SÉMINAIRE N. BOURBAKI

PIERRE SAMUEL

Travaux de Shimura et Taniyama sur la multiplication complexe

Séminaire N. Bourbaki, 1956, exp. n° 129, p. 315-322

<http://www.numdam.org/item?id=SB_1954-1956__3__315_0>

Séminaire BOURBAKI
(Février 1956)

TRAVAUX DE SHIMURA ET TANIYAMA SUR LA MULTIPLICATION COMPLEXE

par Pierre SAMUEL

On sait que certaines courbes elliptiques E admettent d'autres transformations birationnelles sur elles-mêmes que celles que tout le monde connaît (c'est-à-dire autres que les applications $x \to a + x$ et $x \to b - x$, la courbe étant munie de sa structure de variété abélienne); dans le cas classique ces courbes ont pour modèles les cubiques harmoniques ($y^2 = x(x^2 - 1)$), et équianharmonique ($y^2 = x^3 - 1$). Ceci implique que l'anneau $\mathfrak{A}(E)$ des endomorphismes (rationnels) de E contient d'autres éléments que les endomorphismes $x \to nx$ ($n \in Z$). L'hypothèse $\mathfrak{A}(E) \neq Z$ implique que $\mathfrak{A}(E)$ est isomorphe à un sous-anneau $\neq Z$ de l'anneau des entiers algébriques d'un corps imaginaire quadratique K, et qu'on obtient ainsi tous les sous-anneaux $\neq Z$ de tous corps imaginaires quadratiques (les cas particuliers des courbes admettant des transformations birationnelles non triviales sont ceux où K admet des unités $\neq 1, -1$, c'est-à-dire $K = Q(i)$ et $K = Q(j)$ ($j^3 = 1$)). Cette circonstance permet d'étudier les extensions abéliennes d'un corps imaginaire quadratique K, et de développer ainsi la théorie du corps de classes sur K (historiquement ce cas particulier de la théorie du corps de classes a été traité avant le cas général). Dans leurs travaux SHIMURA et TANIYAMA ([2],[4]) considèrent la situation plus générale suivante : on a un corps de nombres algébriques de degré pair 2n sur Q et une variété abélienne A de dimension n dont l'anneau d'endomorphismes contient l'anneau R des entiers de K. Dans ces conditions il est utile de savoir "réduire" la variété" abélienne A et divers objets s'y rattachant (anneau d'endomorphismes par exemple) modulo les idéaux premiers d'un corps de définition de A.

1. Généralités sur la réduction modulo $\mathfrak{p}$ (cf. [3]).

Soient k un corps, v une valuation dicrète de k, $\mathfrak{o}$ son anneau, $\mathfrak{p}$ son idéal maximal, $r(k)$ le corps quotient $\mathfrak{o}/\mathfrak{p}$, et V un k-ensemble algébrique (affine ou projectif). En réduisant mod $\mathfrak{p}$ les polynômes de l'idéal $\mathfrak{J}$ de V (ou plutôt ceux de $\mathfrak{J} \cap \mathfrak{o}[X]$), on obtient un idéal $r(\mathfrak{J})$ de $r(k)[X]$; l'ensemble algébrique correspondant s'appelle l'ensemble algébrique <u>réduit</u> de V mod $\mathfrak{p}$. Il est fort simple d'aller un peu plus loin lorsque V est une variété de codimension 1 : en effet son idéal $\mathfrak{J}$ est alors principal, et peut être engendré par un polynôme $F(X)$ dont tous les coefficients sont dans $\mathfrak{o}$ mais pas

tous dans $\mathfrak{p}$; alors l'idéal réduit $r(\mathfrak{J})$ est engendré par le polynôme réduit $r(F)(X)$; la décomposition de celui-ci en facteurs irréductibles $r(F) = \prod_i G_i^{n(i)}$ permet d'associer à l'idéal $r(\mathfrak{J})$ le cycle $r(V) = \sum_i n(i)W_i$ (W_i : variété d'équation $G_i(X) = 0$) ; on appelle $r(V)$ le cycle réduit de V modulo $\mathfrak{p}$. Cette notion s'étend aussitôt par linéarité aux cycles de codimension 1.

Etant donnée une variété (ou un cycle V) de dimension quelconque, divers procédés équivalents permettent d'associer à V un cycle réduit mod $\mathfrak{p}$. On peut utiliser la technique des "multiplicités de spécialisations" d'A. WEIL (cf. [6] F-III$_4$). Dans le cas projectif on peut aussi réduire mod $\mathfrak{p}$ la forme de Chow de V ; on obtient la forme de Chow de $r(V)$. Le cycle $r(V)$ a même dimension (et même degré dans le cas projectif) que V. Le procédé de réduction mod $\mathfrak{p}$ s'étend aux cycles d'une variété abstraite ambiante $U = (U_\alpha , F_\alpha , T_{\alpha\beta})$ pourvu que U se réduise bien c'est-à-dire que les $r(U_\alpha)$ soient des variétés et les $r(T_{\alpha\beta})$ des correspondances birationnelles qui soient birégulières là où il faut.

La réduction des cycles mod $\mathfrak{p}$ jouit de propriétés analogues à celles de la spécialisation des cycles (cette notion, étudiée par MATSUSAKA et le conférencier, est d'ailleurs essentiellement la même chose que la réduction mod $\mathfrak{p}$ dans le cas d'égales caractéristiques). Plus précisément elle est compatible avec les opérations sur les cycles (addition, projection algébrique, produit cartésien, produit d'intersection). Par exemple si deux cycles X et Y rationnels sur k sont tels que $X.X$ et $r(X).r(Y)$ soient définis, alors on a $r(X.Y) = r(X).r(Y)$..

LEMME utile et facile. - Soient A et B deux variétés complètes telles que $r(A)$ et $r(B)$ soient des variétés, et soit G le graphe d'une application rationnelle de A dans B ; alors $r(G)$ est le graphe d'une apllication rationnelle de $r(A)$ dans $r(B)$ (+ composantes verticales).

En particulier soit A une variété abélienne (définie sur k); supposons que $r(A)$ soit une variété. Le lemme nous fournit des applications rationnelles $r(A)xr(A) \longrightarrow r(A)$ et $r(A) \longrightarrow r(A)$ réduites de l'addition et du passage à l'opposé. Si ces applications sont partout régulières, on dit que A est sans défaut pour $\mathfrak{p}$; ces applications munissent alorq $r(A)$ d'une structure de variété abélienne.

Soit A et B deux variétés abéliennes sans défaut pour $\mathfrak{p}$, et λ un homomorphisme de A dans B. Le lemme nous fournit une application $r(\lambda)$ de $r(A)$ dans $r(B)$, qui est évidemment un homomorphisme. On obtient ainsi une application r :

$$\mathrm{Hom}(A , B) \longrightarrow \mathrm{Hom}(r(A) , r(B)) ,$$

qui est, bien sûr, un homomorphisme ; la considération de la dimension de

$$r(\lambda)(r(A)) = r(\lambda(A))$$

montre aisément que r est un monomorphisme. La conservation des degrés par réduction montre que l'on a $\gamma(r(\lambda)) = \gamma(\lambda)$ (voir dans 2 la définition du symbole γ). Enfin, si l'on note $\mathcal{O}(A)$ l'anneau des endomorphismes de A, le monomorphisme r :

$$\mathcal{O}(A) \longrightarrow \mathcal{O}r(A))$$

est un monomorphisme pour les structures d'anneaux.

Considérons enfin une famille de valuations (v_α) de k telle que, pour tout $x \neq 0$ dans k, on ait $v_\alpha(x) = 0$ pour presque tout α (par exemple la famille des valuations d'un anneau de Dedekind) ; soit r_α l'opération de réduction correspondant à v_α. Si $F(X)$ est un polynôme absolument irréductible, on montre que le polynôme réduit $r_\alpha(F)(X)$ est absolument irréductible pour presque tout α ; on en déduit que, si V est une variété, alors $r_\alpha(V)$ est une variété pour presque tout α. On montre aussi qu'une variété abélienne A est sans défaut pour presque tout α (résultat déjà obtenu par NERON et par MATSUSAKA dans le cas d'égales caractéristiques, c'est-à-dire dans leurs études sur les familles algébriques de variétés abéliennes). De plus, si A est la jacobienne d'une courbe C, alors $r_\alpha(A)$ est la jacobienne de $r_\alpha(C)$ pour presque tout α.

2. Endomorphismes des variétés abéliennes.

Nous complétons ici les résultats exposés par NERON ([1]). Pour plus de détails voir [6].

Etant données deux variétés abéliennes A et B, le groupe $\mathrm{Hom}(A, B)$ des homomorphismes (rationnels, cela va sans dire) de A dans B est un groupe abélien libre de type fini ([6]; théorème 37) ; en particulier l'anneau $\mathcal{O}(A)$ des endomorphismes de A, dont le rang est d'ailleurs majoré par 4 $\dim(A)^2$. L'algèbre étendue $\mathcal{O}_0(A) = \mathcal{O}(A)_{\mathbb{Q}}$ est une $\mathbb{Q}$-algèbre semi-simple. Voici sa structure. On représente A comme un produit de variétés abéliennes simples (c'est-à-dire sans sous-variétés abéliennes non triviales), ce qui est toujours possible, en vertu du théorème de complète réductibilité de Poincaré ([6]) à un "isogénisme" près (rappelons que deux variétés abéliennes A, B sont dites isogènes s'il existe des épimorphismes de A sur B et de B sur A) ; ainsi A est isogène à

$$(A_{1,1} \times \cdots \times A_{1,n(1)}) \times (A_{2,1} \times \cdots \times A_{2,n(2)}) \times \cdots \times (A_{h,1} \times \cdots \times A_{h,n(h)})$$

$A_{i,j}$ et $A_{i',j'}$ étant isogènes si et seulement si $i = i'$. Alors :

1° $\mathfrak{A}_0(A)$ est isomorphe au produit des $\mathfrak{A}_0(A_{i,1} \times \dots \times A_{i,n(i)})$, $(i = 1 , \dots , h)$

2° $\mathfrak{A}_0(A_{i,1} \times \dots \times A_{i,n(i)})$ est isomorphe à l'anneau des matrices carrées d'ordre $n(i)$ sur $\mathfrak{A}_0(A_{i,1})$, lequel est un corps (commutatif ou non).

Pour tout homomorphisme λ d'une variété abélienne A dans une autre B , on note $\gamma(\lambda)$ l'entier $[k(x) : k(\lambda(x))]$ (k : corps de définition de A , B , λ ; (x) point générique de A sur k) si ce nombre est fini, et 0 dans le cas contraire (c'est-à-dire $\dim(\lambda(A)) < \dim(A)$) . Si α désigne un endomorphisme de la variété abélienne A^n $(n = \dim(A))$, et δ l'automorphisme identique de A , il existe un polynôme unitaire F(X) à coefficients entiers et de degré 2n tel que $\gamma(s\,\delta - \alpha) = P(s)$ pour tout entier s ([6]) ; théorème 34 et corollaire 2 su théorème 37) ; ce polynôme s'appelle le polynôme caractéristique de α. .

3. Domaines d'opérateurs d'une variété abélienne.

Soient A une variété abélienne de dimension n , K un corps de nombres algébriques, et R l'anneau des entiers de K . On dit que R est un domaine d'opérateurs de A s'il existe un isomorphisme ι de R dans l'anneau d'endomorphismes $\mathfrak{A}(A)$ de A , et si $[K : \mathbb{Q}] = 2n$. L'existence d'un tel domaine d'opérateurs implique facilement (d'après 2) que A est isogène à un produit de variétés abéliennes simples isomorphes (c'est-à-dire que $\mathfrak{A}_0(A)$ est un anneau de matrices sur un corps), que K est un sous-corps commutatif maximal de $\mathfrak{A}_0(A)$, et que R est son propre commutant dans $\mathfrak{A}(A)$. De plus, pour $\mu \in R$, on a

$$\gamma(\iota(\mu)) = |N_{K/\mathbb{Q}}(\mu)| .$$

Nous identifierons en général R avec son image $\iota(R)$ dans $\mathfrak{A}(A)$. Une variété abélienne admettant R pour domaine d'opérateurs est un R-module ; d'où, pour certaines variétés abéliennes, une "R-structure" plus riche que celle de variété abélienne, et à laquelle se rapportera le préfixe "R-" .

En utilisant le fait que, dans les conditions précédentes, l'algèbre simple $\mathfrak{A}_0(A)$ admet une trace $\sigma : \mathfrak{A}_0(A) \to \mathbb{Q}$, et un antiautomorphisme involutif $\xi \to \xi'$ tels que $\sigma(\xi\xi') > 0$ pour $\xi \neq 0$ ([6]), et en utilisant un raisonnement d'approximations diophantiennes, TANIYAMA montre ([4]) proposition 16) que K est une extension quadratique totalement imaginaire d'un corps totalement réel.

Etant donnés une variété abélienne A admettant R pour domaine d'opérateurs, et un idéal $\alpha \neq (0)$ de R , le corps composé des corps $k(\mu x)$ $(\mu \in \alpha$, x point

générique de A sur k) est un corps de fonctions abéliennes (une variété abélienne correspondant à ce corps s'obtient en prenant un système fini (μ_i) de générateurs de $\mathfrak{a}$; c'est l'image de A dans $A \times A \times \dots \times A$ par $x \to (\mu_1 x, \dots, \mu_r x)$). On obtient ainsi une variété abélienne $A_{\mathfrak{a}}$ et un epimorphisme $\lambda_{\mathfrak{a}}$ de A sur $A_{\mathfrak{a}}$, déterminés à un R-isomorphisme près par $\mathfrak{a}$. La variété $A_{\mathfrak{a}}$ s'appelle <u>la transformée de</u> A <u>par</u> $\mathfrak{a}$. Remarquons que $A_{\mathfrak{a}}$ est isogène à A, et qu'elle admet R pour domaine d'opérateurs. Le noyau de $\lambda_{\mathfrak{a}}$ est le sous-groupe fini $\mathfrak{g}(\mathfrak{a}, A)$ formé par les $z \in A$ tels que $\mu . z = 0$ pour tout $\mu \in \mathfrak{a}$.

Si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux $\neq (0)$ de A, on a $(A_{\mathfrak{a}})_{\mathfrak{b}} = A_{\mathfrak{ab}}$. Si $\mathfrak{a}$ est un idéal principal (μ), on peut prendre $A_{\mathfrak{a}} = A$, l'épimorphisme $\lambda_{\mathfrak{a}}$ étant alors $x \to \mu x$. Il en résulte que $A_{\mathfrak{a}}$ (mais non $\lambda_{\mathfrak{a}}$) <u>ne dépend que de la classe de l'idéal</u> $\mathfrak{a}$ (d'où la notation A_c, au lieu de $A_{\mathfrak{a}}$, c désignant la classe de l'idéal $\mathfrak{a}$). On montre d'autre part que $\mathrm{Hom}_R(A, A_{\mathfrak{a}})$ est R-isomorphe à l'idéal fractionnaire $\mathfrak{a}^{-1}$; donc, <u>pour que</u> $A_{\mathfrak{a}}$ <u>et</u> $A_{\mathfrak{b}}$ <u>soient R-isomorphes, il faut et il suffit que</u> $\mathfrak{a}$ <u>et</u> $\mathfrak{b}$ <u>appartiennent à la même classe d'idéaux de</u> R.

4. <u>Courbes elliptiques et corps imaginaires quadratiques.</u>

On sait que tout corps de fonctions elliptiques (c'est-à-dire tout corps de genre 1) a un modèle E de la forme

$$Y^2 = 4X^3 - g_2 X - g_3 \qquad (g_2, g_3 : \text{nombres complexes}).$$

Le nombre $j(E) = 2^6 3^3 (g_2)^3 / ((g_2)^3 - 27(g_3)^2)$ est un invariant du corps en question, et le détermine de façon unique. Pour tout nombre complexe j, il existe une courbe elliptique définie sur $Q(j)$ telle que $j(E) = j$. Rappelons que les courbes elliptiques ne sont autres que les variétés abéliennes de dimension 1.

Soit K un corps quadratique imaginaire, R l'anneau des entiers de K, h le nombre de ses classes d'idéaux ; il existe h nombres complexes $j_1, \dots, j_h$ tels que, pour q'une courbe elliptique E admette un anneau d'endomorphismes $\mathfrak{A}(E)$ isomorphe à R, il faut et il suffit que $j(E)$ soit égal à l'un des j_i ; alors R est évidemment un domaine d'opérateurs de E (et c'est le seul). Les nombres $j_1, \dots, j_h$ sont d'ailleurs des entiers algébriques (cf. WEBER, [5] p. 422).

Les transformés distincts E_i de E par les idéaux de R sont au nombre de h (n° 3), et admettent R pour domaine d'opérateurs ; donc toute courbe elliptique admettant R pour domaine d'opérateurs est isomorphe à l'une des E_i. En

particulier, pour tout automorphisme s de C sur K, la courbe conjuguée $s(E)$ de E est la transformée $E_{c(s)}$ de E par les idéaux d'une classe $c(s)$ bien déterminée par s. Comme l'invariant de $E_{c(s)}$ est $s(j(E))$, et qu'on montre que tous les éléments de $\mathfrak{A}(E)$ sont définis sur $K(j(E))$, il en résulte que $E_{c(s)}$ est définie sur $K(j(E))$, donc que $s(j(E)) \in K(j(E))$; ainsi $K(j(E))$ est une extension galoisienne de K, et même une extension abélienne, car on voit tout de suite que l'application $s \to c(s)$ est un isomorphisme du groupe de Galois de $K(j(E))$ sur K dans le groupe des classes d'idéaux de K.

Nous sommes tout près d'un des résultats typiques de la théorie du corps de classes. Pour l'obtenir complètement, il faut encore montrer

1° que $K(j(E))$ est non ramifiée ;

2° que $s \to c(s)$ est subjectif, et que son isomorphisme réciproque se déduit par passage aux quotients de l'homomorphisme: $\mathfrak{a} \to \left(\frac{K(j)/K}{\mathfrak{a}}\right)$

(on rappelle que l'automorphisme $\left(\frac{K(j)/K}{\mathfrak{a}}\right)$ se définit par multiplicativité à partir de $\left(\frac{K(j)/K}{\mathfrak{p}}\right)$ qui est l'automorphisme de Frobenius attaché à l'idéal premier $\mathfrak{p}$).

Pour cela on utilise la réduction modulo $\mathfrak{P}$. On montre d'abord que, pour tout idéal premier $\mathfrak{p}$ de R, il existe une variété abélienne E' isomorphe à E et définie sur une extension finie k' de $K(j)$ qui est sans défaut pour tout idéal premier $\mathfrak{P}$ de k' qui divise $\mathfrak{p}$. Soit r l'opérateur de réduction mod $\mathfrak{P}$. Si s est un élément du groupe d'inertie de $\mathfrak{p}$, on a

$$r(E') = r(s(E')) = r(E'_{c(s)}) = r(E')_{c(s)},$$

d'où $c(s) = 1$ et $s = 1$; ainsi $\mathfrak{p}$ est non ramifié. Il suffit alors de montrer que, si s est l'automorphisme de Frobenius attaché à l'idéal premier $\mathfrak{p}$, alors $c(s)$ est la classe de $\mathfrak{p}$, Pour cela on se sert du résultat suivant (qui contient une relation de congruence de Kronecker sur les fonctions elliptiques) :

Avec les hypothèses et notations précédentes, notons q la norme de l'idéal $\mathfrak{p}$, et m_q l'application rationnelle consistant à élever toutes les coordonnées à la puissance q. Alors $m_q(r(E'))$ est la variété abélienne $r(E')_{\mathfrak{p}}$ transformée de $r(E')$ par l'idéal $\mathfrak{p}$, et m_q est l'application canonique de $r(E')$ sur $r(E')_{\mathfrak{p}}$.

5. Autres résultats de Shimura et Taniyama.

Les mémoires étudiés contiennent bien d'autres résultats que ceux qu'on vient d'exposer. Comme ils sont de nature encore plus technique que les précédents,

je les exposerai très succintement.

a. Construction d'extensions abéliennes ramifiées d'un corps imaginaire quadratique ([2]).

b. Généralisation partielle des résultats sur les extensions abéliennes au cas où K est un corps de nombres normal sur Q et de degré $2n$, et où son anneau R d'entiers est un domaine d'opérateurs d'une variété abélienne A^n. Alors tout corps de définition de A contient le corps de classes K_1 sur K correspondant à un certain groupe d'idéaux ([2]).

c. TANIYAMA étudie le cas d'un corps biquadratique K, extension quadratique imaginaire d'un corps quadratique réel. L'anneau R des entiers de K est alors l'anneau $\mathcal{O}(J)$ des endomorphismes de la jacobienne J d'une courbe de genre 2 (nécessairement hyperelliptique). On retrouve ainsi, par voie algébro-géométrique, des résultats de Hecke sur la construction des extensions abélienne non ramifiées de K ([2]).

d. Etude de la fonction dzêta d'une variété abélienne A définie sur un corps de nombres k (en particulier de la jacobienne J d'une courbe C), dans le cas où A admet un domaine d'opérateurs. Rappelons qu'on définit cette fonction $\zeta_A(s)$ comme étant le produit

$$\zeta_A(s) = \prod_{\mathfrak{p}} \zeta_{r_{\mathfrak{p}}(A)}(s)$$

étendu aux idéaux premiers $\mathfrak{p}$ de k tels que A soit sans défaut pour $\mathfrak{p}$. Ici $\zeta_{r_{\mathfrak{p}}(A)}(s)$ désigne la fonction dzêta, d'une variété abélienne définie sur un corps fini $F_q = r_{\mathfrak{p}}(k)$: si N_f est le nombre des points de $r_{\mathfrak{p}}(A)$ qui sont rationnels sur F_{q^f}, on définit $Z(u)$ par

$$Z'(u)/Z(u) = \sum_{f=1}^{\infty} N_f u^{f-1} \quad ,$$

et on pose $\zeta_{r_{\mathfrak{p}}(A)}(s) = Z(q^{-s})$. Le résultat obtenu généralise des résultats partiels de Weil, Hasse et Deuring : la fonction $\zeta_A(s)$ s'exprime au moyen de la fonction $\zeta_k(s)$ du corps k, et de séries L de Hecke "mit Grossencharaktere" de k. Dans le cas d'une jacobienne J, l'idée de la démonstration est la suivante. Les résultats de Weil ([6]) montrent que l'on a

$$\zeta_{r_{\mathfrak{p}}(J)}(s) = (1 - q^{-s})^{-1}(1 - q^{1-s})^{-1} \prod_{i=1}^{2g} (1 - \sigma_i(\pi_{\mathfrak{p}})q^{-s})$$

où $q = N_{k/Q}(\mathfrak{p})$, où $\pi_{\mathfrak{p}}$ est un entier algébrique, et les $\sigma_i(\pi_{\mathfrak{p}})$ ses conjugués sur Q ; on montre que $\pi_{\mathfrak{p}} \in R$, et que l'application

$\chi_i : \mathfrak{p} \to \sigma_i(\pi_\mathfrak{p})/|\pi_\mathfrak{p}|$ (étendue par multiplicativité aux idéaux quelconques) est un "Grössencharakter" au sens de Hecke.

BIBLIOGRAPHIE

[1] NÉRON (A.). - Variétés abéliennes [d'après A. Weil] (en introduction à l'Exposé de P. Samuel sur la Jacobienne), Séminaire Bourbaki, t. 7, 1954/55.

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

[3] SHIMURA (Goro). - Reduction of algebraic varieties with respect to a discrete valuation of the basic valuation of the basic field, Amer. J. of Math., t. 77, 1955, p. 134-176.

[4] 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.

[5] WEBER (Heinrich). - Lehrbuch der Algebra, zweite Auflage, dritter Band : Elliptische Funktionen und algebraische Zahlen. - Braunschweig, Vieweg und Sohn, 1908.

[6] WEIL (André). - Variétés abéliennes et courbes algébriques. - Paris, Hermann, 1948.

ADDITIF

N.B.- Cet exposé a été suivi, en Mai 1956, par un exposé de A. WEIL.

[Juin 1957].