ANDRÉ WEIL

Multiplication complexe des fonctions abéliennes

Séminaire N. Bourbaki, 1956, exp. n° 136, p. 381-387

<http://www.numdam.org/item?id=SB_1954-1956__3__381_0>

Séminaire BOURBAKI
(Mai 1956)

MULTIPLICATION COMPLEXE DES FONCTIONS ABÉLIENNES

par André WEIL

Cet exposé fait suite à celui de P. SAMUEL [1].

L'application de la méthode de Shimura-Taniyama aux variétés abéliennes repose sur la notion de variété polarisée. Sur une variété V, complète et non-singulière (ou du moins non-singulière en codimension 1) on considère la relation d'équivalence suivante entre diviseurs X, X' : "il existe deux entiers m, m', tous deux >0, tels que mX soit algébriquement équivalent à $m'X'$ ". On dit qu'une classe C, pour cette relation, détermine une <u>polarisation</u> de V si elle contient au moins un système linéaire "ample", c'est-à-dire s'il existe un plongement de V dans un espace projectif tel que les sections hyperplanes de V pour ce plongement appartiennent à C. Se donner une polarisation sur une variété abélienne dans le cas classique (où le domaine universel est le corps des complexes) équivaut à se donner sur elle une matrice de Riemann, étant entendu que deux matrices de Riemann déterminent la même polarisation si elles ne diffèrent l'une de l'autre que par un facteur rationnel, et dans ce cas seulement. Une jacobienne de courbe admet une polarisation canonique (déterminée par le "diviseur canonique", qui est bien défini à une translation près). MATSUSAKA a démontré que les automorphismes d'une variété abélienne <u>polarisée</u> sont en nombre fini (alors que les automorphismes d'une variété abélienne, qui sont les éléments inversibles de son anneau d'endomorphismes, peuvent former un groupe infini).

Désormais A désignera une variété abélienne polarisée de dimension n. On notera $\mathfrak{a}(A)$, ou simplement $\mathfrak{a}$, son anneau d'endomorphismes (c'est-à-dire celui de la variété abélienne sous-jacente) ; on sait que le groupe additif des éléments de $\mathfrak{a}$ est abélien libre de type fini ; on notera $\mathfrak{a}_0(A)$, ou $\mathfrak{a}_0$, l'anneau $\mathfrak{a}(A) \otimes \mathbf{Q}$; c'est une algèbre semi-simple de rang fini sur $\mathbf{Q}$. La polarisation de A détermine (canoniquement) un antiautomorphisme involutif de $\mathfrak{a}_0$, noté $\alpha \to \alpha'$, qui, dans le cas d'une jacobienne polarisée canoniquement, n'est autre que l'antiautomorphisme bien connu, dit de Rosati. On définit, canoniquement aussi, sur $\mathfrak{a}_0$, une "trace" σ, c'est-à-dire une forme $\mathbf{Q}$-linéaire, à valeurs entières sur $\mathfrak{a}$, telle que $\sigma(\alpha\beta) = \sigma(\beta\alpha)$; on a $\sigma(\alpha\alpha') > 0$ pour tout $\alpha \neq 0$ dans $\mathfrak{a}_0$ (ce qui généralise le "théorème de Castelnuovo").

L'anneau $\mathfrak{A}$ opère d'une manière évidente sur l'algèbre de Lie de A , c'est-à-dire sur l'espace vectoriel tangent à A en 0 ; dans le cas "classique" (où la caractéristique p est 0), c'est là une représentation fidèle, et on peut l'étendre à une représentation R_o de $\mathfrak{A}_o$; si σ_o est la trace de celle-ci, on a $\sigma = \sigma_o + \bar{\sigma}_o$.

On démontre que toute sous-algèbre commutative semi-simple de $\mathfrak{A}_o$, de rang $\geqslant 2n$ sur $\mathbb{Q}$, est de rang 2n sur $\mathbb{Q}$ et est son propre commutant dans $\mathfrak{A}_o$, ce qui implique qu'elle contient le centre de $\mathfrak{A}_o$; il en est ainsi, en particulier, de tout corps commutatif, de degré $\geqslant 2n$ sur $\mathbb{Q}$, contenu dans $\mathfrak{A}_o$. Supposons que $\mathfrak{A}_o$ contienne un corps K de degré 2n sur $\mathbb{Q}$; on démontre qu'alors A est isogène à un produit de la forme $B \times B \times \ldots \times B$, où B est une variété abélienne simple telle que $\mathfrak{A}_o(B)$ contienne un corps de degré $2\dim(B)$.

Laissant désormais le cas général de côté, on se bornera au cas où A est une variété simple. Si la caractéristique est 0 , et que $\mathfrak{A}_o$ contienne un corps K de degré 2n sur $\mathbb{Q}$, on démontre que $\mathfrak{A}_o = K$ et que K est extension quadratique totalement imaginaire d'un corps totalement réel k . Alors la représentation R_o est somme directe de n isomorphismes $\varphi_1, \ldots, \varphi_n$ de K dans le domaine universel, ceux-ci étant tels qu'ils induisent sur k <u>tous</u> les isomorphismes distincts de k dans le domaine universel. Par une CM-extension d'un corps totalement réel k , de degré n sur $\mathbb{Q}$, on entendra l'objet composite (Chevalley) $(K; \{\varphi_\lambda\}_{1 \leq \lambda \leq n})$ formé d'une extension quadratique totalement imaginaire K de k , et de n isomorphismes φ_λ de K dans $\bar{\mathbb{Q}}$ (clôture algébrique de $\mathbb{Q}$) induisant sur k tous les isomorphismes distincts de k dans $\bar{\mathbb{Q}}$. Pour fixer les idées, supposons que le domaine universel soit $\mathbb{C}$; alors on peut écrire K sous la forme $k(\zeta)$, où ζ est tel que $-\zeta^2$ soit totalement positif dans k et que $-i\varphi_\lambda(\zeta) > 0$ quel que soit λ ; cette condition détermine ζ d'une manière unique à un facteur totalement positif près dans k ; quand ζ est tel, on conviendra de noter $k((\zeta))$ la CM-extension en question. Celle-ci sera dite <u>primitive</u> si on ne peut pas l'écrire sous la forme $k((\zeta_1))$, où ζ_1 est tel que $\mathbb{Q}(\zeta_1) \neq k$. Comme on l'a vu, si une variété abélienne simple A de dimension n est telle que $\mathfrak{A}_o(A)$ contienne un corps K de degré $\geqslant 2n$ sur $\mathbb{Q}$ (en caractéristique 0), alors $\mathfrak{A}_o(A) = K$, K est extension quadratique totalement imaginaire d'un corps k totalement réel de degré n sur $\mathbb{Q}$, et K et sa représentation R_o déterminent une CM-extension de k ; de plus, l'hypothèse que A est simple entraîne que cette CM-extension est primitive. Réciproquement, au moyen de la théorie classique des fonctions abéliennes, on démontre qu'à toute CM-extension primitive d'un corps totalement réel de degré n correspond une classe (ou, comme on dit, une "catégorie") de variétés abéliennes simples, toutes isogènes les unes aux autres, pour lesquelles les conditions ci-dessus sont vérifiées. En gros, la théorie de la multiplication complexe se propose de déterminer, pour une CM-extension donnée :

(a) le plus petit corps sur lequel on puisse définir une variété abélienne admettant (au sens ci-dessus) cette CM-extension ;

(b) les extensions de ce plus petit corps déterminées par les points d'ordre fini sur ces variétés. Ainsi formulé, le problème est mal posé, mais, en le modifiant quelque peu, il acquiert un sens précis.

En premier lieu, il convient de se prescrire, non seulement la CM-extension $(K ; \{\varphi_\lambda\})$, mais aussi l'anneau $\mathfrak{a}$, qui est ici un sous-anneau de l'anneau $\mathfrak{o}$ des entiers de K (un "ordre" de K au sens de Dedekind). Il se trouve que les "ordres" des corps quadratiques ont des propriétés très particulières, qu'on exploite de son mieux dans la multiplication complexe "classique", celle des fonctions elliptiques ; grâce à cela, on a, pour $n = 1$, une théorie qui s'applique à tout ordre de tout corps quadratique imaginaire. Pour n quelconque, on n'a traité jusqu'ici que le cas $\mathfrak{a} = \mathfrak{o}$; il n'y a d'ailleurs aucune raison de penser que le cas général présente des difficultés insurmontables, et SHIMURA et TANIYAMA sont en train de s'y attaquer. La variété étant supposée polarisée, ses automorphismes sont les racines de l'unité dans K (sinon ce seraient toutes les unités de K). On appelle variété de Kummer associée à A le quotient de A par son groupe d'automorphismes (c'est là une surface de Kummer, au sens classique, si $n = 2$ et si K ne contient pas d'autre racine de l'unité que ± 1) ; on la polarise par passage au quotient à partir de la polarisation de A. Pour $n \geqslant 2$, cette variété détermine A d'une manière unique, à un isomorphisme près (ceci, parce que A a été supposée simple) ; il n'en est plus ainsi pour $n = 1$ (la variété de Kummer n'étant autre en ce cas qu'une droite projective), et il y a lieu de la munir d'une structure plus riche que celle de variété algébrique (structure de "V-variété" au sens de Satake), après quoi elle détermine encore A d'une manière unique.

Cela posé, soit k_t le plus petit corps dans lequel on puisse écrire la représentation R_o de K ; c'est le corps engendré par les traces $\sum_\lambda \varphi_\lambda(\xi)$ de cette représentation, quand ξ parcourt K. Par application de théorèmes généraux sur le plus petit corps de définition d'une variété qui n'est donnée qu'à un isomorphisme près sur le domaine universel (voir A. WEIL [5]), on trouve qu'il y a un plus petit corps K_0 contenant k_t sur lequel on puisse définir une variété isomorphe à la variété de Kummer déduite de A dans les conditions décrites ci-dessus ; c'est là une conséquence du fait qu'on a obtenu cette variété en divisant A par le groupe de tous ses automorphismes (c'est bien pour cela qu'il a fallu polariser A , afin que ce groupe soit fini). De plus, les mêmes théorèmes généraux montrent que K_0 est extension algébrique finie de k_t . On se propose de déterminer K_0 .

Pour cela, on observe d'abord que, comme on est en caractéristique 0 , la polarisation de A équivaut à la donnée d'une matrice de Riemann, bien déterminée à un facteur près ; ainsi, parmi toutes les matrices de Riemann qui appartiennent à cette polarisation, il y en a une, qui sera dite basique, dont toutes les autres sont des multiples entiers ; celle-ci déterminera un homomorphisme λ de A sur sa variété duale A^* . Comme d'habitude, on note $\mathcal{H}(A , A^*)$ le groupe additif des homomorphismes de A dans A^* , qui ici est visiblement un module sur l'anneau $\mathfrak{A} = \mathfrak{o}$; on sait que ce groupe est abélien libre de type fini, donc qu'il se laisse plonger dans le produit tensoriel $\mathcal{H}_0(A , A^*) = \mathcal{H}(A , A^*) \otimes \mathfrak{Q}$, qui ici est un espace vectoriel sur le corps K . Cela posé, l'ensemble des $\xi \in K$ tels que $\xi\lambda \in \mathcal{H}(A , A^*)$ est évidemment un idéal (fractionnaire) dans K ; on trouve qu'il est de la forme $\mathfrak{T}_0^{-1}\mathfrak{o}$, où $\mathfrak{T}_0$ est un idéal dans l'anneau des entiers du corps k . Dans ces conditions, si une variété polarisée A , appartenant à la CM-extension $(K ; \{\varphi_\lambda\})$ et admettant $\mathfrak{o}$ pour anneau d'endomorphismes, est définie sur une extension algébrique de k_t , tous ses conjugués sur k_t détermineront le même idéal $\mathfrak{T}_0$. On peut donc se borner à considérer celles de ces variétés pour lesquelles $\mathfrak{T}_0$ est un idéal donné.

Soit A , A' deux telles variétés ; sur chacune, considérons la matrice de Riemann basique ; en vertu de la théorie des variétés abéliennes, celle-ci déterminera (sur A , resp. sur A') un système linéaire complet de diviseurs positifs ; soit X resp. X' un de ces diviseurs ; X détermine un homomorphisme φ_X de A sur sa duale A^* (c'est le même que le λ de tout à l'heure). Soit μ un homomorphisme de A dans A' ; soit $Y = \mu^{-1}(X')$; on montre qu'il y a un entier totalement positif $f(\mu)$ dans k , tel que $\varphi_Y = f(\mu)\varphi_X$. D'ailleurs, le groupe $\mathcal{H}(A , A')$ des homomorphismes de A dans A' est un module sur $\mathfrak{o}$, dont on montre facilement qu'il est "de rang 1", autrement dit isomorphe à un idéal $\mathfrak{a}$ de K (naturellement, $\mathfrak{a}$ n'est pas déterminé d'une manière unique ; mais sa classe l'est, au sens habituel de l'équivalence des idéaux). Comme $f(\mu)$ satisfait à la condition $f(\xi\mu) = \xi\bar{\xi}f(\mu)$ pour tout $\xi \in \mathfrak{o}$, la fonction f, transportée à $\mathfrak{a}$ par transport de structure, s'écrira sur $\mathfrak{a}$ sous la forme $\rho\alpha\bar{\alpha}$, où ρ est dans k et totalement positif ; du fait qu'on a supposé que A, A' déterminent le même idéal $\mathfrak{T}_0$, il résulte de plus que $\rho\alpha\bar{\alpha} = \mathfrak{o}$. On dira que $\rho\alpha\bar{\alpha}$ est une forme hermitienne positive sur $\mathfrak{a}$; on dira que deux formes hermitiennes, $\rho\alpha\bar{\alpha}$, $\rho\beta\bar{\beta}$, définies respectivement sur des idéaux $\mathfrak{a}$, $\mathfrak{b}$, sont équivalentes s'il y a un isomorphisme du $\mathfrak{o}$-module $\mathfrak{a}$ sur le $\mathfrak{o}$-module $\mathfrak{b}$ qui transforme la première en la seconde, c'est-à-dire s'il y a $\xi \in K$ tel que $\mathfrak{b} = \xi\mathfrak{a}$, $\sigma = (\xi\bar{\xi})^{-1}\rho$; la classe de la forme $\rho\alpha\bar{\alpha}$ sur $\mathfrak{a}$ sera notée $(\mathfrak{a}; \rho)$. Il est clair que, si $\mathfrak{a}$ et ρ sont définis comme on a dit ci-dessus à partir des variétés A, A', la classe $(\mathfrak{a}; \rho)$ est définie d'une manière unique ; on la notera $\{A : A'\}$; pour que A, A' soient isomorphes, il faut et il suffit que cette classe soit $(\mathfrak{o}; 1)$. Pour la loi de composition

$$(\mathfrak{a}; \rho).(\mathfrak{a}'; \rho') = (\mathfrak{a}\mathfrak{a}'; \rho\rho') \quad ,$$

les classes de formes pour lesquelles on a $\rho\alpha\bar{\alpha} = \mathfrak{o}$ forment un groupe abélien fini.

Cela posé, le symbole $\{A : A'\}$ permet de mesurer l'effet, sur une variété abélienne du type considéré, d'un automorphisme quelconque (laissant k_t invariant) du corps de tous les nombres algébriques. En effet, si A, A', A'' appartiennent aux données ci-dessus (la CM-extension $(K ; \{\varphi_\lambda\})$, l'anneau $\mathfrak{o}$, et l'idéal $\mathfrak{T}_0$), on aura

$$\{A : A'\}.\{A' : A''\} = \{A : A''\} \quad ;$$

et le symbole $\{A : A'\}$ ne change pas si on applique à un corps de définition commun de A et de A' un isomorphisme quelconque laissant k_t invariant. Si, pour fixer les idées, on suppose A définie sur une extension galoisienne de k_t (qui doit nécessairement contenir K_0 en vertu de la définition de K_0), de groupe de Galois G sur k_t, on aura :

$$\{A^\sigma : A\} = \{A^{\sigma\tau} : A^\tau\}$$

quels que soient σ, τ dans G, d'où résulte que $\sigma \to \{A^\sigma : A\}$ est un homomorphisme de G dans le groupe Γ des classes $(\mathfrak{a}; \rho)$. Si N est le noyau de cet homomorphisme, on voit que $\sigma \in N$ est une condition nécessaire et suffisante pour que A^σ soit isomorphe à A. On conclut de là, par des raisonnements purement formels, que K_0 n'est autre que l'extension de k_t

qui correspond au sous-groupe N de G ; K_o est donc abélien sur k_t , et son groupe de Galois sur k_t peut être identifié à un sous-groupe du groupe des classes $(\mathfrak{a} ; \rho)$.

Pour déterminer K_o exactement, il suffit, en vertu de la théorie du corps de classes, de connaître la substitution de Frobenius pour presque tous les idéaux premiers de k_t . C'est ici qu'intervient la théorie de Shimura ; celle-ci montre, en effet, que, pour presque tous les idéaux premiers $\mathfrak{p}$ d'un corps de définition de A , on peut faire un calcul de ce genre après réduction modulo $\mathfrak{p}$ (les variétés abéliennes considérées restent telles, un homomorphisme d'une variété dans une autre reste tel, etc.). Dans ces conditions, le calcul de la substitution de Frobenius se réduit, après réduction modulo $\mathfrak{p}$, à un problème de géométrie algébrique, qui a été résolu par TANIYAMA. Le résultat est le suivant : si $\mathfrak{p}$ est un idéal premier de k_t , de norme q , sa substitution de Frobenius est $(\mathfrak{q}^{-1} ; q)$, où $\mathfrak{q}$ est un certain idéal entier de K , satisfaisant à $\mathfrak{q}\bar{\mathfrak{q}} = q\mathfrak{o}$. D'une manière précise, il se trouve que k_t est aussi (tout comme K) extension quadratique purement imaginaire d'un corps totalement réel k' , et que la donnée de la CM-extension $(K ; \{\varphi_\lambda\})$ de k détermine complètement une CM-extension (primitive, elle aussi) $(k_t ; \{\psi_\mu\})$ de k' ; il y a d'ailleurs réciprocité entre ces CM-extensions. Dans ces conditions, on a $\mathfrak{q} = \prod_\mu \psi_\mu(\mathfrak{p})$. On en conclut en particulier que K_o est une extension abélienne non ramifiée de k_t . Pour $n = 1$, K est un corps quadratique imaginaire ; on a $k_t = k$; et K_o est l'extension abélienne non ramifiée maximale de k_t ("corps de Hilbert") ; on retrouve bien les résultats de la théorie classique. Déjà pour $n = 2$, HECKE, qui avait étudié la question au moyen de la théorie des fonctions modulaires ("groupe de Hilbert") avait constaté, d'abord, avec stupéfaction, qu'en général k_t diffère de K , et ensuite, avec consternation, que K_o n'est pas le corps de Hilbert de k_t . C'est comme ça, on n'y peut rien.

Ayant résolu le problème de la détermination de K_o (solution provisoirement restreinte au cas $\mathfrak{a} = \mathfrak{o}$, et qu'il reste à étendre au cas où $\mathfrak{a}$ est un ordre quelconque du corps K), on aborde le problème suivant : soit u un point d'ordre fini sur la variété A (satisfaisant toujours aux mêmes conditions) ; par "ordre" de u , il conviendra d'entendre l'idéal $\mathfrak{a}$ de $\mathfrak{o}$ formé des $\nu \in \mathfrak{o}$ tels que $\nu u = 0$; on demande de déterminer le corps engendré sur K_o par l'image de u sur la variété de Kummer de A , celle-ci étant prise définie sur K_o . La solution (toujours en se bornant au cas $\mathfrak{a} = \mathfrak{o}$) est exactement semblable à la précédente ; le résultat aussi. On obtient des extensions abéliennes de k_t , ramifiées, bien entendu.

Comme SAMUEL l'a indiqué, TANIYAMA a aussi obtenu, chemin faisant, la détermination complète des fonctions dzêta des variétés abéliennes en question (résultat qui n'avait été obtenu que tout récemment, par DEURING, pour le cas $n = 1$ de la multiplication complexe classique).

Les méthodes ci-dessus n'ont pas encore permis de retrouver le résultat classique d'après lequel les valeurs de l'invariant absolu j , pour les corps de fonctions elliptiques à multiplication complexe, sont des entiers algébriques ; la difficulté tient à ce qu'il faudrait pour cela réduire modulo tout idéal premier d'un corps convenable (et non pas seulement modulo presque tout idéal premier). Naturellement, il y aurait lieu de formuler et de démontrer aussi le résultat correspondant pour les variétés abéliennes. Signalons enfin que l'étude des variétés abéliennes non supposées simples, à multiplication complexe, devrait donner des résultats intéressants (nullement contenus dans la théorie des variétés simples).

La morale de cette histoire, c'est que la géométrie algébrique a atteint un degré de développement où elle fournit des moyens de travail plus puissants que l'analyse (théorie des fonctions automorphes) pour l'étude des questions qui sont justifiables de l'une et de l'autre.

BIBLIOGRAPHIE

[1] SAMUEL (Pierre). - Travaux de Shimura et Taniyama sur la multiplication complexe, Séminaire Bourbaki, t. 8, 1955/56.

[2] SHIMURA (Gorô). - On complex multiplication, Symposium on algebraic number theory [1955. Tokyo et Nikko] . - Tokyo, Science Council of Japan, 1956 ; p. 23-30.

[3] TANIYAMA (Yutaka). - Jacobian varieties and number fields, Symposium on algebraic number theory [1955. Tokyo et Nikko] . - Tokyo, Science Council of Japan, 1956 ; p. 31-45.

[4] WEIL (André). - On a certain type of characters of the idèle-class group of an algebraic number-field, Symposium on algebraic number theory [1955. Tokyo et Nikko] . - Tokyo, Science Council of Japan, 1956 ; p. 1-7.

[5] WEIL (André). - The field of definition of a variety, Amer. J. Math., t. 78, 1956, p. 509-524.