Goro Shimura

Modules des variétés abéliennes polarisées et fonctions modulaires, I

Séminaire Henri Cartan, tome 10, n° 2 (1957-1958), exp. n° 18, p. 1-8
<http://www.numdam.org/item?id=SHC_1957-1958__10_2_A9_0>

5 mai 1958

MODULES DES VARIÉTÉS ABÉLIENNES POLARISÉES ET FONCTIONS MODULAIRES, I.

par Goro SHIMURA.

On pourrait regarder la théorie des fonctions modulaires de Siegel comme la théorie des modules des variétés abéliennes, ou plus précisément des variétés abéliennes polarisées de la famille principale. En effet, on peut faire correspondre à tout point z de l'espace de Siegel $\mathfrak{S}_n$ une variété abélienne projective $A(z)$ ayant $(z\ 1_n)$ comme matrice des périodes ; et l'application $z \longrightarrow A(z)$ donne une correspondance biunivoque entre l'espace quotient $\mathfrak{S}_n/Sp(n, \mathbf{Z})$ et l'ensemble des structures de variété abélienne polarisée de la famille principale, comme WEIL l'a signalé à la fin de l'exposé 2. L'objet de cet exposé est de représenter d'une manière concrète cette relation en démontrant que les "modules" des variétés $A(z)$ polarisées par les sections hyperplanes, regardés comme fonctions de z, engendrent les fonctions modulaires de Siegel. Dans ce but, on va d'abord s'occuper des notions de "module" d'une variété abélienne polarisée et de variété de Kummer.

1. Variétés polarisées.

Soient V une variété algébrique complète non-singulière en co-dimension 1, définie par rapport à un corps k, et X un diviseur sur V rationnel par rapport à k. Soit $L(X, k)$ l'ensemble des fonctions f sur V, définies par rapport à k, telles que l'on ait $(f) \succ -X$, où (f) désigne le diviseur de la fonction f. On désignera par $\ell(X)$ la dimension de l'espace vectoriel $L(X, k)$ sur k. Soient $\{f_0, \ldots, f_n\}$ une base de $L(X, k)$ sur k, et x un point générique de V par rapport à k ; soit $V(X, f)$ le lieu de $(f_0(x), \ldots, f_n(x))$ par rapport à k dans l'espace projectif de dimension n. On obtient alors une application rationnelle F de V sur $V(X, f)$, ayant k comme corps de définition, définie par $F(x) = (f_0(x), \ldots, f_n(x))$. Nous dirons que le diviseur X est *ample* si cette application F est birationnelle et birégulière ; cette définition ne dépend que de X et non du choix de k, f_i, x.

Avec les mêmes notations V, X, on désignera par $\mathcal{C}(X)$ l'ensemble de tous les diviseurs X' sur V pour lesquels il existe deux entiers strictement positifs m, m' tels que mX soit algébriquement équivalent à $m'X'$. L'ensemble $\mathcal{C}(X)$ s'appellera une *polarisation* de V si $\mathcal{C}(X)$ contient un diviseur ample. Nous entendrons par <u>variété polarisée,</u> une variété algébrique V sur laquelle est donnée une polarisation $\mathcal{C}$ et la désignerons par $(V, \mathcal{C})$. Nous dirons qu'une variété polarisée $(V, \mathcal{C})$ est <u>définie par rapport à</u> un corps k si V est définie par rapport à k, et si $\mathcal{C}$ contient un diviseur rationnel par rapport à k. Soit σ un isomorphisme de k sur un corps k' ; soient $(V, \mathcal{C})$ une variété polarisée définie par rapport à k, et X un diviseur dans $\mathcal{C}$ rationnel par rapport à k. On obtient alors une polarisation $\mathcal{C}(X^{\sigma})$ de V^{σ}, que l'on désignera par $\mathcal{C}^{\sigma}$.

2. <u>Variétés abéliennes polarisées.</u>

Rappelons d'abord quelques notions et propriétés des diviseurs sur une variété abélienne. Soient A une variété abélienne, X un diviseur sur A et a un point de A. On désignera par X_a la transformée de X par la translation $x \longrightarrow x + a$ sur A. Le diviseur X est dit <u>non-dégénéré</u> s'il n'y a qu'un nombre fini d'éléments u de A tels que X_u soit linéairement équivalent à X.

LEMME 1 (WEIL [5]). - <u>Soit X un diviseur sur une variété abélienne A. S'il existe un entier $n > 0$ tel que nX soit ample, X est non-dégénéré. Réciproquement, si X est positif non-dégénéré, il existe un entier $n_0 > 0$ tel que nX soit ample pour $n > n_0$.</u>

LEMME 2. - <u>Soient X un diviseur non-dégénéré sur une variété abélienne A et Y un diviseur sur A, algébriquement équivalent à X. Alors, il existe un point u de A tel que Y soit linéairement équivalent à X_u.</u>

En effet, en faisant correspondre u à la classe de $X_u - X$, on obtient un homomorphisme de A sur la variété de Picard de A ; si X est non-dégénéré, cet homomorphisme est surjectif ; il existe donc un point u de A tel que $Y - X$ soit linéairement équivalent à $X_u - X$; d'où résulte le lemme 2.

Le lemme suivant est dû à MATSUSAKA.

LEMME 3. - <u>Soient A une variété abélienne de dimension n et X un diviseur positif non-dégénéré sur A. Alors on a</u>

$$\ell(X) = \frac{\deg (X^n)}{n!},$$

<u>où $\deg (X^n)$ désigne $\deg (X_{u_1} \dots X_{u_n})$ pour n points $u_1, \dots, u_n$ de A tels que le produit d'intersection soit défini.</u>

LEMME 4. - Soient A et A' deux variétés abéliennes de même dimension, λ un homomorphisme de A sur A', et X' un diviseur positif non-dégénéré sur A'. On a alors

$$\ell(\lambda^{-1}(X')) = \nu(\lambda)\ \ell(X') ,$$

où $\nu(\lambda)$ désigne le degré de l'homomorphisme λ.

C'est une conséquence immédiate du lemme 3.

Soient $(A , \mathcal{C})$ et $(A' , \mathcal{C}')$ deux variétés abéliennes polarisées de même dimension, et λ un homomorphisme (isomorphisme) de A sur A'. Nous appellerons λ un homomorphisme (isomorphisme) de $(A , \mathcal{C})$ sur $(A' , \mathcal{C}')$ s'il existe un diviseur X' dans $\mathcal{C}'$ tel que $\lambda^{-1}(X')$ soit contenu dans $\mathcal{C}$; s'il en est ainsi, $\lambda^{-1}(Y)$ est contenu dans $\mathcal{C}$, pour tout $Y \in \mathcal{C}'$. D'après notre définition et d'après WEIL [5], pour toute variété abélienne polarisée $(A , \mathcal{C})$, il y a toujours un isomorphisme de $(A , \mathcal{C})$ sur une variété abélienne polarisée (A' , X') telle que A' soit une variété projective et $\mathcal{C}'$ contienne les sections hyperplanes de A'.

THÉORÈME 1. - Soient A et A' deux variétés abéliennes dans un espace projectif; soient $\mathcal{C}$ et $\mathcal{C}'$ respectivement les polarisations de A et de A' définies par les sections hyperplanes. Supposons que A et A' ne soient contenus dans aucun hyperplan et que les systèmes linéaires des sections hyperplanes de A et de A' soient complets. Alors, pour que $(A' , \mathcal{C}')$ soit isomorphe à $(A , \mathcal{C})$, il faut et il suffit que A' soit une transformée de A par une transformation projective.

Soit H un hyperplan de l'espace ambiant pour A et A' ; soient $Y = H.A$, $Y' = H.A'$. Supposons que A' soit une transformée de A par une transformation projective φ ; désignons par F l'application de A sur A' induite par φ. Il existe alors un isomorphisme λ de A sur A' et un point $b \in A'$ tel que l'on ait $F(x) = \lambda(x) + b$ pour $x \in A$. Soit a un point de A tel que l'on ait $b = - \lambda(a)$. On vérifie aisément que $\lambda^{-1}(Y') = F^{-1}(Y')_a$; ce dernier est algébriquement équivalent à $F^{-1}(Y')$. Comme Y' est une section hyperplane de A et comme F est induit par une transformation projective, on voit que $F^{-1}(Y')$ est une section hyperplane de A, de sorte que $F^{-1}(Y')$ est algébriquement équivalent à Y ; ceci démontre que $(A , \mathcal{C})$ est isomorphe à $(A' , \mathcal{C}')$. Réciproquement, supposons qu'il existe un isomorphisme ξ de $(A , \mathcal{C})$ sur $(A' , \mathcal{C}')$. D'après notre définition, il existe deux entiers positifs r, s tels que $r\,\xi^{-1}(Y')$ soit algébriquement équivalent à sY. Par suite, d'après le lemme 2 et le lemme 3, on a $r^n \ \ell(\mathcal{E}^{-1}(Y')) = s^n \ \ell(Y)$, où n est la dimension de A. D'autre part, on voit, en vertu de notre hypothèse, que $\ell(\mathcal{E}^{-1}(Y'))$ et $\ell(Y)$ sont égaux à $N + 1$, N étant la dimension de l'espace ambiant pour A. On a donc $r = s$; d'où résulte que $\mathcal{E}^{-1}(Y')$ est algébriquement équivalent à Y. D'après le lemme 2, il existe un point u de A tel que $\mathcal{E}^{-1}(Y')$ soit linéairement équivalent à Y_u ; il existe donc une fonction g sur A telle qu'on ait $(g) = \mathcal{E}^{-1}(Y')_{-u} - Y$. Soit $(X_o , \dots , X_N)$ le système des coordonnées de l'espace ambiant pour A et soient f_i , f'_i les fonctions sur A et sur A' induites par $X_i/\sum_j \gamma_j X_j$, respectivement, où $\sum_j \gamma_j X_j = 0$ est l'équation d'un hyperplan. Soit k un corps de définition pour A , A', $\mathcal{E}$ et g par rapport auquel u et les γ_j sont rationnels. D'après notre hypothèse, les f_i forment une base de $L(Y , k)$. Soit h_i la fonction sur A définie par $h_i(x) = f'_i(\mathcal{E}(x + u))\,g(x)$ par rapport à k , x étant un point générique de A par rapport à k. On vérifie facilement que $h_i \in L(Y , k)$, de sorte que les h_i s'expriment sous les formes $h_i = \sum_j \xi_{ij} f_j$ $(0 \leq i \leq N)$, où les ξ_{ij} sont des éléments de k. Comme les h_i sont linéairement indépendants sur k , la matrice (ξ_{ij}) est inversible. Soit x un point générique de A par rapport à k ; alors les $f_i(x)$ sont les coordonnées de x ; et de plus, on voit que les $h_i(x)$ sont les coordonnées de $\mathcal{E}(x + u)$. Il en résulte que A' est la transformée de A par la transformation projective donnée par la matrice (ξ_{ij}) ; ce qui complète la démonstration du théorème 1.

Soit V une variété algébrique dans l'espace projectif P^N de dimension N. Soient k un corps de définition pour V et (t_{ij}) une matrice de degré $N + 1$, dont les coordonnées sont $(N + 1)^2$ variables indépendantes sur k. Soient V' la transformée de V par la transformation projective $(a_i) \to (\sum_{j=0}^{N} t_{ij} a_j)$ où $(a_i) \in P^N$,et z le point de Chow de V'. Comme le corps $k(z)$ est contenu dans $k(t)$, $k(z)$ est une extension régulière de k ; donc on obtient une variété $\mathfrak{F}$ comme le lieu de z par rapport à k. On peut facilement vérifier que $\mathfrak{F}$ ne dépend que de V et non du choix de k et de (t). La variété $\mathfrak{F}$ s'appellera la <u>famille projective</u> de V. Soient V et V' deux variétés algébriques dans un espace projectif ; soient $\mathfrak{F}$ et $\mathfrak{F}'$ repectivement les familles projectives de V et de V'. Alors, pour que l'on ait $\mathfrak{F} = \mathfrak{F}'$, il faut et il suffit que V' soit une transformée de V par une transformation projective.

THÉORÈME 2. - <u>Soient</u> A <u>une variété abélienne dans un espace projectif,</u> C <u>la polarisation de</u> A <u>définie par les sections hyperplanes et</u> $\mathfrak{F}$ <u>la famille</u>

<u>projective de A. Supposons que A ne soit contenu dans aucun hyperplan et que le système linéaire des sections hyperplanes de A soit complet. Soient k un corps de définition pour A et σ un isomorphisme de k sur un corps k'. Alors, pour que l'on ait $\mathfrak{F}^{\sigma} = \mathfrak{F}$, il faut et il suffit que $(A^{\sigma}, \mathcal{C}^{\sigma})$ soit isomorphe à $(A, \mathcal{C})$.</u>

On vérifie facilement que $\mathfrak{F}^{\sigma}$ est la famille projective de A^{σ}. Alors le théorème 2 est une conséquence du théorème 1.

3. <u>Le corps du module d'une variété abélienne polarisée.</u>

Soit $(A, \mathcal{C})$ une variété abélienne polarisée, et soit $\mathcal{C}^*$ l'ensemble de tous les diviseurs amples dans $\mathcal{C}$. Chaque élément X de $\mathcal{C}^*$ définit une immersion birationnelle birégulière de A dans un espace projectif. Désignons par $\mathfrak{F}(A, X)$ la famille projective de l'image de cette immersion.

D'après le lemme 2, si X' est algébriquement équivalent à X, on a $\mathfrak{F}(A, X') = \mathfrak{F}(A, X)$.

PROPOSITION 1. - <u>Les notations étant comme ci-dessus, soient K et K' respectivement les plus petits corps de définition pour $\mathfrak{F}(A, X)$ et pour $\mathfrak{F}(A, mX)$, où m est un entier positif. Alors, K est une extension purement inséparable de K'. De plus, si la caractéristique p du corps de base ne divise pas m, on a $K = K'$.</u>

Soit z un point générique de $\mathfrak{F}(A, X)$ par rapport à K. D'après notre définition de la famille projective, z est le point de Chow d'une variété abélienne A_0 isomorphe à A. Soit X_0 une section hyperplane de A_0. On voit facilement $\mathfrak{F}(A, X) = \mathfrak{F}(A_0, X_0)$ et $\mathfrak{F}(A, mX) = \mathfrak{F}(A_0, mX_0)$. Comme A_0 est défini par rapport à $K(z)$ et comme A_0 n'est contenu dans aucun hyperplan, on peut prendre X_0 de telle façon qu'il soit rationnel par rapport à $K(z)$. Par suite $\mathfrak{F}(A_0, mX_0)$ est défini par rapport à $K(z)$; d'où résulte qu'on a $K(z) \supset K'$. Soit σ un isomorphisme de $K(z)$ sur un corps, qui est l'identité sur K. On a alors $\mathfrak{F}(A, X)^{\sigma} = \mathfrak{F}(A, X)$; d'après le théorème 2, $(A, \mathcal{C})$ est isomorphe à $(A^{\tau}, \mathcal{C}^{\tau})$; où τ est une prolongation de σ. D'après le même théorème on a $\mathfrak{F}(A, mX)^{\sigma} = \mathfrak{F}(A, mX)$; donc σ est l'identité sur K'. On en déduit que le corps composé KK' est une extension purement inséparable de K. D'après la même raison, KK' est purement inséparable sur K'. Comme $K(z)$ est régulier sur K, on doit avoir $KK' = K$; ce qui démontre la première assertion de la proposition. Supposons maintenant que la caractéristique p ne divise pas m. Soit z' un point générique de $\mathfrak{F}(A, mX)$ par rapport à K' ; il existe une variété abélienne A' dont le point de Chow est z'. Soit Y une section hyperplane de A' rationnelle par rapport à $K'(z')$. D'après notre construction, il existe un diviseur X' sur A' tel que mX' soit algébriquement équivalent à Y. On peut facilement démontrer qu'il existe un corps k séparablement engendré sur $K'(z')$ et une puissance p^r de p tels que $p^r X'$ soit rationnel par rapport à k. Comme m et p^r sont premiers entre eux, il existe deux entiers a, b tels qu'on ait $am + bp^r = 1$; alors $aY + b(p^r X')$ est algébriquement équivalent à X' ; et l'on voit facilement

$$\mathfrak{F}(A', aY + b(p^r X')) = \mathfrak{F}(A', X') = \mathfrak{F}(A, X) .$$

Comme $aY + b(p^r X')$ est rationnel par rapport à k, $\mathfrak{F}(A, X)$ est défini par rapport à k ; il en résulte qu'on a $k \supset K$. D'autre part, k est séparablement engendré sur K' ; on peut en conclure $K = K'$, car on a vu plus haut que K est purement inséparable sur K'.

Soient les notations $(A, \mathcal{C})$, $\mathcal{C}^*$, $\mathfrak{F}(A, X)$ comme ci-dessus. On peut démontrer qu'il existe un diviseur Y sur A tel que tout X dans $\mathcal{C}$ soit algébriquement équivalent à un multiple mY, où m est un entier positif. Soit K_m le corps minimum de définition pour $\mathfrak{F}(A, mY)$ pour chaque entier positif m tel que mY soit ample. Soient m et m' deux entiers positifs tels que mY et $m'Y$ soient amples. Il existe un entier positif s tel que $smm'Y$ soit ample ; où l'on peut supposer que p ne divise pas s. D'après la proposition 1, les corps K_m et $K_{m'}$ sont des extensions purement inséparables de $K_{smm'}$; d'après la même proposition, si p ne divise pas m, on a $K_{m'} = K_{smm'}$, de sorte qu'alors K_m est une extension purement inséparable de $K_{m'}$. Par suite, si p ne divise ni m, ni m', on a $K_m = K_{m'}$. Nous appellerons ce même corps le <u>corps du module</u> de la variété abélienne polarisée $(A, \mathcal{C})$; le corps du module K est une extension purement inséparable de K_m pour tout m ; et l'on a $K = K_m$ si la caractéristique p ne divise pas m. Soient k un corps de définition pour $(A, \mathcal{C})$ contenant K et σ un isomorphisme de k sur un corps k' ; d'après le théorème 2, pour que $(A, \mathcal{C})$ soit isomorphe à $(A^\sigma, \mathcal{C}^\sigma)$, il faut et il suffit que σ soit l'identité sur K. Dans le cas où la caractéristique est 0, le corps du module K est déterminé par cette propriété ; on a $K = K_m$ pour chaque m ; donc, K est engendré par le point de Chow de $\mathfrak{F}(A, mY)$ sur le corps Q des nombres rationnels, pour tout m. De toute façon, on verrait, dans le théorème 1, que les points de Chow des $\mathfrak{F}(A, mY)$ peuvent être regardés, sans restriction pour la caractéristique, comme des "modules" de $(A, \mathcal{C})$.

4. Variétés de Kummer.

Soient $(A, \mathcal{C})$ une variété abélienne polarisée et G le groupe des automorphismes de $(A, \mathcal{C})$; on peut démontrer que G est d'ordre fini. Nous entendrons par une variété de Kummer de A une variété quotient de A par rapport à G, c'est-à-dire un couple (W, h) formé d'une variété W et d'une application rationnelle h de A sur W jouissant des propriétés suivantes :

1° h est défini partout sur A ;

2° $h = h \circ \gamma$ pour tout $\gamma \in G$;

3° si h' est une application rationnelle de A sur une variété W' satisfaisant à $h' = h' \circ \gamma$ pour tout $\gamma \in G$, il existe une application rationnelle g de W sur W' telle que l'on ait $h' = g \circ h$ et que g soit défini en tout point $h(a)$ pour lequel h' est défini en a.

Il existe toujours un tel (W, h) (SERRE [2]) ; on peut construire W comme une variété projective. De plus, on peut démontrer, en vertu des résultats dans WEIL [3], qu'il existe une variété de Kummer (W, h) satisfaisant aux conditions suivantes (MATSUSAKA [1]):

(W1) W est défini sur le corps K du module de $(A, \mathcal{C})$.

(W2) h est défini sur tout corps de définition pour $(A, \mathcal{C})$ contenant K.

(W3) Si σ est un isomorphisme d'un corps de définition pour $(A, \mathcal{C})$ contenant K, et si λ est un isomorphisme de $(A, \mathcal{C})$ sur $(A^{\sigma}, \mathcal{C}^{\sigma})$, on a $h = h^{\sigma} \circ \lambda$.