(1) *Il existe $[V,\psi] \in \mathcal{H}(A,\star,1)$ avec V fidèle et $\psi > 0$,*

(2) *L'involution $\star$ est positive,*

(3) *L'algèbre à involution $(A,\star)$ est un produit de facteurs du type*

$$(M_n(\mathbf{R}),\star) \quad (M_n(\mathbf{C}),\star) \quad et \quad (M_n(\mathbf{H}),\star)$$

avec $(m_{i,j})^\star = (\overline{m}_{j,i})$.

Si ces conditions sont vérifiées, alors pour tout V, *il existe* une *et* une seule *classe d'isomorphisme de $\psi > 0$ dans $\mathcal{H}(A,\star)(V)$.*

Démonstration. (1) $\iff$ (2) : Il est clair que (2) $\Rightarrow$ (1). Inversement, soit $[V,\psi] \in \mathcal{H}(A,\star)$ avec V fidèle et $\psi > 0$. Pour tout A-module simple W, il existe un plongement $W \hookrightarrow V$. Son orthogonal W' pour ψ est alors un supplémentaire de W dans V. On en déduit que V est une somme directe orthogonale de $(V_i, \psi|V_i)$ avec V_i un A-module simple, et que chaque A-module simple est isomorphe à au moins un des V_i. Soit maintenant $0 \neq a \in A$ et $\alpha = aa^\star$. Alors $\alpha|V_i$ est auto-adjoint, donc diagonalisable dans une $\mathbf{R}$-base orthonormée $e_1, \cdots, e_r$ de $(V_i, \psi_{\mathbf{R}}|V_i)$, et de trace $\mathrm{tr}_{\mathbf{R}}(\alpha|V_i) = \sum \psi_{\mathbf{R}}(\alpha e_i, e_i) = \sum \psi_{\mathbf{R}}(ae_i, ae_i)$. Chacun des termes est ici positif, et ils sont tous nuls si et seulement si $a|V_i = 0$. Puisque V est fidèle et $a \neq 0$, on voit donc que pour tout A-module simple, $\mathrm{tr}_{\mathbf{R}}(\alpha|W) \geq 0$ avec $\mathrm{tr}_{\mathbf{R}}(\alpha|W) > 0$ pour au moins un W. Mais $\mathrm{tr}_{A/\mathbf{R}}(\alpha)$ est une combinaison linéaire à coefficient entier > 0 des $\mathrm{tr}_{\mathbf{R}}(\alpha|W)$, donc $\mathrm{tr}_{A/\mathbf{R}}(\alpha) > 0$.

(2) $\iff$ (3) : Si $(A,\star) = \prod (A_i, \star_i)$, alors $\star > 0 \iff (\forall i : \star_i > 0)$. On est donc ramené à l'un des cas suivants :

- $(A,\star) = (A_1 \times A_1^0, \star)$ avec $(a,b)^\star = (b,a)$. Soit $a_1 \neq 0$ dans A_1 et $a = (a_1, 0) \neq 0$ dans A. Alors $aa^\star = 0$ donc $\star \not> 0$.
- $(A,\star) = (\mathrm{End}_D V, \star_\psi)$ pour $\psi \in \mathcal{H}(D,\star)(V)$ avec

$$(D,\star) \in (\mathbf{R}, Id), (\mathbf{C}, can), (\mathbf{H}, can), (\mathbf{C}, Id), (\mathbf{H}, nc).$$

Dans tous ces cas, (V,ψ) admet une décomposition en droite :

$$(V,\psi) = \perp (D, \epsilon_i x y^\star) \qquad \text{avec } \epsilon_i \in \{\pm 1\}.$$

Si $a \in A$ préserve cette décomposition, i.e. $a = (d_i)$, on a donc

$$\mathrm{tr}_{A/\mathbf{R}}(aa^\star) = \mathrm{tr}_{\mathbf{R}}(aa^\star|V) = \sum \epsilon_i \mathrm{tr}_{D/\mathbf{R}}(d_i d_i^\star).$$

On en déduit que $\star > 0$ si et seulement si

- $\star > 0$ sur D, i.e. $(D,\star) \in (\mathbf{R}, Id), (\mathbf{C}, can), (\mathbf{H}, can)$ et
- tous les ϵ_i sont égaux à 1

Ce qui démontre bien que (2) $\iff$ (3).

Supposons enfin que $(A,\star) > 0$ et montrons que l'application

$$R : \mathcal{H}(A,\star) \to \mathcal{P}(A) \qquad [V,\psi] \mapsto [V]$$

induit une bijection

$$R^{>} : \mathcal{H}^{>}(A, \star) \xrightarrow{\simeq} \mathcal{P}(A).$$

On se ramène aux trois cas élémentaires de (3), pour lesquels la signature donne $\mathcal{H}(A, \star) \simeq \mathbf{N} \times \mathbf{N}$ avec $\mathcal{H}^{>}(A, \star) = \mathbf{N} \times \{0\}$, le rang $\mathcal{P}(A) \simeq \mathbf{N}$, avec $R(p, q) = p + q$. Donc $R^{>} : (n, 0) \mapsto n$ est bien une bijection. □

10.5. **Polarisations.** On veut maintenant classifier les triplets (V, ψ, I) où $[V, \psi] \in \mathcal{H}_{\mathbf{R}}(A, \star, -1)$ et I est une structure complexe sur V compatible avec ψ. C'est-à-dire, $I \in \mathrm{End}_A V$, $I^2 = -1$ et $\psi(Iv, Iw) = \psi(v, w)$. La donnée de I est équivalente à celle d'un morphisme d'anneau $h : \mathbf{C} \to \mathrm{End}_A V$ (donné par $h(a + bi) = a + bI$) tel que $\psi(h(z)v, w) = \psi(v, h(\overline{z})w)$. Elle fournit aussi d'autres structures :

(1) V devient un $A \otimes \mathbf{C}$-module V_I,
(2) $\psi(v, w)$ est dans $\mathcal{H}_{\mathbf{R}}(A \otimes \mathbf{C}, \star \otimes c, -1)(V_I)$,
(3) $\psi_I(v, w) = \psi(Iv, w)$ est dans $\mathcal{H}_{\mathbf{R}}(A \otimes \mathbf{C}, \star \otimes c, 1)(V_I)$
(4) $\Psi_I(v, w) = \psi_I(v, w) + i\psi(v, w)$ est dans $\mathcal{H}_{\mathbf{C}}(A \otimes \mathbf{C}, \star \otimes c, 1)(V_I)$

Les données (V, I, ψ), (V_I, ψ), (V_I, ψ_I) et (V_I, Ψ_I) sont équivalentes, de sorte que nos triplets sont classifiés par :

$$\mathcal{H}_{\mathbf{R}}(A \otimes \mathbf{C}, \star \otimes c, -1) \simeq \mathcal{H}_{\mathbf{R}}(A \otimes \mathbf{C}, \star \otimes c) \simeq \mathcal{H}_{\mathbf{C}}(A \otimes \mathbf{C}, \star \otimes c)$$

(c'est évident sur les formules, mais on peut aussi utiliser des arguments plus sophistiqués : le premier isomorphisme est un cas particulier d'équivalence de Morita, le second un cas particulier de trace $\mathcal{H} \simeq \mathcal{H}_{\mathbf{C}} \simeq \mathcal{H}_{\mathbf{R}}$).

Definition 10.4. Un triplet (V, ψ, I) est positif ssi $\psi_I > 0 \iff \Psi_I > 0$.

L'existence d'un seul triplet positif *fidèle* implique donc que $(A, \star) > 0$. **Nous ferons maintenant cette hypothèse**. La dernière assertion de la proposition 10.3 appliquée à $(A \otimes \mathbf{C}, \star \otimes c)$ dit que sur tout $A \otimes \mathbf{C}$-module V_I, il existe une unique classe d'isomorphisme de ψ_I. En particulier :

Proposition 10.5. *Soient (V, ψ, I) et (V', ψ', I') deux triplets > 0. Alors*

$$(V, I) \simeq (V', I') \iff (V, \psi, I) \simeq (V', \psi', I').$$

De plus, toute paire (V, I) peut être complétée en un triplet $(V, \psi, I) > 0$.

Nous aurons aussi besoin de la proposition suivante :

Proposition 10.6. *Soient (V, ψ, I) et (V', ψ', I') deux triplets > 0. Alors*

$$(V, \psi) \simeq (V', \psi') \iff (V, \psi, I) \simeq (V', \psi', I').$$

De plus, toute paire (V, ψ) peut être complétée en un triplet $(V, \psi, I) > 0$.

Démonstration. Il s'agit de voir que l'application d'oubli de la $\mathbf{C}$-structure

$$R : \mathcal{H}_{\mathbf{R}}(A \otimes \mathbf{C}, \star \otimes c, -1) \to \mathcal{H}_{\mathbf{R}}(A, \star, -1) \qquad [V_I, \psi] \mapsto [V, \psi]$$

induit une bijection

$$R^{>} : \mathcal{H}^{>}_{\mathbf{R}}(A \otimes \mathbf{C}, \star \otimes c, -1) \xrightarrow{\simeq} \mathcal{H}_{\mathbf{R}}(A, \star, -1).$$

On se ramène immédiatement aux cas élémentaires où

$$(A, \star) \in \{(M_n(\mathbf{R}), can), (M_n(\mathbf{C}), can), (M_n(\mathbf{H}), can)\}$$

et par une équivalence de Morita au cas où $n = \mathbf{1}$.

– Si $(A,\star)=(\mathbf{R},Id)$, $(A\otimes\mathbf{C},\star\otimes c)=(\mathbf{C},c)$. Alors : (a) (V_I,ψ) est classifié par la signature $(2p,2q)$ de $(V_I,\psi_I)\in\mathcal{Q}(\mathbf{R})$ et $(V_I,\psi)>0\iff q=0$; (b) (V,ψ) est classifié par l'index $2m=\dim_{\mathbf{R}}V$; (c) R s'identifie à $(p,q)\mapsto m=p+q$. Donc $R^{>}:(p,0)\mapsto p$ est une bijection.
– Si $(A,\star)=(\mathbf{C},c)$, $(A\otimes\mathbf{C},\star\otimes c)\simeq(\mathbf{C},c)\times(\mathbf{C},c)$ via $z_1\otimes z_2\mapsto(z_1z_2,\overline{z}_1z_2)$. Alors : (a) $(V_I,\psi)=(V_I^{(1)},\psi^{(1)})\oplus(V_I^{(2)},\psi^{(2)})$ est classifié par les signatures $(2p^{(1)},2q^{(1)})$ et $(2p^{(2)},2q^{(2)})$ de $\psi_I^{(1)}$ et $\psi_I^{(2)}\in\mathcal{Q}(\mathbf{R})$, et $(V_I,\psi)>0$ ssi $q^{(1)}=q^{(2)}=0$; (b) (V,ψ) est classifié par les signatures (p,q) de $i\psi$; et (c) R s'identifie à $\big((p^{(1)},q^{(1)}),(p^{(2)},q^{(2)})\big)\mapsto(p^{(1)}+q^{(2)},q^{(1)}+p^{(2)})$. Donc $R^{>}:\big((p^{(1)},0),(p^{(2)},0)\big)\mapsto(p^{(1)},p^{(2)})$ est une bijection.
– Si $(A,\star)=(\mathbf{H},can)$, $(A\otimes\mathbf{C},\star\otimes c)\simeq(M_2(\mathbf{C}),can)$. Alors (a) (V_I,ψ) est classifié par les signatures $(4p,4q)$ de $(V_I,\psi_I)\in\mathcal{Q}(\mathbf{R})$ et $(V_I,\psi)>0$ ssi $q=0$; (b) (V,ψ) est classifié par le rang $4m=\dim_{\mathbf{R}}V$; et (c) R s'identifie à $(p,q)\mapsto m=p+q$. Donc $R^{>}:(p,0)\mapsto p$ est une bijection.

CQFD. □

Corollary 10.7. *Fixons $[V,\psi]\in\mathcal{H}(A,\star,-1)$. Soit $G=\mathrm{Aut}_A(V,\psi)$. Alors l'ensemble $\mathcal{X}$ des I tels que $(V,\psi,I)>0$ est une classe de $G(\mathbf{R})$-conjugaison dans $G(\mathbf{R})$.*

Démonstration. Pour tout triplet (V,ψ,I), on a $\psi(Ix,Iy)=\psi(x,y)$ donc $I\in G(\mathbf{R})$. Si (V,ψ,I_1) et (V,ψ,I_2) sont positifs, il existe un isomorphisme $\alpha:(V,\psi,I_1)\to(V,\psi,I_2)$, donc $\alpha\in G(\mathbf{R})$ et $\alpha\circ I_1=I_2\circ\alpha$, i.e. $I_2=\alpha I_1\alpha^{-1}$ dans $G(\mathbf{R})$. □

Donnons enfin une description concrète des ensembles $\mathcal{X}$ ainsi obtenus. En décomposant $(A,\star)$ en composantes simples et en utilisant une nouvelle fois l'équivalence de Morita, on voit que $\mathcal{X}$ est un produit des espaces élémentaires suivants :

Type I(+): Si $(A,\star)=(\mathbf{R},Id)$, (V,ψ) est un $\mathbf{R}$-espace symplectique et $G\simeq\mathbf{Sp}_{2n}$. Soit $\mathcal{B}=(e_1,e_{-1},\cdots,e_n,e_{-n})$ une base symplectique de (V,ψ) et $I=I(\mathcal{B})$ l'endomorphisme de V défini par $Ie_k=\mathrm{sign}(k)e_{-k}$.Alors $I\in\mathcal{X}$ et le stabilisateur de I dans $G(\mathbf{R})$ est le groupe des $\mathbf{C}$-automorphismes de V_I qui préservent ψ, ou ψ_I, ou Ψ_I : c'est donc le groupe unitaire de (V_I,Ψ_I), qui est compact puisque $\Psi_I>0$. On a donc

$$\begin{aligned}\mathcal{X} &= G(\mathbf{R})\cdot I=\{I(\mathcal{B})|\mathcal{B}\text{ base symplectique}\}\\ &\simeq \mathbf{Sp}(2n)/U(n).\end{aligned}$$

Type II: Si $(A,\star)=(\mathbf{C},c)$, $\mathrm{Aut}(V,\psi)=\mathrm{Aut}(V,\Psi)$ où $\Psi(v,w)=\psi(iv,w)+i\psi(v,w)$, donc $G\simeq U(p,q)$ où (p,q) est la signature de (V,Ψ). Soit $V=V_+\perp V_-$ une décomposition de V avec $\Psi|V_+>0$ et $\Psi|V_-<0$. Soit $I=I(V_+)$ l'endomorphisme $\mathbf{C}$-linéaire de V qui est la multiplication par $\pm i$ sur $V_\pm$. Alors $I\in\mathcal{X}$ et le stabilisateur de I dans $G(\mathbf{R})$ est $U(V_+)\times U(V_-)\simeq U(p)\times U(q)$, donc

$$\begin{aligned}\mathcal{X} &= G(\mathbf{R})\cdot I=\{I(V_+)|\Psi|V_+>0\text{ et }\Psi|V_+^{\perp}<0\}\\ &\simeq U(p,q)/U(p)\times U(q).\end{aligned}$$

Type I(-): Si $(A,\star)=(\mathbf{H},can)$, choisissons $i\in\mathbf{H}$ avec $i^2=-1$. Soit $\mathcal{B}=(e_1,\cdots,e_n)$ une $(i,\mathbf{H})$-base, i.e. une $\mathbf{H}$-base orthogonale de V telle que $\psi(h_1e_k,h_2e_k)=\mathrm{tr}_{\mathbf{H}/\mathbf{R}}(h_1ih_2^\star)$ pour tout k. Soit $I=I(\mathcal{B})$ l'endomorphisme $\mathbf{H}$-linéaire de (V,ψ) qui envoie e_k sur $-ie_k$. Alors $I\in\mathcal{X}$ et

$$\mathcal{X}=G(\mathbf{R})\cdot I=\{I(\mathcal{B})|\mathcal{B}\ (i,\mathbf{H})-\text{base}\}.$$

10.6. **Les cas simples.** On décrit (1) les $\mathbf{Q}$-algèbres simples à involutions $(B, \star)$ tels que $\star_{\mathbf{R}} > 0$ sur $B_{\mathbf{R}}$, (2) les invariants qui classifient $\mathcal{H}(B, \star, -)$, (3) les espaces $\mathcal{X} = G(\mathbf{R}) \cdot I$. On part de la classification déjà établie.

- **$\mathcal{Q}(F)$:** $B = M_n(F)$ avec $\star = \star_\phi$ pour $\phi \in \mathcal{Q}(F)$. Alors F est totalement réel, $\mathcal{H}(B, \star, -1) \simeq \mathcal{A}(F)$ est classifié par le rang et $\mathcal{X}$ est un produit de $[F : \mathbf{Q}]$ espaces de type $I(+)$.
- **$\mathcal{A}(D)$:** $B = M_n(D)$ avec $\star = \star_\phi$ pour $\phi \in \mathcal{A}(D)$, D/F quaternionique. Alors F est totalement réel, D totalement indéfini, $\mathcal{H}(B, \star, -1) \simeq \mathcal{Q}(D)$ est classifié par le rang et $\mathcal{X}$ est un produit de $[F : \mathbf{Q}]$ espaces de type $I(+)$.
- **$\mathcal{A}(F)$:** ce cas est *exclu,* il n'y a pas d'involution positive. Heureusement, puisque c'est le seul cas ou les invariants plus subtils de type Hasse sont requis pour la classification de $\mathcal{H}(B, \star, -) \simeq \mathcal{Q}(F)$.
- **$\mathcal{Q}(D)$:** $B = M_n(D)$ avec $\star = \star_\phi$ pour $\phi \in \mathcal{Q}(D)$, D/F quaternionique. Alors F est totalement réel, D totalement défini, $\mathcal{H}(B, \star, -1) \simeq \mathcal{A}(D)$ est... problématique, car ne vérifie pas le principe de Hasse, et $\mathcal{X}$ est un produit de $[F : \mathbf{Q}]$-espaces de type $I(-)$.
- **$\mathcal{H}(K)$:** $B = M_n(K)$ avec $\star = \star_\phi$ pour $\phi \in \mathcal{H}(K)$. Alors K est une extension CM de F, $\mathcal{H}(B, \star, -) \simeq \mathcal{H}(K)$ est classifiée par rang, discriminant et signatures, et $\mathcal{X}$ est un produit de $[F : \mathbf{Q}]$-espaces de type II.
- **$\mathcal{H}(D)$:** $B = M_n(D)$ avec $\star = \star_\phi$ pour $\phi \in \mathcal{H}(D)$. Alors K est une extension CM de F, $\mathcal{H}(B, \star, -) \simeq \mathcal{H}(D)$ est classifiée par rang, discriminant et signatures, et $\mathcal{X}$ est un produit de $[F : \mathbf{Q}]$-espaces de type II.

Références

[1] J. Dieudonné, A. Grothendieck, *Eléments de Géométrie algébriques*, Publications de L'IHES.
[2] Katz, B. Mazur, *Moduli of Elliptic Curves.*
[3] Kottwitz, *Zeta functions of some simple Shimura Varieties.*
[4] J. Milne, Class Field Theory Course.
[5] D. Mumford, *Abelian Varieties.*
[6] W. Scharlau
[7] C. Voisin, *Théorie de Hodge et Géométrie Algébrique Complexe.*
[8] J. Tate, *Finite Flat Group Schemes*

THÉORIE DE LA MULTIPLICATION COMPLEXE

On se propose dans cette quatrième partie du cours d'étudier en détail une certaine classe de problèmes de module de type PEL qui est très remarquable à plus d'un titre : (1) les variétés abéliennes que l'on classifie sont distinguées dans la catégorie de toutes les variétés abéliennes par une propriété de maximalité (ce sont les variétés abéliennes *de type CM*), (2) les schémas qui classifient ces variétés abéliennes de type CM sont *finis* (ce sont les variétés de Shimura de dimension 0), et (3) les groupes réductifs qui décrivent les $\mathbf{C}$-points de ces schémas sont des *tores.* Dans la cinquième partie du cours, nous verrons que la théorie des variétés de Shimura s'appuie de manière essentielle sur la théorie de la multiplication complexe.

1. Schémas Abéliens à Multiplications Complexe

1.1. Compléments sur $\mathrm{Hom}_k^0(A, B)$. Soit k un corps (parfait).

Lemma 1.1. *La fonction $\phi \mapsto \deg \phi$ sur $\mathrm{End}_k(A)$ s'étend en une fonction*

$$\deg : \mathrm{End}_k^0(A) \to \mathbf{Q}$$

qui est polynomiale de degré $2g$ où $g = \dim A$.

Démonstration. Puisque $\deg(n\alpha) = n^{2g}\alpha$, il suffit de voir que pour tout α et β dans $\mathrm{End}_k(A)$, la fonction $n \mapsto \deg(n\alpha + \beta)$ est polynomiale. Si $\mathcal{L}$ est ample sur A,

$$\chi(\mathcal{L}) \cdot \deg(n\alpha + \beta) = \chi((n\alpha + \beta)^\star \mathcal{L})$$

Il suffit donc de montrer que la fonction $n \mapsto \chi((n\alpha + \beta)^\star \mathcal{L})$ est polynomiale sur $\mathcal{L}$, ce qui résulte du théorème du cube, cf [1, §19, Theorem 2]. □

Corollary 1.2. *Pour tout sous-groupe M de $\mathrm{Hom}_k(A, B)$ de type fini sur $\mathbf{Z}$, l'intersection N de $\mathbf{Q}M$ et $\mathrm{Hom}_k(A, B)$ dans $\mathrm{Hom}_k^0(A, B)$ est de type fini sur $\mathbf{Z}$.*

Démonstration. On se ramène au cas où A et B sont simples, puis au cas où $A = B$. Le polynome $\phi \mapsto \deg \phi$ sur $\mathrm{End}_k^0(A)$ se restreint au $\mathbf{Q}$-espace vectoriel de dimension finie $\mathbf{Q}M$, puis s'étend au $\mathbf{R}$-espace vectoriel $V = \mathbf{Q}M \otimes_{\mathbf{Q}} \mathbf{R}$ en une application polynomiale (donc continue) $V \to \mathbf{R}$. L'ensemble $U = \{v \in V : |\deg(v)| < 1\}$ est alors un voisinage ouvert de 0 dans V dont l'intersection avec $N = \mathbf{Q}M \cap \mathrm{End}_k(A)$ est réduite à 0. Donc N est un sous-groupe discret de V : on sait que de tels sous-groupes sont de type fini sur $\mathbf{Z}$. □

Proposition 1.3. *Pour tout $\ell \neq \mathrm{car} k$ et A, B sur k,*

$$\mathrm{Hom}_k(A, B) \otimes \mathbf{Z}_\ell \hookrightarrow \mathrm{Hom}_{\mathbf{Z}_\ell}(T_\ell A, T_\ell B).$$

Démonstration. Il suffit de montrer que pour tout sous-groupe M de $\mathrm{Hom}_k(A, B)$ qui est de type fini sur $\mathbf{Z}$, $T_\ell : M \otimes \mathbf{Z}_\ell \hookrightarrow \mathrm{Hom}_{\mathbf{Z}_\ell}(T_\ell A, T_\ell B)$, et l'on peut supposer d'après le corollaire précédent que M est saturé dans $\mathrm{Hom}_k(A, B)$. Soit $\alpha_1, \cdots, \alpha_r$ une $\mathbf{Z}$-base de M, $\lambda_1, \cdots, \lambda_r \in \mathbf{Z}_\ell$ tels que $T_\ell(\alpha_1 \otimes \lambda_1 + \cdots + \alpha_r \otimes \lambda_r) = 0$, et $n_i(s) \in \mathbf{Z}$ avec $n_i(s) \equiv \lambda_i \bmod \ell^s$. Alors $\alpha(s) = n_1(s)\alpha_1 + \cdots + n_r(s)\alpha_r \in \mathrm{Hom}_k(A, B)$ est nul sur $A[\ell^k]$, donc $\alpha(s) = \ell^s \cdot \beta(s)$ pour un $\beta(s) \in \mathrm{Hom}_k(A, B) \cap \mathbf{Q}M = M$, donc $\ell^s \mid n_i(s)$ pour tout i, donc $\lambda_i \equiv 0 \bmod \ell^s$ pour tout i et tout s, et $\lambda_i = 0$. □

Proposition 1.4. $\mathrm{Hom}_k(A,B) \simeq \mathbf{Z}^r$ *avec* $r \leq 4 \dim A \cdot \dim B$.

Démonstration. D'après le lemme précédent, $\mathrm{Hom}^0_k(A,B) \otimes_{\mathbf{Q}} \mathbf{Q}_\ell \hookrightarrow \mathrm{Hom}_{\mathbf{Q}_\ell}(V_\ell A, V_\ell B)$, donc $\mathrm{Hom}^0_k(A,B)$ est un $\mathbf{Q}$-espace vectoriel de dimension finie $r \leq 4 \dim A \cdot \dim B$. Soit $\alpha_1, \cdots, \alpha_r$ une $\mathbf{Q}$-base de $\mathrm{Hom}^0_k(A,B)$ contenue dans $\mathrm{Hom}_k(A,B)$, M le sous-module de $\mathrm{Hom}_k(A,B)$ engendré (sur $\mathbf{Z}$) par cette base. Alors

$$\mathrm{Hom}_k(A,B) = \mathrm{Hom}^0_k(A,B) \cap \mathrm{Hom}_k(A,B) = \mathbf{Q}M \cap \mathrm{Hom}_k(A,B)$$

est encore un $\mathbf{Z}$-module de type fini, donc en fait un $\mathbf{Z}$-module libre de rang r. □

Corollary 1.5. $\mathrm{End}^0_k(A)$ *est une* $\mathbf{Q}$*-algèbre semi-simple* de dimension finie $\leq 4g^2$.

1.2. **Schémas abéliens à multiplication complexe.**

Proposition 1.6. *Soit S un schéma connexe, A un S-schéma abélien de dimension g et $E \subset \mathrm{End}^0_S(A)$ une sous-algèbre commutative réduite. Alors $[E : \mathbf{Q}] \leq 2g$ avec égalité si et seulement si pour un (resp. tout) point géométrique s de S, pour un (resp. tout) $\ell \neq \mathrm{car} s$, le $E \otimes \mathbf{Q}_\ell$-module $V_\ell(A,s)$ est libre de rang 1.*

Démonstration. Par rigidité, $E \subset \mathrm{End}^0_s(A_s)$, donc d'après la proposition 1.3, le $E \otimes \mathbf{Q}_\ell$-module $V_\ell(A,s)$ est fidèle. Décomposons $E \otimes \mathbf{Q}_\ell = \prod E_i$ en produit de corps et $V_\ell(A,s) = \prod V_i$ en produit de E_i-espaces vectoriels. Alors $\dim_{E_i} V_i > 0$ par fidélité, et

$$2g = \dim_{\mathbf{Q}_\ell} V_\ell(A,s) = \sum \dim_{\mathbf{Q}_\ell} V_i = \sum \dim_{\mathbf{Q}_\ell} E_i \cdot \dim_{E_i} V_i \geq \sum \dim_{\mathbf{Q}_\ell} E_i = [E : \mathbf{Q}]$$

donc $[E : \mathbf{Q}] \leq 2g$ avec égalité si et seulement si $\dim_{E_i} V_i = 1$ pour tout i, i.e. $V_\ell(A,s)$ est un $E \otimes \mathbf{Q}_\ell$-module libre de rang 1. □

Definition 1.7. On dit que le S-schéma abélien A a multiplication complexe par E si $[E : \mathbf{Q}] = 2g$.

Remark 1.8. Si A/S a multiplication complexe par E, alors E est une sous-algèbre commutative maximale de $\mathrm{End}^0_S(A)$. Si ℓ est inversible dans S, alors pour tout point géométrique s de S, l'action de $\pi(S,s)$ sur $V_\ell(A,s)$ est donnée par un caractère $\chi_{A,\ell} : \pi(S,s) \to V_\ell(A,s)$. En particulier, cette action est abélienne.

Definition 1.9. Soit (A_i, ι_i) deux S-schémas abéliens à multiplication complexe par $\iota_i : E \hookrightarrow \mathrm{End}^0_S A_i$. On note $\mathrm{Hom}^0_S((A_1,\iota_1),(A_2,\iota_2))$ le sous-espace vectoriel de $\mathrm{Hom}^0_S(A_1,A_2)$ formé des éléments E-linéaires, i.e. des f tels que $f \circ \iota_1(e) = \iota_2(e) \circ f$ pour tout E. Une E-isogénie $(A_1,\iota_1) \to (A_2,\iota_2)$ est une isogénie qui est E-linéaire.

Corollary 1.10. *L'ensemble des isogénies est soit vide, soit un $E^\times$-espace homogène principal.*

Démonstration. L'ensemble des isogénies $(A_1,\iota_1) \to (A_2,\iota_2)$ est l'ensemble des isomorphismes E-linéaires $(A_1,\iota_1) \to (A_2,\iota_2)$ dans une catégorie convenable. C'est donc vide, ou bien un espace homogène principal sous $\mathrm{End}^0_S(A_1,\iota_1)^\times$. Mais $\mathrm{End}^0_S(A_1,\iota_1)$ est le commutant de $\iota_1(E)$ dans $\mathrm{End}^0_S(A_1)$, et c'est donc $\iota_1(E)$ puisque $\iota_1(E)$ est une sous-algèbre commutative maximale de $\mathrm{End}^0_S(A_1)$. □

Lemma 1.11. *Si $A \sim \oplus A_i$ dans $\mathbf{Ab}^0_S$ avec A_i simples, alors A a de la multiplication complexe $\iff$ pour tout i, A_i a de la multiplication complexe.*

Démonstration. On écrit $A \sim \oplus A_i^{n_i}$ où les A_i sont simples et deux à deux non-isogènes. Alors $\mathrm{End}_k^0 A = \prod M_{n_i}(D_i)$ où $D_i = \mathrm{End}_S^0 A_i$ est un corps gauche. Soit F_i le centre de D_i, $d_i^2 = [D_i : F_i]$, $f_i = [F_i : \mathbf{Q}]$ et $g_i = \dim A_i$. Les $\mathbf{Q}$-sous-algèbres commutatives maximales de D_i sont les F_i-sous-algèbres commutatives maximales de D_i, et elles ont donc une F_i-dimension égale à d_i (d'après le formule du bicommutant) et une $\mathbf{Q}$-dimension égale à $d_i f_i$. Donc $d_i f_i \leq 2g_i$ avec égalité si et seulement si A_i a de la multiplication complexe. De même, les $\mathbf{Q}$-sous-algèbres commutatives maximales de $\mathrm{End}^0 A$ sont des produits $E = \prod E_i$ de F_i-sous-algèbres commutatives E_i de $M_{n_i}(D_i)$ lesquelles ont pour F_i-dimension $n_i d_i$ et pour $\mathbf{Q}$-dimension $n_i d_i f_i$. On trouve donc

$$[E : \mathbf{Q}] = \sum_i [E_i : \mathbf{Q}] = \sum_i n_i d_i f_i \leq 2 \sum_i n_i g_i = 2g$$

avec égalité si et seulement si $d_i f_i = 2g_i$ pour tout i, CQFD. □

Exercise 1.12. Si $S = \mathrm{Spec} k$ est le spectre d'un corps parfait, et A/k a multiplication complexe par un *corps*, alors $A \sim A_1^n$ pour une variété abélienne simple A_1 a multiplication complexe par un autre corps.

1.3. **Variétés abéliennes CM et points complexes.** On suppose toujours que S est connexe, et admet un point géométrique $s \in S(\mathbf{C})$. Le cas que l'on a en vue est celui où $S = \mathrm{Spec} k$ pour un sous-corps k de $\mathbf{C}$.

Lemma 1.13. *Soit A un S-schéma abélien de dimension relative g. On suppose que A est simple, i.e. $E = \mathrm{End}_S^0(A)$ est un corps, et admet de la multiplication complexe, i.e. E contient un corps commutatif C de $\mathbf{Q}$-dimension $2g$. Alors $C = E$ est un corps CM et toute polarisation $\lambda : A \to A^t$ est $(E, \star)$-linéaire, où $\star$ est l'involution canonique de E.*

Démonstration. Sur $\mathbf{C}$, $A_s(\mathbf{C}) = V_{\mathbf{R},I}/\Lambda$ correspond à un couple (polarisable) (Λ, I) où Λ est un réseau de dimension $2g$ et I une structure complexe sur $V_{\mathbf{R}}$, avec $V = \Lambda \otimes \mathbf{Q}$. On a donc $C \subset E \subset D$, où

$$D = \mathrm{End}_{\mathbf{C}}^0(A_s) = \{\alpha \in \mathrm{End}_{\mathbf{Q}}(V) : \alpha_{\mathbf{R}} \circ I = I \circ \alpha_{\mathbf{R}}\}$$

n'est à priori qu'une $\mathbf{Q}$-algèbre semi-simple de dimension finie. Décomposons $D \simeq \prod_i D_i$ et $V \simeq \prod V_i$ avec D_i simple et V_i un D_i-module, de sorte que chacun des V_i est aussi un E-espace vectoriel, qui est *non-nul* puisque V est un M-module fidèle. Alors

$$2g = \dim_{\mathbf{Q}} V = \sum_i \dim_{\mathbf{Q}} V_i = [E : C][C : \mathbf{Q}] \cdot \sum_i \dim_E V_i = 2g \cdot [E : C] \cdot \sum_i \dim_E V_i.$$

Donc : $E = C$ est commutatif, D est simple, et V est un E-espace vectoriel de dimension 1. La structure complexe I induit un morphisme de $\mathbf{R}$-algèbre $\mathbf{C} \hookrightarrow \mathrm{End}_{E_{\mathbf{R}}}(V_{\mathbf{R}}) = E_{\mathbf{R}}$, donc E est totalement imaginaire. Soit enfin $\lambda : A \to A^t$ une polarisation (sur S). Alors λ induit une involution $\star_E$ sur $E = \mathrm{End}_S^0 A$ par la formule $\alpha^{\star_E} = \lambda^{-1} \alpha^t \lambda$, de sorte que $\lambda : A \to A^t$ est $(E, \star_E)$ linaire par définition. De même, $\lambda_s : A_s \to A_s^t$ induit une involution $\star_D$ sur D, qui bien sûr fixe E et y induit $\star_E$. Mais la polarisation λ_s de A_s correspond à une polarisation $\psi_{\mathbf{R}}$ de la paire (Λ, I). Puisque $\psi_{\mathbf{R},I} > 0$, l'involution $\star_D$ est positive, donc $\star_E$ aussi. En particulier, le sous-corps F de E fixé par $\star_E$ est totalement réel, donc distinct de E. Mais alors E est un corps CM, F est son sous-corps totalement réel, et $\star_E$ est l'involution canonique de E. □

Corollary 1.14. *Toute variété abélienne CM sur $k \subset \mathbf{C}$ admet de la multiplication complexe par une $\mathbf{Q}$-algèbre CM.*

Remark 1.15. Le lemme est faux en caractéristique p : une courbe elliptique supersingulière E sur $k = \overline{\mathbf{F}}_p$est simple et CM, mais $\mathrm{End}_k^0 E$ n'est pas commutatif.

Mentionnons également une espèce de réciproque du corollaire ci-dessus :

Lemma 1.16. *Sur $k = \mathbf{C}$, tout tore complexe X de dimension g sur lequel agit fidèlement un produit de corps* CM *de dimension $2g$ est une variété abélienne CM.*

Démonstration. Nous verrons cela plus bas. □

Remark 1.17. Le lemme est faux si l'on ne suppose pas que E est CM.

1.4. **Propriétés de Bonne Réduction.** Soit S un schéma de Dedekind intègre, ξ le point générique de S, et x un point fermé de S. Soit Soit A une variété abélienne sur ξ. On dit que A a bonne réduction en x si et seulement si A s'étend en un schéma abélien sur $S(x) = \mathrm{Spec}\mathcal{O}_{S,x}$. En général, partant d'un modèle quelconque $\mathcal{A}$ de la variété A sur S, il existe un ouvert U de S au-dessus duquel $\mathcal{A}$ est un schéma abélien : donc A a bonne réduction en presque tous les points de S (i.e. tous sauf un nombre fini).

Cependant, il existe sur S un modèle qui est meilleur que les autres : le modèle de Néron $\mathcal{A}/S$. C'est un modèle qui est déjà *lisse* et qui vérifie la propriété universelle suivante : pour tout schéma X qui est lisse sur S, tout ξ-morphisme $X_\xi \to A$ s'étend en un S-morphisme $X \to \mathcal{A}$. En particulier, ce modèle de Néron est uniquement déterminé (à isomorphisme unique près) par cette propriété, et c'est canoniquement un S-schéma *en groupes.*

Si A a bonne réduction en x et $\mathcal{A}$ est un schéma abélien sur $S(x)$ tel que $\mathcal{A}_\xi = A$, alors $\mathcal{A}$ est le modèle de Néron de A sur $S(x)$. Les points de S où A a bonne réduction sont donc exactement ceux où le modèle de Néron est propre (donc propre et lisse à fibre *générique* géométriquement connexe, ce qui implique que toutes les fibres le sont, comme on voit par exemple en considérant la factorisation de Stein). L'existence du modèle de Néron permet de démontrer le critére suivant :

Proposition 1.18. *On fixe un point géométrique s au-dessus de η. Pour tout point fermé $x \in S$, les conditions suivantes sont équivalentes* (1) *A a bonne réduction en x, et* (2) *pour un (resp. tout) $\ell \neq \mathrm{car}k(x)$, l'action de $\pi(\xi, s)$ sur $T_\ell(A, s)$ est non-ramifiée en x, i.e. se factorise à travers $\pi(S(x), s)$.*

Dans un langage plus familier, cela s'énonce ainsi.

Proposition 1.19. *Soit R un anneau de valuation discrète de corps résiduel k, K le corps des fractions de R, K^s une clôture séparable de K, $I \subset \mathrm{Gal}(K^s/K)$ le groupe d'inertie d'une place de K^s au-dessus de R. Soit A une variété abélienne sur K. Alors A a bonne réduction sur R si et seulement si I agit trivialement sur $T_\ell(A, K^{sep})$ pour un (resp. tout) $\ell \neq \mathrm{car}k$.*

Démonstration. [2] Soit $\mathcal{A}$ le modèle de Néron de A sur $S = \mathrm{Spec}R$, $\widetilde{K}$ le sous-corps de K^s fixé par I, $\widetilde{R}$ l'anneau de sa valuation, $\widetilde{k}$ le corps résiduel de cet anneau (c'est une extension séparable de k). La propriété universelle du modèle de Néron implique $\mathcal{A}(\widetilde{R}) = \mathcal{A}(\widetilde{K}) = A(\widetilde{K}) = A(K^s)^I$. Si $\ell \neq \mathrm{car}k$, la multiplication $\ell : \mathcal{A} \to \mathcal{A}$ est étale (et quasi-finie, mais pas nécessairement propre, i.e. pas nécessairement fini). Donc $\mathcal{A}[\ell^n]$ est étale et $\mathcal{A}[\ell^n](\widetilde{R}) = \mathcal{A}[\ell^n](\widetilde{k})$. Finalement,

$$T_\ell(A, K^s)^I = T_\ell(\mathcal{A}_k, \widetilde{k}) \quad \text{et} \quad V_\ell(A, K^s)^I = V_\ell(\mathcal{A}_k, \widetilde{k})$$

Or $\mathcal{A}_{\widetilde{k}}$ admet une filtration $0 \subset \mathcal{A}^1_{\widetilde{k}} \subset \mathcal{A}^2_{\widetilde{k}} \subset \mathcal{A}^3_{\widetilde{k}} \subset \mathcal{A}_{\widetilde{k}}$ dont les quotients successifs sont respectivement un produit $\mathbf{G}_a^r$, un produit $\mathbf{G}_m^s$, un variété abélienne de dimension d et un groupe fini. On a donc $r + s + d = g$ où g est la dimension de A. Chaque étape contribue à la $\mathbf{Q}_\ell$-dimension de $V_\ell(\mathcal{A}_k, \widetilde{k})$ pour respectivement 0, s, et $2d$. Donc I agit trivialement sur $V_\ell(A, K^s)$ si et seulement si $s + 2d = 2g$, i.e. $r = s = 0$, i.e. $\mathcal{A}_{\widetilde{k}}$ est propre, i.e. $\mathcal{A}$ est propre, CQFD. □

Appliquons tout ceci au cas qui nous intéresse : K est un corps de nombre, $S = \mathrm{Spec}\mathcal{O}_K$ où $\mathcal{O}_K$ est l'anneau des entiers de K, et A est une variété abélienne sur K à multiplication complexe par E. On sait alors que l'action de $\mathrm{Gal}(K^s/K)$ sur $V_\ell(A, s)$ se factorise à travers un caractère continu $\chi_{A,\ell} : \mathrm{Gal}(K^{ab}/K) \to \mathcal{O}_{E_\ell}^\times$, où $\mathcal{O}_{E_\ell}$ est l'anneau des entiers de $E_\ell = E \otimes \mathbf{Q}_\ell$. D'autre part, si $I(P) \subset \mathrm{Gal}(K^{ab}/K)$ est le groupe d'inertie en un idéal premier $P \in \mathrm{Spec}\mathcal{O}_K$ de caractéristique résiduelle $p \neq \ell$, alors $I(P)$ est une extension d'un groupe fini par un pro-p-groupe. On en déduit facilement que $\chi_{A,\ell}(I(P))$ est fini. Donc : A a bonne réduction potentielle en P, et plus précisément, il existe une extension abélienne finie L de K telle que A_L a bonne réduction au-dessus de P. En travaillant un peu plus, on peut montrer qu'il existe même une extension cyclique finie L de K telle que A_L a bonne réduction *partout,* cf Remarque *3.10.*

1.5. **Groupes de Mumford-Tate.** Soit $A \simeq V_{\mathbf{R},I}/\Lambda$ une variété abélienne sur $\mathbf{C}$. Le groupe de Mumford-Tate $\mathbf{MT}(A)$ est le plus petit sous-groupe algébrique H de $G = GL(V)$ (sur $\mathbf{Q}$!) tel que le morphisme $h_I : \mathbf{S} \to G_{\mathbf{R}}$ défini par I se factorise par $H_{\mathbf{R}}$. Rappelons que ce morphisme envoie $z \in \mathbf{C}^\times = \mathbf{S}(\mathbf{R})$ sur la multiplication par z dans le $\mathbf{C}$-espace vectoriel $V_{\mathbf{R},I}$. Alors :

Lemma 1.20. *Pour toute variété abélienne A sur $\mathbf{C}$,*

$$A \text{ est CM} \iff \mathbf{MT}(A) \text{ est un tore.}$$

Démonstration. Si A a de la multiplication complexe par E, V est un E-module libre de rang 1 donc $T_E = \mathrm{Res}_{E/\mathbf{Q}}\mathbf{G}_{m,E} = GL_E(V)$ est un $\mathbf{Q}$-tore (maximal) de $G = GL(V)$. Puisque E commute à l'action de I sur $V_{\mathbf{R}}$, $h_I : \mathbf{S} \to GL_{\mathbf{R}}(V_{\mathbf{R}})$ se factorise par T_E, donc $\mathbf{MT}(A) \subset T_E$ est un tore. Inversement, si $\mathbf{MT}(A) = T$ est un $\mathbf{Q}$-tore dans $G = GL(V)$, alors V est une représentation fidèle de T et l'anneau des endomorphismes de cette représentation contient une $\mathbf{Q}$-sous-algèbre commutative réduite E de $\mathrm{End}(V)$ de $\mathbf{Q}$-dimension $2g = \dim_{\mathbf{Q}} V$. Puisque l'action de E sur $V_{\mathbf{R}}$ commute à celle de I, $E \subset \mathrm{End}^0(A)$ et A a multiplication complexe par E. □

1.6. **Conclusion.** Tout cela suggère que les variétés CM sont très remarquables, qu'il conviendrait donc de les classifier, et qu'il suffit pour cela (au moins sur $\mathbf{C}$) de classifier les variétés abéliennes à multiplication complexe par un produits de corps *CM* fixé.

2. La Multiplication Complexe sur C

2.1. **Les Q-algèbres CM.** On note $\tau : \mathbf{C} \to \mathbf{C}$ la conjugaison complexe $\tau(z) = \overline{z}$.

Lemma 2.1. *Pour un corps de nombre E, les conditions suivantes sont équivalentes : (1) Il existe un automorphisme $\tau_E \neq 1$ de E tel que $\iota \circ \tau_E = \tau \circ \iota$ pour tout plongement $\iota : E \hookrightarrow \mathbf{C}$, et (2)$E = F(\sqrt{a})$ pour un corps F totalement réel et un élément a totalement négatif.*

Démonstration. Exercice. □

Definition 2.2. Un corps CM est un corps de nombre qui vérifie les conditions équivalentes ci-dessus. Une $\mathbf{Q}$-algèbre CM est un produit de corps CM.

Remark 2.3. Les corps CM sont stables par composition, mais un sous-corps d'un corps CM n'est bien sûr pas forcément CM. La clôture galoisienne d'un corps CM est encore CM. La réunion $\mathbf{Q}^{cm} \subset \overline{\mathbf{Q}} \subset \mathbf{C}$ de tous les corps CM est l'extension Galoisienne de $\mathbf{Q}$ qui est fixée par $[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1}$ pour tout $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

Definition 2.4. Soit E une $\mathbf{Q}$-algèbre CM de dimension $2g$ et S un schéma. Un S-schéma abélien à multiplication complexe par E est une paire (A, ι) où A est un S-schéma abélien de dimension relative g et $\iota : E \hookrightarrow \mathrm{End}^0_S(A)$ une action fidèle de E sur A. Une E-isogénie $\lambda : (A_1, \iota_1) \to (A_2, \iota_2)$ est un isomorphisme E-linéaire $A_1 \to A_2$ dans la catégorie des S-schémas abéliens à isogénie près, i.e. un élément inversible $\lambda \in \mathrm{Hom}^0_S(A_1, A_2)$ tel que $\lambda \circ \iota_1(e) = \iota_2(e) \circ \lambda$ pour tout $e \in E$. On note $\mathrm{Hom}^0_S((A_1, \iota_1), (A_2, \iota_2))$ l'ensemble de ces E-isogénies. En particulier, $\mathrm{End}^0_{E,S}(A, \iota)$ est le commutant de $\iota(E)$ dans $\mathrm{End}^0_S(A)$.

2.2. **Classification sur C.** Soit E une $\mathbf{Q}$-algèbre CM de dimension $2g$. On se propose de décrire l'ensemble $\mathcal{H}(E)$ des classes d'isomorphismes de variétés abéliennes à multiplication complexe par E sur $S = \mathrm{Spec}\mathbf{C}$. Il revient au même de décrire l'ensemble des classes d'isomorphismes de couples polarisables (Λ, I) où Λ est un réseau dans un E-module fidèle $V = \Lambda \otimes \mathbf{Q}$ de $\mathbf{Q}$-dimension $2g$, et I une structure complexe $E \otimes \mathbf{R}$-linéaire sur $V_{\mathbf{R}}$. La variété abélienne CM associée est alors $A = V_{\mathbf{R},I}/\Lambda$. Dans ce contexte, une E-isogénie $\lambda : (\Lambda_1, I_1) \to (\Lambda_2, I_2)$ est un isomorphisme E-linéaire $V_1 \to V_2$ tel que $\lambda_{\mathbf{R}} : V_{1,\mathbf{R}} \to V_{2,\mathbf{R}}$ est $\mathbf{C}$-linéaire, i.e. $\lambda_{\mathbf{R}} \circ I_1 = I_2 \circ \lambda_{\mathbf{R}}$.

2.2.1. *Le E-module V.*

Lemma 2.5. *V est un E-module libre de rang 1.*

Démonstration. C'est un E-module fidèle de $\mathbf{Q}$-dimension $2g$. Décomposant $E = \prod E_j$ en produit de corps et $V = \prod V_j$ en produit de E_j-espaces vectoriels non-nuls (puisque V est un E-module fidèle), on obtient

$$2g = \dim_{\mathbf{Q}} V = \sum_j \dim_{\mathbf{Q}} V_j = \sum_j \dim_{\mathbf{Q}} E_j \cdot \dim_{E_j} V_j \geq \sum_j \dim_{\mathbf{Q}} E_j = \dim_{\mathbf{Q}} E = 2g$$

donc $\dim_{E_j} V_j = 1$ pour tout j, CQFD. □

Remark 2.6. On comparera utilement cette preuve à celle de la proposition 1.6.

On peut donc supposer que $V = E$.

2.2.2. *La structure complexe I.*

Definition 2.7. Si E est une $\mathbf{Q}$-algèbre CM, un type CM sur E est un sous-ensemble Φ de $\mathrm{Hom}_{\mathbf{Q}-alg}(E,\mathbf{C})$ tel que $\Phi\coprod\overline{\Phi}=\mathrm{Hom}_{\mathbf{Q}-alg}(E,\mathbf{C})$. Une paire CM est un couple (E,Φ) formé d'une $\mathbf{Q}$-algèbre CM E et d'un type CM Φ sur E.

Lemma 2.8. *Soit V un E-module libre de rang 1. Il revient au même de se donner (1) une structure complexe E-linéaire I sur $V_{\mathbf{R}}$, (2) un morphisme de $\mathbf{R}$-algèbre $\iota:\mathbf{C}\to E_{\mathbf{R}}$, (3) un type CM Φ sur E. Dans cette correspondance,*

$$(V_{\mathbf{R}},I)\simeq\oplus_{\phi\in\Phi}\mathbf{C}(\phi)\quad\textit{comme module sur } E\otimes\mathbf{C}=\prod_{\phi\in\mathrm{Hom}_{\mathbf{Q}-alg}(E,\mathbf{C})}\mathbf{C}(\phi).$$

Démonstration. Une structure complexe E-linéaire I sur $V_{\mathbf{R}}$ est un morphisme de $\mathbf{R}$-algèbre $\iota:\mathbf{C}\to\mathrm{End}_{E_{\mathbf{R}}}(V_{\mathbf{R}})=E_{\mathbf{R}}$ donc (1) $\iff$ (2). Pour le reste, on décompose

$$E=\prod E_j\quad\text{et}\quad E_{j,\mathbf{R}}=\textstyle\prod_{v:F_j\hookrightarrow\mathbf{R}}E_{j,v}$$

où F_j est le sous-corps totalement réel de E_j et $E_{j,v}=E_j\otimes_{F_j,v}\mathbf{R}$. Alors

$$\mathrm{Hom}_{\mathbf{R}-alg}(\mathbf{C},E_{\mathbf{R}})=\prod_{j,v:F_j\to\mathbf{R}}\mathrm{Hom}_{\mathbf{R}-alg}(\mathbf{C},E_{j,v})=\prod_{j,v}\mathrm{Aut}_{\mathbf{R}-alg}(\mathbf{C},E_{j,v}).$$

Le choix d'un morphisme de $\mathbf{R}$-algèbre $\mathbf{C}\to E_{\mathbf{R}}$ est donc le choix pour tout j et tout v d'un isomorphisme $E_{j,v}\to\mathbf{C}$, i.e. d'une extension de $v:F_j\hookrightarrow\mathbf{R}$ à $\phi:E_j\hookrightarrow\mathbf{C}$, donc (2) $\iff$ (3). □

Definition 2.9. La *donnée de Shimura* associée à (E,Φ) est $(T_E,\{h_\Phi\})$ où T_E est le $\mathbf{Q}$-tore $T_E=\mathrm{Res}_{E/\mathbf{Q}}\mathbf{G}_{m,E}$ et $h_\Phi:\mathbf{S}\to T_{E,\mathbf{R}}$ est le morphisme qui envoie $z\in\mathbf{C}^\times=\mathbf{S}(\mathbf{R})$ sur $\iota_\Phi(z)\in(E\otimes\mathbf{R})^\times=T_{E,\mathbf{R}}(\mathbf{R})$, où $\iota_\Phi:\mathbf{C}\to E_{\mathbf{R}}$ est le morphisme de $\mathbf{R}$-algèbre associé à Φ.

2.2.3. *Les polarisations.* Soit F la sous-algèbre de E fixé par l'incolution canonique $\star$ de E. C'est donc un produit de corps totalement réels. On note $F_>^\times$ le sous-groupe de $F^\times$ formé des éléments λ qui sont totalement positifs, i.e. tels que $\phi(\lambda)>0$ pour tout morphisme de $\mathbf{Q}$-algèbre $\phi:F\to\mathbf{R}$. On note $N_{E/F}:E\to F$ la norme définie par $N_{E/F}(x)=x^\star x$, donc $N_{E/F}(E^\times)\subset F_>^\times$.

Soient Φ un type CM sur E, V un E-module libre de rang 1 et I la structure complexe sur $V_{\mathbf{R}}$ induite par Φ, i.e. I est la multiplication par $I=\iota_\Phi(i)\in(E\otimes\mathbf{R})^\times$. On se propose de décrire l'ensemble $\mathcal{P}(V,I)$ (resp. $\mathcal{P}[V,I]$) des polarisations de (V,I) (resp. des polarisations modulo les automorphismes $E^\times$ de (V,I)). On fixe pour cela un élément $\eta\in E^\times$ tel que

$$\forall\phi\in\Phi:\quad\phi(\eta)\in\mathbf{R}_<^\times i.$$

Exercise 2.10. Montrer que l'ensemble de ces éléments est une $F_>^\times$-orbite *non-vide* dans $E^\times$.

En particulier, $\eta^\star=-\eta$ donc l'ensemble des formes symplectiques $\psi:V\times V\to\mathbf{Q}$ induisant $\star$ sur E est en bijection avec l'ensemble des formes $(E,\star)$-hermitiennes $\Psi:V\times V\to E$ par l'application qui à Ψ associe $\psi(x,y)=\mathrm{Tr}_{E/\mathbf{Q}}(\eta\Psi(x,y))$. Ces formes sont elles-mêmes classifiées par leur discriminant $d(\Psi)$, un élément de $\widehat{H}^0(\star,E^\times)=F^\times/NE^\times$ défini par $d(\Psi)=\Psi(v,v)$ où v est une E-base de V.

Lemma 2.11. *ψ est une polarisation de (V,I) $\iff$ $d(\Psi)\in F_>^\times/NE^\times$.*

Démonstration. Soit $\phi(\eta) = -\lambda_\phi i$ avec donc $\lambda_\phi > 0$ pour $\phi \in \Phi$. Pour $x, y \in E \otimes \mathbf{R}$,

$$\psi_{\mathbf{R},I}(xv, yv) = \mathrm{Tr}_{E\otimes\mathbf{R}}\left(\eta I x y^\star \Psi(v,v)\right) = \sum_{\phi\in\Phi} \lambda_\phi \phi(x)\overline{\phi}(y)\phi(\Psi(v,v))$$

donc $\psi_{\mathbf{R},I} > 0$ si et seulement si $\phi(\Psi(v,v)) > 0$ pour tout $\phi \in \Phi$, i.e. $d(\Psi) \in F_>^\times$. □

Corollary 2.12. *L'action $(\lambda \cdot \psi)(x,y) = \psi(\lambda x, y)$ fait de $\mathcal{P}(V,I)$ un $F^\times$-espace homogène principal et de $\mathcal{P}[V,I]$ un $F_>^\times/N_{E/F}E^\times$-espace homogène principal.*

2.2.4. *Classifications.* Il résulte de ce qui précède que si $V_{\mathbf{R},I}/\Lambda$ est un tore complexe à multiplication complexe par E, alors $V_{\mathbf{R},I}/\Lambda$ est polarisable, i.e. c'est une variété abélienne. D'autre part, si (A,ι) est une variété abélienne à multiplication complexe par E, le $E \otimes \mathbf{C}$-module $\mathrm{Lie}(A) \simeq V_{\mathbf{R},I}$ est de la forme $\oplus_{\phi\in\Phi}\mathbf{C}(\phi)$ pour un unique type CM Φ de E. On dit alors que (A,ι) est de type CM (E,Φ). Deux variétés abéliennes (A,ι) et (A',ι') sont E-isogènes, i.e. liés par une E-isogénie, si et seulement si elles ont le même type CM. On note $\mathcal{H}(E,\Phi) \subset \mathcal{H}(E)$ la classe de E-isogénie définie par le type CM Φ. Alors $\mathcal{H}(E,\Phi)$ est en bijection avec l'ensemble des classes de réseaux Λ de V $(= E)$ modulo l'action du groupe des automorphismes $E^\times$ de V, i.e. avec l'ensemble des classes de $E^\times$-homothétie de réseaux Λ de V. La variété abélienne associée à Λ est $A = V_{\mathbf{R},I}/\Lambda$ où I la structure complexe E-linéaire sur $V_{\mathbf{R}}$ déterminé par Φ, i.e. I est la multiplication par $I = \iota_\Phi(i) \in (E\otimes\mathbf{R})^\times$.

2.3. **Le corps réflexe.**

Lemma 2.13. *Avec les notations ci-dessus, le corps réflexe $E(\Phi)$ de (E,Φ) est*

(1) *Le sous-corps de $\mathbf{C}$ fixé par $\{\sigma \in \mathrm{Aut}(\mathbf{C}) | \sigma\circ\Phi = \Phi\}$,*
(2) *Le sous-corps de $\mathbf{C}$ engendré par $\{\mathrm{Tr}_\Phi(e), e \in E\}$ où $\mathrm{Tr}_\Phi(e) = \sum_{\phi\in\Phi}\phi(e)$,*
(3) *Le corps réflexe de la donnée de Shimura $(T_E, \{h_\Phi\})$,*
(4) *Le corps de définition de la représentation $V(\Phi)_{\mathbf{C}} = \oplus_{\phi\in\Phi}\mathbf{C}(\phi)$ de $E\otimes\mathbf{C}$.*

Démonstration. On note $E(\Phi)_i$ le sous-corps de $\mathbf{C}$ défini par la condition i. Il est clair que $E(\Phi)_2 \subset E(\Phi)_1$ et inversement $E(\Phi)_1 \subset E(\Phi)_2$ d'après le théorème sur l'indépendance linéaire des caractères. On a $X_\star(T_{E,\mathbf{C}}) = \mathbf{Z}[\mathrm{Hom}(E,\mathbf{C})]$ avec l'action évidente de $\mathrm{Aut}(\mathbf{C})$. Via cet isomorphisme, le caractère $\mu_\Phi : \mathbf{G}_{m,\mathbf{C}} \to T_{E,\mathbf{C}}$ associé à h_Φ est $\sum_{\phi\in\Phi}\phi$, donc $E(\Phi)_1 = E(\Phi)_3$. On a aussi $E(\Phi)_2 \subset E(\Phi)_4$ puisque

$$\forall e \in E : \qquad \mathrm{Tr}_\Phi(e) = \mathrm{Tr}_{\mathbf{C}}(e|V(\Phi)).$$

Soit enfin $k \subset \mathbf{C}$ une extension Galoisienne de $E(\phi)_1$ qui contient $\phi(E)$ pour tout $\phi\in\Phi$. Alors $V(\Phi)_k = \oplus_{\phi\in\Phi}k(\phi)$ est un $E\otimes k$-module et

$$V(\Phi)_{E(\Phi)_1} = \left\{\textstyle\sum_{\phi\in\Phi} w_\phi : \forall\gamma \in \mathrm{Gal}(k/E(\phi)_1),\ \gamma w_\phi = w_{\gamma\phi}\right\}$$

est un modèle sur $E(\phi)_1$ du $E\otimes\mathbf{C}$-module $V(\Phi)$, donc $E(\Phi)_4 \subset E(\Phi)_1$. □

Example 2.14. Si $E = FE_0$ pour une extension quadratique imaginaire E_0 de $\mathbf{Q}$ et $\Phi = \{\phi : E \to \mathbf{C}$ tel que $\phi|E_0 = \phi_0\}$ où $\phi_0 : E_0 \to \mathbf{C}$ est un plongement fixé, alors $E(\Phi) = \phi_0(E_0)$.

Exercise 2.15. En général, montrer que $E(\Phi)$ est à nouveau un corps CM.

Definition 2.16. Soit k un sous-corps de $\mathbf{C}$ et (A,ι) une k-variété abélienne à multiplication complexe par E. Le type CM Φ de (A,ι) est le type CM de $(A,\iota)_{\mathbf{C}}$, i.e. $(A,\iota)_{\mathbf{C}} \in \mathcal{H}(E,\Phi)$.

Fact 2.17. *Si (A,ι) est de type CM Φ, le $E\otimes k$-module $(\mathrm{Lie}A)(k)$ est un modèle sur k du $E\otimes\mathbf{C}$-module $(\mathrm{Lie}A)(\mathbf{C})\simeq\oplus_{\phi\in\Phi}\mathbf{C}(\phi)$, donc k contient le corps réflexe $E(\Phi)$ de Φ. Si de plus k contient tous les $\phi(E)$ pour $\phi\in\Phi$, alors $(\mathrm{Lie}A)(k)\simeq\oplus_{\phi\in\Phi}k(\phi)$ comme $E\otimes k$-module.*

Remark 2.18. Si (A_1,ι_1) et (A_2,ι_2) sont deux k-variétés abéliennes à multiplication complexe par E, elles ont le même type CM (E,Φ) si et seulement si elles E-isogènes sur $\mathbf{C}$. Elles sont alors déjà E-isogènes sur la clôture algébrique de k dans $\mathbf{C}$, mais pas forcément E-isogènes sur k. Cependant :

Exercise 2.19. Montrer que si (A_1,ι_1) et (A_2,ι_2) sont E-isogènes sur k, alors

$$\mathrm{Hom}^0_k\left((A_1,\iota_1),(A_2,\iota_2)\right)=\mathrm{Hom}^0_{\mathbf{C}}\left((A_1,\iota_1)_{\mathbf{C}},(A_2,\iota_2)_{\mathbf{C}}\right).$$

En particulier, toute E-isogénie $(A_1,\iota_1)_{\mathbf{C}}\to(A_2,\iota_2)_{\mathbf{C}}$ est déjà définie sur k.

3. Le théorème principal de la multiplication complexe

3.1. **Les Q-tores.** Pour toute $\mathbf{Q}$-algèbre réduite de dimension finie k, on note $T_k=\mathrm{Res}_{k/\mathbf{Q}}\mathbf{G}_{m,k}$ le $\mathbf{Q}$-schéma en groupes dont les points sur une $\mathbf{Q}$-algèbre R sont donnés par $T_k(R)=(k\otimes R)^\times$. En particulier, $T_k|\overline{\mathbf{Q}}\simeq\prod_{\phi:k\hookrightarrow\Omega}\mathbf{G}_{m,\overline{\mathbf{Q}}}$ et T_k est un tore $\mathbf{Q}$-rationnel avec

$$X^\star(T_k)\simeq\mathcal{F}\left(\mathrm{Hom}_{\mathbf{Q}-alg}(k,\overline{\mathbf{Q}}),\mathbf{Z}\right)\quad\text{et}\quad X_\star(T_k)\simeq\mathbf{Z}\left[\mathrm{Hom}_{\mathbf{Q}-alg}(k,\overline{\mathbf{Q}})\right]$$

munis des actions évidentes de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Nous rencontrerons dans la suite divers sous-quotients des groupes $T_k(\mathbf{A}_f)=(k\otimes\mathbf{A}_f)^\times=\widehat{k}^\times$. Ces sous-quotients seront toujours munis de la topologie induite par la topologie adélique de $\widehat{k}^\times$.

On fixe dans toute la suite de cette section une paire CM (E,Φ). On note $\star$ l'involution canonique de E et $F=\{\lambda\in E:\lambda^\star=\lambda\}$, qui est un produit de corps totalement réels. On note $F^\times_>$ le sous-groupe de $F^\times$ formé des éléments totalement positifs. La norme $N_{E/F}:E\to F$ et l'inclusion $\mathbf{Q}\hookrightarrow F$ induisent des morphismes de $\mathbf{Q}$-tores

$$N_{E/F}:T_E\to T_F\quad\text{et}\quad\mathbf{G}_{m,\mathbf{Q}}\hookrightarrow T_F.$$

On note T^1_E le noyau de $N_{E/F}$ et $T^0_E=N^{-1}_{E/F}(\mathbf{G}_{m,\mathbf{Q}})$, de sorte que $T^1_E\subset T^0_E\subset T_E$. On montre facilement que la norme $N_{E/F}:T_E(\mathbf{A}_f)\to T_F(\mathbf{A}_f)$ est un morphisme ouvert, de même que sa restriction $N_{E/F}:T^0_E(\mathbf{A}_f)\to\mathbf{A}^\times_f$. Pour se familiariser un peu avec ces différents tores, montrons le lemme suivant.

Lemma 3.1. *Les lignes du diagramme commutatif suivant sont exactes*

$$\begin{array}{ccccccc}
0 & \to & T^1_E(\mathbf{A}_f)/T^1_E(\mathbf{Q}) & \to & T^0_E(\mathbf{A}_f)/T^0_E(\mathbf{Q}) & \xrightarrow{N} & \mathbf{A}^\times_f/\mathbf{Q}^\times_> \\
 & & \| & & \downarrow & & \downarrow \\
0 & \to & T^1_E(\mathbf{A}_f)/T^1_E(\mathbf{Q}) & \to & T_E(\mathbf{A}_f)/T_E(\mathbf{Q}) & \xrightarrow{N} & T_F(\mathbf{A}_f)/F^\times_>
\end{array}$$

et les groupes topologiques de la première ligne sont compacts.

Démonstration. L'exactitude à gauche est immédiate. Pour l'exactitude au milieu, il suffit de le démontrer pour la seconde ligne. Soit donc $x\in T_E(\mathbf{A}_f)$ tel que $N(x)=\lambda\in F^\times_>$. Alors λ est un élément de $F^\times$ qui est dans l'image de la norme $N_{E_v/F_v}:E^\times_v\to F^\times_v$ pour toute place v de $\mathbf{Q}$, donc $\lambda=N_{E/F}\mu$ pour un $\mu\in E^\times=$

$T_E(\mathbf{Q})$. Alors $N(x) = N(\mu)$ donc $x = \mu t^1$ avec $t^1 \in T^1(\mathbf{A}_f)$ et $\mu \in T_E(\mathbf{Q})$, cqfd. Dans $T_E(\mathbf{A}_f) = \widehat{E}$, on a

$$T_E^0(\mathbf{Q}) \cap \widehat{\mathcal{O}}_E^\times = \{\lambda \in \mathcal{O}_E^\times : \lambda\lambda^\star \in \mathbf{Q}^\times\} = \{\lambda \in \mathcal{O}_E^\times : \lambda\lambda^\star = 1\}.$$

Soit λ une telle unité. Puisque $[\mathcal{O}_E^\times : \mathcal{O}_F^\times]$ est fini, $\lambda^n \in \mathcal{O}_F^\times$ pour n assez grand, donc $\lambda^{2n} = \lambda^n(\lambda^n)^\star = (\lambda\lambda^\star)^n = 1$ et $\lambda \in \mu(E^\times)$, qui est fini. Donc $T_E^0(\mathbf{Q}) \cap \widehat{\mathcal{O}}_E^\times$ est fini et $T_E^0(\mathbf{Q})$ est discret (donc fermé) dans $T_E(\mathbf{A}_f)$. A fortiori, $T_E^1(\mathbf{Q})$ est discret (donc fermé) dans $T_E^1(\mathbf{A}_f)$. D'après Hilbert 90, $T_E^1(\mathbf{A}_f)$ est l'image du morphisme $h : T_E(\mathbf{A}_f) \to T_E(\mathbf{A}_f)$ qui envoie z sur $h(z) = z/z^\star$. On montre facilement que ce morphisme est ouvert, donc $h(\widehat{\mathcal{O}}_E^\times)$ est un sous-groupe ouvert et compact de $T_E^1(\mathbf{A}_f)$. Mais

$$\mathbf{Pic}(\mathcal{O}_E) = T_E(\mathbf{A}_f)/T_E(\mathbf{Q}) \cdot \widehat{\mathcal{O}}_E^\times \twoheadrightarrow T_E^1(\mathbf{A}_f)/T_E^1(\mathbf{Q}) \cdot h(\widehat{\mathcal{O}}_E^\times).$$

Puisque $\mathbf{Pic}(\mathcal{O}_E)$ est fini, $T_E^1(\mathbf{A}_f)/T_E^1(\mathbf{Q}) \cdot h(\widehat{\mathcal{O}}_E^\times)$ est fini donc $T_E^1(\mathbf{A}_f)/T_E^1(\mathbf{Q})$ est compact. Puisque tout idéal fractionnaire de $\mathbf{Z}$ est engendré par un élément de $\mathbf{Q}_>^\times$, $\mathbf{A}_f^\times = \widehat{\mathbf{Z}}^\times \times \mathbf{Q}_>^\times$ donc $\mathbf{A}_f^\times/\mathbf{Q}_>^\times$ est compact. Enfin, $T_E^0(\mathbf{A}_f)/T_E^0(\mathbf{Q})$ est compact comme extension séparée de deux groupes compacts. □

3.2. **L'action de** $\mathrm{Aut}(\mathbf{C})$ **sur** $\mathcal{H}(E)$**.** Le groupe $\mathrm{Aut}(\mathbf{C})$ des automorphismes de $\mathbf{C}$ agit sur $\mathcal{H}(\Phi)$ par $\sigma(A,\iota) = (\sigma A, \sigma\iota)$ où $\sigma A = (\mathrm{Spec}\sigma)^\star A$ et $(\sigma\iota)(e) = (\mathrm{Spec}\sigma)^\star(\iota(e))$ pour tout $e \in E$:

$$\begin{array}{ccc} \sigma A & \to & A \\ \downarrow & & \downarrow \\ \mathrm{Spec}\mathbf{C} & \xrightarrow{\mathrm{Spec}\sigma} & \mathrm{Spec}\mathbf{C} \end{array}$$

C'est bien une action à gauche, puisque

$$\mathrm{Spec}(\sigma_1\sigma_2)^\star = (\mathrm{Spec}(\sigma_2) \circ \mathrm{Spec}(\sigma_1))^\star = \mathrm{Spec}(\sigma_1)^\star \circ \mathrm{Spec}(\sigma_2)^\star.$$

L'action de $\mathrm{Aut}(\mathbf{C})$ sur l'ensemble des classes de E-isogénie se décrit aisément.

Lemma 3.2. *Pour tout* $\sigma \in \mathrm{Aut}(\mathbf{C})$, $\sigma \cdot \mathcal{H}(E,\Phi) = \mathcal{H}(E, \sigma\Phi)$.

Démonstration. Soit $(A,\iota) \in \mathcal{H}(E)$. Alors $\mathrm{Lie}(\sigma A) = \mathrm{Lie}(A) \otimes_{\mathbf{C},\sigma} \mathbf{C}$, donc

$$\mathrm{Lie}(A) \simeq \oplus_{\phi\in\Phi}\mathbf{C}(\phi) \quad \Rightarrow \quad \mathrm{Lie}(\sigma A) \simeq \oplus_{\phi\in\Phi}\mathbf{C}(\sigma\circ\phi)$$

comme $E \otimes \mathbf{C}$-module, CQFD. □

3.3. **Le morphisme** $r_\Phi : \mathrm{Gal}_{E(\Phi)}^{ab} \to T_E(\mathbf{Q})\backslash T_E(\mathbf{A}_f)$**.**

Proposition 3.3. *Il existe un unique morphisme de groupes topologiques*

$$r_\Phi : \mathrm{Gal}_{E(\Phi)}^{ab} \to T_E(\mathbf{Q})\backslash T_E(\mathbf{A}_f)$$

tel que pour tout $(A,\iota) \in \mathcal{H}(E,\Phi)$, $\sigma \in \mathrm{Aut}(\mathbf{C}/E(\Phi))$ *et* $\widehat{t} \in T_E(\mathbf{A}_f)$ *tel que* $r_\Phi(\sigma) = T_E(\mathbf{Q})\widehat{t}$, *il existe une E-isogénie* $\lambda : (A,\iota) \to \sigma(A,\iota)$ *telle que*

$$\forall x \in \widehat{V}_f(A,\mathbf{C}) : \qquad \lambda(\widehat{t}\cdot x) = \sigma\cdot x \quad \textit{dans } \widehat{V}_f(\sigma A, \mathbf{C}).$$

Remark 3.4. L'isogénie du lemme est alors unique.

Démonstration. Soit $(A,\iota) \in \mathcal{H}(E,\Phi)$ et $\sigma \in \mathrm{Aut}(\mathbf{C}/E(\Phi))$ comme dans l'énoncé. Puisque $\sigma(A,\iota) \in \mathcal{H}(E,\Phi)$, il existe une E-isogénie $\lambda : (A,\iota) \to \sigma(A,\iota)$, uniquement déterminée modulo $E^\times = T_E(\mathbf{Q})$. Les deux morphismes $V_f(A,\mathbf{C}) \to V_f(\sigma A,\mathbf{C})$ induits respectivement par σ et λ sont $\widehat{E}$-linéaires, et diffèrent donc d'un élément $\widehat{t} \in \widehat{E}^\times = T_E(\mathbf{A}_f)$ qui est uniquement déterminé par λ, i.e.

$$\forall x \in V_f(A,\mathbf{C}) : \qquad \lambda(\widehat{t}\cdot x) = \sigma \cdot x \quad \text{dans } V_f(\sigma A,\mathbf{C}).$$

On obtient ainsi une application bien définie

$$r_{(A,\iota)} : \mathrm{Aut}(\mathbf{C}/E(\Phi)) \to T_E(\mathbf{Q})\backslash T_E(\mathbf{A}_f)$$

qui vérifie la conclusion du lemme pour (A,ι) : pour tout $\sigma \in \mathrm{Aut}(\mathbf{C}/E(\Phi))$ et tout $\widehat{t} \in T_E(\mathbf{A}_f)$ tel que $r_{(A,\iota)}(\sigma) = T_E(\mathbf{Q})\cdot \widehat{t}$, il existe une unique E-isogénie $\lambda : (A,\iota) \to \sigma(A,\iota)$ telle que $\lambda(\widehat{t}\cdot x) = \sigma x$ dans $V_f(\sigma A,\mathbf{C})$ pour tout $x \in V_f(A,\mathbf{C})$. Il s'agit maintenant de vérifier que (1) cette application ne dépend pas du choix de (A,ι) dans $\mathcal{H}(E,\Phi)$, que (2) c'est un morphisme de groupes, que (3) ce morphisme de groupes se factorise par $\mathrm{Gal}(\overline{\mathbf{Q}}/E(\Phi))$, et (4) que le morphisme qui en résulte $r_\Phi : \mathrm{Gal}(\overline{\mathbf{Q}}/E(\Phi)) \to T_E(\mathbf{Q})\backslash T_E(\mathbf{A}_f)$ est continu.

Pour (1) : soient (A,ι) et (A',ι') dans $\mathcal{H}(E,\Phi)$ et $\sigma \in \mathrm{Aut}(\mathbf{C}/E(\Phi))$. Choisissons des E-isogénies $\alpha : (A,\iota) \to (A',\iota')$ et $\lambda : (A,\iota) \to \sigma(A,\iota)$. Alors

$$\beta = (\sigma\alpha)\circ\lambda\circ\alpha^{-1} : (A',\iota') \to (A,\iota) \to \sigma(A,\iota) \to \sigma(A',\iota')$$

est une E-isogénie. Soit $\widehat{t} \in T_E(\mathbf{A}_f)$ tel que $\lambda(\widehat{t}\cdot x) = \sigma x$ pour tout $x \in V_f(A,\mathbf{C})$. Alors

$$\beta(\widehat{t}\cdot y) = \left((\sigma\alpha)\circ\lambda\circ\alpha^{-1}\right)(\widehat{t}\cdot y) = (\sigma\alpha)\left(\lambda(\widehat{t}\cdot \widehat{x})\right) = (\sigma\alpha)(\sigma\cdot\widehat{x}) = \sigma\cdot\alpha(x) = \sigma\cdot y$$

pour tout $y \in V_f(A',\mathbf{C})$ avec $x \in V_f(A,\mathbf{C})$, $\alpha(x) = y$. Donc $r_{(A,\iota)}(\sigma) = T_E(\mathbf{Q})\cdot\widehat{t} = r_{(A',\iota')}(\sigma)$. On note r_Φ :

Pour (2) : soient (A,ι) dans $\mathcal{H}(E,\Phi)$ et σ_1, $\sigma_2 \in \mathrm{Aut}(\mathbf{C}/E(\Phi))$. Choisissons des E-isogénies $\lambda_i : (A,\iota) \to \sigma_i(A,\iota)$. Soient $\widehat{t}_i \in T_E(\mathbf{A}_f)$ tels que $\lambda_i(\widehat{t}_i\cdot x) = \sigma_i\cdot x$ pour tout $x \in V_f(A,s)$. Alors

$$\beta = (\sigma_1\lambda_2)\circ\lambda_1 : (A,\iota) \to \sigma_1(A,\iota) \to \sigma_1\sigma_2(A,\iota)$$

est une E-isogénie et pour tout $x \in V_f(A,\mathbf{C})$,

$$\beta(\widehat{t}_1\widehat{t}_2 x) = (\sigma_1\lambda_2)\left(\lambda_1\left(\widehat{t}_1(\widehat{t}_2 x)\right)\right) = (\sigma_1\lambda_2)\left(\sigma_1\cdot(\widehat{t}_2 x)\right) = \sigma_1\cdot\left(\lambda_2(\widehat{t}_2 x)\right) = \sigma_1\sigma_2\cdot x.$$

Donc $r_{(A,\iota)}(\sigma_1\sigma_2) = T_E(\mathbf{Q})\widehat{t}_1\widehat{t}_2 = T_E(\mathbf{Q})\widehat{t}_1\cdot T_E(\mathbf{Q})\widehat{t}_2 = r_{(A,\iota)}(\sigma_1)\cdot r_{(A,\iota)}(\sigma_2)$.

Pour (3), nous montrerons ultérieurement que $\mathcal{H}(E,\Phi)$ contient un élément (A,ι) défini sur $\overline{\mathbf{Q}}$. Pour tout $\sigma \in \mathrm{Aut}(\mathbf{C}/\overline{\mathbf{Q}})$, on a alors $\sigma(A,\iota) = (A,\iota)$ et $\sigma = Id$ sur $V_f(A,\mathbf{C})$, donc $\lambda = Id$ et $\widehat{t} = 1$ donnent $\lambda(\widehat{t}\cdot x) = \sigma\cdot x$ pour tout $x \in V_f(A,\mathbf{C})$, i.e. $r_{(A,\iota)}(\sigma) = T_E(\mathbf{Q})\cdot 1$.

Pour (4), on note que l'élément ci-dessus est même défini sur un corps de nombre $k \subset \overline{\mathbf{Q}}$ (qui contient nécessairement $E(\Phi)$ d'après 2.17), et l'on peut supposer que $\mathcal{O}_E = \mathrm{End}_k(A)\cap E$. Pour tout $n \geq 1$, notons $K(n)$ le sous-groupe de $T_E(\mathbf{A}_f)$ formé des éléments $\widehat{t} \in \widehat{\mathcal{O}}_E^\times$ tels que $\widehat{t} \equiv 1 \bmod n$. Soient $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/k(A[n]))$ et $\widehat{t} \in T_E(\mathbf{A}_f)$ tel que $\widehat{t}x = \sigma x$ pour tout $x \in V_f(A,\overline{\mathbf{Q}})$. Alors $\widehat{t} \in \widehat{\mathcal{O}}_E^\times$ puisque $\sigma T_f(A,\overline{\mathbf{Q}}) = T_f(A,\overline{\mathbf{Q}})$ et $\widehat{t} \in K(n)$ puisque $\sigma \equiv 1$ sur $T_f(A,\overline{\mathbf{Q}})/nT_f(\mathbf{A},\overline{\mathbf{Q}})$. Donc $r_\Phi^{-1}(T_E(\mathbf{Q})\cdot K(n))$ contient le sous-groupe ouvert $\mathrm{Gal}(\overline{\mathbf{Q}}/k(A[n]))$ de $\mathrm{Gal}(\overline{\mathbf{Q}}/E(\Phi))$. Puisque les $K(n)$ forment une base de voisinages ouverts de $1 \in T_E(\mathbf{A}_f)$, le morphisme $r_\Phi : \mathrm{Gal}(\overline{\mathbf{Q}}/E(\Phi)) \to T_E(\mathbf{Q})\backslash T_E(\mathbf{A}_f)$ est continu. $\square$

Corollary 3.5. *L'action de* $\mathrm{Aut}(\mathbf{C}/E(\Phi))$ *sur* $\mathcal{H}(E,\Phi)$ *se factorise par*

$$r_\Phi : \mathrm{Gal}^{ab}_{E(\Phi)} \to T_E(\mathbf{Q})\backslash T_E(\mathbf{A}_f)$$

et $\sigma[V_{\mathbf{R},I}/\Lambda] = [V_{\mathbf{R},I}/\Lambda']$ *pour* $\Lambda' \in r_\Phi(\sigma)\cdot\Lambda$.

Démonstration. Si $r_\Phi(\sigma) = T_E(\mathbf{Q})\widehat{t}$ et $(A,\iota) \simeq V_{\mathbf{R},I}/\Lambda$, il existe une E-isogénie $\lambda : (A,\iota) \to \sigma(A,\iota)$ telle que $\lambda(\widehat{t}\cdot x) = \sigma\cdot x$ pour tout $x \in V_f(A,\mathbf{C})$. Soit $(A',\iota') = V_{\mathbf{R},I}/\widehat{t}\cdot\Lambda$ et $\lambda_0 : V_{\mathbf{R},I}/\widehat{t}\cdot\Lambda \to V_{\mathbf{R},I}/\Lambda$ la E-isogénie qui correspond à l'identité de V. Alors λ_0 identifie $T_f(A',\iota')$ et $\widehat{t}\cdot T_f(A,\iota)$, donc

$$\lambda\circ\lambda_0\left(T_f(A',\iota')\right) = \lambda\left(\widehat{t}\cdot T_f(A,\iota)\right) = \sigma T_f(A,\iota) = T_f(\sigma A,\sigma\iota)$$

donc $\lambda\circ\lambda_0 : V_{\mathbf{R},I}/\widehat{t}\cdot\Lambda \to \sigma(A,\iota)$ est un isomorphisme de variété abélienne à multiplication complexe par E, CQFD. □

3.4. **La théorie du corps de classe.** Pour tout corps de nombres k, il existe un morphisme surjectif

$$\mathrm{Art}_k : T_k(\mathbf{Q})\backslash T_k(\mathbf{A}) \to \mathrm{Gal}^{ab}_k$$

tel que pour toute extension abélienne finie K/k, pour tout premier $\mathfrak{p}$ de k qui est non-ramifié dans K, si $s_\mathfrak{p} \in T_k(\mathbf{A}) = (k\otimes\mathbf{A})^\times = \prod' k_v^\times$ est l'idèle qui vaut 1 en $v \nmid p$ et une uniformisante en $v = v_\mathfrak{p}$, alors $\mathrm{Art}_k(s_\mathfrak{p}) = \mathrm{Frob}_\mathfrak{p}^{-1}$ dans $\mathrm{Gal}(K/k)$.

Le noyau de Art_k est la composante connexe de $1 \in T_k(\mathbf{Q})\backslash T_k(\mathbf{A})$. Si k est totalement imaginaire, ce noyau contient donc $T_k(\mathbf{R})$ et Art_k se factorise en

$$\mathrm{Art}_k : \overline{T_k(\mathbf{Q})}\backslash T_k(\mathbf{A}_f) \xrightarrow{\sim} \mathrm{Gal}^{ab}_k.$$

C'est le cas de tous les corps de nombres qui contiennent $E(\Phi)$. Le théorème principal de la multiplication complexe décrit le morphisme

$$r_\Phi\circ\mathrm{Art}_{E(\Phi)} : T_{E(\Phi)}(\mathbf{Q})\backslash T_{E(\Phi)}(\mathbf{A}_f) \to \mathrm{Gal}^{ab}_{E(\Phi)} \to T_E(\mathbf{Q})\backslash T_E(\mathbf{A}_f).$$

3.5. **La norme réflexe $N_\Phi : T_{E(\Phi)} \to T_E$.**

3.5.1. *Le morphisme algébrique.* Soit $k \subset \mathbf{C}$ un corps de nombre tel que $V(\Phi)_\mathbf{C} = \oplus_{\phi\in\Phi}\mathbf{C}(\phi)$ admette un modèle $V(\Phi)_k$ sur k (donc $E(\Phi)\subset k$). Ce modèle est alors unique à isomorphisme près, et se décompose comme $E = \prod E_j$ en $V(\Phi)_k = \prod V(\Phi)^j_k$. Chacun des $V(\Phi)^j_k$ est un $E_j\otimes k$-module. Pour toute $\mathbf{Q}$-algèbre R, on peut donc considérer $V(\Phi)^j_k\otimes R$ comme un $E_j\otimes R$-module libre, et prendre sur ce module le déterminant des éléments de $(k\otimes R)^\times = T_k(R)$: on obtient ainsi un morphisme de $\mathbf{Q}$-tores

$$N_{\Phi,k} : T_k \to \prod T_{E_j} = T_E$$

Si k contient tous les $\phi(E)$, $\phi\in\Phi$, alors

$$N_{\Phi,k}(\lambda) \mapsto \prod_{\phi\in\Phi}\phi^{-1}(N_{k/\phi(E)}\lambda).$$

Pour $k = E(\Phi)$, on note simplement $N_\Phi = N_{\Phi,E(\Phi)}$. C'est un morphisme

$$N_\Phi : T_{E(\Phi)} \to T_E.$$

On vérifie que $N_{\Phi,k} = N_\Phi\circ N_{k/E(\phi)}$ où $N_{k/E(\phi)} : T_k \to T_{E(\phi)}$ est induit par la norme.

3.5.2. *Le morphisme adélique/sur les idéaux.* La norme réflexe $N_{\Phi,k}$ induit un morphisme

$$N_{\Phi,k} : T_k(\mathbf{A}_f) = \widehat{k}^\times \to T_E(\mathbf{A}_f) = \widehat{E}^\times$$

dont on vérifie qu'il envoie $\widehat{\mathcal{O}}_k^\times$ dans $\widehat{\mathcal{O}}_E^\times$. On obtient donc

$$N_{\Phi,k} : I(k) \to I(E)$$

où $I(k) = \widehat{k}^\times / \widehat{\mathcal{O}}_k^\times$ est le groupe des idéaux fractionaires de k (et idem pour E) qui vérifie à nouveau $N_{\Phi,k} = N_\Phi \circ N_{k/E(\Phi)}$. En particulier, si $\mathcal{I}$ est un idéal fractionnaire de $E(\phi)$, k une extension de $E(\phi)$ qui contient tous les $\phi(E)$, $\phi \in \Phi$, et $\mathcal{O}_k\mathcal{I}$ l'idéal fractionnaire de k induit par $\mathcal{I}$, alors

$$N_\Phi(\mathcal{I})^{[k:E(\Phi)]} = N_{\Phi,k}(\mathcal{O}_k\mathcal{I}) = \prod_{\phi\in\Phi} \phi^{-1}(N_{k/\phi(E)}(\mathcal{O}_k\mathcal{I})).$$

3.5.3. *Le morphisme $N_\Phi \cdot N_\Phi^\star : T_{E(\Phi)} \to T_E$.* On peut calculer le morphisme

$$N_{E/F} \circ N_\Phi = N_\Phi \cdot N_\Phi^\star : T_{E(\Phi)} \to T_E.$$

Puisque

$$V(\Phi) \oplus V(\Phi)^\star \simeq \oplus_{\phi:E\hookrightarrow\mathbf{C}} \mathbf{C}(\phi) \simeq E \otimes \mathbf{C}$$

comme $E \otimes \mathbf{C}$-module, pour toute $\mathbf{Q}$-algèbre R et tout $\lambda \in (E(\Phi) \otimes R)^\times$,

$$(N_\Phi \cdot N_\Phi^\star)(\lambda) = \det{}_{E\otimes R}\,(\lambda | E(\Phi) \otimes E \otimes R) = N_{E(\Phi)/\mathbf{Q}}(\lambda)$$

où $N_{E(\Phi)/\mathbf{Q}} : T_{E(\Phi)} \to T_{\mathbf{Q}} = \mathbf{G}_{m,\mathbf{Q}}$ est induit par la norme. En particulier,

$$N_\Phi : T_{E(\Phi)} \to T_E^0 \subset T_E.$$

3.6. Le théorème principal de la multiplication complexe.

Theorem 3.6. *Avec les notations ci-dessus,*

$$r_\Phi \circ \mathrm{Art}_{E(\Phi)} = N_\Phi : T_{E(\Phi)}(\mathbf{Q})\backslash T_E(\mathbf{A}_f) \to T_E(\mathbf{Q})\backslash T_E(\mathbf{A}_f).$$

Corollary 3.7. *Pour tout $(A,\iota) \in \mathcal{H}(E,\Phi)$, $\sigma \in \mathrm{Aut}(\mathbf{C}/E(\Phi))$ et $s \in T_{E(\Phi)}(\mathbf{A}_f)$ tel que $\mathrm{Art}_{E(\Phi)}(s) = \sigma|E(\Phi)^{ab}$, il existe une unique E-isogénie $\lambda : (A,\iota) \to \sigma(A,\iota)$ telle que*

$$\forall x \in V_f(A,\mathbf{C}) : \qquad \lambda(N_\Phi(s)\cdot x) = \sigma x \quad \textit{dans } V_f(\sigma A, \mathbf{C}).$$

Démonstration. C'est immédiat. □

Corollary 3.8. *Avec ces notations, pour toute polarisation $\alpha : A \to A^t$ qui est $(E,\star)$-linéaire, l'isogénie $\lambda : (A,\iota) \to \sigma(A,\iota)$ envoie $\mathbf{Q}\alpha$ sur $\mathbf{Q}\sigma\alpha$.*

Démonstration. Pour tout $x, y \in V_f(A,\mathbf{C})$,

$$\langle x,y\rangle_f^{\lambda^t\circ\sigma\alpha\circ\lambda} = \left\langle x, \lambda^t\circ\sigma\alpha\circ\lambda(y)\right\rangle_f^A = \langle\lambda(x), \sigma\alpha\circ\lambda(y)\rangle_f^{\sigma A} = \langle\lambda(x),\lambda(y)\rangle_f^{\sigma\alpha}$$

donc si $\widehat{t} = N_\Phi(s)$,

$$\left\langle \widehat{t}x, \widehat{t}y\right\rangle_f^{\lambda^t\circ\sigma\alpha\circ\lambda} = \left\langle\lambda(\widehat{t}x),\lambda(\widehat{t}y)\right\rangle_f^{\sigma\alpha} = \langle\sigma\cdot x, \sigma\cdot y\rangle_f^{\sigma\alpha} = \chi_{cyl}(\sigma)\cdot\langle x,y\rangle_f^\alpha.$$

Mais la théorie du corps de classe fournit un $c \in \mathbf{Q}_>^\times$ tel que

$$\chi_{cyc}(\sigma) = \chi_{cyc}\circ\mathrm{Art}_{E(\Phi)}(s) = c\cdot N_{E(\Phi)/\mathbf{Q}}(s) = c\cdot N_\Phi(s)\cdot N_\Phi(s)^\star = c\cdot\widehat{tt^\star}$$

Puisque $\langle \widehat{t}x, \widehat{t}y \rangle_f^{\lambda^t \circ \sigma\alpha\circ\lambda} = \langle x, \widehat{t}^\star \widehat{t}y \rangle_f^{\lambda^t \circ \sigma\alpha\circ\lambda} = c^{-1}\chi_{cyc}(\sigma)\, \langle x, y\rangle_f^{\lambda^t \circ \sigma\alpha\circ\lambda}$, on obtient

$$\forall x, y \in V_f(A, \mathbf{C}) : \qquad \langle x, y\rangle_f^{\lambda^t \circ \sigma\alpha\circ\lambda} = c\, \langle x, y\rangle_f^{\alpha} = \langle x, y\rangle_f^{c\alpha}$$

donc $c\alpha = \lambda^\star(\sigma\alpha)$. □

Corollary 3.9. *Soit* $(A, \iota) \in \mathcal{H}(E, \Phi)$ *défini sur un corps de nombre* $k \subset \overline{\mathbf{Q}}$ *et*

$$\chi_A : \mathrm{Gal}_k^{ab} \to \widehat{E}^\times = T_E(\mathbf{A}_f)$$

le caractère qui donne l'action de $\mathrm{Gal}(\overline{\mathbf{Q}}/k)$ *sur* $V_f(A, \overline{\mathbf{Q}})$*, i.e.*

$$\forall x \in V_f(A, \overline{\mathbf{Q}}) \textit{ et } \sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/k) : \qquad \sigma \cdot x = \chi_A(\sigma) \cdot x \quad \textit{dans } V_f(A, \overline{\mathbf{Q}})$$

Alors : il existe un (unique) caractère $\epsilon_k : T_k(\mathbf{A}_f) \to E^\times$ *tel que*

$$\chi_A \circ \mathrm{Art}_k = \epsilon_k \cdot N_{\Phi,k} : T_k(\mathbf{A}_f) \to T_E(\mathbf{A}_f).$$

Démonstration. D'après le théorème, pour tout $s \in T_k(\mathbf{A}_f)$ donnant $s' = N_{k/E(\Phi)}(s)$ dans $T_{E(\Phi)}(\mathbf{A}_f)$ et $\sigma' = \mathrm{Art}_{E(\Phi}(s')$ dans $\mathrm{Gal}_{E(\Phi)}^{ab}$ relevé en $\widetilde{\sigma}'$ dans $\mathrm{Gal}(\overline{\mathbf{Q}}/E(\Phi))$, il existe une unique E-isogénie $\lambda : (A, \iota) \to \widetilde{\sigma}'(A, \iota)$ telle que

$$\forall x \in V_f(A, \overline{\mathbf{Q}}) : \qquad \lambda(N_\Phi(s') \cdot x) = \widetilde{\sigma}' \cdot x.$$

Mais $\sigma' = \sigma | E(\Phi)^{ab}$ où $\sigma = \mathrm{Art}_k(s)$. Si l'on choisit $\widetilde{\sigma}'$ tel que $\widetilde{\sigma'}|k^{ab} = \sigma$, on a donc $\widetilde{\sigma}'(A, \iota) = (A, \iota)$, i.e. $\lambda : (A, \iota) \to (A, \iota)$ est un élément $\lambda(s) \in E^\times$, et

$$\forall x \in V_f(A, \overline{\mathbf{Q}}) : \qquad \lambda(s) N_\Phi(s') \cdot x = \chi_A(\sigma) \cdot x$$

i.e. $\chi_A \circ \mathrm{Art}_k(s) = \lambda(s) \cdot N_{\phi,k}(s)$. Alors $s \mapsto \lambda(s)$ est le caractère recherché. □

Remark 3.10. Si K est une extension finie de k, $\epsilon_K = \epsilon_k \circ N_{K/k}$. D'autre part, puisque χ_A et N_Φ sont continus et atterrissent dans $T_E^0(\mathbf{A}_f)$, ϵ_k atterrit en fait dans $T_E^0(\mathbf{Q}) \subset E^\times$, et est un morphisme continu si l'on met sur $T_E^0(\mathbf{Q})$ la topologie induite par celle de $T_E^0(\mathbf{A}_f)$, i.e. la topologie discrète (c.f. la preuve du lemme 3.1). En particulier, $\epsilon_k(\widehat{\mathcal{O}}_k^\times)$ est un sous-groupe fini de $E^\times$, donc de $\mu(E^\times)$. D'après la théorie du corps de classe, on peut donc bricoler une extension cyclique K de k (de degré divisant l'ordre de $\mu(E^\times)$), telle que $\epsilon_K(\widehat{\mathcal{O}}_K^\times) = 1$. Mais alors pour tout nombre premier p, $\chi_A \circ \mathrm{Art}_K(\mathcal{O}_{K,p}^\times) = N_{K,\Phi}(\mathcal{O}_{K,p}^\times) \subset T_E(\mathbf{Q}_p) \subset T_E(\mathbf{A}_f)$, et en particulier $\mathrm{Art}_K(\mathcal{O}_{K,p}^\times)$ est trivial sur $V_\ell(A, \overline{\mathbf{Q}})$ pour tout $\ell \neq p$, donc A_K a bonne réduction *partout.*

4. La preuve du Théorème Principal

4.1. Le formalisme des "$\mathfrak{a}$-transforms".

4.1.1. *Généralités.* Soit $\mathcal{O}$ un anneau noethérien et A un S-schéma abélien muni d'une action de $\mathcal{O}$. Pour tout $\mathcal{O}$-module M de type fini, on note

$$A^M : (\mathbf{Sch}/S)^0 \to \mathbf{Ab} \qquad A^M(T) = \mathrm{Hom}_{\mathcal{O}}(M, A(T)).$$

Cette construction est compatible au changement de base sur S, covariante en A, contravariante en M et exacte d'un côté : si

$$M_1 \to M_2 \to M_3 \to 0$$

est une suite exacte de $\mathcal{O}$-module, alors la suite de préfaisceau abélien

$$0 \to A^{M_3} \to A^{M_2} \to A^{M_1}$$

est exacte. En particulier, A^{M_3} est représentable si A^{M_2} et A^{M_1} le sont, donc A^M est représentable pour tout M (de type fini) puisque $A^M \simeq A^n$ l'est pour $M = \mathcal{O}^n$. On obtient ainsi un foncteur contravariant $M \mapsto A^M$ de la catégorie des $\mathcal{O}$-modules de type fini dans celle des S-schémas en groupes commutatifs. Puisque A est propre sur S, tous les A^M le sont aussi. De plus :

Exercise 4.1. Si M est un $\mathcal{O}$-module projectif, alors A^M est un S-schéma abélien.

4.1.2. *Le cas CM.*

Lemma 4.2. *Soit A un S-schéma abélien à multiplication complexe par l'anneau des entiers $\mathcal{O}_E$ d'une $\mathbf{Q}$-algèbre réduite E, i.e. $\mathcal{O}_E \subset \mathrm{End}_S(A)$ et $\dim_{\mathbf{Q}} E = 2\dim_S A$. Alors pour tout idéal inversible I de $\mathcal{O}_E$, l'inclusion $I \hookrightarrow \mathcal{O}_E$ induit une isogénie $\alpha_A^I : A \to A^I$ de degré $[\mathcal{O}_E : I]$.*

Démonstration. On suppose pour simplifier que E est un corps. Tout idéal non nul est alors inversible, donc projectif, et A^I est un S-schéma abélien de même dimension que A, comme on voit par exemple en calculant un module de Tate. Le noyau de $\alpha_A^I : A \to A^I$ est $A^{\mathcal{O}/I} = A[I]$, qui est fini, donc α_A^I est une isogénie (en particulier, elle est surjective : il résulte alors du Critère de Baer que pour tout point géométrique s de S, $A(s)$ est un $\mathcal{O}$-module injectif). Pour $I = (\lambda)$ principal, $A[I] = \ker \lambda$ donc

$$\deg \alpha_A^I = \deg \lambda = \mathrm{nr}\lambda = [\mathcal{O}_E : I].$$

On le vérifie en effet directement pour $\alpha = [n]$, puis pour tout α en utilisant le fait que les deux fonctions deg et nr sur $\mathrm{End}_s^0(A_s)$ sont polynomiales, voir plus bas. Pour $I = I_1 I_2$ le produit de deux idéaux, on a

$$(\alpha_A^{I_1 I_2} : A \to A^{I_1 I_2}) = (\alpha_{A^{I_1}}^{I_2} \circ \alpha_A^{I_1} A \to A^{I_1} \to (A^{I_1})^{I_2})$$

et $A^{I_1}[I_2] \simeq A[I_2]$, donc $I \mapsto \deg \alpha_A^I$ est une fonction multiplicative sur l'ensemble des idéaux. On conclut en utilisant la finitude de $\mathrm{Pic}\mathcal{O}$. □

Remark 4.3. Lorsque S est connexe et admet un point complexe $s \in S(\mathbf{C})$, on peut vérifier la formule $\deg \alpha_A^I = [\mathcal{O}_E : I]$ directement sur les points complexes. En effet, si $A_s(\mathbf{C}) \simeq V_{\mathbf{R},I}/\Lambda$, alors Λ est un $\mathcal{O}_E$-réseau dans $V = \Lambda \otimes E$. On montre comme dans le cas CM que V est un E-module libre de rang 1, donc Λ un $\mathcal{O}_E$-module inversible, et on vérifie facilement que $A_s^I(\mathbf{C}) \simeq V_{\mathbf{R},I}/I^{-1}\Lambda$. Donc $A_s[I](\mathbf{C}) \simeq I^{-1}\Lambda/\Lambda \simeq \mathcal{O}_E/I$ comme $\mathcal{O}_E$-module.

4.2. **La formule de Giraud.**

4.2.1. *Préliminaires sur les algèbres de Lie.* Soit $k = \mathbf{F}_q$, $\alpha : A \to B$ un morphisme entre deux variétés abéliennes, $\alpha_0^{\#} : \mathcal{O}_{B,0} \to \mathcal{O}_{A,0}$ le morphisme déduit de α entre les anneaux locaux de B en $\alpha(0) = 0$ et A en 0. C'est un morphisme de k-algèbres locales régulières augmentées qui permet de retrouver le morphisme induit par α sur les espaces cotangents en 0, $\alpha_0^{\#} : \mathcal{I}_{B,0}/\mathcal{I}_{B,0}^2 \to \mathcal{I}_{A,0}/\mathcal{I}_{A,0}^2$, et donc aussi le morphisme $\mathrm{Lie}\alpha : \mathrm{Lie}A \to \mathrm{Lie}B$, qui est le dual du précédent. Ce morphisme induit aussi un morphisme entre les complétions de ces deux k-algèbres en leur idéal d'augmentation : $\alpha_0^{\#} : \widehat{\mathcal{O}}_{B,0} \to \widehat{\mathcal{O}}_{A,0}$. Le choix d'une k-base $y_1, \cdots, y_{g'}$ de $\mathcal{I}_{B,0}/\mathcal{I}_{B,0}^2$ (resp. $(x_1, \cdots, x_g)$ de $\mathcal{I}_{A,0}/\mathcal{I}_{A,0}^2$), où $g = \dim A$ et $g' = \dim B$ fournit des identifications de ces k-algèbres augmentées complètes avec des algèbres de séries formelles,

$$\alpha_0^{\#} : k[[y_1, \cdots, y_{g'}]] \to k[[x_1, \cdots, x_g]].$$

Si α est une isogénie, $\alpha_0^{\#}$ est un morphisme fidèlement plat et fini, qui fait donc de $\mathcal{O}_{A,0}$ une $\mathcal{O}_{B,0}$-algèbre qui est un $\mathcal{O}_{B,0}$-module libre de rang fini. L'anneau local en 0 du k-schéma en groupe fini $\ker\alpha$ est alors

$$\begin{aligned}\mathcal{O}_{\ker\alpha,0} &= \mathcal{O}_{A,0}/\alpha_0^{\#}(\mathcal{I}_{B,0})\mathcal{O}_{A,0}\\ &= \widehat{\mathcal{O}}_{A,0}/\alpha_0^{\#}(\mathcal{I}_{B,0})\widehat{\mathcal{O}}_{A,0}\\ &= k[[x_1,\cdots,x_g]]/(\alpha_0^{\#}(y_1),\cdots\alpha_0^{\#}(y_{g'})).\end{aligned}$$

Prenons pour α le Frobénius $\pi : A \to A$. Alors

$$\alpha_0^{\#} : k[[x_1,\cdots,x_g]] \to k[[x_1,\cdots,x_g]] \qquad x_i \mapsto x_i^q$$

Puisque $(\ker\pi)(k^{alg}) = 0$, le k-schéma fini $\ker\pi$ est local, et c'est le Spec de

$$\mathcal{O}_{\ker\pi,0} = k[[x_1,\cdots,x_g]]/(x_1^q,\cdots,x_g^q) = k[x_1,\cdots,x_g]/(x_1^q,\cdots,x_g^q).$$

On en déduit que

$$\mathrm{rang}(\ker\pi) = q^g = |\mathrm{Lie}(\ker\pi)| = |\mathrm{Lie}(A)|\,.$$

Prenons ensuite pour $\alpha : A \to B$ un morphisme qui factorise π, i.e. $\ker\alpha \subset \ker\pi$. Choisissons les bases $(y_1,\cdots,y_g)$ et $(x_1,\cdots,x_g)$ des espaces cotangents de sorte que $y_j \mapsto x_{g-j}$ pour $j \leq g-s$ et $y_j \mapsto 0$ pour $j > g-s$, donc s est la dimension du conoyau du morphisme cotangent, i.e. la dimension du noyau $\mathrm{Lie}(\ker\alpha)$ de α : $\mathrm{Lie}A \to \mathrm{Lie}B$. D'autre part,

$$\mathcal{O}_{\ker\alpha,0} = k[x_1,\cdots,x_g]/I$$

pour un idéal $(x_1^q,\cdots,x_g^q) \subset I \subset (x_1,\cdots,x_g)$ contenant $x_{g-s+1},\cdots,x_g$, donc $\mathcal{O}_{\ker\alpha,0}$ est un quotient d'un anneau de $k[x_1,\cdots,x_s]/(x_1^q,\cdots,x_s^q)$, donc

$$\mathrm{rang}(\ker\alpha) \leq q^s = |\mathrm{Lie}(\ker\alpha)|\,.$$

On en déduit que

Lemma 4.4. *Pour tout sous-schéma en groupe K de $\ker\pi$, $\mathrm{rang}K \leq |\mathrm{Lie}(K)|$.*

4.2.2. *La formule de Giraud.* Soit $k = \mathbf{F}_q$ un corps fini et A/k une variété abélienne à multiplication complexe par l'anneau des entiers $\mathcal{O}_E$ d'une $\mathbf{Q}$-algèbre réduite E, i.e. $\mathcal{O}_E \subset \mathrm{End}_k A$. Soit $\pi : A \to A$ le Frobenius. C'est une isogénie inséparable de degré q^g qui commute à tout le monde, qui est donc dans le commutant de $\mathcal{O}_E$ dans $\mathrm{End}_k A$, i.e. dans $\mathcal{O}_E$ (cf. plus bas). Soit $(\pi) = P_1^{n_1}\cdots P_r^{n_r}$ la décomposition de l'idéal (π) de $\mathcal{O}_E$ en produit d'idéaux premiers, avec $P_i \neq P_j$. Puisque $\pi = 0$ sur le $\mathcal{O}_E \otimes k$-module $\mathrm{Lie}A$,

$$\mathrm{Lie}A = \mathrm{Lie}A[P_1^{n_1}] \times \cdots \times \mathrm{Lie}A[P_r^{n_r}].$$

D'après le lemme 4.4,

$$q^g = |\mathrm{Lie}A| = \prod_j \left|\mathrm{Lie}A[P_j^{n_j}]\right| \geq \prod_j \deg A[P_j^{n_j}] = \deg\pi = q^g$$

donc $\left|\mathrm{Lie}A[P_j^{n_j}]\right| = \deg A[P_j^{n_j}] = \left|\mathcal{O}_E/P_j^{n_j}\right|$. On en déduit la formule de Giraud :

Proposition 4.5. $[\mathrm{Lie}A] = [\mathcal{O}_E/(\pi)]$ *dans le groupe de Grothendieck $K_0(\mathcal{O}_E)$.*

4.3. **La formule de Shimura-Taniyama.**

Proposition 4.6. *Soit A une variété abélienne de type CM (E, Φ) sur un corps de nombre $k \subset \mathbf{C}$. On suppose que k contient $\phi(E)$ pour tout $\phi \in \Phi$ et que $\mathcal{O}_E \subset \mathrm{End}_k(A)$ où $\mathcal{O}_E$ est l'anneau des entiers de E. Soit P un idéal premier de $\mathcal{O}_k$ où A a bonne réduction. Alors le Frobenius de la réduction $\overline{A}$ de A sur $k(P)$ se relève en un endomorphisme π de $\mathcal{O}_E \subset \mathrm{End}_k(A)$, et l'idéal principal qu'il engendre dans $\mathcal{O}_E$ est*

$$(\pi) = N_{k,\Phi}(P) = \prod_{\phi \in \Phi} \phi^{-1}(N_{k/\phi(E)}P)$$

où $N_{k,\Phi} : \mathcal{I}(k) \to \mathcal{I}(E)$ est la norme réflexe au niveau des idéaux.

Remark 4.7. Puisque $\deg \pi = q^g$, la formule ci-dessus est équivalente à

$$v_{\mathfrak{p}}(\pi) = \sum_{\phi \in \Phi} v_{\phi(\mathfrak{p})}(N_{k/\phi(E)}P) = \sum_{\phi \in \Phi \cap H(\mathfrak{p})} f(P : \phi(\mathfrak{p}))$$

pour tout $\mathfrak{p} \mid p$ de $\mathcal{O}_E$, où

$$H(\mathfrak{p}) = \{\phi : E \to k | \phi^{-1}(P) = \mathfrak{p}\}.$$

Multipliant tout par $f(\mathbf{p} : p) = f(\phi(\mathfrak{p}) : p)$, on obtient

$$v_{\mathfrak{p}}(\pi) \cdot f(\mathbf{p} : p) = f(P : p) \cdot |H(\mathfrak{p}) \cap \Phi|$$

Multipliant encore tout par $e(\mathbf{p}, p)$, on obtient finalement

$$v_{\mathfrak{p}}(\pi) \cdot |H(\mathfrak{p})| = v_{\mathfrak{p}}(q) \cdot |H(\mathfrak{p}) \cap \Phi|$$

puisque

$$v_{\mathfrak{p}}(q) = f(P : p) e(\mathfrak{p} : p) \quad \text{et} \quad |H(\mathfrak{p})| = \deg_{\mathbf{Q}_p} E_{\mathfrak{p}} = f(\mathfrak{p} : p) \cdot e(\mathfrak{p} : p)$$

La formule de Shimura-Tanyiama est donc équivalente à

$$\forall \mathfrak{p} \mid p \text{ de } \mathcal{O}_E : \qquad \frac{v_{\mathfrak{p}}(\pi)}{v_{\mathfrak{p}}(q)} = \frac{|H(\mathfrak{p}) \cap \Phi|}{|H(\mathfrak{p})|}.$$

Démonstration. Soit $\mathcal{A}$ le modèle de Néron de A sur $\mathcal{O}_k$ et $L = \mathrm{Lie}(\mathcal{A})$. C'est un $\mathcal{O}_E \otimes \mathcal{O}_k$-module qui est un $\mathcal{O}_k$-module localement libre de rang g. Soit $\det_L : \mathcal{O}_E \to \mathcal{O}_k$ le déterminant qui en résulte. Puisque A est de type CM (E, Φ) et $\phi(E) \subset k$ pour tout $\phi \in \Phi$, on sait que $L \otimes k \simeq \prod_{\phi \in \Phi} k(\phi)$ comme $E \otimes k$-module, donc $\det_L(e) = \prod_{\phi \in \Phi} \phi(e)$. Considérons d'autre part le $\mathcal{O}_E \otimes k(P)$-module $L \otimes_{\mathcal{O}_k} k(P)$. C'est un module de longueur finie sur $\mathcal{O}_E / p\mathcal{O}_E \otimes_{\mathbf{F}_p} k(P)$, et il admet donc une suite de composition (de Jordan-Holder) dont les quotients sont des $\mathcal{O}_E / p\mathcal{O}_E \otimes k(P)$-modules simples, lesquels sont des quotients de $\mathcal{O}_E / \mathfrak{p} \otimes_{\mathbf{F}_p} k(P)$ pour des idéaux premiers $\mathfrak{p} \mid p$ de $\mathcal{O}_E$, donc de la forme $k(P)(\phi)$ pour un morphisme $\phi \in H_{\mathfrak{p}}$. La formule qui donne le déterminant montre que ces facteurs simples sont exactement les $k(P)(\phi)$ pour $\phi \in \Phi$, sans multiplicité. Si $\phi \in H_{\mathfrak{p}}$ (i.e. $\phi^{-1}(P) = \mathfrak{p}$), le $\mathcal{O}_E/\mathfrak{p}$-espace vectoriel $k(P)$ est de $\mathbf{F}_p$-dimension $f(P : p) = f(P : \phi(\mathfrak{p})) \cdot f(\mathfrak{p} : p)$, donc de $\mathcal{O}_E/\mathfrak{p}$-dimension $f(P : \phi(\mathfrak{p}))$. On en déduit donc que la multiplicité de $\mathcal{O}_E$-module simple $\mathcal{O}_E/\mathfrak{p}$ dans $L \otimes_{\mathcal{O}_k} k(P)$ est la somme sur tous les $\phi \in H_{\mathfrak{p}} \cap \Phi$ de $f(P : \phi(\mathfrak{p}))$. Mais puisque $L \otimes_{\mathcal{O}_k} k(P)) = \mathrm{Lie} A_{k(P)}$, cette multiplicité est aussi celle de $\mathcal{O}_E/\mathfrak{p}$ dans $\mathcal{O}_E/(\pi)$, d'après la formule de Giraud 4.5. On a donc

$$v_{\mathfrak{p}}(\pi) = \sum_{\phi \in H_{\mathfrak{p}} \cap \Phi} f(P : \phi(\mathfrak{p}))$$

pour tout $\mathfrak{p} \mid p$ de $\mathcal{O}_E$, ce qui est précisément la formule de Shimura-Taniyama. $\square$

4.4. **Preuve du théorème principal.** On veut montrer que

$$r_\Phi \circ \mathrm{Art}_{E(\Phi)} = N_\Phi \quad : \quad T_{E(\Phi)}(\mathbf{Q})\backslash T_{E(\Phi)}(\mathbf{A}_f) \to T_E(\mathbf{Q})\backslash T_E(\mathbf{A}_f).$$

4.4.1. *Niveau fini.* Pour tout n entier, notons $K_E(n) = \{\lambda \in \widehat{\mathcal{O}}_E^\times : \lambda \equiv 1 \bmod n\}$. C'est un sous-groupe ouvert et compact de $T_E(\mathbf{A}_f)$. Puisque $r_\Phi \circ \mathrm{Art}_{E(\Phi)}$ et N_Φ sont continus, il existe un idéal $\mathcal{N}$ de $\mathcal{O}_{E(\Phi)}$ tels que ces les deux applications $r_\Phi \circ \mathrm{Art}_{E(\Phi)} \bmod K(n)$ et $N_\Phi \bmod K(n)$ se factorisent en un diagramme

$$\begin{array}{lccc} r_\Phi \circ \mathrm{Art}_{E(\Phi)} \text{ ou } N_\Phi : & T_E(\mathbf{Q})\backslash T_{E(\Phi)}(\mathbf{A}_f) & \to & T_E(\mathbf{Q})\backslash T_E(\mathbf{A}_f) \\ & \downarrow & & \downarrow \\ r_\Phi \circ \mathrm{Art}_{E(\Phi)} \text{ ou } N_\Phi : & T_E(\mathbf{Q})\backslash T_E(\mathbf{A}_f)/K(\mathcal{N}) & \to & T_E(\mathbf{Q})\backslash T_E(\mathbf{A}_f)/K(n) \end{array}$$

où $K(\mathcal{N}) = \{\lambda \in \widehat{\mathcal{O}}_{E(\Phi)}^\times : \lambda \equiv 1 \bmod \mathcal{N}\}$. Or

$$T_E(\mathbf{Q})\backslash T_E(\mathbf{A}_f)/K(n) = E^\times \backslash \left(\widehat{E}^{(n)\times}/K(n)^n \times \prod_{\mathfrak{q}\mid n} E_\mathfrak{q}^\times / K(n)_\mathfrak{q} \right)$$

avec des notations évidentes, et $E^\times$ est dense dans $\prod_{\mathfrak{q}\mid n} E_\mathfrak{q}^\times$, donc

$$T_E(\mathbf{Q})\backslash T_E(\mathbf{A}_f)/K(n) \simeq \Gamma(E^\times, n)\backslash \widehat{E}^{(n)\times}/K(n)^n \simeq i(\Gamma(E^\times, n))\backslash I^n(E) = C(E, n)$$

où $I^n(E)$ est l'ensemble des idéaux fractionnaires de E qui sont premiers à n,

$$\Gamma(E^\times, n) = \{\lambda \in E^\times : \forall \mathfrak{q} \mid n,\ v_\mathfrak{q}(\lambda - 1) \geq v_\mathfrak{q}(n)\}$$

et i est l'application qui à un élément de $E^\times$ associe le $\mathcal{O}_E$-idéal engendré par cet élément. De même et avec des notations similaires,

$$T_{E(\Phi)}(\mathbf{Q})\backslash T_{E(\Phi)}(\mathbf{A}_f)/K(\mathcal{N}) \simeq i(\Gamma(E(\Phi)^\times, \mathcal{N}))\backslash I^{\mathcal{N}}(E(\Phi)) = C(E(\Phi), \mathcal{N}).$$

Les morphismes ainsi obtenus sont

$$r_\Phi \circ \mathrm{Art}_{E(\Phi)} \text{ et } N_\Phi \quad : \quad C(E(\Phi), \mathcal{N}) \to C(E, n).$$

Le morphisme N_Φ se décrit aisément : il est induit par le morphisme N_Φ sur les idéaux. Quant au morphisme $r_\Phi \circ \mathrm{Art}_{E(\Phi)}$, il se décrit de la manière suivante.

4.4.2. *Description de $r_\Phi \circ \mathrm{Art}_{E(\Phi)}$ en niveau fini.* Soit $E(\Phi, \mathcal{N})$ l'extension abélienne de $E(\Phi)$ qui est fixée par $\mathrm{Art}_{E(\Phi)}(K(\mathcal{N}))$. C'est une extension non-ramifiée en dehors de $\mathcal{N}$, et les isomorphismes ci-dessus induisent

$$\mathrm{Art}_{E(\Phi)} : C(E(\Phi), \mathcal{N}) \xrightarrow{\simeq} \mathrm{Gal}\,(E(\Phi, \mathcal{N})/E(\Phi))$$

qui envoient (la classe d') un idéal premier $\mathfrak{p} \nmid \mathcal{N}$ de $E(\Phi)$ sur l'inverse $\mathrm{Frob}_\mathfrak{p}^{-1}$ du Frobénius $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(E(\Phi, \mathcal{N})/E(\Phi))$. Soient $\mathcal{X} \in C(E(\Phi), \mathcal{N})$, $\sigma \in \mathrm{Aut}(\mathbf{C}/E(\Phi))$ tel que

$$\sigma | E(\Phi, \mathcal{N}) = \mathrm{Art}_{E(\Phi)}(X) \quad \text{dans} \quad \mathrm{Gal}\,(E(\Phi, \mathcal{N})/E(\Phi)),$$

$(A, \iota) \in \mathcal{H}(E, \Phi)$, $\lambda : (A, \iota) \to \sigma(A, \iota)$ une E-isogénie et $\widehat{t}$ l'unique élément de $T_E(\mathbf{A}_f)$ tel que

$$\forall x \in V_f(A, \mathbf{C}) : \qquad \lambda(\widehat{t} \cdot x) = \sigma \cdot x \quad \text{dans } V_f(\sigma A, \mathbf{C}).$$

Quitte à modifier λ par un élément convenable de $E^\times$, on peut supposer que $\widehat{t}_\mathfrak{p} \in K(n)_\mathfrak{p}$ pour tout $\mathfrak{p} \mid n$. Si $\mathcal{O}_E = \mathrm{End}(A) \cap \iota(E)$, cette condition est équivalente à une condition sur λ, à savoir : $\lambda(a) = \sigma a$ pour tout $a \in A[n]$. Soit enfin $J = \widehat{t} \cdot \mathcal{O}_E \in I^n(E)$ et $\mathcal{Y}$ la classe de Y dans $C(E, n)$. Alors

$$r_\Phi \circ \mathrm{Art}_{E(\Phi)}(\mathcal{X}) = \mathcal{Y}.$$

Nous allons montrer que pour de bons choix de

$$\mathfrak{p} \in \mathcal{X}, \quad \sigma \in \mathrm{Aut}(\mathbf{C}/E(\Phi)), \quad (A, \iota) \in \mathcal{H}(E, \Phi) \quad \text{et} \quad \lambda : (A, \iota) \to \sigma(A, \iota)$$

vérifiant toutes les conditions ci-dessus, on obtient $J = N_\Phi(\mathfrak{p})$.

4.4.3. *Choix de* (A, ι). Choisissons une extension Galoisienne finie k de $E(\Phi)$ telle que (1) $E(\Phi, \mathcal{N}) \subset k$, et (2) il existe une variété abélienne $(A, \iota) \in \mathcal{H}(E, \Phi)$ qui est définie sur k et telle que $\mathcal{O}_E = \mathrm{End}_k(A) \cap \iota(E)$. Quitte à agrandir encore k, on peut supposer que (3) $\phi(E) \subset k$ pour tout $\phi \in \Phi$, et (4) pour tout $\sigma \in \mathrm{Gal}(k/E(\Phi))$, il existe une $\mathcal{O}_E$-isogénie $A \to \sigma A$ qui est définie sur k.

Exercise 4.8. Toute $\mathcal{O}_E$-isogénie $A \to \sigma A$ est alors également définie sur k.

4.4.4. *Choix de* $\mathfrak{p}$ *et* σ. On choisit dans $\mathcal{X} \in C(E(\Phi), \mathcal{N})$ l'inverse $\mathfrak{p}^{-1}$ d'un idéal premier $\mathfrak{p} \nmid \mathcal{N}$ tel que la variété abélienne A sur k a bonne réduction en tous les idéaux premiers $P \mid \mathfrak{p}$ de k. On fixe un tel idéal premier $P \mid \mathfrak{p}$ de $\mathcal{O}_k$, de sorte que σA a bonne réduction en P pour tout $\sigma \in \mathrm{Gal}(k/E(\Phi))$. On choisit $\sigma \in \mathrm{Aut}(\mathbf{C}/E(\Phi))$ de sorte que

$$\sigma | k = \mathrm{Frob}_P \in \mathrm{Gal}(k/E(\Phi)).$$

4.4.5. *Calcul de* $r_\Phi \circ \mathrm{Art}_{E(\Phi)}(\mathcal{X})$.

Lemma 4.9. *Il existe* $J \in I(E)$ *et un* k*-isomorphisme* $\mathcal{O}_E$*-linéaire* $\beta : A^J \simeq \sigma A$.

Démonstration. D'après l'hypothèse (4) sur (A, ι), tout isomorphisme $\mathcal{O}_E$-linéaire $A^J(\mathbf{C}) \simeq (\sigma A)(\mathbf{C})$ est défini sur k, cf Exercice 4.8. Si $A(\mathbf{C}) \simeq V_{\mathbf{R},I}/\Lambda$ et $(\sigma A)(\mathbf{C}) \simeq V_{\mathbf{R},I}/\Lambda'$, il existe un idéal fractionnaire J de E tel que $\Lambda' = J^{-1}\Lambda$. Les isomorphismes $\mathrm{Hom}_{\mathcal{O}_E}(J, V_{\mathbf{R},I}) \simeq \mathrm{Hom}_E(E, V_{\mathbf{R},I}) \simeq V_{\mathbf{R},I}$ induisent un isomorphisme

$$\mathrm{Hom}_{\mathcal{O}_E}(J, \Lambda) \simeq \{f : E \to V_{\mathbf{R},I} : f(J) = Jf(1) \subset \Lambda\} \simeq J^{-1}\Lambda$$

d'où l'on déduit que $\mathrm{Hom}_{\mathcal{O}_E}(J, V_{\mathbf{R},I}/\Lambda) \simeq V_{\mathbf{R},I}/J^{-1}\Lambda$, i.e. $A^J(\mathbf{C}) \simeq (\sigma A)(\mathbf{C})$, cqfd. □

Soit $\overline{A}/k(P)$ la réduction de A en P. Alors $\overline{A}^{(q^i)}$ est celle de $\sigma^i A$. En particulier, le composé des Frobenius "absolus"

$$\overline{A} \to \overline{A}^{(q)} \to \overline{A}^{(q^2)} \to \cdots \to \overline{A}^{(q^f)} = \overline{A}$$

est le Frobénius $\pi \in \mathcal{O}_E$ de la variété abélienne $\overline{A}$ sur $k(P)$. Notons que tous ces morphismes sont $\mathcal{O}_E$-linéaires, et se déduisent de $F : \overline{A} \to \overline{A}^{(q)}$ par application itérée de $\star^{(q)}$.

Lemma 4.10. *Il existe un idéal* $J \subset \mathcal{O}_E$ *et un isomorphisme* $\mathcal{O}_E$*-linéaire* $\beta : A^J \xrightarrow{\simeq} \sigma A$ *tel que* $\beta \circ \alpha_J^A : A \to A^J \to \sigma A$ *se réduise sur* $F : \overline{A} \to \overline{A}^{(q)}$.

Démonstration. Soit J un idéal fractionnaire de E tel qu'il existe un k-isomorphisme $\mathcal{O}_E$-linéaire $\beta : A^J \xrightarrow{\simeq} \sigma A$. La réduction de cet isomorphisme est un isomorphisme $\overline{\beta} : \overline{A}^J \xrightarrow{\simeq} \overline{A}^{(q)}$. Alors $\overline{\beta}^{-1} \circ F : \overline{A} \to \overline{A}^J$ est un élément de

$$\begin{aligned} \mathrm{Hom}_{\mathcal{O}_E}(\overline{A}, \overline{A}^J) &= \mathrm{Hom}_{\mathcal{O}_E}(\overline{A}, \mathrm{Hom}_{\mathcal{O}_E}(J, \overline{A})) \\ &= \mathrm{Hom}_{\mathcal{O}_E}(\overline{A} \otimes J, \overline{A}) \\ &= \mathrm{Hom}_{\mathcal{O}_E}(J, \mathrm{Hom}_{\mathcal{O}_E}(\overline{A}, \overline{A})) \\ &= \mathrm{Hom}_{\mathcal{O}_E}(J, \mathcal{O}_E) \end{aligned}$$

i.e., provient d'un $f : J \to \mathcal{O}_E$, qui est injectif puisque $\overline{\alpha} \circ F$ est une isogénie. Remplaçant J par $f(J)$, on peut donc supposer que $J \subset \mathcal{O}_E$ et $\overline{\beta}^{-1} \circ F = \overline{\alpha}_J^A : \overline{A} \to \overline{A}^J$. Alors

$$\beta \circ \alpha_J^A : A \to A^J \xrightarrow{\simeq} \sigma A$$

se réduit bien sur $F : \overline{A} \to \overline{A}^{(q)}$. □

Soit $\lambda = \beta \circ \alpha_J^A : A \to A^J \xrightarrow{\simeq} \sigma A$. C'est une isogénie $\mathcal{O}_E$-linéaire de degré $[\mathcal{O}_E : J] = \deg F = (\deg \mathfrak{p})^g$ premier à n, et puisque λ se réduit sur F, $\lambda(a) = \sigma a$ pour tout $a \in A[n]$. Donc si $\widehat{t}$ est l'élément de $T_E(\mathbf{A}_f)$ tel que

$$\forall x \in V_f(A, \overline{\mathbf{Q}}) : \qquad \lambda(\widehat{t} \cdot x) = \sigma \cdot x \quad \text{dans } V_f(\sigma A, \overline{\mathbf{Q}})$$

alors $\widehat{t}_\mathfrak{q} \in K(n)_\mathfrak{q}$ pour tout $\mathfrak{q} \mid n$ et $r_\Phi \circ \mathrm{Art}(\mathcal{X}) \in C(E, n)$ est représenté par l'idéal $\widehat{t} \cdot \mathcal{O}_E \in I^n(E)$. Pour calculer cet idéal, on note que $\alpha_J^A : V_f(A, \overline{\mathbf{Q}}) \to V_f(A^J, \overline{\mathbf{Q}})$ envoie $\widehat{t} \cdot T_f(A, \overline{\mathbf{Q}})$ sur $T_f(A^J, \overline{\mathbf{Q}})$, et que les isomorphismes

$$V_f(A^J, \overline{\mathbf{Q}}) \simeq \mathrm{Hom}_{\mathcal{O}_E}\left(J, V_f(A, \overline{\mathbf{Q}})\right) \simeq \mathrm{Hom}_E\left(E, V_f(A, \mathbf{Q})\right) \simeq V_f(A, \mathbf{Q})$$

identifient $T_f(A^J, \overline{\mathbf{Q}})$ à $J^{-1} \cdot T_f(A, \overline{\mathbf{Q}})$ et α_J^A à l'identité, donc $\widehat{t} \cdot T_f(A, \overline{\mathbf{Q}}) = J^{-1} \cdot T_f(A, \overline{\mathbf{Q}})$. On en déduit que $\widehat{t} \cdot \mathcal{O}_E = J^{-1}$, donc $r_\Phi \circ \mathrm{Art}(\mathcal{X}) = [J^{-1}] \in C(E, n)$.

Posant $\beta_\ell = (\sigma^{\ell-1}\beta) \circ (\sigma^{\ell-2}\beta^J) \circ \cdots \circ (\sigma\beta^{J^{\ell-2}}) \circ \beta^{J^{\ell-1}}$, qui est un isomorphisme $\mathcal{O}_E$-linéaire

$$\beta_\ell : A^{J^\ell} \to \sigma A^{J^{\ell-1}} \to \sigma^2 A^{J^{\ell-2}} \to \cdots \to \sigma^\ell A$$

on obtient un diagramme commutatif

$$\begin{array}{ccccccccc} A & \to & A^J & \to & A^{J^2} & \to & \cdots & \to & A^{J^f} \\ \| & & \beta_1 \downarrow & & \beta_2 \downarrow & & & & \beta_f \downarrow \\ A & \to & \sigma A & \to & \sigma^2 A & \to & \cdots & \to & \sigma^f A = A \end{array}$$

dont la deuxième ligne se réduit sur le Frobenius $\pi : \overline{A} \to \overline{A}$. On a donc

$$J^f = (\pi) = N_{\Phi,k}(P) = N_\Phi(\mathfrak{p}^f) = N_\Phi(\mathfrak{p})^f$$

d'après la formule de Shimura-Taniyama, donc $J = N_\Phi(\mathfrak{p})$ puisque $I^n(E)$ est sans torsion. Ainsi $J^{-1} = N_\Phi(\mathfrak{p}^{-1})$, et puisque $\mathcal{X} = [\mathfrak{p}^{-1}]$ dans $C(E(\Phi), \mathcal{N})$, on a bien

$$r_\Phi \circ \mathrm{Art}_{E(\Phi)} = N_\Phi \quad : \quad C(E(\phi), \mathcal{N}) \to C(E, n).$$

4.4.6. *Fin de la preuve.* On a donc vu que

$r_\Phi \circ \mathrm{Art}_{E(\Phi)} \equiv N_\Phi \bmod K(n) \quad : \quad T_{E(\Phi)}(\mathbf{Q})\backslash T_{E(\Phi)}(\mathbf{A}_f) \to T_E(\mathbf{Q})\backslash T_E(\mathbf{A}_f)/K(n).$

Cela montre déjà que $\theta = r_\Phi \circ \mathrm{Art}_{E(\Phi)}/N_\Phi^{-1}$ est un morphisme

$$\theta : T_{E(\Phi)}(\mathbf{Q})\backslash T_{E(\Phi)}(\mathbf{A}_f) \to T_E(\mathbf{Q})\backslash \overline{T_E(\mathbf{Q})}$$

où $\overline{T_E(\mathbf{Q})} = \cap_n T_E(\mathbf{Q}) \cdot K(n)$ est l'adhérence de $T_E(\mathbf{Q})$ dans $T_E(\mathbf{A}_f)$. On conclut grâce aux deux lemmes suivants, où $\star$ est l'involution de $T_E(\mathbf{A}_f)$ induite par l'involution canonique $\star$ de E :

Lemma 4.11. *Avec les notations ci-dessus, $\theta \cdot \theta^\star = 1$.*

Démonstration. Soient $s \in T_{E(\Phi)}(\mathbf{A}_f)$, $\sigma \in \mathrm{Aut}(\mathbf{C}/E(\Phi))$ tel que $\sigma|E(\Phi)^{ab} = \mathrm{Art}_{E(\Phi)}(s)$, $(A,\iota) \in \mathcal{H}(E,\Phi)$, λ une E-isogénie $(A,\iota) \to \sigma(A,\iota)$, $\widehat{t} \in T_E(\mathbf{A}_f)$ tel que

$$\forall x \in V_f(A,\mathbf{C}) : \quad \lambda(\widehat{t} \cdot x) = \sigma x \text{ dans } V_f(\sigma A, \mathbf{C}).$$

Soit $\alpha : A \to A^t$ une polarisation $(E,\star)$-linéaire de A. Alors $\sigma\alpha : \sigma A \to \sigma(A^t) \simeq (\sigma A)^t$ est une polarisation $(E,\star)$-linéaire de σA et $\lambda^t \circ \sigma\alpha \circ \lambda : A \to A^t$ est à nouveau une polarisation de A. D'après le corollaire 2.12, il existe donc une constante $c \in F_>^\times$ telle que $c\alpha = \lambda^t \circ \sigma\alpha \circ \lambda$. Pour tout $x, y \in V_f(A,\mathbf{C})$, on a alors

$$\begin{aligned}\left\langle \widehat{t} \cdot x, c\widehat{t} \cdot y \right\rangle_f^\alpha &= \left\langle \widehat{t} \cdot x, \widehat{t} \cdot y \right\rangle_f^{\lambda^t \circ \sigma\alpha \circ \lambda} = \left\langle \lambda(\widehat{t} \cdot x), \lambda(\widehat{t} \cdot y) \right\rangle_f^{\sigma\alpha} \\ &= \langle \sigma x, \sigma y)\rangle_f^{\sigma\alpha} = \sigma \langle x, y\rangle_f^\alpha = \chi_{cyc}(\sigma) \langle x, y\rangle_f^\alpha\end{aligned}$$

donc $\left\langle x, c\widehat{t\,t^\star} \cdot y \right\rangle_f^\alpha = \langle x, \chi_{cyc}(\sigma) y\rangle_f^\alpha$, de sorte que $c\widehat{t\,t^\star} = \chi_{cyc}(\sigma)$ et

$$(\theta \cdot \theta^\star)(s) = \frac{r_\Phi(\sigma) \cdot r_\Phi(\sigma)^\star}{N_\Phi(s) \cdot N_\Phi(s)^\star} = \frac{\widehat{t} \cdot \widehat{t}^\star}{N_\Phi(s) \cdot N_\Phi(s)^\star} \in T_E(\mathbf{Q}),$$

puisque $\chi_{cyc}(\sigma) \equiv N_\Phi(s) \cdot N_\phi(s)^\star \bmod T_E(\mathbf{Q})$. □

Lemma 4.12. *Le groupe $\overline{T_E(\mathbf{Q})}/T_E(\mathbf{Q})$ est un $\mathbf{Q}$-espace vectoriel sur lequel $\star = 1$.*

Démonstration. On admet le résultat suivant : la topologie de $T_E(\mathbf{A}_f)$ induit sur $\mathcal{O}_E^\times$ la topologie profinie, i.e. celle dont une base de voisinage ouvert (et fermé) de 1 est formé des sous-groupes U qui sont d'indice fini dans $\mathcal{O}_E^\times$. Pour un tel sous-groupe U, l'adhérence $\overline{U}$ de U dans $T_E(\mathbf{A}_f)$ s'identifie donc à la complétion profinie $\widehat{U}$ de U. D'autre part,

$$\left(T_E(\mathbf{Q}) \cdot \overline{U}\right) \cap \widehat{\mathcal{O}}_E^\times = \mathcal{O}_E^\times \cdot \overline{U} = \cup_{x \in \mathcal{O}_E^\times/U}\, x \cdot \overline{U}$$

est fermé dans $\widehat{\mathcal{O}}_E^\times$, donc $T_E(\mathbf{Q}) \cdot \overline{U}$ est un sous-groupe localement fermé, donc fermé, de $T_E(\mathbf{A}_f)$. Il en résulte que $T_E(\mathbf{Q}) \cdot \overline{U} = \overline{T_E(\mathbf{Q})}$, et l'on obtient donc une suite exacte

$$1 \to \overline{U} \cap T_E(\mathbf{Q})/U \to \widehat{U}/U \simeq \overline{U}/U \to \overline{T_E(\mathbf{Q})}/T_E(\mathbf{Q}) \to 1$$

avec un noyau fini puisque $\overline{U} \cap T_E(\mathbf{Q}) \subset \mathcal{O}_E^\times$. Puisque $\mathcal{O}_F^\times$ et $\mathcal{O}_E^\times$ sont des groupes abéliens de type fini et de même rang $r = [F : \mathbf{Q}] - |\mathrm{Spec} F|$, on peut choisir pour U un sous-groupe de $\mathcal{O}_F^\times$ qui est sans torsion (et de rang r). Alors $\overline{U}/U \simeq \widehat{U}/U \simeq (\widehat{\mathbf{Z}}/\mathbf{Z})^r$. Mais $\widehat{\mathbf{Q}} = \widehat{\mathbf{Z}} + \mathbf{Q}$ avec $\widehat{\mathbf{Z}} \cap \mathbf{Q} = \mathbf{Z}$. On obtient alors

$$\overline{T_E(\mathbf{Q})}/T_E(\mathbf{Q}) \simeq \overline{U}/U \simeq \widehat{U}/U \simeq (\widehat{\mathbf{Z}}/\mathbf{Z})^r \simeq (\widehat{\mathbf{Q}}/\mathbf{Q})^r$$

et le lemme en résulte immédiatement. □

Références

[1] D. Mumford, *Abelian Varieties.*

[2] J-P. Serre et J. Tate, *Good Reduction of Abelian Varieties.* Annals of Math., Second Series, **88.3** (1968).

VARIÉTÉS DE SHIMURA

1. Données de Shimura et Variétés de Shimura

1.1. Définitions.

Definition 1.1. Une donnée de Shimura est une paire $(G, \mathcal{X})$ où G est un groupe réductif sur $\mathbf{Q}$ et $\mathcal{X}$ une classe de $G(\mathbf{R})$-conjugaison de morphismes $h : \mathbf{S} \to G_{\mathbf{R}}$ vérifiant des conditions **SV1**, **SV2**, et **SV3** explicitées ci-dessous. La variété de Shimura associée à $(G, \mathcal{X})$ est le système projectif, indexé par les sous-groupes ouverts et compacts de $G(\mathbf{A}_f)$, des ensembles

$$\mathrm{Sh}_K(G, \mathcal{X})(\mathbf{C}) = G(\mathbf{Q}) \backslash \left(G(\mathbf{A}_f)/K \times \mathcal{X} \right)$$

munis de l'action à droite du groupe $G(\mathbf{A}_f)$ définie par

$$\sigma : \mathrm{Sh}_K(G, \mathcal{X})(\mathbf{C}) \to \mathrm{Sh}_{K^\sigma}(G, \mathcal{X})(\mathbf{C}) \qquad [g, h] \mapsto [g\sigma, h]$$

où $K^\sigma = \sigma^{-1} K \sigma$.

Definition 1.2. Un morphisme de donnée de Shimura $\phi : (G, \mathcal{X}) \to (G', \mathcal{X}')$ est un morphisme de $\mathbf{Q}$-schémas en groupes $\phi : G \to G'$ qui envoie $\mathcal{X}$ dans $\mathcal{X}'$. Ce morphisme induit un morphisme entre les variétés de Shimura

$$\phi : \left(\mathrm{Sh}_K(G, \mathcal{X})(\mathbf{C})\right)_K \to \left(\mathrm{Sh}_{K'}(G', \mathcal{X}')(\mathbf{C})\right)_{K'}$$

où pour $\phi(K) \subset K'$,

$$\phi_{K,K'} : \mathrm{Sh}_K(G, \mathcal{X})(\mathbf{C}) \to \mathrm{Sh}_{K'}(G', \mathcal{X}')(\mathbf{C}) \qquad [g, h] \to [\phi(g), \phi(h)].$$

1.2. **Structure Différentielle sur $\mathcal{X}$.** Soit $Z_G(h) \subset G_{\mathbf{R}}$ le centralisateur de h dans $G_{\mathbf{R}}$. C'est un sous-schéma en groupe fermé de $G_{\mathbf{R}}$ qui est connexe, comme le sont les centralisateurs des tores, et $K(h) = Z_G(h)(\mathbf{R})$ est le centralisateur de h dans $G(\mathbf{R})$. En particulier, $K(h)$ est un sous-groupe de Lie fermé de $G(\mathbf{R})$, et

$$G(\mathbf{R})/K(h) \simeq G(\mathbf{R}) \cdot h = \mathcal{X}$$

est donc muni d'une structure de variété lisse sur laquelle $G(\mathbf{R})$ agit par difféomorphismes. Puisque $G(\mathbf{R})$ n'a qu'un nombre fini de composantes connexes, il en est de même de l'espace topologique $\mathcal{X}$, et chacune de ces composantes connexes est de la forme $G(\mathbf{R})^+ \cdot h$ où $G(\mathbf{R})^+$ est la composante neutre de $G(\mathbf{R})$. L'espace tangent de $\mathcal{X}$ en h s'identifie à

$$T_h\mathcal{X} = \mathrm{Lie}G(\mathbf{R})/\mathrm{Lie}K(h) = \mathrm{Lie}G(\mathbf{R})/\mathrm{Lie}Z_G(h)(\mathbf{R})$$

et cette identification transporte l'action de $K(h) = \mathrm{Stab}_{G(\mathbf{R})}(h)$ sur $T_h(x)$ sur l'action adjointe de $K(h)$ sur les algèbres de Lie.

Lemma 1.3. *Soit $\mathcal{X}^{ad} = G^{ad}(\mathbf{R}) \cdot h^{ad}$ la classe de $G^{ad}(\mathbf{R})$-conjugaison de*

$$h^{ad} = \mathrm{ad} \circ h : \mathbf{S} \to G^{ad}_{\mathbf{R}}.$$

Alors $\mathrm{ad} : \mathcal{X} \to \mathcal{X}^{ad}$ *identifie $\mathcal{X}$ à une réunion de composantes connexes de $\mathcal{X}^{ad}$.*

Démonstration. On sait que $\mathcal{X} = \coprod_{h\in\mathcal{H}} G(\mathbf{R})^+ \cdot h$ pour un ensemble fini $\mathcal{H} \simeq \pi_0(\mathcal{X}) \subset \mathcal{X}$. Puisque ad : $G(\mathbf{R}) \to G^{ad}(\mathbf{R})$ induit une surjection ad : $G(\mathbf{R})^+ \twoheadrightarrow G^{ad}(\mathbf{R})^+$, on obtient

$$\mathrm{ad}(\mathcal{X}) = \mathrm{ad}(\coprod_{h\in\mathcal{H}} G(\mathbf{R})^+ \cdot h) = \coprod_{h\in\mathcal{H}'} G^{ad}(\mathbf{R})^+ \cdot h^{ad}$$

pour un sous-ensemble fini $\mathcal{H}'$ de $\mathcal{H}$. Il reste à voir que ad : $\mathcal{X} \to \mathcal{X}^{ad}$ est injective (ce qui impliquera par ailleurs que $\mathcal{H}' = \mathcal{H}$). Soit donc $h \in \mathcal{X}$ et $g \in G(\mathbf{R})$ tel que $\mathrm{ad}(ghg^{-1}) = \mathrm{ad}(h)$, i.e. $ghg^{-1} \equiv h \bmod Z_{\mathbf{R}}$, ou encore $ghg^{-1}h^{-1} : \mathbf{S} \to G_{\mathbf{R}}$ se factorise par $Z_{\mathbf{R}}$, donc aussi par $Z_{\mathbf{R}} \cap G^{der}_{\mathbf{R}} = Z(G^{der}_{\mathbf{R}})$ qui est *fini.* Puisque $\mathbf{S}$ est connexe, $ghg^{-1}h^{-1} = 1$ donc $ghg^{-1} = h$. □

On peut donc aussi décrire les espaces tangents comme

$$T_h\mathcal{X} = T_{h^{ad}}\mathcal{X}^{ad} = \mathrm{Lie}G^{ad}(\mathbf{R})/\mathrm{Lie}K(h^{ad})$$

où $K(h^{ad})$ est le stabilisateur de h^{ad} dans $G^{ad}(\mathbf{R})$.

2. L'hypothèse SV1

2.1. **Représentations de S.** Puisque $\mathbf{S} = \mathrm{Res}_{\mathbf{C}/\mathbf{R}}\mathbf{G}_{m,\mathbf{C}}$, $X^\star(\mathbf{S}) = \mathbf{Z}[\mathrm{Gal}(\mathbf{C}/\mathbf{R})]$ avec l'action évidente de $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$. Les représentations de $\mathbf{S} \to GL(V)$ (pour V un $\mathbf{R}$-espace vectoriel) correspondent donc bijectivement aux bigraduations de $V \otimes \mathbf{C} = \oplus V^{p,q}$ telles que $\overline{V^{p,q}} = V^{q,p}$ - ce sont les structures de Hodge sur V. Le type d'une telle bigraduation est l'ensemble des couples $(p,q) \in \mathbf{Z}^2$ tels que $V^{p,q} \neq 0$. Par convention, $z \in \mathbf{S}(\mathbf{R})$ agit sur $V^{p,q}$ par $z^{-p} \cdot \overline{z}^{-q}$. Les structures complexes correspondent donc aux bigraduations de type $\{(-1,0),(0,-1)\}$.

2.2. **L'hypothèse SV1.** Revenant aux données de Shimura, on demande :

SV1: Pour tout $h \in \mathcal{X}$, l'action de $\mathbf{S}$ sur $\mathrm{Lie}G_{\mathbf{R}}$ est de type $\{(-1,1), 0, (1,-1)\}$

Du diagramme $G \xrightarrow{\mathrm{ad}} G^{ad} \overset{\mathrm{Ad}}{\hookrightarrow} GL(\mathrm{Lie}(G))$ on tire alors que

$$\begin{array}{ccc} \mathbf{G}_{m,\mathbf{R}} & \xrightarrow{h} & Z_{\mathbf{R}} \\ \downarrow & & \downarrow \\ \mathbf{S} & \xrightarrow{h} & G_{\mathbf{R}} \end{array}$$

où Z est le centre de G. Le morphisme $h : \mathbf{G}_{m,\mathbf{R}} \to Z_{\mathbf{R}}$ est un cocaractère qui ne dépend pas du choix de $h \in \mathcal{X} = G(\mathbf{R}) \cdot h$. On note $\omega_{\mathcal{X}} : \mathbf{G}_{m,\mathbf{R}} \to Z_{\mathbf{R}}$ son *inverse.* On note aussi $C_h = h(i)$, qui est un élément de carré $h(i^2) = h(-1)$ central dans $G(\mathbf{R})$, et qui définit donc une *involution* $\mathrm{Int}C_h$ de $G_{\mathbf{R}}$. On a bien sûr $K(h) \subset K(C_h)$ où $K(C_h)$ est le centralisateur (= le commutant) de C_h dans $G(\mathbf{R})$.

On obtient aussi une factorisation de $h^{ad} = \mathrm{ad} \circ h$:

$$\mathbf{S} \xrightarrow{h} G \xrightarrow{\mathrm{ad}} G^{ad} = \mathbf{S} \xrightarrow{\pi} \mathbf{S}^1 \xrightarrow{u_h} G^{ad}$$

où $\mathbf{S}^1 = \ker(N : \mathbf{S} \to \mathbf{G}_{m,\mathbf{R}})$ et $\pi(z) = z/\overline{z}$. En particulier,

$$C_h^{ad} = h^{ad}(i) = u_h(-1) \in G^{ad}(\mathbf{R})$$

et $K(h^{ad}) = K(u_h) \subset K(C_h^{ad})$ où $K(C_h)$ est le commutant de C_h dans $G^{ad}(\mathbf{R})$.

2.3. **La structure presque complexe.** La représentation $\mathrm{Ad}\circ h : \mathbf{S} \to GL(\mathrm{Lie}G_{\mathbf{R}})$ se décompose en partie de type $(0,0)$ et partie de type $\{(1,-1),(-1,1)\}$, i.e. $\mathrm{Lie}G(\mathbf{R}) = L_h^+ \oplus L_h^-$ avec

$$\begin{aligned} L_h^+ &= \mathrm{Lie}G(\mathbf{R}) \cap \mathrm{Lie}G(\mathbf{C})^0 = \mathrm{Lie}G(\mathbf{R})[C_h - 1] \\ L_h^- &= \mathrm{Lie}G(\mathbf{R}) \cap \left(\mathrm{Lie}G(\mathbf{C})^{1,-1} \oplus \mathrm{Lie}G(\mathbf{C})^{-1,1}\right) = \mathrm{Lie}G(\mathbf{R})[C_h + 1] \end{aligned}$$

On a donc $L_h^+ = \mathrm{Lie}K(h) = \mathrm{Lie}K(C_h)$ (les groupes $K(h) \subset K(C_h)$ ont donc la même composante neutre), et $\mathcal{T}_h\mathcal{X} \simeq L_h^-$, qui est une représentation de $\mathbf{S}$ de type $\{(-1,1),(1,-1)\}$. On peut aussi procéder de même avec $\mathrm{Ad}\circ h^{ad} \to GL(\mathrm{Lie}G_{\mathbf{R}}^{ad})$, qui donne une décomposition

$$\mathrm{Lie}G^{ad}(\mathbf{R}) = L_{h^{ad}}^+ \oplus L_{h^{ad}}^- \quad \text{où} \quad L_{h^{ad}}^{\pm} = \mathrm{Lie}G^{ad}(\mathbf{R})[C_h^{ad} \mp 1].$$

Alors $L_{h^{ad}}^+ = \mathrm{Lie}K(h^{ad}) = \mathrm{Lie}K(C_h^{ad})$ (les groupes $K(h^{ad}) \subset K(C_h^{ad})$ ont donc la même composante neutre), et $\mathcal{T}_h\mathcal{X} \simeq L_{h^{ad}}^-$, qui est une représentation de $\mathbf{S}$ de type $\{(-1,1),(1,-1)\}$. En relabellisant la décomposition de Hodge de $\mathcal{T}_h\mathcal{X}\otimes\mathbf{C}$ associée à cette décomposition, on obtient une représentation de type $\{(-1,0),(0,-1)\}$, i.e. une *structure complexe* sur $\mathcal{T}_h\mathcal{X} \simeq L_{h^{ad}}^-$. Cette structure est caractérisée par la relation

$$\forall z \in \mathbf{S}^1(\mathbf{R}) = U^1 : \qquad \mathrm{Ad}(u_h(z)) : L_{h^{ad}}^- \ni v \mapsto z\cdot v \in L_{h^{ad}}^-.$$

Puisque $K(h)$ centralise u_h, cette structure complexe est $K(h)$-invariante, et plus généralement pour tout $g \in G(\mathbf{R})$ et $x \in \mathcal{X}$, la différentielle $\mathcal{T}_x(g) : \mathcal{T}_x\mathcal{X} \to \mathcal{T}_{g\cdot x}\mathcal{X}$ est $\mathbf{C}$-linéaire. On obtient donc sur $\mathcal{X}$ une structure presque complexe. Notant $\mathrm{Hol}(\mathcal{X})$ les difféomorphismes de $\mathcal{X}$ qui préservent cette structure complexe, on voit en particulier que :

Lemma 2.1. *Pour tout $x \in \mathcal{X}$, il existe un morphisme $u_x : U^1 \to \mathrm{Hol}(\mathcal{X})$ qui fixe x et vérifie $\forall z \in U^1$, $T_x(u_x(z)) : T_x\mathcal{X} \ni v \mapsto z\cdot v \in T_x\mathcal{X}$*

3. L'hypothèse SV2

3.1. **Involutions de Cartan.**

Definition 3.1. Soit G un groupe algébrique (affine, connexe) sur $\mathbf{R}$. Une involution de Cartan est une involution $\theta \in \mathrm{Aut}_{\mathbf{R}}G$ telle que

$$G^{(\theta)}(\mathbf{R}) = \{g \in G(\mathbf{C}) : g = \theta(\overline{g})\} \quad \text{est compact.}$$

Example 3.2. Sur $G = GL_{n,\mathbf{R}}$, $\theta_0(g) = {}^tg^{-1}$ est une involution de Cartan.

Theorem 3.3. *Un groupe algébrique sur $\mathbf{R}$ possède une involution de Cartan si et seulement si il est réductif, et alors toutes les involutions de Cartan sont conjuguées.*

Démonstration. [REF]. □

Si G est un groupe réductif, il existe une représentation fidèle $G \hookrightarrow GL(V)$ et un produit scalaire sur $V \simeq \mathbf{R}^n$ tel que G soit stable sous la transposition définie par ce produit scalaire. Alors G est stable sous l'involution de Cartan $\theta_0(g) = {}^tg^{-1}$ de $GL(V)$, donc $\theta = \theta_0|G$ est une involution de Cartan de G. Le théorème implique que toutes les involutions de Cartan sont de ce type, pour un produit scalaire convenable sur V.

Proposition 3.4. *Soit θ une involution de Cartan de $G_{\mathbf{R}}$,*

$$K = G^{\theta}(\mathbf{R}) = \{g \in G(\mathbf{R}) : \theta(g) = g\} \quad et \quad \mathcal{P} = \{x \in \mathbf{Lie}G(\mathbf{R}) : \theta(g) = -g\}.$$

Alors K est un sous-groupe compact maximal de $G(\mathbf{R})$ et

$$K \times \mathcal{P} \to G(\mathbf{R}) \qquad (k,p) \mapsto k \cdot \exp p$$

est un homéomorphisme.

Démonstration. Supposons d'abord que $\theta = \theta_0$ sur $G = GL_{n,\mathbf{R}}$. Alors

$$K = \{g \in G(\mathbf{R}) : g^t g = 1\} = O_n(\mathbf{R}) \quad \text{et} \quad \mathcal{P} = \{x \in M_n(\mathbf{R}) :^t x = x\} = Sym_n(\mathbf{R})$$

Les matrices symétriques sont les matrices diagonalisables à valeurs propres réelles dans une base orthonormée, donc $\exp \mathcal{P}$ est l'ensemble des matrices > 0, i.e. diagonalisables à valeurs propres réelles strictement positives dans une base orthonormée, et $\exp : \mathcal{P} \to \exp(\mathcal{P})$ est un homéomorphisme (d'inverse le logarithme). Si $g \in GL_n(\mathbf{R})$, alors ${}^t gg > 0$ donc ${}^t gg = \exp 2p = (\exp p)^2$ pour un $p \in \mathcal{P}$ et $\exp(-p){}^t gg \exp(-p) = 1$, i.e. $g\exp(-p) = k \in K$: l'application est surjective. Inversement si $g = k \exp p$, alors ${}^t gg = (\exp p)^2 = \exp 2p$, donc $p = \frac{1}{2}\ln({}^t gg)$ et $k = g \cdot \exp(-p)$, CQFD. Dans le cas général, on peut supposer que $\theta = \theta_0 | G$ pour un plongement $G \hookrightarrow GL_{n,\mathbf{R}}$ et il suffit de montrer que si $g = k \cdot \exp p \in G(\mathbf{R})$ avec $k \in O_n(\mathbf{R})$ et $p \in Sym_n(\mathbf{R})$, alors $k \in G(\mathbf{R})$ et $p \in \mathrm{Lie}G(\mathbf{R})$. Or $\exp(2p) = \theta(g)^{-1} g \in G(\mathbf{R})$ donc $p \in \mathrm{Lie}G(\mathbf{R})$, et alors $k = g \cdot \exp(-p) \in G(\mathbf{R})$. □

Corollary 3.5. *K est un sous-groupe compact maximal de $G(\mathbf{R})$ et*

$$\pi_0(K) \xrightarrow{\simeq} \pi_0(G(\mathbf{R})).$$

3.2. **L'hypothèse SV2.** Revenant aux notations des données de Shimura, on demande :

> **SV2:** Pour tout $h \in \mathcal{X}$, $\mathrm{Int}(C_h^{ad})$ est une involution de Cartan de $G_{\mathbf{R}}^{ad}$.

Alors $K(C_h^{ad})$ est un sous-groupe compact maximal de $G^{ad}(\mathbf{R})$, et son sous-groupe $K(h^{ad})$ est aussi compact. Puisque $\mathrm{Lie}K(h^{ad}) = \mathrm{Lie}K(C_h^{ad}) = \mathrm{Lie}G^{ad}(\mathbf{R})[C_h^{ad} - 1]$, $K(h^{ad})$ et $K(C_h^{ad})$ ont la même composante neutre. Mais $K(h^{ad})$ est déja connexe, puisque c'est le groupe des $\mathbf{R}$-points du $\mathbf{R}$-schéma en groupe connexe $Z_{G_{\mathbf{R}}^{ad}}(h^{ad})$ et que ce groupe est compact. On en déduit que le stabilisateur dans $G^{ad}(\mathbf{R})$ de toute composante connexe $G^{ad}(\mathbf{R})^+ \cdot h^{ad}$ de $\mathcal{X}^{ad}$ est la composante neutre $G^{ad}(\mathbf{R})^+$ de $G^{ad}(\mathbf{R})$, et donc d'après le lemme 1.3 :

Lemma 3.6. *Les composantes connexes $\mathcal{X}^+ = G(\mathbf{R})^+ \cdot h$ de $\mathcal{X}$ ont pour stabilisateur (commun) dans $G(\mathbf{R})$ l'image inverse $G(\mathbf{R})_+$ de $G^{ad}(\mathbf{R})^+$ dans $G(\mathbf{R})$.*

3.3. **Structure Hermitienne.** Soit $x \in \mathcal{X}$. Choisissons sur l'espace tangent $T_x\mathcal{X}$ une forme hermitienne définie positive. En intégrant cette forme sur le compact $K(x) = \mathrm{Stab}_{G^{ad}(\mathbf{R})}(x)$ (qui agit $\mathbf{C}$-linéairement sur $T_x\mathcal{X}$), on obtient une nouvelle forme qui est maintenant $K(x)$-invariante, et toujours définie positive. En transportant cette forme à $T_{g\cdot x}\mathcal{X}$ par $T_x(g) : T_x\mathcal{X} \to T_{g\cdot x}\mathcal{X}$, on obtient sur $\mathcal{X}$ une forme Hermitienne $G(\mathbf{R})$-invariante, et notamment une métrique $G(\mathbf{R})$-invariante (donnée par la forme Riemanienne associée).

On peut d'ailleurs rendre la construction de cette forme encore plus canonique, en choisissant comme point de départ la forme de Killing sur $\mathrm{Lie}G^{ad}(\mathbf{R})$, qui est donnée par

$$\phi(x,y) = \mathrm{Tr}_{\mathbf{R}}\left([x,[y,\bullet] : \mathrm{Lie}G^{ad}(\mathbf{R})\right).$$

Cette forme est en effet déjà invariante (à un caractère près) sous l'action adjointe de $G(\mathbf{R})$, et elle est non-dégénérée puisque $G^{ad}_{\mathbf{R}}$ est semi-simple. Pour tout $h \in \mathcal{X}$, la décomposition de Lie$G^{ad}(\mathbf{R})$ donnée par C_h^{ad} est une décomposition orthogonale pour ϕ, et en fait Lagrangienne, i.e.

$$L^+_{h^{ad}} \perp L^-_{h^{ad}} = \mathrm{Lie} G^{ad}(\mathbf{R})$$

avec $\phi|L^+_{h^{ad}} < 0$ et $\phi|L^-_{ad} > 0$ (on le voit par exemple en travaillant avec un plongement $G^{ad}_{\mathbf{R}} \hookrightarrow GL_{n,\mathbf{R}}$ tel que IntC_h^{ad} soit $g \mapsto {}^t g^{-1}$). L'action du compact $K(h^{ad})$ sur $T_h(\mathcal{X}) \simeq L^-_{h^{ad}}$ préserve ϕ, et en particulier $\phi(ix, iy) = 1$ puisque $i = u_h(i) \in K(h^{ad})$. Donc

$$\psi_h(x,y) = \phi(x,y) + i\phi(x, iy)$$

est une forme hermitienne définie positive et $K(h)$-invariante sur $T_h(\mathcal{X})$.

Proposition 3.7. *Les composantes connexes $\mathcal{X}^+$ de $\mathcal{X}$ sont des espaces symétriques hermitiens, i.e. des variétés holomorphes connexes, munies d'une forme hermitienne définie positive ψ, et telle qu'en tout point $x \in \mathcal{X}^+$, il existe une symétrie $s_x \in \mathrm{Is}(\mathcal{X}, \psi)$ qui admet x pour point fixe isolé.*

Démonstration. Il faut d'abord montrer que la structure presque complexe est intégrable (i.e. définit sur $\mathcal{X}$ une structure de variété holomorphe). Comme symétrie en $h \in \mathcal{X}$, on prend bien sûr le difféomorphisme induit par $C_h^{ad} = h^{ad}(i) \in G^{ad}(\mathbf{R})$. Ce difféomorphisme préserve la composante connexe $G^{ad}(\mathbf{R})^+ \cdot h$ de h puisque $C_h^{ad} \in G^{ad}(\mathbf{R})^+$ (car $\mathbf{S}$ est connexe), il préserve ψ et la structure presque complexe par construction, il fixe bien sûr le point h de $G^{ad}(\mathbf{R})$ (puisque $h^{ad}(\mathbf{S}) \subset K(h^{ad})$ car $\mathbf{S}$ est commutatif). Puisqu'il induit -1 sur l'espace tangent $T_h\mathcal{X}$, h est un point fixe isolé. □

On peut montrer que de tels espaces sont totalement géodésiques, que s_x stabilise toutes les géodésiques qui passent par x, et induit sur chacune d'elles l'inversion : $s_x\gamma(t) = \gamma(-t)$ si $\gamma(0) = x$. Les espaces symétriques hermitiens ont été totalement classifiés. Ceux que l'on obtient par la procédure ci-dessus sont exactement ceux qui sont de courbures négatives : on les appelle les domaines symétriques hermitiens.

3.4. **Retour à la variété de Shimura.** Soit $\mathcal{X}^+ \subset \mathcal{X}$ une composante connexe de $\mathcal{X}$. Puisque $G(\mathbf{Q})$ est dense dans $G(\mathbf{R})$, $G(\mathbf{Q})$ agit transitivement sur l'ensemble des composantes connexes, et le stabilisateur dans $G(\mathbf{Q})$ de $\mathcal{X}^+$ est l'intersection $G(\mathbf{Q})_+ = G(\mathbf{R})_+ \cap G(\mathbf{Q})$. On obtient donc

$$\mathrm{Sh}_K(G, \mathcal{X})(\mathbf{C}) = G(\mathbf{Q})_+ \backslash \left(G(\mathbf{A}_f)/K \times \mathcal{X}^+\right).$$

Lemma 3.8. *$G(\mathbf{Q})_+ \backslash G(\mathbf{A}_f)/K$ est fini.*

Démonstration. Cf. [REF], qui dit que $G(\mathbf{Q})\backslash G(\mathbf{A}_f)/K$ est fini. □

Soit $\mathcal{C} \subset G(\mathbf{A}_f)$ un système de représentants pour $G(\mathbf{Q})^+ \backslash G(\mathbf{A}_f)/K$. Alors

$$\mathrm{Sh}_K(G, \mathcal{X})(\mathbf{C}) \simeq \coprod_{g \in \mathcal{C}} \Gamma_{gKg^{-1}} \backslash \mathcal{X}^+ = \coprod_{g \in \mathcal{C}} \Gamma^{ad}_{gKg^{-1}} \backslash \mathcal{X}^+$$

où $\Gamma_{gKg^{-1}}$ est le stabilisateur de $g \cdot K$ dans $G(\mathbf{Q})_+$, i.e. $\Gamma_{gKg^{-1}} = G(\mathbf{Q})_+ \cap gKg^{-1}$, et $\Gamma(g)^{ad}$ son image dans $G^{ad}(\mathbf{Q})^+ \subset G^{ad}(\mathbf{R})^+$.

3.5. **La structure holomorphe sur** $\mathrm{Sh}_K(G,\mathcal{X})(\mathbf{C})$**.**

Lemma 3.9. *Pour tout compact K de $G(\mathbf{A}_f)$, le sous-groupe $\Gamma_K = G(\mathbf{Q}) \cap K$ de $G(\mathbf{Q})$ est discret dans $G(\mathbf{R})$ et son image Γ_K^{ad} dans $G^{ad}(\mathbf{Q})$ est discrète dans $G^{ad}(\mathbf{R})$. Si K est suffisamment petit, alors $\Gamma_{gKg^{-1}}$ et $\Gamma_{gKg^{-1}}^{ad}$ sont sans torsion pour tout $g \in G(\mathbf{A}_f)$.*

Démonstration. On choisit une représentation fidèle $\rho : G \hookrightarrow GL(V)$ et un réseau L de V fixé par K. Une base de ce réseau identifie $GL(V)$ à $GL_{n,\mathbf{Q}}$ et Γ_K à un sous-groupe de $GL_n(\mathbf{Z})$. Puisque $GL_n(\mathbf{Z})$ est discret dans $GL_n(\mathbf{R})$, Γ_K est discret dans $G(\mathbf{R})$. Si K agit trivialement sur $L/\ell L$ pour un premier $\ell \geq 3$, Γ_K est contenu dans $\Gamma(\ell) = \{g \in GL_n(\mathbf{Z}) : g \equiv 1 \bmod \ell\}$ qui est sans torsion, donc Γ_K est sans torsion. Mais alors gKg^{-1} agit trivialement sur $L'/\ell \cdot L'$ où $L' = g \cdot L$, donc $\Gamma_{gKg^{-1}}$ est à nouveau sans torsion. Pour G^{ad}, on procède de même avec une représentation fidèle de G^{ad}. □

Corollary 3.10. *Si K est assez petit, $\mathrm{Sh}_K(G,\mathcal{X})(\mathbf{C})$ est une variété holomorphe.*

Démonstration. On suppose que K est assez petit, i.e. tel que $\Gamma_{gKg^{-1}}^{ad}$ est sans torsion pour tout $g \in G(\mathbf{A}_f)$. On a vu que

$$\mathrm{Sh}_K(G,\mathcal{X})(\mathbf{C}) = \coprod_{g \in \mathcal{C}} \Gamma_K^{ad}(g) \backslash \mathcal{X}^+ \quad \text{où } \mathcal{X}^+ \simeq G^{ad}(\mathbf{R})^+/K(h^{ad})$$

et le lemme suivant permet facilement de munir chacun des espaces $\Gamma_K^{ad}(g)\backslash\mathcal{X}^+$ d'une structure holomorphe – telle que la projection $\mathcal{X}^+ \twoheadrightarrow \Gamma_K^{ad}(g)\backslash\mathcal{X}^+$ soit un isomorphisme local. □

Lemma 3.11. *Soit G un groupe localement compact, K un sous-groupe compact de G, Γ un sous-groupe discret de G. On munit $\mathcal{X} = G/K$ de la topologie quotient. Alors :*

(1) *Pour tout $x \in \mathcal{X}$, $\Gamma_x = \{\gamma \in \Gamma : \gamma x = x\}$ est fini.*
(2) *Pour tout compact $A, B \subset \mathcal{X}$, $\{\gamma \in \Gamma : \gamma A \cap B \neq \emptyset\}$ est fini.*
(3) *Pour tout $x \in \mathcal{X}$, il existe un voisinage ouvert U de x tel que $\gamma U \cap U \neq \emptyset \Rightarrow \gamma x = x$.*
(4) *Pour tout $\Gamma x \neq \Gamma y \in \mathcal{X}$, il existe des voisinages ouverts U de x et V de y tels que $\Gamma U \cap \Gamma V = \emptyset$.*

Démonstration. Puisque K est fermé, $\mathcal{X}$ est séparé. Pour tout $x \in \mathcal{X}$, le stabilisateur K_x de x dans G est compact, car c'est un conjugué de K. Donc $\Gamma_x = \Gamma \cap K_x$ est compact et discret, i.e. fini, ce qui prouve (1). L'application $\pi : G \to G/K = \mathcal{X}$ est ouverte par définition de la topologie de $\mathcal{X}$, et elle est aussi rétro-compact : si A est un compact de $\mathcal{X}$, $\pi^{-1}(A)$ est un compact de G. En effet, si $G = \cup U_i$ avec U_i ouvert et $\overline{U}_i$ compact, alors $\mathcal{X} = \cup \pi(U_i)$ avec $\pi(U_i)$ ouvert, donc $A \subset \cup_{i \in I} \pi(U_i)$ avec I fini et $\pi^{-1}(A) \subset \cup_{i \in I} U_i \cdot K \subset \cup_{i \in I} \overline{U_i} \cdot K$ qui est compact. Si A et B sont des compacts de $\mathcal{X}$ et $\gamma A \cap B \neq \emptyset$, alors $\gamma\pi^{-1}(A) \cap \pi^{-1}(B) \neq \emptyset$, donc $\gamma \in \pi^{-1}(B) \cdot (\pi^{-1}(A))^{-1} \cap \Gamma$, qui est compact et discret donc fini, ce qui prouve (2). Pour (3), on commence par choisir un voisinage compact V de x, et on note que d'après (2), $\Gamma_V = \{\gamma \in \Gamma : \gamma V \cap V \neq \emptyset\}$ est fini. Pour chaque $\gamma \in \Gamma_V - \Gamma_x$, on choisit des voisinages disjoints V_γ de x et W_γ de γx. On pose $U = V \cap \cap_{\gamma \in \Gamma_V - \Gamma_x} V_\gamma \cap \gamma^{-1} W_\gamma$, qui est un voisinage de x contenu dans V. On a donc $\Gamma_x \subset \Gamma_U \subset \Gamma_V$. Mais si $\gamma \in \Gamma_V - \Gamma_x$, $\gamma U \subset W_\gamma$

et $U \subset V_\gamma$, donc $\gamma U \cap U = \emptyset$ et $\gamma \notin \Gamma_U$: donc $\Gamma_x = \Gamma_U$, i.e. (3). Pour (4), on commence de même par prendre des voisinages compacts A de x et B de y, puis on considère l'ensemble fini $\Gamma(A,B) = \{\gamma \in \Gamma : \gamma A \cap B \neq \emptyset\}$, et on choisit pour tout $\gamma \in \Gamma(A,B)$ des voisinages disjoints V_γ de γx et W_γ de y. On pose alors $V = A \cap \cap_{\gamma\in\Gamma(A,B)} \gamma^{-1} V_\gamma$ et $W = B \cap \cap_{\gamma \in \Gamma(A,B)} W_\gamma$. Ce sont respectivement des voisinages de A et B. Si $\gamma \in \Gamma(V,W)$, alors $\gamma \in \Gamma(A,B)$, donc $\gamma V \subset V_\gamma$ tandis que $W \subset W_\gamma$, donc $\gamma V \cap W = \emptyset$, une contradiction. Donc $\Gamma(V,W) = \emptyset$, ce qui prouve (4). □

Ci-dessus, nous n'avons utilisé que la compacité des sous-groupes K de $G(\mathbf{A}_f)$, dont nous avons vu essentiellement qu'elle implique que les groupes de type $\Gamma_K = G(\mathbf{Q}) \cap K$ sont petits, i.e. discret dans $G(\mathbf{R})$. D'un autre côté, les sous-groupes K de $G(\mathbf{A}_f)$ considérés dans la définition des variétés de Shimura sont *aussi* assez gros : ils sont ouverts en plus d'être compacts. Cette hypothèse implique que les sous-groupes $\Gamma_K \subset G(\mathbf{Q})$ sont aussi assez gros (en plus d'être discrets). Plus précisément, ces sous-groupes sont exactement ceux que l'on appelle les *sous-groupes de congruences*, qui sont eux-mêmes des *sous-groupes arithmétiques*. Pour donner un énoncé qualitatif, on peut noter que la métrique Riemannienne $G^{ad}(\mathbf{R})$ -invariante sur $\mathcal{X}^+$ descend en une métrique Riemannienne sur chacun des $\Gamma^{ad}_{gKg^{-1}} \backslash \mathcal{X}$, lesquelles se recollent en une métrique Riemannienne sur $\mathrm{Sh}_K(G,\mathcal{X})$, d'où une notion de volume. Et bien :

Proposition 3.12. *Le volume de* $\mathrm{Sh}_K(G,\mathcal{X})(\mathbf{C})$ *est fini.*

Démonstration. Cf. [5, Theorem 4.13], qui implique que $\Gamma\backslash G^{ad}(\mathbf{R})$ est déjà de volume fini pour tout sous-groupe arithmétique Γ de $G^{ad}(\mathbf{R})$. □

4. Les Autres Hypothèses

4.1. **L'hypothèse SV3.** Décomposons $G^{ad} = \prod G_j$ en produit de facteurs $\mathbf{Q}$-simples et soient $h_j^{ad} = \mathbf{S} \to G_{j,\mathbf{R}}$ les projections correspondantes de $h^{ad} : \mathbf{S} \to G^{ad}_{\mathbf{R}}$. Si $h_j^{ad} = 1$, l'identité est une involution de Cartan de $G_{j,\mathbf{R}}$, donc $G_j(\mathbf{R})$ est *compact*. Inversement, si $G_j(\mathbf{R})$ est compact, l'involution de Cartan $\mathrm{Int} h_j^{ad}(i)$ est conjuguée à l'identité, donc *est* l'identité, c'est-à-dire que $h_j^{ad}(i)$ est central donc trivial (puisque G_j est adjoint), donc $K(h_j^{ad}) = G_j(\mathbf{R})^+ = G_j(\mathbf{R})$, i.e. $h_j^{ad} : \mathbf{S} \to G_{j,\mathbf{R}}$ est central donc trivial.

SV3: $h_j^{ad} \neq 1$ pour tout j, i.e. aucun des $G_j(\mathbf{R})$ n'est compact[1].

Cette hypothèse est toujours requise pour les variétés de Shimura. Elle est utilisée en conjonction avec le théorème d'*approximation forte*, qui dit que

Theorem 4.1. *Si G est semi-simple, simplement connexe et $G(\mathbf{R})$ n'est pas compact, alors $G(\mathbf{Q})$ est dense dans $G(\mathbf{A}_f)$, donc $G(\mathbf{Q})\backslash G(\mathbf{A}_f)/K = \{\bullet\}$ pour tout sous-groupe ouvert K.*

Démonstration. [5, Theorem 7.12]. □

Ce théorème permet de calculer par dévissage l'ensemble des composantes connexes $\pi_0(\mathrm{Sh}_K(G,\mathcal{X}))$ des variétés de Shimura. Pour le calcul lorsque G^{der} est semi-simple, voir [4, Theorem 5.17]. Le calcul dans le cas général est plus ardu, cf. [2].

[1]On veut cependant que cette condition n'exclue pas les tores, dont le groupe adjoint est trivial : il faut donc convenir que le groupe trivial $\{1\}$ est *sans* facteur simple.

Ce calcul est préliminaire à l'analyse de la *loi de réciprocité pour les composantes connexes*, dont nous ne parlerons pas.

4.2. **Hypothèses auxiliaires.** Le morphisme de poids $\omega_{\mathcal{X}} : \mathbf{G}_{m,\mathbf{R}} \to Z_{\mathbf{R}}$ est un cocaractère de Z, il est donc défini sur $\overline{\mathbf{Q}}$.

SV4: $\omega_{\mathcal{X}}$ est défini sur $\mathbf{Q}$.

SV5: $Z(\mathbf{Q})$ est discret dans $Z(\mathbf{A}_f)$.

Ces axiomes correspondent aux variétés de Shimura dont on espère qu'elles classifient des objets de nature géométrique : les motifs.

5. Exemples

5.1. **Exemple n°1 : courbes modulaires.** On prend $G = GL_{2,\mathbf{Q}}$ et pour $\mathcal{X}$ la classe de $G(\mathbf{R})$-conjugaison du morphisme $h : \mathbf{S} \to GL_{2,\mathbf{R}}$ défini par

$$h(z) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \quad \text{pour } z = a + ib \in \mathbf{S}(\mathbf{R}) = \mathbf{C}^\times.$$

On a $K(h) = K(C_h) = SO(2, \mathbf{R})$ mais

$$K(h^{ad}) = SO(2, \mathbf{R})/\{\pm 1\} \subsetneq K(C_h^{ad}) = O(2, \mathbf{R})/\{\pm 1\}.$$

Puisque $SO(2, \mathbf{R})$ est aussi le stabilisateur de $i \in \mathbf{C} - \mathbf{R}$ pour l'action transitive

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbf{R}) \quad \text{et} \quad z \in \mathbf{C} - \mathbf{R} : \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d} \in \mathbf{C} - \mathbf{R},$$

cette action identifie $\mathcal{X} \simeq \mathbf{C} - \mathbf{R}$, par $g \cdot h \mapsto g \cdot i$. On a Lie$G = M_2$ avec l'action par conjugaison de G, et pour tout $z = a + ib \in \mathbf{C}^\times = \mathbf{S}(\mathbf{R})$,

$$h(z) \begin{pmatrix} x & y \\ -y & x \end{pmatrix} h(z)^{-1} = \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \quad \text{et} \quad h(z) \begin{pmatrix} 1 & \pm i \\ \pm i & -1 \end{pmatrix} h(z)^{-1} = \frac{(a \pm ib)}{(a \mp ib)} \begin{pmatrix} 1 & \pm i \\ \pm i & 1 \end{pmatrix}$$

donc Lie$G(\mathbf{C}) = V^{0,0} \oplus V^{1,-1} \oplus V^{-1,1}$ avec

$$V^{0,0} = \mathbf{C} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \oplus \mathbf{C} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{et} \quad V^{\pm 1, \mp 1} = \mathbf{C} \cdot \begin{pmatrix} 1 & \mp i \\ \mp i & 1 \end{pmatrix}$$

i.e. $(G, \mathcal{X})$ vérifie **SV1**. La décomposition de Lie$G(\mathbf{R}) = L_h^+ \oplus L_h^-$ est

$$L_h^+ = \left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} : x, y \in \mathbf{R} \right\} \qquad L_h^- = \left\{ \begin{pmatrix} x & y \\ y & -x \end{pmatrix} : x, y \in \mathbf{R} \right\}.$$

Le morphisme $u_h : \mathbf{S}^1 \to G^{ad}(\mathbf{R}) = PGL_2(\mathbf{R}) = GL_2(\mathbf{R})/\mathbf{R}^\times$ est

$$\frac{a + ib}{a - ib} \mapsto \mathbf{R}^\times \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \quad \text{donc } i = \frac{1 + i}{1 - i} \mapsto \mathbf{R}^\times \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}.$$

La structure complexe I_h sur $T_h\mathcal{X} \simeq L_h^-$ est donc

$$I_h \cdot \begin{pmatrix} x & y \\ y & -x \end{pmatrix} = u_h(i) \begin{pmatrix} x & y \\ y & -x \end{pmatrix} u_h(i)^{-1} = \begin{pmatrix} y & -x \\ -x & -y \end{pmatrix}.$$

Le difféomorphisme $g \cdot h \mapsto g \cdot i$ identifie $L_h^- \simeq T_h\mathcal{X} \simeq T_i(\mathbf{C} - \mathbf{R}) \simeq \mathbf{C}$ par

$$\begin{pmatrix} x & y \\ y & -x \end{pmatrix} \in L_h^- \mapsto 2(y + ix) \in \mathbf{C}$$

et envoie donc I_h sur $[\times i] = d_i(z \mapsto \frac{z+1}{-z+1})$. Puisque l'action de $G(\mathbf{R})$ sur $\mathbf{C} - \mathbf{R}$ est holomorphe, on en déduit que notre difféomorphisme $\mathcal{X} \simeq \mathbf{C} - \mathbf{R}$ est compatible avec les structures complexes, i.e. est holomorphe. La symétrie $u_h(-1)$ sur $\mathcal{X}$ correspond à $z \mapsto \frac{-1}{z}$ sur $\mathbf{C}-\mathbf{R}$. Pour $\theta = \mathrm{Int}C_h$,

$$\begin{aligned} G^{(\theta)}(\mathbf{C}) &= \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} : a, b \in \mathbf{C},\, a\bar{a}+b\bar{b} \neq 0 \right\} \\ (G^{ad})^{(\theta)}(\mathbf{C}) &\simeq \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} : a\bar{a}+b\bar{b} = 1 \right\} / \{\pm 1\} \end{aligned}$$

qui est compact, donc θ est une involution de Cartan de $G^{ad}_{\mathbf{R}}$ et $(G, \mathcal{X})$ vérifie **SV2**. Pour la forme de Killing sur $\mathrm{Lie}G(\mathbf{R})$, on a une décomposition orthogonale

$$\mathrm{Lie}G(\mathbf{R}) = \mathbf{R}\cdot\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \perp \mathbf{R}\cdot\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \perp \mathbf{R}\cdot\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \perp \mathbf{R}\cdot\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

et la forme quadratique associée vaut $0, -8, 8, 8$ sur la base indiquée, qui induit

$$\phi\left(\begin{pmatrix} x & y \\ y & -x \end{pmatrix}, \begin{pmatrix} x' & y' \\ y' & -x' \end{pmatrix}\right) = 8(xx'+yy') \quad \text{sur } L_h^- \simeq T_h\mathcal{X}.$$

Sur $\mathcal{X} \simeq \mathbf{C}-\mathbf{R}$, la forme induite sur l'espace tangent $\mathbf{C}$ en $i \in \mathbf{C}-\mathbf{R}$ est donc exactement la forme standard $\phi(z_1, z_2) = \mathrm{Tr}_{\mathbf{C}/\mathbf{R}}(z_1\bar{z}_2)$. En $z = x+iy$, on transporte cette forme de l'espace tangent $\mathbf{C}$ de $i \in \mathbf{C}-\mathbf{R}$ à l'espace tangent $\mathbf{C}$ de $z = gi \in \mathbf{C}-\mathbf{R}$ avec

$$g = \begin{pmatrix} \mathrm{signe}(y)\cdot\sqrt{|y|} & x/\sqrt{|y|} \\ & 1/\sqrt{|y|} \end{pmatrix} \text{ qui donne } dg = [y\times] : \mathbf{C} \to \mathbf{C}.$$

On obtient donc la métrique riemanienne $\frac{dx\cdot dy}{y^2}$ sur $\mathbf{C}-\mathbf{R}$. Il est clair que $(G, \mathcal{X})$ vérifie aussi **SV3**, **SV4** et **SV5**. Les variétés $\mathrm{Sh}_K(G, \mathcal{X})$ que l'on obtient sont les courbes modulaires.

Remark 5.1. Soit B un corps de quaternion sur $\mathbf{Q}$ tel que $B_{\mathbf{R}} \simeq M_2(\mathbf{R})$. On prend pour G le groupe multiplicatif de B, i.e $G(R) = (B\otimes R)^\times$ pour toute $\mathbf{Q}$-algèbre R. Et pour $\mathcal{X}$, on prend la $G(\mathbf{R})$-classe de conjugaison de h... comme ci-dessus, puisque $G(\mathbf{R}) \simeq GL_2(\mathbf{R})$. Alors $(G, \mathcal{X})$ est encore une donnée de Shimura. Les variétés que l'on obtient ainsi sont les courbes de Shimura.

5.2. **Exemple n°2 : variétés de type PEL.** Soit B une $\mathbf{Q}$-algèbre semi-simple, $\star$ une involution positive sur B, $(V, \psi) \in \mathcal{H}_{\mathbf{Q}}(B, \star, -1)$ un $(B, \star)$-module symplectique. On prend pour G le groupe des similitudes B-linéaires de (V, ψ) et pour $\mathcal{X}$ la classe de conjugaison d'un morphisme $h_I : \mathbf{S} \to G(\mathbf{R})$ provenant d'une structure complexe $(B, \star)$ linéaire I sur $V_{\mathbf{R}}$ telle que $\psi_{\mathbf{R},I} > 0$, i.e. $h_I : \mathbf{S} \to G_{\mathbf{R}}$ envoie $a+bi \in \mathbf{C}^\times = \mathbf{S}(\mathbf{R})$ sur la multiplication par $a+bI$ dans $V_{\mathbf{R}}$. Vérifions les axiomes.

Pour vérifier l'axiome **SV1**, on plonge G dans $\mathbf{GL}(V)$. Sur $V_{\mathbf{R}}$, l'action de $\mathbf{S}$ est de type $\{(-1,0),(0,-1)\}$ puisqu'elle provient d'une structure complexe. Cela signifie que $V_{\mathbf{C}} = V^+ \oplus V^-$ avec $h_I(z)(v) = zv$ pour $v \in V^+$ et $\bar{z}v$ pour $v \in V^-$. Donc sur

$$\mathrm{Lie}G(\mathbf{C}) \subset \mathrm{Lie}\mathbf{GL}(V)(\mathbf{C}) = \mathrm{Hom}_{\mathbf{C}}(V_{\mathbf{C}}, V_{\mathbf{C}}) = \oplus_{\pm_1,\pm_2}\mathrm{Hom}_{\mathbf{C}}(V^{\pm_1}, V^{\pm_2})$$

l'action adjointe est

$$\mathrm{Ad}(h_I(z)) = \begin{cases} 1 & \text{sur } \mathrm{Hom}_{\mathbf{C}}(V^\pm, V^\pm), \\ z/\bar{z} & \text{sur } \mathrm{Hom}_{\mathbf{C}}(V^-, V^+), \\ \bar{z}/z & \text{sur } \mathrm{Hom}_{\mathbf{C}}(V^+, V^-). \end{cases}$$

i.e., elles est de type $\{(1,-1),0,(-1,1)\}$, CQFD.

Pour l'axiome **SV2**, il faut vérifier que $\mathrm{Int}(\mathrm{ad}(I))$ est une involution de Cartan de $G^{ad}_{\mathbf{R}}$. Il suffit pour cela de vérifier que $\theta = \mathrm{Int}(I)$ est une involution de Cartan du groupe dérivé $G^{der}_{\mathbf{R}}$. On plonge cette fois-ci G dans $\mathbf{GSp}(V,\psi)$, donc G^{der} dans $\mathbf{Sp}(V,\psi)$. Pour tout $g \in \mathbf{Sp}(V,\psi)(\mathbf{C})$ et $v, w \in V_{\mathbf{C}}$, on a

$$(\psi_{\mathbf{R},I})_{\mathbf{C}}(gv, \overline{gw}) = (\psi_{\mathbf{R}})_{\mathbf{C}}(Igv, \overline{gw}) = \psi_{\mathbf{C}}(gv, I^{\star}\overline{gw})$$

avec $I^{\star} = -I$. Donc si $I\overline{g} = gI$, $I^{\star}\overline{g} = gI^{\star}$ et

$$(\psi_{\mathbf{R},I})_{\mathbf{C}}(gv, \overline{gw}) = \psi_{\mathbf{C}}(gv, gI^{\star}\overline{w}) = \psi_{\mathbf{C}}(v, I^{\star}\overline{w}) = \psi_{\mathbf{C}}(Iv, \overline{w}) = (\psi_{\mathbf{R},I})_{\mathbf{C}}(v, \overline{w}).$$

Mais $\psi_{\mathbf{R},I} > 0$, donc $(\psi_{\mathbf{R},I})_{\mathbf{C}}(v,\overline{w})$ est une forme hermitienne $\Psi > 0$ sur $V_{\mathbf{C}}$. Donc

$$(G^{der})^{\theta}(\mathbf{R}) \subset \mathbf{Sp}(V,\psi)^{\theta}(\mathbf{R}) \subset U(\Psi) \subset \mathbf{Sp}(V_{\mathbf{C}}, \psi_{\mathbf{C}})$$

est compact, CQFD.

Pour l'axiome **SV3**, il faut faire des hypothèses supplémentaires. Le composé du poids $\omega_{\mathcal{X}} : \mathbf{G}_{m,\mathbf{R}} \to Z_{\mathbf{R}}$ avec l'inclusion $Z_{\mathbf{R}} \to \mathbf{GL}(V_{\mathbf{R}})$ correspond à l'inverse du morphisme évident $\mathbf{G}_{m,\mathbf{R}} \to \mathbf{GL}(V_{\mathbf{R}})$, et ce poids est donc défini sur $\mathbf{Q}$, i.e. $(G,\mathcal{X})$ vérifie **SV4**.

5.3. **Exemple n°2bis : Un cas PEL simple.** Il y a un cas particulier qui a été abondamment étudié, notamment dans le cadre du programme de Langlands. C'est celui où le centre de B est un corps CM E. Alors B est simple et l'involution $\star$ de B induit l'involution canonique de E. Dans ce cas,

$$(B_{\mathbf{R}}, \star) \simeq \prod_{\phi} (M_n(\mathbf{C}), \star)$$

Le choix d'un tel isomorphisme fournit un type CM Φ sur E, et une équivalence

$$\mathcal{H}(B_{\mathbf{R}}, \star, -) \simeq \prod_{\phi} \mathcal{H}(\mathbf{C}, \star).$$

En particulier, $G(\mathbf{R}) \subset \prod \mathbf{GU}(V_{\phi}) = \mathbf{GU}(p_{\phi}, q_{\phi})$ pour des signatures (p_{ϕ}, q_{ϕ}). Les domaines symétriques hermitiens associés à chacun des facteurs sont en bijection avec l'ensemble des décompositions $V_{\phi} = V_{\phi}^{+} \perp V_{\phi}^{-}$ en partie où la forme hermitienne est respectivement définie positive et définie négative. On peut de plus choisir Φ de sorte que le morphisme $h_{\phi} : \mathbf{S} \hookrightarrow G_{\mathbf{R}}$ correspondant à une telle décomposition envoie z sur $(z \,\text{sur}\, V_{\phi}^{+}, \overline{z} \,\text{sur}\, V_{\Phi}^{-})$.

5.4. **Exemple n°3 : Tores.** Si T est un tore et $h : \mathbf{S} \to T_{\mathbf{R}}$ un morphisme quelconque, alors h agit trivialement sur $\mathrm{Lie}T_{\mathbf{R}}$ et $T^{ad}_{\mathbf{R}}$ est trivial : les conditions **SV1,2,3** sont donc automatiquement vérifiées. Les variétés de Shimura correspondantes sont de dimension 0 : juste un ensemble fini de points

$$\mathrm{Sh}_K(T,\{h\})(\mathbf{C}) = T(\mathbf{Q})\backslash T(\mathbf{A}_f)/K.$$

5.5. **Exemple n°4 : variétés de type B ou D.** Soit F un corps totalement réel, (V,ϕ) un F-espace quadratique de dimension $n \geq 3$ tel que pour tout plongement $\tau : F \hookrightarrow \mathbf{R}$, (V_{τ}, ϕ_{τ}) est de signature

$$(p_{\tau}, q_{\tau}) \in \{(n,0),(0,n),(2,n-2),(n-2,2)\}.$$

On suppose aussi qu'*au moins une* de ces signatures est dans $\{(2,n-2),(n-2,2)\}$. On fixe dans chaque V_{τ} de signature $(2,n-2)$ ou $(n-2,2)$ un sous-espace totalement anisotrope W_{τ} maximal et de dimension 2, et une orientation sur ce sous-espace.

On munit W_τ de la structure complexe déduite de cette orientation, i.e. de celle pour laquelle la multiplication par i est une rotation d'angle $\pi/2$. On prend alors $G = \mathrm{Res}_{F/\mathbf{Q}} SO(V,\phi)$ et pour $\mathcal{X}$, la classe de $G(\mathbf{R})$-conjugaison du morphisme $h : \mathbf{S} \to G_{\mathbf{R}}$ qui envoie $z \in \mathbf{C}^\times = \mathbf{S}(\mathbf{R})$ sur l'élément qui agit par $z/\overline{z}$ sur $\oplus W_\tau$ et qui est trivial sur $(\oplus W_\tau)^\perp$.

Exercise 5.2. Vérifier les axiomes **SV1-5.**

6. Structure algébrique sur $\mathbf{C}$

A ce stade, on a déjà une structure de variété holomorphe (ou analytique complexe) sur

$$\mathrm{Sh}_K(G,\mathcal{X})(\mathbf{C}) = G(\mathbf{Q})\backslash \left(G(\mathbf{A}_f)/K \times \mathcal{X}\right),$$

au moins lorsque K est assez petit. Si cette variété est projective, i.e. isomorphe à un fermé d'un $\mathbf{P}^n(\mathbf{C})$, on peut appliquer le théorème suivant pour obtenir une variété *algébrique projective lisse* sur $\mathbf{C}$ dont $\mathrm{Sh}_K(G,\mathcal{X})(\mathbf{C})$ est l'ensemble des points complexes :

Theorem 6.1. *Le foncteur $V \mapsto V(\mathbf{C})^{an}$ est une équivalence de catégorie entre variété algébrique lisse projective sur $\mathbf{C}$ et variété analytique complexe projective.*

En règle générale, $\mathrm{Sh}_K(G,\mathcal{X})(\mathbf{C})$ n'est cependant pas compacte. Mais un théorème de Bailly et Borel permet de compactifier chacune des composantes connexes $\Gamma\backslash\mathcal{X}^+$de $\mathrm{Sh}_K(G,\mathcal{X})(\mathbf{C})$ en la réalisant comme un ouvert de Zariski d'une variété algébrique projective $(\Gamma\backslash\mathcal{X}^+)^\star$. On obtient alors une variété algébrique lisse et quasi-projective $\mathrm{Sh}_K(G,\mathcal{X})_{\mathbf{C}}$ sur $\mathbf{C}$ dont la variété analytique complexe sous-jacente $\mathrm{Sh}_K(G,\mathcal{X})_{\mathbf{C}}(\mathbf{C})^{an}$ est bien ce qu'il faut, à savoir notre variété analytique complexe $\mathrm{Sh}_K(G,\mathcal{X})(\mathbf{C})$! Un théorème de Borel dit que la structure algébrique ainsi obtenue est universelle - donc unique à unique isomorphisme près :

Theorem 6.2. *Pour toute variété algébrique quasi-projective lisse V sur $\mathbf{C}$, tout morphisme analytique complexe $V^{an}(\mathbf{C}) \to \mathrm{Sh}_K(G,\mathcal{X})(\mathbf{C})^{an}$ est induit par un morphisme algébrique $V \to \mathrm{Sh}_K(G,\mathcal{X})_{\mathbf{C}}$.*

Pour les variétés qui nous concernent principalement - à savoir les variétés de Shimura de type PEL, nous verrons plus bas pourquoi ces résultats ne nous concernent guère, compte-tenu de ce que l'on a déjà fait dans ce cours : on sait déjà que $\mathrm{Sh}_K(G,\mathcal{X})(\mathbf{C})$ est l'ensemble des $\mathbf{C}$-points d'une variété, celle qui représente le problème de module ad-hoc.

7. Modèles Canoniques

7.1. **Le corps reflex d'une donnée de Shimura.** Soit $(G,\mathcal{X})$ une donnée de Shimura. Pour tout $h \in \mathcal{X}$, on note

$$\mu_h : \mathbf{G}_{m,\mathbf{C}} \hookrightarrow \mathbf{G}_{m,\mathbf{C}} \times \mathbf{G}_{m,\mathbf{C}} \simeq \mathbf{S}_{\mathbf{C}} \xrightarrow{h_{\mathbf{C}}} G_{\mathbf{C}}$$

où le premier morphisme envoie z sur $(z,1)$ et l'inverse du second $z \in \mathbf{S}(\mathbf{R}) \subset \mathbf{S}(\mathbf{C})$ sur $(z,\overline{z}) \in \mathbf{G}_m(\mathbf{C}) \times \mathbf{G}_m(\mathbf{C})$. On obtient ainsi un élément bien défini $\mu(G,\mathcal{X}) \in \mathcal{C}(G,\mathbf{C})$, où pour tout corps $k \subset \mathbf{C}$, on note

$$\mathcal{C}(G,k) = G(k)\backslash\mathrm{Hom}_{k-gr}(\mathbf{G}_{m,k}, G_k)$$

l'ensemble des classes de $G(k)$-conjugaison de cocaractères de G_k.

Lemma 7.1. *Si G_k est décomposé, i.e. contient un tore maximal déployé $T = \mathbf{G}_{m,k}^r$, alors*

$$W(k)\backslash \mathrm{Hom}_{k-gr}(\mathbf{G}_{m,k}, T) \simeq G(k)\backslash \mathrm{Hom}_{k-gr}(\mathbf{G}_{m,k}, G_k)$$

où $W(k) = N_{G(k)}(T_k)/Z_{G(k)}(T_k)$ est le groupe de Weyl.

Démonstration. L'application est surjective car deux tores déployés maximaux sont nécessairement conjugués. Elle est injective : si $\mu, \mu' : \mathbf{G}_{m,k} \hookrightarrow T$ sont conjugués dans G_k, i.e. il existe $g \in G(k)$ tel que $\mu = \mathrm{Int}(g) \circ \mu'$. Alors μ est à valeur dans $T \cap \mathrm{Int}(g)(T)$, donc μ commute à T et $\mathrm{Int}(g)(T)$, i.e. T et $\mathrm{Int}(g)(T)$ sont deux tores maximaux dans le centralisateur $Z_\mu(G_k)$ de μ dans G_k, qui est un groupe connexe réductif, donc ils sont conjugués aussi par un élément $h \in Z_\mu(G_k)(k)$. On a donc

$$\mathrm{Int}(h) \circ \mu = \mu = \mathrm{Int}(h) \circ \mathrm{Int}(g) \circ \mu' = \mathrm{Int}(hg) \circ \mu'$$

avec maintenant $\mathrm{Int}(hg)(T) = T$, i.e. $hg \in N_{G(k)}(T_k)$, CQFD. □

On en déduit que $\mu(G, \mathcal{X}) \in \mathcal{C}(E)$ pour un corps de nombre $E \subset \mathbf{C}$ suffisamment gros.

Definition 7.2. Le corps reflex $E(G, \mathcal{X}) \subset \mathbf{C}$ est le corps de définition de $\mu(G, \mathcal{X}) \in \mathcal{C}(\overline{\mathbf{Q}})$.

Lemma 7.3. *Si $(H, \mathcal{Y}) \subset (G, \mathcal{X})$, alors $E(H, \mathcal{Y}) \supset E(G, \mathcal{X})$.*

Démonstration. Immédiat. □

7.2. **Les points spéciaux.**

Definition 7.4. Un point $h \in \mathcal{X}$ est dit spécial si et seulement si il existe un $\mathbf{Q}$-tore $T \subset G$ tel que $h : \mathbf{S} \hookrightarrow G_{\mathbf{R}}$ se factorise par $T_{\mathbf{R}}$. Un point $x \in \mathrm{Sh}_K(G, \mathcal{X})(\mathbf{C})$ est dit spécial si et seulement si il existe un élément $g \in G(\mathbf{A}_f)$ et un point spécial h de $\mathcal{X}$ tel que

$$x = [g, h] \in G(\mathbf{Q})\backslash \left(G(\mathbf{A}_f)/K \times \mathcal{X}\right) = \mathrm{Sh}_K(G, \mathcal{X})(\mathbf{C}).$$

Remark 7.5. Si T est un $\mathbf{Q}$-tore *maximal* (ce que l'on peut toujours supposer dans la définition ci-dessus), pour que $h \in \mathcal{X}$ se factorise par $T_{\mathbf{R}}$, il faut et il suffit que $h(\mathbf{C}^\times)$ et $T(\mathbf{R})$ commutent. En effet, h se factorise alors par le centralisateur $Z_{G_{\mathbf{R}}}(T_{\mathbf{R}}) = T_{\mathbf{R}}$ de $T_{\mathbf{R}}$ dans $G_{\mathbf{R}}$.

Remark 7.6. Pour tout $h \in \mathcal{X}$, le groupe de Mumford-Tate $\mathbf{MT}(h)$ de h est le plus petit sous-groupe H de G qui est défini sur $\mathbf{Q}$ et tel que $h : \mathbf{S} \to G_{\mathbf{R}}$ se factorise par $H_{\mathbf{R}}$. Presque par définition, $h \in \mathcal{X}$ est spécial si et seulement si $\mathbf{MT}(h) \subset G$ est un tore.

Soit h un point spécial de $\mathcal{X}$ et $T \subset G$ un $\mathbf{Q}$-tore tel que $h : \mathbf{S} \to G_{\mathbf{R}}$ se factorise par $T_{\mathbf{R}}$. Alors $(T, \{h\})$ est une sous-donnée de Shimura de $(G, \mathcal{X})$. Le corps reflex de $(T, \{h\})$ est le corps de définition du cocaractère $\mu_h : \mathbf{G}_{m,\mathbf{C}} \to T_{\mathbf{C}} \hookrightarrow G_{\mathbf{C}}$: il ne dépend pas du choix de T, mais seulement de $h \in \mathcal{X}$. On le note $E(h)$. Puisque pour tout corps $k \subset \overline{\mathbf{Q}}$,

$$\begin{aligned}
\mathrm{Hom}_{k-gr}\left(\mathbf{G}_{m,k}, T_{/k}\right) &= \mathrm{Hom}_{\mathbf{Z}[\mathrm{Gal}_k]}\left(X^\star(T), X^\star(\mathbf{G}_{m,k})\right) \\
&= \mathrm{Hom}_{\mathbf{Z}[\mathrm{Gal}_{\mathbf{Q}}]}\left(X^\star(T), \mathrm{Ind}_{\mathrm{Gal}_k}^{\mathrm{Gal}_{\mathbf{Q}}} X^\star(\mathbf{G}_{m,\mathbf{Q}})\right) \\
&= \mathrm{Hom}_{\mathbf{Z}[\mathrm{Gal}_{\mathbf{Q}}]}\left(X^\star(T), X^\star(T_k)\right) \\
&= \mathrm{Hom}_{\mathbf{Q}-gr}\left(T_k, T\right)
\end{aligned}$$

le cocaractère $\mu_h : \mathbf{G}_{m,E(h)} \to T_{/E(h)}$ induit à son tour un morphisme de $\mathbf{Q}$-tores

$$r_h : T_{E(h)} = \mathrm{Res}_{E(h)/\mathbf{Q}}\mathbf{G}_{m,E(h)} \to T.$$

On obtient ainsi un morphisme

$$r_h : T_{E(h)}(\mathbf{A}) \to T(\mathbf{A}) \xrightarrow{\text{proj}} T(\mathbf{A}_f) \hookrightarrow G(\mathbf{A}_f)$$

qui ne dépend à nouveau pas du choix de T.

7.3. **Le modèle canonique.**

Definition 7.7. Soit $(G, \mathcal{X})$ une donnée de Shimura et K un sous-groupe ouvert et compact de $G(\mathbf{A}_f)$.

(1) Un modèle M_K de $\mathrm{Sh}_K(G, \mathcal{X})$ sur $E(G, \mathcal{X})$ est dit canonique si et seulement si il vérifie la propriété suivante : pour tout point spécial h de $\mathcal{X}$ et tout $g \in G(\mathbf{A}_f)$, le point $[g, h]$ de $M_K(\mathbf{C})$ est défini sur l'extension abélienne maximale $E(h)^{ab}$ de $E(h) \supset E(G, \mathcal{X})$ dans $\mathbf{C}$, et pour tout $\sigma \in \mathrm{Aut}(\mathbf{C}/E(h))$, pour tout $s \in T_{E(h)}(\mathbf{A})$ tel que $\sigma|E(h)^{ab} = \mathrm{Art}_{E(h)}(s)$,
$$\sigma \cdot [g, h] = [r_x(s)g, h] \quad \text{dans } \mathrm{Sh}_K(G, \mathcal{X})(\mathbf{C}).$$

(2) Un modèle de $\mathrm{Sh}(G, \mathcal{X})$ est un système projectif de modèles canoniques $(\mathrm{Sh}_K(G, \mathcal{X}))_K$ sur $E(G, \mathcal{X})$, indexé par les sous-groupes ouverts et compacts (suffisamment petits) K de $G(\mathbf{A}_f)$, muni d'une action à droite de $G(\mathbf{A}_f)$ qui induit celle que l'on a déjà sur $(\mathrm{Sh}_K(G, \mathcal{X})(\mathbf{C}))_K$.

Cette définition peut paraître bien singulière. Nous verrons plus bas pourquoi elle est au contraire tout à fait naturelle : la loi de réciprocité qui exprime l'action de Galois sur les points spéciaux est, tout au moins pour les variétés de Shimura de type PEL, rien d'autre qu'un avatar du théorème principal de la multiplication complexe.

7.4. **Unicité des modèles canoniques.** On veut montrer que

Theorem 7.8. *Si $\mathrm{Sh}_K(G, \mathcal{X})$ a un modèle canonique, celui-ci est unique à isomorphisme unique près.*

Démonstration. On applique le théorème suivant avec $K = K'$ et $\sigma = 1$. □

Theorem 7.9. *Soit $\mathcal{T}(n) : \mathrm{Sh}_K(G, \mathcal{X}) \to \mathrm{Sh}_{K'}(G, \mathcal{X})$ un morphisme $[g, h] \mapsto [gn, h]$ avec donc $n \in G(\mathbf{A}_f)$, pour des sous-groupes ouverts et compacts K et K' de $G(\mathbf{A}_f)$ tels que $n^{-1}Kn \subset K'$. Si $\mathrm{Sh}_K(G, \mathcal{X})$ et $\mathrm{Sh}_{K'}(G, \mathcal{X})$, ont un modèle canonique, alors $\mathcal{T}(n)$ est défini sur $E(G, \mathcal{X})$.*

Démonstration. Il suffit de voir que $\sigma(\mathcal{T}(n)) = \mathcal{T}(n)$ pour tout $\sigma \in \mathrm{Aut}(\mathbf{C}/E(G, \mathcal{X}))$ (par descente fpqc des morphismes), ou encore que
$$\sigma \cdot \mathcal{T}(n)(x) = \mathcal{T}(n)(\sigma \cdot x)$$
pour un ensemble Zariski dense de points $x \in \mathrm{Sh}_K(G, \mathcal{X})(\mathbf{C})$. Si $x = [g, h]$ pour un point spécial $h \in \mathcal{X}$ de corps réflexe $E(h) \supset E(G, \mathcal{X})$ et σ fixe $E(h)$, alors pour tout $s \in T_{E(x)}(\mathbf{A})$ tel que $\sigma|E(h)^{ab} = \mathrm{Art}_{E(h)}(s) \in \mathrm{Gal}_{E(h)}^{ab}$, on a
$$\sigma \cdot \mathcal{T}(n)([g, h]) = \sigma \cdot [gn, h] = [r_h(s)gn, h] = \mathcal{T}(n)[r_h(s)g, h] = \mathcal{T}(n)(\sigma \cdot [g, h]).$$
Le théorème résulte donc des deux lemmes suivants. □

Lemma 7.10. *Pour tout $h \in \mathcal{X}$, $[G(\mathbf{A}_f), h]$ est Zariski dense dans $\mathrm{Sh}_K(G, \mathcal{X})(\mathbf{C})$.*

Démonstration. Exercice. □

Lemma 7.11. (1) *Il existe un point spécial* $h \in \mathcal{X}$*, et* (2) $\mathrm{Gal}(\overline{\mathbf{Q}}/E(G,\mathcal{X}))$ *est engendré par les* $\mathrm{Gal}(\overline{\mathbf{Q}}/E(h))$ *pour* $h \in \mathcal{X}$ *spécial.*

Démonstration. (1) On part d'un point $h \in \mathcal{X}$, on choisit un tore maximal $T \subset G_{\mathbf{R}}$ à travers lequel h se factorise. Alors T est le centralisateur de tout point régulier $t \in \mathrm{Lie}T(\mathbf{R})$. Mais si $t_0 \in \mathrm{Lie}G(\mathbf{Q})$ est suffisamment proche de $t \in \mathrm{Lie}G(\mathbf{R}) = \mathrm{Lie}G(\mathbf{Q}) \otimes \mathbf{R}$, alors t_0 est encore régulier, donc son centralisateur T_0 est encore un tore maximal dans G, qui est maintenant défini sur $\mathbf{Q}$. Tous les tores maximaux de $G_{\mathbf{R}}$ ne sont malheureusement pas conjugués, mais il n'y a qu'un nombre fini de classes de conjugaisons - et si t_0 est suffisamment proche de t, alors $T_{0\mathbf{R}} = gTg^{-1}$ pour un $g \in G(\mathbf{R})$. Alors $ghg^{-1} = g \cdot h$ se factorise par T_0 : c'est donc un point spécial de $\mathcal{X}$. (2) Voir la version originale de [1, 5.1]. □

Remark 7.12. On montre de même que si tous les $\mathrm{Sh}_K(G,\mathcal{X})$ ont un modèle canonique, alors $\mathrm{Sh}(G,\mathcal{X})$ en a un aussi (i.e. les applications de transitions et l'action de $G(\mathbf{A}_f)$ sont données par des morphismes algébriques définis sur le corps reflex $E(G,\mathcal{X})$.

Remark 7.13. On montre encore de même que les modèles canoniques sont fonctoriels en la donnée de Shimura : si $\iota : (G,\mathcal{X}) \to (G',\mathcal{X}')$ est un morphisme de données de Shimura, si $\iota(K) \subset K'$ sont des sous-groupes ouverts et compacts de $G(\mathbf{A}_f)$ et de $G'(\mathbf{A}_f)$, et si $\mathrm{Sh}_K(G,\mathcal{X})$ et $\mathrm{Sh}_{K'}(G',\mathcal{X}')$ ont des modèles canoniques, alors $\iota : \mathrm{Sh}_K(G,\mathcal{X}) \to \mathrm{Sh}_K(G',\mathcal{X}')$ est défini sur $E(G,\mathcal{X}) \cdot E(G',\mathcal{X}')$.

7.5. **Existence des modèles canoniques.** Il s'agit d'un problème de descente fpqc, le long de $S = \mathrm{Spec}\mathbf{C} \to S_0 = \mathrm{Spec}E$ où $E = E(G,\mathcal{X})$. Dans ce contexte, une donnée de descente sur un $\mathrm{Spec}\mathbf{C}$-schéma X est - comme d'habitude - un isomorphisme $p_1^\star X \simeq p_2^\star X$ de S'-schémas vérifiant une condition de cocycle, où $p_1, p_2 : S' = S \times_{S_0} S \to S$ sont les deux projections, et une telle donnée de descente est effective lorsque X est quasi-projectif. Malheureusement, le schéma $S' = \mathrm{Spec}\mathbf{C} \otimes_E \mathbf{C}$ est nettement plus compliqué qu'il n'en a l'air. Cependant tout élément $\sigma \in \mathrm{Aut}(\mathbf{C}/E)$ définit un morphisme $\mathbf{C}\otimes_E\mathbf{C} \to \mathbf{C}$ donné par $x\otimes y \mapsto \sigma(x)y$, donc un morphisme $(\sigma, 1) : \mathrm{Spec}(\mathbf{C}) \to S'$. En faisant le pull-back de notre isomorphisme $p_1^\star X \simeq p_2^\star X$, par $(\sigma, 1)$, on obtient un isomorphisme $f_\sigma : \sigma X \simeq X$. La condition de cocycle implique alors que $f_{\sigma\tau} = f_\sigma \circ \sigma(f_\tau) : \sigma\tau X \to \sigma X \to X$, et la collection de ces isomorphismes est presque aussi bonne que la donnée de descente elle-même : Milne décrit dans [4] une condition suffisante, dite de continuité, pour qu'une telle (variante de) donnée de descente sur un schéma quasi-projectif X sur $\mathbf{C}$ soit effective. Si de plus X est lisse, on peut encore décrire les f_σ au moyen de l'action qu'ils induisent sur $X(\mathbf{C})$: $\sigma \cdot x = f_\sigma(\sigma x)$. Une action de $\mathrm{Aut}(\mathbf{C}/E)$ sur l'ensemble $X(\mathbf{C})$ est dite régulière si elle provient de tels morphismes f_σ. Au final, une action *régulière* et *continue* sur $X(\mathbf{C})$ est donc effective si X est quasi-projectif et lisse.

D'après l'unicité des modèles canoniques, il existe au plus une donnée de descente canonique sur $\mathrm{Sh}_K(G,\mathcal{X})(\mathbf{C})$, c'est-à-dire au plus une action régulière et continue telle que $\sigma \cdot [g,h] = [r_h(s)g, h]$ pour tout $g \in G(\mathbf{A}_f)$, tout $h \in \mathcal{X}$ spécial, tout $\sigma \in \mathrm{Aut}(\mathbf{C}/E(h))$ et tout $s \in T_{E(h)}(\mathbf{A})$ tel que $\mathrm{Art}_{E(h)}(s) = \sigma|E(h)^{ab}$. Il reste à *construire* une telle action de $\mathrm{Aut}(\mathbf{C}/E)$ sur $\mathrm{Sh}_K(G,\mathcal{X})$, et à *vérifier* qu'elle est bien *régulière* et *continue.*

Lorsque les points de $\mathrm{Sh}_K(G,\mathcal{X})(\mathbf{C})$ classifient des objets algébriques sur $\mathbf{C}$, comme c'est le cas pour les variétés de type PEL, l'action de $\mathrm{Aut}(\mathbf{C}/E)$ sur les objets classifiés fournit déjà une action de $\mathrm{Aut}(\mathbf{C}/E)$ sur $\mathrm{Sh}_K(G,\mathcal{X})(\mathbf{C})$ et Milne vérifie dans [4, §14] que cette action est bien régulière et continue. Nous n'avons pas besoin de vérifier cela pour les variétés qui nous intéressent : nous savons déjà que cette action est une donnée de descente effective, puisque c'est celle qui provient du modèle que nous avons construit dans le début du cours. En revanche, et comme Milne, nous devons vérifier que notre modèle est bien *canonique*, ce que l'on fait dans la section suivante.

Remark 7.14. La démonstration de l'existence des modèles canoniques pour toutes les variétés de Shimura est beaucoup plus fastidieuse, et les dernières ramifications de la preuve ne datent que d'une dizaine d'année.

8. Le cas des Variétés de Shimura de Type PEL

Soient B une $\mathbf{Q}$-algèbre semi-simple, $\star$ une involution positive de B, $(V,\psi) \in \mathcal{H}_{\mathbf{Q}}(B,\star,-1)$ un espace $(B,\star)$-symplectique, I une structure complexe $(B,\star)$ linéaire sur $(V_{\mathbf{R}},\psi_{\mathbf{R}})$ telle que $\psi_{\mathbf{R},I} > 0$, G le groupe des similitudes symplectiques B-linéaire de (V,ψ), $\mathcal{X}$ la classe de $G(\mathbf{R})$-conjugaison du morphisme $h_I : \mathbf{S} \to G_{\mathbf{R}}$ donné par la structure complexe I, et K un sous-groupe compact ouvert de $G(\mathbf{A}_f)$. On s'intéresse à la variété de Shimura $\mathrm{Sh}_K(G,\mathcal{X})$.

8.1. **Les points complexes.** L'ensemble des points complexes

$$\mathrm{Sh}_K(G,\mathcal{X})(\mathbf{C}) = G(\mathbf{Q})\backslash\left(G(\mathbf{A}_f)/K \times \mathcal{X}\right)$$

paramètre les classes d'isomorphismes de quadruplets $(A,\iota,[\lambda],[\kappa])$ où

(1) A est une variété abélienne à isogénie près sur $\mathbf{C}$,
(2) $\iota : B \to \mathrm{End}^0(A)$ est une action de B telle que le $B\otimes\mathbf{C}$-module $\mathrm{Lie}(A)$ soit isomorphe à $V_{\mathbf{R},I}$,
(3) $[\lambda] = \mathbf{Q}\lambda$ où $\lambda : A \to A^t$ est une polarisation $(B,\star)$-linéaire,
(4) $[\kappa] = \kappa K$ est une K-orbite d'isomorphismes $\widehat{B}$-linéaires $\kappa : \widehat{V} \to V_f(A,\mathbf{C})$ tels qu'il existe un isomorphisme $\nu : \mathbf{A}_f \to V_f(\mu,\mathbf{C})$ qui fait commuter le diagramme

$$\begin{array}{cccc} \widehat{\psi} : & \widehat{V}\times\widehat{V} & \to & \mathbf{A}_f \\ & \kappa\downarrow & & \nu\downarrow \\ \langle\bullet,\bullet\rangle_f^\lambda : & V_f(A,\mathbf{C})\times V_f(A,\mathbf{C}) & \to & V_f(\mu,\mathbf{C}) \end{array}$$

(les isomorphismes sont alors automatiquement $\widehat{B}$-linéaires),

Le tout étant de plus assujetti à la condition suivante :

$$[V,\mathbf{Q}^\times\psi] = [H_1(A,\mathbf{Q}),\mathbf{Q}^\times\psi_\lambda] \quad \text{dans } \mathcal{H}_{\mathbf{Q}}(B,\star,-1). \tag{8.1}$$

i.e. les $(B,\star)$-modules symplectiques (V,ψ) et $(H_1(A,\mathbf{Q}),\psi_\lambda)$ sont isomorphes à une similitude près. En effet, soit $(A,\iota,[\lambda],[\kappa])$ un tel quadruplet. Choisissons un isomorphisme B-linéaire

$$\nu : H_1(A,\mathbf{Q}) \to V$$

qui envoie $\mathbf{Q}\psi_\lambda$ sur $\mathbf{Q}\psi$. Alors

$$\widehat{\nu}\circ\kappa : V\otimes\mathbf{A}_f = \widehat{V} \to V_f(A,\mathbf{C}) \simeq H_1(A,\mathbf{Q})\otimes\mathbf{A}_f \to V\otimes\mathbf{A}_f$$

est un élément $g \in G(\mathbf{A}_f)$ et $J = \nu_{\mathbf{R}} \circ [i] \circ \nu_{\mathbf{R}}^{-1} : V_{\mathbf{R}} \to V_{\mathbf{R}}$

$$J : V \otimes \mathbf{R} \to H_1(A, \mathbf{R}) \simeq \mathrm{Lie}(A)(\mathbf{C}) \xrightarrow{i} \mathrm{Lie}(A)(\mathbf{C}) \simeq H_1(A, \mathbf{R}) \to V \otimes \mathbf{R}$$

est une structure complexe $(B, \star)$-linéaire sur $(V_{\mathbf{R}}, \psi_{\mathbf{R}})$ telle que les $B \otimes \mathbf{C}$-modules $V_{\mathbf{R},I}$ et $W_{\mathbf{R},J}$ soient isomorphes, et $\pm\psi_{\mathbf{R},J} > 0$, donc J est conjugué à I par un élément de $G(\mathbf{R})$, i.e. $h_J \in \mathcal{X}$. Puisque κK et $G(\mathbf{Q})\nu$ sont bien déterminés, on obtient

$$[g, h_J] \in \mathrm{Sh}_K(G, \mathcal{X})(\mathbf{C}) = G(\mathbf{Q}) \backslash (G(\mathbf{A}_f)/K \times \mathcal{X}) .$$

Inversement, un tel élément détermine le quadruplet $[A, \iota, [\lambda], [\kappa]]$ où $A = V_{\mathbf{R},J}/\Lambda$, $\psi_\lambda = \pm\psi$, $\kappa = g$ et $\iota(b) \in \mathrm{End}^0(A) = \{\alpha \in \mathrm{End}_{\mathbf{Q}}(V) : \alpha_{\mathbf{R}} \circ J = J \circ \alpha_{\mathbf{R}}\}$ est la multiplication par b. Ici, Λ est un réseau quelconque de A sur lequel ψ est entier.

Remark 8.1. Si le groupe des similitudes de (V, ψ) vérifie le principe de Hasse, la condition (8.1) est superflue : la structure de niveau détermine la classe de similitude de $(H_1(A, \mathbf{Q}), \psi_\lambda) \otimes \mathbf{Q}_p$ pour tout nombre premier p, et la condition sur le déterminant détermine celle de $(H_1(A, \mathbf{Q}), \psi_\lambda) \otimes \mathbf{R}$.

8.2. **Le corps reflex.** Pour $h : \mathbf{S} \to G_{\mathbf{R}}$ dans $\mathcal{X}$, on note $\mu_h : \mathbf{G}_{m,\mathbf{C}} \to G_{\mathbf{C}}$ le cocaractère défini par

$$\mu_h : \mathbf{G}_{m,\mathbf{C}} \xrightarrow{i_1} \mathbf{G}_{m,\mathbf{C}} \times \mathbf{G}_{m,\mathbf{C}} \simeq \mathbf{S}_{\mathbf{C}} \xrightarrow{h_{\mathbf{C}}} G_{\mathbf{C}}.$$

Si $\iota : G \hookrightarrow GL_B(V)$ est l'inclusion naturelle, on obtient donc aussi

$$\iota h : \mathbf{S} \to GL_B(V)_{\mathbf{R}} \quad \text{et} \quad \iota\mu_h : \mathbf{G}_{m,\mathbf{C}} \to GL_B(V)_{\mathbf{C}}.$$

On note $V \otimes \mathbf{C} = V_h^{-1,0} \oplus V_h^{0,-1}$ la décomposition de Hodge associée à h. C'est une décomposition du $B \otimes \mathbf{C}$-module $V \otimes \mathbf{C}$ en somme directe de deux $B \otimes \mathbf{C}$-sous-modules échangés par la conjugaison. Le morphisme $h_{\mathbf{C}}$ envoie $(z_1, z_2) \in \mathbf{S}(\mathbf{C}) = \mathbf{C}^\times \times \mathbf{C}^\times$ sur l'isomorphisme $B \otimes \mathbf{C}$-linéaire $([z_1], [z_2])$ qui est la multiplication par z_1 sur $V_h^{-1,0}$ et la multiplication par z_2 sur $V_h^{0,-1}$. Le cocaractère μ_h envoie donc $z \in \mathbf{C}^\times$ sur $([z], [1])$ tandis que $(\tau\mu_h)$ envoit $z \in \mathbf{C}^\times$ sur $([1], [z])$. D'autre part, l'inclusion $V \otimes \mathbf{R} \hookrightarrow V \otimes \mathbf{C}$ induit un isomorphisme de $B \otimes \mathbf{R}$-module $V \otimes \mathbf{R} \simeq V \otimes \mathbf{C}/V_h^{0,-1}$, et cet isomorphisme envoie l'isomorphisme $B \otimes \mathbf{R}$-linéaire $h(i)$ de $V \otimes \mathbf{R}$ sur la multiplication par i. On peut donc voir cet isomorphisme comme un isomorphisme de $B \otimes \mathbf{C}$-module

$$V_{\mathbf{R},h(i)} \simeq V \otimes \mathbf{C}/V_h^{0,-1} \simeq V \otimes \mathbf{C}/(V \otimes \mathbf{C})^{\mu_h(\mathbf{C}^\times)}.$$

On définit trois corps reflex :

- E_{Shi} est le corps de définition de la classe de $G(\mathbf{C})$-conjugaison $\mathcal{C}(\mu_h)$,
- E_{Rep} est le corps de définition de la classe de $GL_B(V)(\mathbf{C})$-conjugaison $\mathcal{C}(\iota\mu_h)$,
- E_{Mod} est le corps de définition du déterminant $d(\mathcal{X}) : B \otimes \mathbf{C} \to \mathbf{C}$ de $V_{\mathbf{R},h(i)}$.

Lemma 8.2. *On a* $E_{Mod} \subset E_{Rep} \subset E_{Shi}$.

Démonstration. Soit $\sigma \in \mathrm{Aut}(\mathbf{C}/E_{Shi})$. Alors $\sigma\mu_h = \mathrm{Int}(g) \circ \mu_h$ pour un $g \in G(\mathbf{C})$, donc

$$\sigma(\iota \circ \mu_h) = \iota \circ (\sigma\mu_h) = \iota \circ \mathrm{Int}(g) \circ \mu_h = \mathrm{Int}(\iota(g)) \circ (\iota \circ \mu_h)$$

donc $\sigma\mathcal{C}(\iota\mu_h) = \mathcal{C}(\iota\mu_h)$, i.e. σ fixe E_{Rep} et $E_{Rep} \subset E_{Shi}$. Soit ensuite $\sigma \in \mathrm{Aut}(\mathbf{C}/E_{Rep})$. Alors $\sigma\mu_h = \mathrm{Int}(g) \circ \mu_h$ pour un $g \in GL_{B\otimes\mathbf{C}}(V \otimes \mathbf{C})$, i.e.

$$\forall z \in \mathbf{C}^\times : \qquad (Id_V \otimes \sigma) \circ \mu_h(\sigma^{-1}z) \circ (Id_V \otimes \sigma)^{-1} = g \circ \mu_h(z) \circ g^{-1} \text{ sur } V \otimes \mathbf{C}.$$

Alors $(Id_V \otimes \sigma)^{-1} \circ g : V \otimes \mathbf{C} \to V \otimes \mathbf{C}$ induit un isomorphisme $B \otimes \mathbf{C}$-linéaire

$$V \otimes \mathbf{C}/(V \otimes \mathbf{C})^{\mu_h(\mathbf{C}^\times)} \to \sigma^\star(V \otimes \mathbf{C}/(V \otimes \mathbf{C})^{\mu_h(\mathbf{C}^\times)})$$

où pour tout $B \otimes \mathbf{C}$-module W, $\sigma^\star W$ est le $B \otimes \mathbf{C}$-module dont le B-module sous-jacent est W, et où $\lambda \in \mathbf{C}$ agit par $\sigma^{-1}(\lambda)$. Donc $\sigma^\star(V_{\mathbf{R},h(i)}) \simeq V_{\mathbf{R},h(i)}$ comme $B \otimes \mathbf{C}$-module, donc $\sigma d(\mathcal{X}) = d(\mathcal{X})$, i.e. σ fixe E_{Mod}. □

Remark 8.3. On doit pouvoir montrer que $E_{Mod} = E_{Rep} = E_{Shi}$.

8.3. **Le problème de module.** On a définit un problème de module

$$M_K : (\mathbf{Sch}/E_{Mod})^0 \to \mathbf{Ens}$$

qui à un E_{Mod}-schéma S associe l'ensemble des classes d'isomorphismes de quadruplets $(A, \iota, [\lambda], [\kappa])$ où

(1) A est un S-schéma abélien à isogénie près,
(2) $\iota : B \to \mathrm{End}^0(A)$ est un action de B sur A, telle que le déterminant du $B \otimes \mathcal{O}_S$-module $\mathrm{Lie}(A)$ soit égal à $d(\mathcal{X})$.
(3) $[\lambda] = \mathbf{Q}\lambda$ où $\lambda : A \to A^t$ est une polarisation,
(4) $[\kappa]$ est la donnée, pour un point géométrique s dans chacune des composantes connexes de S, d'une K-orbite κK d'isomorphismes B-linéaires $\kappa : \widehat{V} \to V_f(A, s)$ tels qu'il existe un isomorphisme $\nu : \mathbf{A}_f \to V_f(\mu, s)$ qui fait commuter le diagramme

$$\begin{array}{lccc} \widehat{\psi} : & \widehat{V} \times \widehat{V} & \to & \mathbf{A}_f \\ & \kappa \downarrow & & \nu \downarrow \\ \langle \bullet, \bullet \rangle_f^\lambda : & V_f(A,s) \times V_f(A,s) & \to & V_f(\mu, s) \end{array}$$

Notons que l'on ne peut pas imposer la condition (8.1), qui n'a aucun sens dans ce contexte plus général. On a vu que ce problème de module était représentable par un E_{Mod}-schéma que l'on note encore M_K. Sur les $\mathbf{C}$-points, on obtient donc une inclusion

$$p : \mathrm{Sh}_K(G, \mathcal{X})(\mathbf{C}) \hookrightarrow M_K(\mathbf{C}).$$

Remark 8.4. Si le groupe des similitudes G de (V, ψ) vérifie le principe de Hasse, cette inclusion est une bijection. En général, $M_K(\mathbf{C})$ est la réunion d'un nombre fini de variétés de Shimura de même type, indexées par les classes de similitudes de couples $(V', \psi') \in \mathcal{H}_{\mathbf{Q}}(B, \star, -1)$ qui sont partout localement isomorphes (=similaires) à (V, ψ).

8.4. **Les points spéciaux.** Soit $x = [g, h]$ un point de $\mathrm{Sh}_K(G, \mathcal{X})(\mathbf{C})$ et $p(x) = [A, \iota, [\lambda], [\kappa]]$ le point correspondant de $M_K(\mathbf{C})$. Soit $\mathbf{MT}(x) \subset GL(V)$ le groupe de Mumford-Tate de h, i.e. le plus petit sous-groupe algébrique H défini sur $\mathbf{Q}$ de $GL(V)$ tel que $h : \mathbf{S} \hookrightarrow GL(V)_{\mathbf{R}}$ se factorise par $H_{\mathbf{R}}$. On a donc $\mathbf{MT}(x) \subset G$, et :

Lemma 8.5. *x est spécial $\iff$ $\mathbf{MT}(x)$ est un tore $\iff$ A est à multiplication complexe.*

Démonstration. La première équivalence est tautologique, la seconde a déjà été démontrée. □

On suppose dorénavant que c'est le cas. Alors

Lemma 8.6. *Il existe une sous-$\mathbf{Q}$-algèbre CM E de $\mathrm{End}^0(A)$ telle que (1) $\dim_{\mathbf{Q}} E = 2\dim A$ et (2) l'involution de Rosati $\star_\lambda$ induite par la polarisation λ stabilise E.*

Démonstration. Si $A \sim \oplus A_i^{n_i}$ avec A_i simples et deux à deux non-isogènes, alors $\mathrm{End}^0(A) = \prod M_{n_i}(E_i)$ où $E_i = \mathrm{End}^0 A_i$ est un corps CM. Puisque l'involution $\star_\lambda$ est positive, elle fixe chaque facteur simple $M_{n_i}(E_i)$ et induit sur celui-ci une involution positive du centre E_i - qui est donc l'involution canonique de E_i. On a vu qu'une telle involution (de seconde espèce de $M_{n_i}(E_i)$) était de la forme $\star_{\psi_i}$ pour une forme hermitienne (définie positive) sur $E_i^{n_i}$. Une telle forme est diagonalisable dans une base β_i de $E_i^{n_i}$, et le produit E des sous-algèbres $E_i^{n_i} \subset M_{n_i}(E_i)$ correspondant à ces choix de bases est la $\mathbf{Q}$-algèbre CM recherchée. □

On fixe une telle sous-algèbre CM, de sorte que A a maintenant aussi multiplication complexe par E, et V est un E-module libre de rang 1, T_E un sous-tore de $GL(V)$ défini sur $\mathbf{Q}$, et $h : \mathbf{S} \to GL(V)_{\mathbf{R}}$ se factorise par $T_{E,\mathbf{R}}$, donc $T \subset G \cap T_E \subset T_E$:

$$\begin{array}{ccc} T & \hookrightarrow & T_E \\ \cap & & \cap \\ G & \hookrightarrow & GL(V) \end{array}$$

On a $E(T,\{h\}) = E(T_E,\{h\}) = E(\Phi)$ où $\Phi \subset \mathrm{Hom}_{\mathbf{Q}-alg}(E,\mathbf{C})$ est le type CM sur E défini par h, de sorte que le $E \otimes \mathbf{C}$-module $V_{\mathbf{R},h(i)} \simeq \mathrm{Lie}A(\mathbf{C})$ est isomorphe à $\oplus_{\phi\in\Phi}\mathbf{C}(\phi)$.

Lemma 8.7. *Les morphismes $r_x : T_{E(\Phi)} \to T \hookrightarrow T_E$ et $N_\Phi : T_{E(\Phi)} \to T_E$ coincident.*

Démonstration. Il suffit de vérifier que les (σ,ϕ)-composantes des deux morphismes

$$r_x, N_\Phi : \left(T_{E(\Phi)}(\mathbf{C}) = \prod_{\sigma:E(\Phi)\to\mathbf{C}} \mathbf{C}^\times \right) \to \left(T_E(\mathbf{C}) = \prod_{\phi:E\to\mathbf{C}} \mathbf{C}^\times \right)$$

coïncident. En revenant aux définitions, on voit que

$$(r_x)_{\sigma,\phi} = (N_\Phi)_{\sigma,\phi} = \begin{cases} Id & \text{si } \phi \in \Phi, \\ 1 & \text{si } \phi \notin \Phi. \end{cases}$$

CQFD. □

Soit $\sigma \in \mathrm{Aut}(\mathbf{C}/E(x))$ et $s \in T_{E(\Phi)}(\mathbf{A}_f)$ tel que $\sigma|E(x)^{ab} = \mathrm{Art}_{E(\Phi)}(s)$. Soit $\alpha : A \to \sigma A$ l'unique E-isogénie telle que $\alpha(r_x(s)\cdot v) = \sigma v$ pour tout $v \in V_f(A,\mathbf{C})$, qui existe d'après le théorème principal de la multiplication complexe et le lemme précédent.

Lemma 8.8. *Avec ces notations, α est une B-isogénie, et*

$$\alpha^{-1}[\sigma\lambda] = [\lambda] \quad et \quad \alpha^{-1}[\sigma\kappa] = [r_x(s)\kappa].$$

Démonstration. Pour (1), il suffit de vérifier que $V_f(\alpha) : V_f(A,\mathbf{C}) \to V_f(\sigma A,\mathbf{C})$ est $\widehat{B}$-linéaire. Mais $\sigma : V_f(A,\mathbf{C}) \to V_f(\sigma A,\mathbf{C})$ l'est par définition de $\sigma\iota$, et $r_x(s) : V_f(A,\mathbf{C}) \to V_f(A,\mathbf{C})$ l'est aussi puisque $r_x(T_{E(\Phi)}) \subset G \subset GL_B(V)$, donc $V_f(\alpha) =$

$\sigma \circ r_x(s)^{-1}$ est $\widehat{B}$-linéaire. Pour (2), calculons la forme symplectique induite par la polarisation $\alpha^{-1}(\sigma\lambda) = \alpha^t \circ \sigma\lambda \circ \alpha$ sur $V_f(A, \mathbf{C})$:

$$\begin{aligned} \langle v, w \rangle_f^{\alpha^t \circ \sigma\lambda \circ \alpha} &= \langle \alpha(v), \alpha(w) \rangle_f^{\sigma\lambda} = \left\langle \sigma(r_x(s)^{-1}v), \sigma(r_x(s)^{-1}w) \right\rangle_f^{\sigma\lambda} \\ &= \chi_{cyc}(\sigma) \left\langle r_x(s)^{-1}v, r_x(s)^{-1}w \right\rangle_f^{\lambda} = c \, \langle v, w \rangle_f^{\lambda} \end{aligned}$$

où $c = \frac{\chi_{cyc}(\sigma)}{N_\Phi(s) \cdot N_\Phi(s)^\star} \in \mathbf{Q}_>^\times$, donc $\alpha^{-1}(\sigma\lambda) = c\lambda$ et $\alpha^{-1}[\sigma\lambda] = [\lambda]$. Pour (3), choisissons $\kappa : \widehat{V} \to V_f(A, \mathbf{C}) \in [\kappa] = \kappa K$. Alors $\alpha^{-1} \circ \sigma \circ \kappa = r_x(s) \cdot \kappa$ donc $\alpha^{-1}[\kappa] = [r_x(s) \cdot \kappa]$. □

Corollary 8.9. *Pour tout point spécial* $x = [g, h] \in \mathrm{Sh}_K(G, \mathcal{X})(\mathbf{C})$*, pour tout* $\sigma \in \mathrm{Aut}(\mathbf{C}/E(x))$ *et* $s \in T_{E(x)}(\mathbf{A})$ *tel que* $\mathrm{Art}_{E(x)}(s) = \sigma|E(x)^{ab}$*,*

$$\sigma p([g, h]) = p([r_x(s)g, h]) \quad \textit{dans } M_K(\mathbf{C})$$

Démonstration. Le lemme précédent montre que

$$\sigma[A, \iota, [\lambda], [\kappa]] = [A, \iota, [\lambda], [r_x(s)\kappa]] \quad \text{dans } M_K(\mathbf{C}).$$

On conclut aisément en revenant à la définition de p. □

8.5. **Modèle canonique, I.** Si l'on admet le théorème de Bailly-Borel, qui nous dit que $\mathrm{Sh}_K(G, \mathcal{X})$ existe en tant que variété algébrique sur $\mathbf{C}$, on peut utiliser le corollaire ci-dessus pour construire le modèle canonique de cette variété, i.e. pour construire la donnée de descente (continue, régulière) canonique sur $\mathrm{Sh}_K(G, \mathcal{X})(\mathbf{C})$. On procède comme suit.

Le groupe $\mathrm{Aut}(\mathbf{C})$ agit sur les quadruplets $(A, \iota, [\lambda], [\kappa])$ qui sont classifiés par nos variétés de Shimura. La condition sur le déterminant est préservée par $\mathrm{Aut}(\mathbf{C}/E_{Mod})$, mais il n'est pas clair (pour moi) que la condition (8.1) l'est aussi. On relâche donc d'abord cette condition, ce qui nous donne une action du groupe $\mathrm{Aut}(\mathbf{C}/E_{Mod})$ sur les $\mathbf{C}$-points d'une réunion de variétés de Shimura (qui n'est autre que l'action naturelle de $\mathrm{Aut}(\mathbf{C}/E_{Mod})$ sur $M_K(\mathbf{C})$). On montre comme Milne dans [4, §14] que cette "donnée de descente" est continue et régulière, dans le sens de [4, §14]. Du corollaire, on déduit dans un premier temps que pour tout point spécial h de $\mathcal{X}$, le sous-groupe $\mathrm{Aut}(\mathbf{C}/E(x))$ de $\mathrm{Aut}(\mathbf{C}/E_{Mod})$ stabilise le sous-ensemble Zariski dense $[G(\mathbf{A}_f), h]$ de $\mathrm{Sh}_K(G, \mathcal{X})(\mathbf{C})$. Ce sous-groupe stabilise donc tout $\mathrm{Sh}_K(G, \mathcal{X})(\mathbf{C})$. D'après le lemme 7.11, on obtient alors une action (régulière et continue) de $\mathrm{Aut}(\mathbf{C}/E_{Shi})$ sur $\mathrm{Sh}_K(G, \mathcal{X})(\mathbf{C})$, et le corollaire montre exactement que cette donnée de descente est canonique.

8.6. **Modèle canonique, II.** On peut aussi ne vouloir rien admettre du tout, et essayer de montrer directement que M_K *est* le modèle canonique recherché (de notre réunion de variétés de Shimura). Le corollaire nous dit en effet que l'action naturelle de $\mathrm{Aut}(\mathbf{C}/E_{Mod})$ sur $M_K(\mathbf{C})$ donne bien ce qu'il faut sur les points spéciaux. Mais alors, que s'agit-il de démontrer ? Essentiellement ceci : que pour K suffisamment petit, le E_{Mod}-schéma M_K est *lisse*.

Dans ce cas : (1) une extension convenable de l'équivalence de catégorie entre (variétés abéliennes sur $\mathbf{C}$) et (tores complexes polarisables) en une équivalence de catégorie entre (schémas abéliens sur une base S lisse sur $\mathbf{C}$) et (objets analytiques complexes analogues sur $S(\mathbf{C})^{an})$[2] permet de montrer que le morphisme

$$p : \mathrm{Sh}_K(G, \mathcal{X})(\mathbf{C}) \to M_K(\mathbf{C})$$

est compatible avec les structures analytiques complexes. En particulier, il identifie $\mathrm{Sh}_K(G, \mathcal{X})(\mathbf{C})$ à une réunion de composantes connexes de $M_K(\mathbf{C})$. Puis : (2) le théorème de Borel montre alors que ce morphisme est aussi compatible avec les structures algébriques sur $\mathbf{C}$.

8.7. **Autour de la lissité de M_K.** Elle peut se vérifier directement sur le problème de module - comme il résulte de la définition Grothendieckienne de la lissité :

Definition 8.10. [3, IV, 17.1.1] Un morphisme localement de présentation finie $f : X \to S$ est lisse si et seulement si il est formellement lisse, i.e. pour tout anneau R, et tout idéal nilpotent I de R (ou même seulement pour tout idéal I de R tel que $I^2 = 0$), l'application $X(R) \to X(R/I)$ est *surjective*.

La vérification de ce critère est alors un problème de *déformation* : si A_0 est une variété abélienne sur R/I (avec des structures telles que polarisation, endomorphismes, structures de niveaux...), peut-on la relever en une variété abélienne sur R (avec ses structures) ? On peut d'ailleurs prolonger ce point de vue : pour un morphisme $f : X \to S$ localement de type fini (avec S noethérien), la propriété pour f d'être lisse en un point x est une propriété du morphisme entre les anneaux locaux complétés $\widehat{\mathcal{O}}_{S,f(x)} \to \widehat{\mathcal{O}}_{X,x}$. Si par exemple $f(x)$ et x ont le même corps résiduel k, il faut que $\widehat{\mathcal{O}}_{X,x} \simeq \widehat{\mathcal{O}}_{S,f(x)}[[T_1, \cdots, T_n]]$, cf. [3, 17.5.3]. Or si X représente $\mathcal{F} = \mathrm{Hom}_S(\bullet, X)$, on peut calculer le $\widehat{\mathcal{O}}_{S,f(x)}$-anneau local complété $\widehat{\mathcal{O}}_{X,x}$ comme l'anneau qui pro-représente le foncteur $\mathcal{F}_x(R) = \{z \in \mathcal{F}(R) : z \bmod m_R = x \in \mathcal{F}(k(x))\}$, foncteur qui est défini sur la catégorie des $\mathcal{O}_{S,f(x)}$-algèbres artiniennes locales R de corps résiduel $R/m_R \simeq k$. Les anneaux locaux complétés de nos schémas de modules sont donc les *anneaux de déformation universels* des objets classifiés.

Remark 8.11. Ce point de vue est surtout utile lorsqu'il s'agit d'étudier les anneaux locaux des problèmes de modules sur des anneaux d'entiers, en un point d'une fibre fermée (= spéciale). Si la caractéristique du corps résiduel k est p, la théorie de Serre-Tate ramène l'étude des déformations de variétés abéliennes A sur k à celle des déformations du groupe p-divisible $A(p^\infty)$. Pour ces derniers, on dispose de tout un éventail d'outils (groupes formels, modules de Dieudonné, théorie de Fontaine-Messing...) dont nous ne parlerons pas. C'est ainsi que l'on arrive finalement parfois à démontrer que ces anneaux locaux sont, par exemple, réguliers.

Références

[1] P. Deligne. *Travaux de Shimura.*

[2] P. Deligne, *Variétés de Shimura : interprétation modulaire et techniques de construction de modèles canoniques*, in Automorphic Forms, representations and L-functions (alias **Corvallis**). Proc. Symp. Pure Math. ,XXXIII, Amer. Math. Soc. Providence RI.

[3] J. Dieudonné et A. Grothendieck, *Eléments de Géométrie Algébrique.* Publications Scientifiques de l'IHES n°**4**, **8**, **11**, **17**, **20**, **24**, **28**, **32.**

[4] J. Milne, *Shimura Varieties.*

[2]Dans ce contexte, la notion pertinente est celle de *variations de structures de Hodge*, cf. [4, §2 et Theorem 14.8].

[5] V. Platonov et A. Rapinchuk, *Algebraic Groups and Number Theory*, Vol **139**, de Pure and Applied Mathematcis, Academic Press.

POINTS DES VARIÉTÉS DE SHIMURA SUR LES CORPS FINIS

Le but de cette dernière partie du cours est de donner les outils qui permettent d'étudier, et notamment de dénombrer l'ensemble des points d'une variété de Shimura de type PEL sur un corps fini. L'idée est très basique : (1) on regroupe les points en classe d'isogénie, puis (2) on étudie séparément chaque classe d'isogénie.

Première partie 1. La théorie de Honda-Tate

Soit k un corps parfait. On a vu précédemment que la catégorie $\mathbf{Ab}_k^0$ des variétés abéliennes sur k à isogénie près était abélienne semi-simple, et que les anneaux d'endomorphismes y sont des $\mathbf{Q}$-algèbres semi-simples de dimension finie. On a donc

$$\mathbf{Ab}_k^0 \simeq \oplus_{[A]\in\mathcal{S}} \mathbf{Mod}_{\mathrm{End}_k^0(A)}$$

où $\mathcal{S}$ est l'ensemble des classes d'isomorphismes de variétés abéliennes simples sur k, et où $\mathrm{Mod}_{\mathrm{End}_k^0(A)}$ est la catégorie des modules à gauche sur le corps gauche $\mathrm{End}_k^0(A)$. Lorsque k est un *corps fini*, la théorie de Honda-Tate achève de décrire complètement cette catégorie, en ce sens qu'elle donne une description explicite de l'ensemble $\mathcal{S}$ et une recette pour déterminer le corps gauche $\mathrm{End}_k^0(A)$ pour tout $[A] \in \mathcal{S}$.

1. Le Frobénius

1.1. Rappels sur les polynômes caractéristiques. Soit A une variété abélienne sur un corps parfait k. Nous avons vu que la fonction $\alpha \in \mathrm{End}_k(A) \mapsto \deg(\alpha) \in \mathbf{Z}$ est polynomiale (c'est la partie difficile), multiplicative et homogène de degré $2\dim A$. Pour tout anneau commutatif R, on obtient donc une fonction

$$\deg_R : \mathrm{End}_k(A) \otimes R \to R.$$

Pour $R = \mathbf{Q}_\ell$ (ou $\mathbf{Z}_\ell$), on note simplement $\deg_\ell$ cette fonction.

Proposition 1. *Soit $\ell \neq \mathrm{car} k$ un nombre premier. Alors*

$$\forall \alpha \in \mathrm{End}_k^0(A) \otimes \mathbf{Q}_\ell : \qquad \deg_\ell(\alpha) = \det_{\mathbf{Q}_\ell}\left(\alpha | V_\ell(A, \overline{k})\right) \text{ dans } \mathbf{Q}_\ell.$$

Démonstration. Décomposons la $\mathbf{Q}_\ell$-algèbre semi-simple $E = \mathrm{End}_k^0(A) \otimes \mathbf{Q}_\ell$ en produit $E = \prod E_i$ de $\mathbf{Q}_\ell$-algèbres simples. Soit $N_i : E_i \to \mathbf{Q}_\ell$ la norme réduite. Puisque les deux fonctions $\deg_\ell$ et $\det_\ell = \det_{\mathbf{Q}_\ell}(\star | V_\ell(A, \overline{k}))$ sont polynomiales et multiplicatives, il existe des entiers $a_i, b_i \in \mathbf{N}$ tels que pour tout $\alpha = (\alpha_i) \in E = \prod E_i$,

$$\deg_\ell(\alpha) = \prod N_i(\alpha_i)^{a_i} \quad \text{et} \quad \det_\ell(\alpha) = \prod N_i(\alpha_i)^{b_i},$$

cf. [3, Lemme p.179]. On sait certes aussi que $\deg_\ell$ et $\det_\ell$ sont homogènes de même degré $2\dim A$, ce qui fournit une équation $\sum a_i d_i = \sum b_i d_i$ où d_i est le degré de N_i, mais ça ne suffit pas pour conclure. En revanche, on voit facilement qu'il suffit maintenant de montrer que pour tout $\alpha \in E$, $\deg_\ell(\alpha)$ et $\det_\ell(\alpha)$ ont la même *valuation*. Par homogénéité et continuité, il suffit de le vérifier pour $\alpha \in \mathrm{End}_k(A)$.

Si α n'est pas une isogénie, $\deg_\ell(\alpha) = 0 = \det_\ell(\alpha)$. Si α est une isogénie, on conclut grâce aux formules

$$\ell^{v_\ell(\det_\ell \alpha)} = \left|T_\ell(A,\overline{k})/\alpha T_\ell(A,\overline{k})\right| = \left|\ker(\alpha)(\overline{k})[\ell^\infty]\right| = \ell^{v_\ell(\deg_\ell \alpha)}$$

où l'égalité centrale provient de l'exercice suivant. □

Exercise 2. Si $\alpha : A \to B$ est une isogénie, le conoyau de $\alpha : T_\ell(A,\overline{k}) \to T_\ell(B,\overline{k})$ est canoniquement isomorphe au ℓ-sylow $\ker(\alpha)(\overline{k})[\ell^\infty]$ de $\ker\alpha(s)$.

Definition 3. Le polynôme caractéristique de $\alpha \in \mathrm{End}_k(A) \otimes R$ est

$$P_\alpha(X) = \deg(\alpha \otimes 1_E - Id_A \otimes X) \in R[X].$$

Pour $\alpha \in \mathrm{End}_k^0(A)$, $P_\alpha \in \mathbf{Q}[X]$ est donc aussi le polynôme caractéristique de α agissant sur $V_\ell(A,\overline{k})$. En particulier, c'est un polynôme unitaire de degré $2\dim A$, et qui annule α (il annule l'action de α sur $V_\ell(A,\overline{k})$ par Cayley-Hamilton, donc il annule α par fidélité de V_ℓ). Pour $\alpha \in \mathrm{End}_k(X)$, $P_\alpha \in \mathbf{Z}[X]$ est caractérisé par $P_\alpha(n) = \deg(\alpha - n)$ pour tout $n \in \mathbf{Z}$. En particulier, $P_\alpha(\mathbf{Z}) \subset \mathbf{N}$.

Remark 4. On peut associer d'autres polynômes à un élément $\alpha \in E = \mathrm{End}_k^0(A)$: le polynôme minimal $P_{Min,\alpha}$ de α, le polynôme caractéristique $P_{Car,\alpha}$ de α agissant sur E par multiplication à gauche ou à droite, le polynôme $P_{Red,\alpha} = N_{E/\mathbf{Q}}(\alpha - X)$ où $N_{E/\mathbf{Q}}$ est la norme réduite de $E/\mathbf{Q}$. Pour les comparer, on décompose $A \sim \oplus A_i^{m_i}$ en composantes isotypiques, donc $E = \prod E_i$ en composantes simples, avec $E_i = M_{m_i}(D_i)$ où $D_i = \mathrm{End}_k^0(A_i)$ est un corps gauche, et $\alpha = (\alpha_i)$. On a alors

$$P_\alpha = \prod P_{\alpha_i} \quad P_{Min,\alpha} = \mathrm{pgcd}(P_{Min,\alpha_i}) \quad P_{Car,\alpha} = \prod P_{Car,\alpha_i} \quad \text{et} \quad P_{Red,\alpha} = \prod P_{Red,\alpha_i}$$

ce qui nous ramène au cas isotypique, i.e. $A \sim A_0^m$ et $E = M_m(D)$ où D est un corps gauche de centre F. Puisque les applications $\deg\alpha$, $\det(\alpha|E)$ et $N_{E/\mathbf{Q}}(\alpha)$ sont polynomiales, multiplicatives et homogènes de degré respectivement égal à $2mg_0$, m^2d^2f et mdf où $g_0 = \dim A_0$, $d = [D : F]$ et $f = [F : \mathbf{Q}]$, on en déduit (comme dans la preuve de la proposition) que $df \mid 2g_0$ et

$$\deg = N_{E/\mathbf{Q}}^{2g_0/df} \quad \text{et} \quad \det(\star|E) = N_{E/\mathbf{Q}}^{md}$$

donc aussi $P_\alpha = P_{Red,\alpha}^{2g_0/df}$ et $P_{Car,\alpha} = P_{Red,\alpha}^{md}$. Puisqu'il est bien connu que $P_{Min,\alpha}$ et $P_{Car,\alpha}$ ont les mêmes facteurs irréductibles, on en déduit que, en toute généralité, ces quatre polynômes ont *les mêmes facteurs irréductibles*. En particulier, si A est simple, $E = D$ est un corps donc $P_{Min,\alpha}$ est irréductible et P_α est une puissance d'un polynôme irréductible.

1.2. **Le polynôme caractéristique du Frobénius.** On suppose maintenant que A est une variété abélienne de dimension g sur un corps fini $k = \mathbf{F}_q$. On note $\pi_A \in \mathrm{End}_k(A)$ le Frobénius de A et $P_A \in \mathbf{Z}[X]$ son polynôme caractéristique. On sait déjà que c'est un polynôme unitaire de degré $2g$, de terme constant $q^g = \deg\pi_A$, et tel que $P_A(\mathbf{Z}) \subset \mathbf{N}$.

Theorem 5. *Si $P_A(X) = \prod_{i=1}^{2g}(X - \alpha_i)$ dans $\overline{\mathbf{Q}}[X]$ alors*

(1) $|A(\mathbf{F}_{q^n})| = \prod_{i=1}^{2g}(1 - \alpha_i^n)$ *pour tout $n \geq 1$ et*

(2) $|\alpha_i| = q^{\frac{1}{2}}$ *pour tout $i = 1, \cdots, 2g$.*

Démonstration. (de (1)) Pour tout $n \geq 1$, on a tout d'abord

$$|A(\mathbf{F}_{q^n})| \overset{(a)}{=} \left|\ker\left(\pi_A^n - Id_A : A(\overline{\mathbf{F}}_q) \to A(\overline{\mathbf{F}}_q)\right)\right| \overset{(b)}{=} \deg(\pi_A^n - Id_A) \overset{\text{def}}{=} P_{\pi_A^n}(1)$$

car (a) π_A agit par Frob_k sur $A(\overline{\mathbf{F}}_q)$ et (b) π_A agit par 0 sur Lie$A$. D'autre part, choisissons un plongement de $\overline{\mathbf{Q}}$ dans $\overline{\mathbf{Q}}_\ell$. D'après la proposition précédente,

$$P_{\pi_A^n}(X) = \det_{\mathbf{Q}_\ell}\left(\pi_A^n - X \cdot Id | V_\ell(A, \overline{\mathbf{F}}_q)\right) = \textstyle\prod_{i=1}^{2g}(X - \alpha_i^n)$$

dans $\overline{\mathbf{Q}}_\ell[X]$, donc aussi dans $\overline{\mathbf{Q}}[X]$, et $|A(\mathbf{F}_{q^n})| = P_{\pi_A^n}(1) = \prod_{i=1}^{2g}(X - \alpha_i^n)$, CQFD. □

Lemma 6. *Soit † une involution de Rosati sur* $\mathrm{End}_k^0(A)$*. Alors* $\pi_A^\dagger \circ \pi_A = q$.

Démonstration. Soit $\mathcal{L}$ un faisceau inversible ample sur A, donnant une polarisation $\lambda : A \to A^t$ qui induit † sur $\mathrm{End}_k^0(A)$. Posant $\pi = \pi_A$, on veut donc voir que $q = \pi^\dagger \circ \pi = \lambda^{-1} \circ \pi^t \circ \lambda \circ \pi$, où encore que

$$q\lambda = \pi^t \circ \lambda \circ \pi : A \to A \to A^t \to A^t$$

Soit donc $a \in A$, de sorte que $\lambda(a) = \mathcal{T}_a^\star \mathcal{L} \otimes \mathcal{L}^{-1}$ dans $A^t = \mathrm{Pic}_{A/k}^0$ et

$$\pi^t \circ \lambda \circ \pi(a) = [\pi]^\star(\mathcal{T}_{\pi(a)}^\star \mathcal{L} \otimes \mathcal{L}^{-1}) = \pi^\star \mathcal{T}_{\pi(a)}^\star \mathcal{L} \otimes \pi^\star \mathcal{L}^{-1} = \mathcal{T}_a^\star \pi^\star \mathcal{L} \otimes \pi^\star \mathcal{L}^{-1}.$$

Mais dans Pic$A$, $\pi^\star \mathcal{L} = \mathcal{L}^q$ (comme on voit bien sur les diviseurs de Cartier), donc

$$\pi^t \circ \lambda \circ \pi(a) = \mathcal{T}_a^\star \mathcal{L}^q \otimes \mathcal{L}^{-q} = (\mathcal{T}_a^\star \mathcal{L} \otimes \mathcal{L}^{-1})^q = q\lambda(a),$$

CQFD. □

Montrons alors la deuxième partie du théorème. La sous-algèbre $\mathbf{Q}(\pi)$ de $E = \mathrm{End}_k^0(A)$ est commutative, stable par † (puisque $\pi^\dagger = q\pi^{-1} \in \mathbf{Q}(\pi)$), et centrale dans E (puisque π commute à tout le monde). Puisque le centre de E est un produit de corps, $\mathbf{Q}(\pi)$ est donc aussi réduite, i.e. un produit de corps. On *admet* le résultat suivant, que l'on a démontré sur $\mathbf{C}$ mais qui reste vrai sur tous les corps, cf [3, §21] : l'involution de Rosati † est positive, i.e. $\mathrm{tr}(x^\dagger x) > 0$ pour tout $x \in E$. La restriction de cette involution à E est donc encore positive, et E est finalement un produit de corps totalement réels (où † est trivial) et de corps CM (où † est l'involution canonique). Donc, pour tout morphisme de $\mathbf{Q}$-algèbres $\phi : E \to \mathbf{C}$, on a $q = \phi(q) = \phi(\pi \cdot \pi^\dagger) = \phi(\pi) \cdot \overline{\phi}(\pi)$, et $|\phi(\pi)| = q^{1/2}$. Mais les $\phi(\pi)$ sont exactement les racines du polynôme minimal $P_{Min,\pi}$de π, i.e. d'après la remarque 4, les racines du polynôme $P_\pi = P_A$: CQFD.

Exercise 7. Calculer la fonction Zêta de A.

Remark 8. Pour une courbe elliptique $E = A$, $g = 1$, et

$$P_E = (X - \alpha_1)(X - \alpha_2) = X^2 - a_q X + q$$

avec $a_q = \alpha_1 + \alpha_2 \in \mathbf{Z}$. La première partie du théorème dit que

$$|E(\mathbf{F}_q)| = P_E(1) = 1 + q - a_q$$

ou encore que $a_q = (1 + q) - |E(\mathbf{F}_q)| = \left|\mathbf{P}^1(\mathbf{F}_q)\right| - |E(\mathbf{F}_q)|$, et la seconde implique que

$$|a_q| = \left|\left|\mathbf{P}^1(\mathbf{F}_q)\right| - |E(\mathbf{F}_q)|\right| \leq 2\sqrt{q},$$

(formule qui a pour corollaire $|E(\mathbf{F}_q)| \sim_q \left|\mathbf{P}^1(\mathbf{F}_q)\right|$). En particulier, le discriminant $\Delta_E = a_q^2 - 4q \leq 0$. D'ailleurs, on peut retrouver dans ce cas plus facilement la seconde partie du théorème : puisque $P_E(\frac{n}{d}) = \deg(\alpha - \frac{n}{d}) = \frac{1}{d^2}\deg(\alpha - n) \geq 0$ pour tout $\frac{n}{d} \in \mathbf{Q}$, $\Delta_E \leq 0$ donc $|a_q| \leq 2\sqrt{q}$. En appliquant ceci à $E/\mathbf{F}_{q^n}$, on obtient :

$$|\alpha_1^n + \alpha_2^n| \leq 2q^{\frac{n}{2}}$$

d'où l'on déduit facilement que $|\alpha_1| = |\alpha_2| = q^{1/2}$.

1.3. Les q-nombres de Weil.

Definition 9. Un q-nombre de Weil (de poids -1) est un *entier* algébrique $\pi \in \overline{\mathbf{Q}}$ tel que pour tout plongement $\phi : \mathbf{Q}(\pi) \hookrightarrow \mathbf{C}$, $|\phi(\pi)| = q^{1/2}$. On note $\mathcal{W}(q) \subset \overline{\mathbf{Q}}$ l'ensemble des q-nombres de Weil.

Si A est une variété abélienne sur $k = \mathbf{F}_q$, π_A son Frobénius et P_A le polynôme caractéristique de π_A, toutes les racines de P_A dans $\overline{\mathbf{Q}}$ sont donc des q-nombres de Weil. Si A est simple, $\mathbf{Q}(\pi_A)$ est un corps et P_A est une puissance du polynôme minimal de π_A, qui est irréductible sur $\mathbf{Q}$. Toutes les racines de P_A dans $\overline{\mathbf{Q}}$ sont donc conjuguées sous $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. On obtient ainsi une application

$$w : \mathcal{S}(q) \to \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})\backslash\mathcal{W}(q)$$

où $\mathcal{S}(q)$ est l'ensemble des classes d'isomorphismes de variétés abéliennes simples sur k.

2. Le Théorème de Tate

Il affirme que lorsque k est un corps fini de caractéristique p,

Theorem 10. [4] *Pour toutes variétés abéliennes A et B sur k et tout $\ell \neq p$,*

$$\rho_\ell : \mathrm{Hom}_k(A, B) \otimes \mathbf{Z}_\ell \to \mathrm{Hom}_{\mathrm{Gal}(\overline{k}/k)}\left(T_\ell(A, \overline{k}), T_\ell(B, \overline{k})\right)$$

est un isomorphisme.

Remark 11. (1) On sait déjà que ρ_ℓ est injective, il suffit de démontrer la surjectivité. (2) Ce théorème est encore vrai lorsque k est un corps de nombre, mais la démonstration, due à Faltings, est *considérablement* plus difficile !

2.1. Réductions préliminaires.

Il suffit de montrer que

$$\rho_\ell : \mathrm{Hom}_k^0(A, B) \otimes \mathbf{Q}_\ell \to \mathrm{Hom}_{\mathrm{Gal}_k}(V_\ell A, V_\ell B)$$

est un isomorphisme car

$$\mathrm{Hom}_{\mathrm{Gal}_k}(T_\ell A, T_\ell B) \cap \rho_\ell\left(\mathrm{Hom}_k^0(A, B) \otimes \mathbf{Q}_\ell\right) = \mathrm{Hom}_k^0(A, B) \otimes \mathbf{Z}_\ell.$$

Il suffit aussi de traiter le cas où $A = B$, puisque pour $C = A \times B$,

$$\rho_\ell : \mathrm{End}_k^0(C) \otimes \mathbf{Q}_\ell \to \mathrm{End}_{\mathrm{Gal}_k}(V_\ell C, V_\ell C)$$

s'identifie à

$$\rho_\ell : \begin{pmatrix} \mathrm{End}_k^0(A) & \mathrm{Hom}_k^0(B, A) \\ \mathrm{Hom}_k^0(A, B) & \mathrm{End}_k^0(B) \end{pmatrix} \otimes \mathbf{Q}_\ell \to \begin{pmatrix} \mathrm{End}_{\mathrm{Gal}_k}(V_\ell A) & \mathrm{Hom}_{\mathrm{Gal}_k}(V_\ell B, V_\ell A) \\ \mathrm{Hom}_{\mathrm{Gal}_k}(V_\ell A, V_\ell B) & \mathrm{End}_{\mathrm{Gal}_k}(V_\ell B) \end{pmatrix}$$

On doit donc voir que $\dim_{\mathbf{Q}} \mathrm{End}_k^0(A) = \dim_{\mathbf{Q}_\ell} \mathrm{End}_{\mathrm{Gal}_k}(V_\ell A)$. Puisque π_A agit sur $V_\ell A$ comme le Frobénius Frob_k, on peut écrire

$$\mathrm{End}_{\mathrm{Gal}_k}(V_\ell A) = \mathrm{End}_{\mathbf{Q}_\ell(\pi_A)}(V_\ell A)$$

où $\mathbf{Q}_\ell(\pi_A)$ est la sous-algèbre commutative engendrée par π_A dans $\mathrm{End}_{\mathbf{Q}_\ell}(V_\ell A)$, i.e. $\rho_\ell(\mathbf{Q}(\pi_A) \otimes \mathbf{Q}_\ell)$ où $\mathbf{Q}(\pi_A)$ est la sous-algèbre commutative de $\mathrm{End}_k^0(A)$ engendrée par π_A. Or dans $\mathrm{End}_{\mathbf{Q}_\ell}(V_\ell A) \simeq M_{2g}(\mathbf{Q}_\ell)$ (où $g = \dim A$), le commutant C' d'une sous-algèbre semi-simple C vérifie la formule $[C' : \mathbf{Q}_\ell] \cdot [C : \mathbf{Q}_\ell] = 4g^2$. On voit donc que

$$\dim_{\mathbf{Q}_\ell} \mathrm{End}_{\mathbf{Q}_\ell(\pi_A)}(V_\ell A) \cdot \dim_{\mathbf{Q}} \mathbf{Q}(\pi_A) = 4g^2$$

donc $\dim_{\mathbf{Q}_\ell} \mathrm{End}_{\mathbf{Q}_\ell(\pi_A)}(V_\ell A)$ ne dépend pas de ℓ. Il suffit donc de démontrer le théorème pour un $\ell \neq p$ convenablement choisi.

Remark 12. Soit K un corps, Π une indéterminée, et V_A, V_B deux $K[\Pi]$-modules semi-simples. Donc $V_X \simeq \oplus_P V(P)^{x(P)}$ où $V(P) = K[\Pi]/P$ avec $\prod P^{x(P)} = f_X$ est le polynôme *caractéristique* de Π agissant sur V_X (pour $X \in \{A, B\}$). Alors

$$\mathrm{Hom}_{K[\Pi]}(V_A, V_B) = \prod_P \mathrm{Hom}_{K[\Pi]}(V(P)^{a(P)}, V(P)^{b(P)}) = \prod_P M_{b(P),a(P)}(K[\Pi]/P)$$

qui est de K-dimension $r(f_A, f_B) = \sum_P a(P)b(P) \deg P$ où P parcourt les polynômes irréductibles de $K[X]$. On vérifie facilement que $r(f_A, f_B)$ est invariant par changement de base $K \hookrightarrow L$. Appliquant ceci à la situation qui nous intéresse, on en déduit le lemme suivant.

Lemma 13. *Pour toute variétés abéliennes A et B sur k de polynômes caractéristiques*

$$P_A = \textstyle\prod_{i=1}^{2\dim A}(X - \alpha_i) \quad \textit{et} \quad P_B = \prod_{j=1}^{2\dim B}(X - \beta_j) \qquad (\textit{dans } \overline{\mathbf{Q}}[X])$$

et pour tout $\ell \neq p$,

$$\dim_{\mathbf{Q}_\ell} \mathrm{Hom}_{\mathrm{Gal}_k}(V_\ell A, V_\ell B) = r(P_A, P_B) = |\{(i,j) | \alpha_i = \beta_j\}| .$$

En particulier, cette dimension ne dépend pas du choix de $\ell \neq p$.

2.2. **Preuve du théorème.** Soit donc A une variété abélienne sur k. On pose $F = \mathbf{Q}(\pi)$ qui est centrale dans $E = \mathrm{End}_k(A)$. Pour tout $\ell \neq p$, on note $F_\ell = F \otimes \mathbf{Q}_\ell$, $E_\ell = E \otimes \mathbf{Q}_\ell$, $V_\ell = V_\ell A$, $D_\ell = \mathrm{End}_{F_\ell}(V_\ell)$ et $M_\ell = \mathrm{End}_{\mathbf{Q}_\ell}(V_\ell)$. On a donc une suite de $\mathbf{Q}_\ell$-algèbre simples $F_\ell \subset E_\ell \subset D_\ell \subset M_\ell$ et on veut montrer que $E_\ell = D_\ell$ (pour un choix convenable de ℓ), i.e. que E_ℓ est le commutant de F_ℓ dans M_ℓ, ou encore que F_ℓ est le commutant de E_ℓ dans M_ℓ (ce qui impliquera d'ailleurs que F_ℓ est le centre de E_ℓ, donc que F est le centre de E). Notons $C_\ell = \mathrm{End}_{E_\ell}(V_\ell)$ ce commutant, de sorte que $F_\ell \subset C_\ell$ et on veut montrer que $F_\ell = C_\ell$ (pour un choix convenable de ℓ).

Décomposons $F = \prod F_i$ en produit de corps et choisissons pour $\ell \neq p$ un nombre premier qui se décompose totalement dans tous les F_i (il en existe une infinité). On a alors $F_\ell \simeq \mathbf{Q}_\ell^r$, et $V_\ell = \oplus_{i=1}^r V_\ell^i$ se décompose de même en espaces propres pour l'action de F_ℓ, où F_ℓ agit sur V_ℓ^i par la i-ème projection $F_\ell \to \mathbf{Q}_\ell$. Ces sous-espaces sont stables sous C_ℓ, puisque F_ℓ est centrale dans C_ℓ. Pour voir que $F_\ell = C_\ell$, il suffit alors de démontrer que *pour toute $\mathbf{Q}_\ell$-droite $W \subset V_\ell$ qui est stable sous F_ℓ (i.e. contenu dans l'un des V_ℓ^i), W est également stable sous C_ℓ.*

Choisissons sur A une polarisation $\lambda : A \to A^t$, disons de degré d^2 et soit $\psi_\ell : V_\ell A \times V_\ell A \to V_\ell \mu$ la forme symplectique qu'elle induit sur V_ℓ. Il suffit alors de démontrer que *pour tout sous-espace totalement isotrope maximal W de (V_ℓ, ψ_ℓ) qui est stable sous F_ℓ, W est également stable sous C_ℓ.* Cette hypothèse implique en effet que tout sous-espace totalement isotrope (mais pas forcément maximal) W de (V_ℓ, ψ_ℓ) qui est stable sous F_ℓ (par exemple une $\mathbf{Q}_\ell$-droite stable sous F_ℓ) est encore stable sous C_ℓ. On le montre par récurrence descendante sur la dimension de W, le cas initial où $\dim_{\mathbf{Q}_\ell} W = g$ étant précisément notre hypothèse. Soit donc W un tel sous-espace, avec $g - \dim_{\mathbf{Q}_\ell} W = s > 0$. Puisque F est stable sous l'involution de Rosati $\dagger$ induite par λ, F_ℓ est stable sous l'involution $\dagger$ induite par ψ_ℓ, donc l'orthogonal $W^\perp$ de W est encore F_ℓ-stable, i.e. de la forme $W^\perp = W \oplus \oplus_{i=1}^{2s} D_i$ pour des $\mathbf{Q}_\ell$-droites D_i qui sont F_ℓ-stables ; alors $W_1 = W \oplus D_1$ et $W_2 = W \oplus D_2$ sont deux sous-espaces totalement isotropes et F_ℓ-stables de V_ℓ, ils sont stables sous C_ℓ d'après l'hypothèse de récurrence, et leur intersection W est donc également stable sous V_ℓ.

Le théorème de Tate résulte alors de la proposition suivante, dans laquelle il n'est plus nécessaire de supposer que $F_\ell \simeq \mathbf{Q}_\ell^r$, mais où l'on demande en revanche que $\ell \nmid pd$ (concrètement, il faut donc choisir d'abord λ d'un degré d^2 arbitraire, puis ensuite $\ell \nmid pd$ décomposant E).

Proposition 14. *Pour tout sous-espace totalement isotrope maximal W de (V_ℓ, ψ_ℓ) qui est stable sous F_ℓ, il existe un élément $e \in E_\ell$ tel que $e \cdot V_\ell = W$. En particulier, W est stable sous C_ℓ.*

Démonstration. Dire que W est F_ℓ-stable revient à dire que c'est un sous $\mathbf{Q}_\ell[\mathrm{Gal}_k]$-module. Pour tout $n \geq 0$, on pose $X_n = (T_\ell A \cap W) + \ell^n T_\ell A \subset T_\ell A$. C'est donc un $\mathbf{Z}_\ell$-sous-réseau d'indice ℓ^{ng} dans $T_\ell A$ qui est stable sous Gal_k. Soit $\alpha_n : A_n \to A$ l'isogénie (de degré ℓ^{ng}) telle que $\alpha_n(T_\ell A_n) = X_n$ dans $T_\ell A$. Pour tout $x, y \in T_\ell A_n$, on a donc

$$\langle x, (\alpha_n^\star \lambda)(y) \rangle_\ell^{A_n} = \langle x, y \rangle_\ell^{\alpha_n^\star \lambda} = \langle \alpha_n(x), \alpha_n(y) \rangle_\ell^\lambda \subset \ell^n T_\ell(\mu)$$

puisque $W \subset V_\ell A$ est totalement isotrope, donc $(\alpha_n^\star \lambda)(T_\ell A_n) \subset \ell^n T_\ell A_n^t$, i.e.

$$\alpha_n^\star \lambda = \alpha_n^t \circ \lambda \circ \alpha_n : A_n \to A_n^t \text{ est triviale sur } A_n[\ell^n].$$

Soit $\lambda_n : A_n \to A_n^t$ telle que $\ell^n \lambda_n = \alpha_n^\star \lambda$. C'est encore une polarisation de A_n, et

$$(\ell^n)^{2g} \deg(\lambda_n) = \deg(\ell^n \lambda_n) = \deg(\alpha_n^\star \lambda) = (\ell^{ng})^2 \deg(\lambda)$$

puisque $\deg \alpha_n = \deg \alpha_n^t = \ell^{ng}$. Donc $\deg \lambda_n = \deg \lambda$. D'après le lemme ci-dessous, il y a un ensemble infini $I \subset \mathbf{N}$ tel que $(A_i, \lambda_i) \simeq (A_j, \lambda_j)$ pour tout $i, j \in I$. Soit n le plus petit élément de I, et pour tout $i \in I$, choisissons arbitrairement un isomorphisme $\theta_i : A_n \to A_i$. Alors $e_i = \alpha_i \circ \theta_i \circ \alpha_n^{-1} \in E$ induit sur $V_\ell A$ un morphisme tel que $e_i(X_n) = X_i \subset X_n$. Vus dans E_ℓ, ces morphismes restent donc dans le compact $E_\ell \cap \mathrm{End}_{\mathbf{Z}_\ell}(X_n)$. On peut donc extraire de (e_i) une sous-suite $(e_{\phi(i)})$ qui converge vers un élément e de E_ℓ. On montre facilement que $e(X_n) = \cap X_i = T_\ell A \cap W$, puis que $e(V_\ell A) = W$. □

Lemma 15. *L'ensemble $\mathbf{M}_{d,1}^g(k)$ des classes d'isomorphismes de paires (B, ν) où B est une variété abélienne de dimension g sur k et $\nu : B \to B^t$ est une polarisation de degré d^2 est* fini.

Démonstration. Ce serait trivial si l'on savait qu'il s'agit là des k-points d'un schéma de type fini sur $\mathrm{Spec}\mathbf{Z}$ (ou $\mathbf{F}_p$). Malheureusement, $\mathbf{M}_{d,1}^g$ n'est pas représentable. On peut rajouter une structure de niveau $N \geq 3$ premier à p : si B est une variété abélienne de dimension g sur k, le noyau de $\mathrm{Gal}_k \to \mathrm{Aut}(B[N](\overline{k}))$ est d'indice majoré par le cardinal de $\mathrm{Aut}(B[N](\overline{k})) \simeq GL_{2g}(\mathbf{Z}/N\mathbf{Z})$, donc il existe une extension finie K de k telle que toute variété abélienne B sur k de dimension g admet une structure de niveau N sur K. Puisque $\mathbf{M}_{d,N}^g(K)$ est fini, on en déduit que l'ensemble $\mathbf{M}_{d,1}^g(k)$ est d'image finie dans $\mathbf{M}_{d,1}^g(K)$, mais il resterait alors à vérifier que les fibres de $\mathbf{M}_{d,1}^g(k) \to \mathbf{M}_{d,1}^g(K)$ sont finies (ce qui n'est pas très difficile). On peut aussi rajouter une rigidification : puisque k est un corps, $\mathbf{RM}^g_{d,1}(k) \to \mathbf{M}^g_{d,1}(k)$ est surjective : on conclut alors directement, puisqu'on a vu que $\mathbf{RM}^g_{d,N}$ était représentable (sans restriction sur N) par un schéma de type fini sur Spec$\mathbf{Z}$. □

2.3. Conséquences.

Proposition 16. *Les conditions suivantes sont équivalentes :* (1) $A \hookrightarrow B$ *dans* $\mathbf{Ab}^0_k$, (2) $V_\ell A \hookrightarrow V_\ell B$ *dans* $\mathbf{Mod}_{\mathbf{Q}_\ell[\mathrm{Gal}_k]}$ *pour un (resp. pour tout)* $\ell \neq p$, (3) $P_A \mid P_B$.

Démonstration. (1) ⇒ (2) est évident et inversement si $f : V_\ell A \hookrightarrow V_\ell B$ est Gal_k-équivariant, on peut d'après le théorème de Tate approcher f par un élément de $\rho_\ell(f') \in \rho_\ell(\mathrm{Hom}^0_k(A,B))$, et si $\rho_\ell(f')$ est suffisamment proche de f, alors $\rho_\ell(f')$ sera encore injective, donc $f' : A \hookrightarrow B$ dans $\mathbf{Ab}^0_k$. Pour (2) $\iff$ (3), il suffit de noter que le $\mathbf{Q}_\ell[X]$-module $V_\ell A$ (où X agit par $\mathrm{Frob}_k = \pi_A$) est

$$V_\ell A \simeq \oplus_Q \left(\mathbf{Q}_\ell[X]/Q \cdot \mathbf{Q}_\ell[X]\right)^{v_Q(P_A)}$$

où Q parcourt les polynômes irréductibles (unitaires) de $\mathbf{Q}_\ell[X]$. □

Corollary 17. *Les conditions suivantes sont équivalentes :* (1) $A \sim B$ *dans* $\mathbf{Ab}^0_k$, (2) $V_\ell A \simeq V_\ell B$ *dans* $\mathbf{Mod}_{\mathbf{Q}_\ell[\mathrm{Gal}_k]}$ *pour un (resp. pour tout)* $\ell \neq p$, (3) $P_A = P_B$.

Remark 18. Il en résulte que deux variétés abéliennes A et B sur k qui sont isogènes ont le même nombre de points sur les extensions finies de k, et donc aussi la même fonction Zêta (ce qui n'est à priori pas du tout évident). D'ailleurs, cette condition caractérise aussi le fait que A et B soient isogènes !

Corollary 19. *L'application* $w : \mathcal{S}(q) \to \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})\backslash\mathcal{W}(q)$ *est injective.*

Démonstration. Ce n'est pas complètement tautologique. Si A et B sont simples et $w(A) = w(B)$, les polynômes *minimaux* de π_A et π_B sont égaux donc $P_A^a = P_B^b$ pour des entiers a et b convenables, donc $A^a \sim B^b$ dans $\mathbf{Ab}^0_k$ puis $A \sim B$ car A et B sont simples (donc aussi $P_A = P_B$ et $a = b$). □

3. Le théorème de Honda

Disons qu'un q-nombre de Weil $\pi \in \mathcal{W}(q)$ est effectif si et seulement si il est conjugué au Frobénius d'une variété abélienne simple A sur $\mathbf{F}_q$. Le théorème de Honda dit tout simplement que

Theorem 20. [1, 5] *Tous les nombres de Weil sont effectifs.*

Corollary 21. *L'application* $w : \mathcal{S}(q) \to \mathrm{Gal}(\overline{\mathbf{Q}}\backslash\mathbf{Q})\backslash\mathcal{W}(q)$ *est bijective.*

3.1. Un lemme préliminaire.

Lemma 22. *Soit* $\pi \in \mathcal{W}(q)$ *et* $n \geq 1$. *Si* $\pi^n \in \mathcal{W}(q^n)$ *est effectif, alors* π *l'est également.*

Démonstration. Soit A' simple sur $k' = \mathbf{F}_{q^n}$ telle que $\pi_{A'} \sim \pi^n$ et $A = \mathrm{Res}_k^{k'} A'$, qui est une variété abélienne sur $k = \mathbf{F}_q$. Alors $V_\ell A = \mathrm{Ind}_{\mathrm{Gal}_{k'}}^{\mathrm{Gal}_k} V_\ell A'$ pour tout $\ell \neq p$, donc $P_A(X) = P_{A'}(X^n)$. Puisque $P_A(\pi) = P_{A'}(\pi^n) = 0$, on a donc $P_B(\pi) = 0$ pour un facteur simple B de A. □

Soit π un q-nombre de Weil, $P \in \mathbf{Z}[X]$ son polynôme minimal (irréductible, unitaire). On va montrer que π^n est effectif pour n assez grand.

3.2. **Le corps $F = \mathbf{Q}(\pi)$.** On pose $F = \mathbf{Q}(\pi)$. Pour tout plongement $\phi : F \hookrightarrow \mathbf{C}$,

$$\overline{\phi(\pi)} = \frac{\phi(\pi) \cdot \overline{\phi(\pi)}}{\phi(\pi)} = \frac{q}{\phi(\pi)} = \phi(\frac{q}{\pi})$$

donc $0 = \overline{\phi}(P(\pi)) = P(\overline{\phi}(\pi)) = P(\phi(\frac{q}{\pi})) = \phi(P(\frac{q}{\pi}))$, de sorte que $\frac{q}{\pi}$ est encore une racine de P. Soit $\star$ l'automorphisme de F qui envoie π sur $\frac{q}{\pi}$. C'est une involution de F, et puisque $\overline{\phi(\pi)} = \phi(\pi^\star)$ pour tout $\phi : F \hookrightarrow \mathbf{C}$, on trouve les deux possibilités suivantes :

- $\star \neq Id$ sur F, donc F est un *corps CM.*
- $\star = Id$ sur F, i.e. $\pi^2 = q$ donc $\pi = \pm\sqrt{q}$. Si $q = p^{2a}$, on obtient deux orbites galoisiennes $\pi = \pm p^a$, pour lesquelles $F = \mathbf{Q}$ et $P = X \pm p^a$. Si $q = p^{2a+1}$, on obtient une seule orbite galoisienne, $\pi \in \{\pm p^a\sqrt{p}\}$, pour laquelle $F = \mathbf{Q}(\sqrt{p})$.

3.3. **Le corps gauche $D = D(\pi)$.** Pour toute place v de $F = \mathbf{Q}(\pi)$ on note $\|\star\|_v : F_v \to \mathbf{R}_\geq$ la valuation normalisée en v et on définit $i_v(\pi)$ par $\|\pi\|_v = q^{-i_v(\pi)}$. Puisque $\|\pi\|_v = q^{\frac{1}{2}}$ pour tout $v \mid \infty$, la formule du produit $\prod \|\star\|_v = 1$ montre que $\|\pi\|_v \neq 1$ (i.e. $i_v(\pi) \neq 0$) seulement pour $v \mid p\infty$, et l'on a $i_v(\pi) = \frac{-1}{2}$ pour $v \mid \infty$, et

$$i_v(\pi) = \frac{v(\pi)}{v(q)} \cdot [F_v : \mathbf{Q}_p] \in \mathbf{Q} \quad \text{pour } v \mid p.$$

Definition 23. On note $D(\pi)$ un corps gauche de centre F tel que

$$\forall v \text{ de } F : \qquad \mathrm{inv}_v D(\pi) = i_v(\pi) \bmod \mathbf{Z}.$$

Vérifions qu'un tel corps existe bien. Si $F = \mathbf{Q}$, donc $\pi = \pm p^a$ et $q = p^{2a}$, on a $i_v(\pi) = \frac{1}{2} \bmod \mathbf{Z}$ pour $v \mid p\infty$ et 0 sinon : $D(\pi)$ est alors le corps de quaternion sur $\mathbf{Q}$ avec $\mathrm{Ram} D(\pi) = \{p, \infty\}$. Si $F = \mathbf{Q}(\sqrt{p})$, donc $\pi = \pm p^a\sqrt{p}$ et $q = p^{2a+1}$, on a $i_v(\pi) = \frac{1}{2} \bmod \mathbf{Z}$ pour $v \mid \infty$ et 0 sinon : $D(\pi)$ est alors le corps de quaternion sur $\mathbf{Q}(\sqrt{p})$ tel que $\mathrm{Ram} D(\pi) = \{\infty_1, \infty_2\}$. Dans tous les autres cas, F est un corps CM (donc sans place réelle), et il faut voir que

$$\sum_{v \mid p} \frac{v(\pi)}{v(q)} \cdot [F_v : \mathbf{Q}_p] = \sum_{\{v \neq v^\star\}} \frac{v(\pi) + v^\star(\pi)}{v(q)} \cdot [F_v : \mathbf{Q}_p] + \sum_{\{v = v^\star\}} \frac{v(\pi)}{v(q)} \cdot [F_v : \mathbf{Q}_p] \in \mathbf{Z}.$$

Or $v(\pi) + v(\pi^\star) = v(\pi\pi^\star) = v(q)$ dans tous les cas, et si $v = v^\star$, alors $2 \mid [F_v : \mathbf{Q}_p]$: CQFD.

3.4. **Un corps CM $E \subset D(\pi)$.** On note $D = D(\pi)$, $i_v = i_v(\pi)$ et $d^2 = [D : F]$ (donc d est le pgcd des dénominateurs des i_v).

Lemma 24. *Il existe des corps CM $F \subset E \subset D$ avec $[E : F] = d$.*

Démonstration. A nouveau, on traite séparément les cas où F n'est pas CM, qui sont faciles. Si F est CM de sous-corps totalement réel F_0, on choisit une extension E_0 de F_0 qui est (1) de degré d, (2) totalement réelle, et (3) telle que pour toute place $v \neq v^\star$ de F sur p, pour toute place w de E_0 au-dessus de $v|F_0$, $[E_{0,w} : F_{0,v}] \cdot i_v \in \mathbf{Z}$. Alors $E = E_0 \cdot F$ est un corps CM de degré d, et pour toute place $w \mid p$ de E au dessus de $v = w|F$,

$$\mathrm{inv}_w(D \otimes_F E) = \mathrm{inv}_w(D_v \otimes_{F_v} E_w) = [E_w : F_v] \cdot i_v \in \mathbf{Z},$$

soit parce que $v = v^\star$ (donc $i_v = 0$), soit parce que $v \neq v^\star$ (donc $[E_w : F_v] = [E_{0,w} : F_{0,v}]$). Donc E splitte D, et puisque $[D : F] = d^2 = [E : F]^2$, E se plonge dans D. $\square$

3.5. **Un type CM Φ sur E.** On fixe un plongement $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_p$. On a alors :

$$\mathrm{Hom}_{\mathbf{Q}-alg}(E, \mathbf{C}) = \mathrm{Hom}_{\mathbf{Q}_p}(E \otimes \mathbf{Q}_p, \overline{\mathbf{Q}}_p) = \coprod_{w|p} H(w)$$

où $H(w) = \mathrm{Hom}_{\mathbf{Q}_p-alg}(E_w, \overline{\mathbf{Q}}_p)$.

Lemma 25. *Il existe un type CM Φ sur E tel que pour tout $w \mid p$,*

$$\frac{w(\pi)}{w(q)} = \frac{|H(w) \cap \Phi|}{|H(w)|}.$$

Démonstration. On veut que pour tout $w \mid p$ de E sur v de F,

$$|H(w) \cap \Phi| = |H(w)| \cdot \frac{w(\pi)}{w(q)} = [E_w : \mathbf{Q}_p] \cdot \frac{v(\pi)}{v(q)} = [E_w : F_v] \cdot i_v.$$

Si $w^\star = w$, $v^\star = v$ et $[E_w : F_v] \cdot i_v = \frac{1}{2}[E_w : \mathbf{Q}_p] = \frac{1}{2}|H(w)|$: on choisit pour $\Phi \cap H(w)$ un système de représentant (quelconque) des orbites de $\star$ dans $H(w)$. Si $w^\star \neq w$, on a

$$[E_w : F_v] \cdot i_v + [E_{w^\star} : F_{v^\star}] \cdot i_{v^\star} = [E_w : \mathbf{Q}_p] = |H(w)| = |H(w^\star)|.$$

On choisit alors pour $\Phi \cap (H(w) \coprod H(w^\star))$ un système de représentant des orbites de $\star$ tel que $\Phi \cap H(w)$ contienne $[E_w : F_v] \cdot i_v$ éléments, et alors $\Phi \cap H(w^\star)$ en contient bien $[E_{w^\star} : F_{v^\star}] \cdot i_{v^\star}$. $\square$

3.6. **Conclusion.** Soit (E, Φ) comme ci-dessus, $k \subset \overline{\mathbf{Q}}$ une extension telle que $\phi(E) \subset k$ pour tout $\phi \in \Phi$. Quitte à agrandir k, on peut supposer que (1) il existe sur k une variété abélienne A de type CM (E, Φ) à multiplication complexe par $\mathcal{O}_E$, que (2) A a bonne réduction en la place P de $\mathcal{O}_K$ déterminée par le plongement $\overline{\mathbf{Q}} \hookrightarrow \mathbf{Q}_p$, et que (3) $\mathcal{O}_K/P = \mathbf{F}_{q^n}$. D'après la formule de Shimura-Tanyiama, le Frobénius de la réduction de A en P est un élément π_1 de $\mathcal{O}_E$ tel que pour tout $w \mid p$ de E,

$$\frac{w(\pi_1)}{w(q^n)} = \frac{|H(w) \cap \Phi|}{|H(w)|} = \frac{w(\pi^n)}{w(q^n)}.$$

Donc $(\pi_1) = (\pi^n)$ et $\pi_1 = u\pi^n$ pour une unité u de $\mathcal{O}_E^\times$. Puisque π_1 et π^n sont des q^n-nombres de Weil, u est un $q^0 = 1$-nombre de Weil, i.e. une racine de l'unité. Donc pour un entier m convenable, $\pi_1^m = \pi^{nm}$. Puisque π_1^m est effectif, π l'est également.

4. Le théorème de Milne-Waterhouse

D'après le dernier corollaire, il devrait être possible de décrire entièrement $\mathrm{End}_k^0 A$ à partir de π_A. C'est ce que fait le théorème de Milne-Waterhouse, d'abord énoncé sans preuve complète dans [4]. Tout d'abord, il résulte du théorème de Tate que

Proposition 26. *Pour toute variété abélienne A sur k, $\mathbf{Q}(\pi_A)$ est le centre de $\mathrm{End}_k^0(A)$.*

Démonstration. On sait déjà que $F = \mathbf{Q}(\pi_A)$ est contenu dans le centre C de $E = \mathrm{End}_k^0(A)$. Puisque E_ℓ est le commutant de F_ℓ dans $M_\ell = \mathrm{End}_{\mathbf{Q}_\ell}(V_\ell A)$, F_ℓ est le commutant de E_ℓ dans M_ℓ. En particulier $C_\ell \subset F_\ell$, donc $C = F$. $\square$

Si A est simple de Frobénius π, $D = \mathrm{End}_k^0(A)$ est donc un corps gauche de centre $F = \mathbf{Q}(\pi)$. La classe d'isomorphisme de ce corps est alors entièrement décrite par son image dans le groupe de Brauer, i.e. par la collection des invariants locaux $\mathrm{inv}_v D \in \mathbf{Q}/\mathbf{Z}$. Le théorème de Milne-Waterhouse s'énonce ainsi :

Theorem 27. *Soit A simple sur k, π son Frobénius, $F = \mathbf{Q}(\pi)$ et $D = \mathrm{End}_k^0 A$. Alors*

$$2\dim A = [D:F]^{\frac{1}{2}} \cdot [F:\mathbf{Q}]$$

et pour toute place v de F, $|\pi|_v \in q^{-\mathrm{inv}_v D}$, i.e. $\mathrm{inv}_v D = \frac{1}{2} \bmod \mathbf{Z}$ si v est réel, 0 si $v \nmid p\infty$ et

$$\mathrm{inv}_v D = \frac{v(\pi)}{v(q)} \cdot [F_v : \mathbf{Q}_p] \bmod \mathbf{Z} \quad \text{si } v \mid p.$$

Démonstration. (Partielle) D'après le théorème de Tate, pour tout $\ell \nmid p$, D_ℓ est le commutant de F_ℓ dans $M_\ell = \mathrm{End}_{\mathbf{Q}_\ell}(V_\ell A)$. On en tire d'une part que $[D_\ell : \mathbf{Q}_\ell] \cdot [F_\ell : \mathbf{Q}_\ell] = (2\dim A)^2$, donc

$$2\dim A = [D_\ell : F_\ell]^{\frac{1}{2}} \cdot [F_\ell : \mathbf{Q}_\ell] = [D:F]^{\frac{1}{2}} \cdot [F:\mathbf{Q}]$$

et d'autre part que pour tout $v \mid \ell$,

$$E_v = E_\ell \otimes_{F_\ell} F_v = \mathrm{End}_{F_\ell}(V_\ell A) \otimes_{F_\ell} F_v = \mathrm{End}_{F_v}(V_\ell A \otimes_{F_\ell} F_v),$$

i.e. $\mathrm{inv}_v E_\ell = 0$. pour tout $v \mid \ell$. □

Example 28. Soit A une courbe elliptique sur $k = \mathbf{F}_q = \mathbf{F}_{p^a}$, π_A son Frobénius, $P_A = X^2 - a_q X + q$ le polynôme caractéristique de π_A, $F = \mathbf{Q}[\pi_A]$ et $E = \mathrm{End}_k^0(A)$, qui sont des corps puisque A est simple. D'après le théorème de Tate, $[F_\ell : \mathbf{Q}] \cdot [E_\ell : \mathbf{Q}] = \dim \mathrm{End}_{\mathbf{Q}_\ell}^0(V_\ell A) = 4$, donc $[F:\mathbf{Q}]^2 \cdot [E:F] = 4$ et (1) $F = \mathbf{Q}$ et E est un corps de quaternion, ou bien (2) $E = F$ est une extension quadratique de $\mathbf{Q}$.

Dans le premier cas, $E_\ell \simeq M_2(\mathbf{Q}_\ell)$ pour tout $\ell \neq p$, donc E est non-ramifiée en $\ell \neq p$. Mais puisque E est tout de même ramifiée quelque part, et en un nombre paire de places de $\mathbf{Q}$, $\mathrm{Ram}(E) = \{p, \infty\}$. Puisque π_A est un q-nombre de Weil dans $F = \mathbf{Q}$, $\pi_A = \pm\sqrt{q} \in \mathbf{Q}$ donc $a = 2a'$ est pair et $\pi_A \in \{\pm p^{a'}\}$. Alors $P_A(n) = \deg(n \mp p^{a'}) = n^2 \mp 2p^{a'} n + p^a$, i.e. $P_A = (X \mp p^{a'})^2$ et $a_q = \mp 2p^{a'}$.

Dans le second cas, $E = F$ est de dimension 2, donc P_A est irréductible. Puisque $\Delta = a_q^2 - 4q \leq 0$, $\Delta < 0$ et $E/\mathbf{Q}$ est une extension CM. Si p est inerte ou ramifié dans $\mathcal{O}_E$, $\pi_A^n \in \mathbf{Q}$ pour n assez grand, i.e. $A_{\overline{k}}$ est supersingulière. Sinon, soit $\mathfrak{p}_1$ le noyau de l'action de $\mathcal{O}_E$ sur $\mathrm{Lie}A(k)$. La formule de Giraud donne alors $(\pi_A) = \mathfrak{p}_1^r$, donc $\pi_A^n \notin \mathbf{Q}$ pour tout n et $A_{\overline{k}}$ reste ordinaire.

Références

[1] Honda, ***, J. Math. Soc. Japan **20**, 1968.

[2] J.S. Milne et W.C. Waterhouse, Abelian Varieties over Finite Fields.

[3] D. Mumford, *Abelian Varieties.*

[4] J. Tate, Endomorphisms of Abelian Varieties over Finite Fields, Inventiones n°**2**.

[5] J. Tate, ***, Séminaire Bourbaki n°**352**, 1968-1969.