Inventiones math. 8, 238–243 (1969)

Variétés abéliennes ordinaires sur un corps fini

PIERRE DELIGNE (Bures-sur-Yvette)

On donne une description terre à terre de la catégorie des variétés abéliennes ordinaires sur un corps fini $\mathbf{F}_q$. Le résultat obtenu a été inspiré par Ihara [2] ch V (voir aussi [3]).

1. Soient p un nombre premier, $\mathbf{F}_p$ le corps $\mathbf{Z}/(p)$, $\bar{\mathbf{F}}_p$ une clôture algébrique de $\mathbf{F}_p$ et, pour toute puissance q de p, soit $\mathbf{F}_q$ le sous-corps à q éléments de $\bar{\mathbf{F}}_p$. Pour toute extension algébrique k de $\mathbf{F}_p$, on désigne par $W_0(k)$ l'anneau de valuation discrète hensélien essentiellement de type fini sur $\mathbf{Z}$, absolument non ramifié, de corps résiduel k; soient $W(k)$ l'anneau des vecteurs de Witt sur k, i.e. le complété de $W_0(k)$, $W=W(\bar{\mathbf{F}}_p)$ et φ un plongement de W dans le corps $\mathbf{C}$ des nombres complexes. On désigne par $\mathbf{Z}(1)$ le sous-groupe $2\pi i\,\mathbf{Z}$ de $\mathbf{C}$. L'application exponentielle définit un isomorphisme entre $\mathbf{Z}(1)\otimes\mathbf{Z}_l$ et $\mathbf{Z}_l(1)(\mathbf{C})=\varprojlim \mu_{l^n}(\mathbf{C})$.

On désigne par A^* la variété abélienne duale d'une variété abélienne A. Pour tout corps k, on désigne par $\bar{k}$ une clôture algébrique de k.

2. Soit A une variété abélienne de dimension g, définie sur un corps k de caractéristique p. Rappelons que A est dite *ordinaire* si les conditions équivalentes suivantes sont vérifiées:

(I) A a p^g points d'ordre divisant p à valeur dans $\bar{k}$.

(II) La «matrice de Hasse-Witt» F^*: $H^1(A^{(p)}, \mathcal{O}_{A^{(p)}})\to H^1(A, \mathcal{O}_A)$ est inversible.

(III) La composante neutre du schéma en groupe A_p noyau de la multiplication par p est de type multiplicatif, (donc géométriquement isomorphe à une puissance de μ_p).

Si $k=\mathbf{F}_q$, si F est l'endomorphisme de Frobenius de A et $Pc_A(F;x)$ son polynôme caractéristique, ces conditions équivalent encore à.

(IV) La moitié au moins des racines de $Pc_A(F;x)$ dans $\bar{\mathbf{Q}}_p$ sont des unités p-adiques. En d'autres termes, si $n=\dim A$, la réduction modulo p du polynôme $Pc_A(F;x)$ n'est pas divisible par x^{n+1}.

3. Soit A une variété abélienne ordinaire sur $\bar{\mathbf{F}}_p$. On désigne par $\tilde{A}$ le relèvement canonique de Serre-Tate [4] de A sur W. Rappelons que $\tilde{A}$ dépend fonctoriellement de A et est caractérisé par le fait que le groupe p-divisible $T_p(\tilde{A})$ sur W attaché à $\tilde{A}$ [5] est le produit des groupes

p-divisibles (uniquement déterminés d'après 2. (III)) relevant respectivement la composante neutre et le plus grand quotient étale de $T_p(A)$. Le relèvement canonique $\tilde{A}$ est encore l'unique relèvement de A tel que tout endomorphisme de A se relève à $\tilde{A}$. On désigne par $T(A)$ l'homologie entière de la variété abélienne complexe $A_{\mathbf{C}}$ déduite de $\tilde{A}$ et de φ par extension des scalaires de W à $\mathbf{C}$:

$$T(A)=H_1(\tilde{A}\underset{\varphi}{\otimes}\mathbf{C}).$$

On sait que $\tilde{A}$ se descend de façon unique à $W_0(\bar{\mathbf{F}}_p)$, de sorte que $A_{\mathbf{C}}$ ne dépend que de A et de la restriction de φ à $W_0(\bar{\mathbf{F}}_p)$. Le $\mathbf{Z}$-module libre $T(A)$ est de rang $2.\dim(A)$; il est fonctoriel en A. De plus, si l est un nombre premier $\neq p$, on a fonctoriellement

$$T(A)\otimes\mathbf{Z}_l=T_l(A). \tag{3.1}$$

Le relèvement canonique de la variété abélienne A^* duale de A est la duale de $\tilde{A}$, de sorte que $(A_{\mathbf{C}})^*=A^*_{\mathbf{C}}$ et que $T(A)$ et $T(A^*)$ sont en dualité parfaite à valeurs dans $\mathbf{Z}(1)$:

$$T(A)\otimes T(A^*)\to\mathbf{Z}(1) \tag{3.2}$$

(il est indispensable d'utiliser $\mathbf{Z}(1)$ de préférence à $\mathbf{Z}$ pour obtenir une théorie invariante par conjugaison complexe). Les accouplements (3.2) sont compatibles, via (3.1), aux accouplements

$$T_l(A)\otimes T_l(A^*)\to\mathbf{Z}_l(1);$$

un morphisme $\xi: A\to A^*$ définit une polarisation de A si et seulement si $\xi_{\mathbf{C}}: A_{\mathbf{C}}\to A^*_{\mathbf{C}}$ définit une polarisation de $A_{\mathbf{C}}$. Posons $T'_p(A)=\mathrm{Hom}(\mathbf{Q}_p/\mathbf{Z}_p, A(\bar{\mathbf{F}}_p))$ et $T''_p(A)=\mathrm{Hom}_{\mathbf{Z}_p}(T_p(A^*), \mathbf{Z}(1)\otimes\mathbf{Z}_p)$. Ces $\mathbf{Z}_p$-modules sont des foncteurs covariants de A.

Par définition du relèvement canonique, le groupe p-divisible $T_p(\tilde{A})$ est somme du groupe proétale constant $T'_p(A)$ et du dual de Cartier de $T''_p(A^*)$. Pour tout morphisme $u: A\to B$, le morphisme induit $u: T_p(\tilde{A})\to T_p(\tilde{B})$ s'identifie à la somme de $u|T'_p(A): T'_p(A)\to T'_p(B)$ et du transposé de Cartier de ${}^t u|T'_p(B^*): T'_p(B^*)\to T'_p(A^*)$. Sur $\mathbf{C}$, on a canoniquement $\mathbf{Z}(1)/(p^n)\sim\mu_{p^n}$, d'où un isomorphisme de foncteurs:

$$T_{(p)}(A)=T(A)\otimes\mathbf{Z}_p=T'_p(A)\oplus T''_p(A). \tag{3.2}$$

4. Rappelons que si $\varphi: X\to Y$ est une isogénie entre variétés abéliennes complexes, la suite exacte d'homotopie se réduit à une suite exacte courte

$$0\to H_1(X)\to H_1(Y)\to\mathrm{Ker}(\varphi)\to 0.$$

Les variétés abéliennes quotients de X par un sous-groupe fini, et ces sous-groupes finis de X, correspondent bijectivement aux sous-réseaux de $H_1(X)\otimes\mathbf{Q}$ contenant $H_1(X)$.

Soit A une variété abélienne ordinaire sur $\bar{\mathbf{F}}_p$. Si n est un entier premier à p, les sous-schémas en groupe finis d'ordre n de A, de $\tilde{A}$ et de $A_{\mathbf{C}}$ se correspondent bijectivement, et correspondent encore aux sur-réseaux R de $T(A)$ tels que $[R\colon T(A)]=n$.

Posons $V'_p=T'_p(A)\otimes\mathbf{Q}_p$ et $V''_p(A)=T''_p(A)\otimes\mathbf{Q}_p$. Les sous-schémas en groupes finis d'ordre p^k de A sont produits d'un sous-groupe étale et d'un sous-groupe infinitésimal. Les sous-groupes étales d'ordre p^k de A correspondent à ceux des sous-groupes d'ordre p^k de $A_{\mathbf{C}}$ tels que le sur-réseau R correspondant de $T(A)$ soit contenu dans $T_{(p)}(A)+V'_p(A)$. Par dualité, les sous-groupes infinitésimaux de A correspondent aux sur-réseaux R de $T(A)$, p-isogènes à $T(A)$, i.e. tels que $[R\colon T(A)]$ soit une puissance de p, et contenus dans $T_{(p)}(A)+V''_p(A)$.

Au total, les sous-groupes finis de A, ou les variétés abéliennes quotient de A, correspondent bijectivement aux sur-réseaux R de $T(A)$ tels que,

$$R\otimes\mathbf{Z}_p=(R\otimes\mathbf{Z}_p\cap V'_p)+(R\otimes\mathbf{Z}_p\cap V''_p). \tag{4.1}$$

5. En particulier, $A^{(p)}$, quotient de A par le plus grand sous-groupe infinitésimal de A tué par p (pour A ordinaire), est défini par le sur-réseau $T(A)^{(p)}$ de $T(A)$, p-isogène à $T(A)$, tel que

$$T(A)^{(p)}\otimes\mathbf{Z}_p=T'_p(A)+\frac{1}{p}\,T''_p(A).$$

6. Soient A une variété abélienne sur $\mathbf{F}_q$ et $F\colon x\to x^q$ son endomorphisme de Frobenius. Rappelons que A est uniquement déterminée par le couple $(\bar{A},F)$ déduit de (A,F) par extension des scalaires de $\mathbf{F}_q$ à $\bar{\mathbf{F}}_q$; l'endomorphisme F de $\bar{A}$ se factorise par le Frobenius relatif $Fr^{(q)}\colon \bar{A}\to\bar{A}^{(q)}$ et un isomorphisme $F'\colon \bar{A}^{(q)}\to\bar{A}$. Si A est ordinaire, on désignera par $T(A)$ le $\mathbf{Z}$-module $T(\bar{A})$ muni de l'endomorphisme F induit par l'endomorphisme de Frobenius de A. En vertu de 5., de ce qui précède, et de (3.2), les réseaux $T(A)$ et $F(T(A))$ sont p-isogènes et on *a*

$$F(T'_p(A))=T'_p(A), \tag{6.1}$$

$$F(T''_p(A))=q\,T''_p(A). \tag{6.2}$$

7. Théorème. *Le foncteur $A\mapsto(T(A),F)$ est une équivalence de catégories entre la catégorie des variétés abéliennes ordinaires sur $\mathbf{F}_q$ et la catégorie des $\mathbf{Z}$-modules libres de type fini T munis d'un endomorphisme F vérifiant les conditions suivantes*

(a) *F est semi-simple, et ses valeurs propres sont de valeur absolue complexe $q^{\frac{1}{2}}$,*

(b) *la moitié au moins des racines dans $\bar{\mathbf{Q}}_p$ du polynôme caractéristique de F sont des unités p-adiques; en d'autres termes, si T est de rang d, la réduction mod p du polynôme $Pc_T(F; x)$ n'est pas divisible par $x^{[d/2]+1}$,*

(c) *il existe un endomorphisme V de T tel que $FV=q$.*

Si la condition (a) *est vérifiée, les conditions* (b) *et* (c) *équivalent à,*

(d) *Le module $T\otimes\mathbf{Z}_p$ admet une décomposition, stable par F, en deux sous-$\mathbf{Z}_p$-modules T_p' et T_p'' de même dimension, tels que $F|T_p'$ soit inversible et $F|T_p''$ divisible par q.*

Preuve. (A) Prouvons que (a)+(b)+(c)$\Rightarrow$(d). Si α est une valeur propre complexe de F, $\bar{\alpha}$ en est une autre, de même multiplicité, et $\alpha\bar{\alpha}=q$. Si l'on excepte celles égales à $\pm q^{\frac{1}{2}}$, les valeurs propres de F dans $\mathbf{C}$, donc dans $\bar{\mathbf{Q}}_p$, se rangent en paires de racines α et q/α. Les racines α et q/α ne pouvant être simultanément des unités p-adiques, il résulte de (b) que $\pm q^{\frac{1}{2}}$ n'est pas valeur propre de F, que la moitié des valeurs propres de F dans $\bar{\mathbf{Q}}_p$ est formée d'unités p-adiques, soit $\alpha_1, \ldots, \alpha_{d/2}$, et que l'autre moitié est formée de $\beta_1=q/\alpha_1, \ldots, \beta_{d/2}=q/\alpha_{d/2}$. Soient $T_{(p)}=T\otimes\mathbf{Z}_p$, $V_p=T\otimes\mathbf{Q}_p$, V_p' le sous-espace de V_p noyau de $\prod_i (F-\alpha_i)$ et V_p'' le noyau de l'endomorphisme $\varphi=\prod_i (F-\beta_i)$. On a $V_p=V_p'\oplus V_p''$. Soient T_p' la projection de $T_{(p)}$ sur V_p' et $T_p''=T_{(p)}\cap V_p''$. Puisque φ annule V_p'', et respecte T, il envoie T_p' dans $T_{(p)}\cap V_p'\subset T_p'$. Par ailleurs, $\det(\varphi|V_p')=\prod_{i,j}(\alpha_i-\beta_j)$ est une unité p-adique, donc $\varphi(T_p')=T_p'$ et $T_{(p)}\cap V_p'=T_p'$, de sorte que $T_{(p)}=T_p'\oplus T_p''$.

(B) *Pleine fidélité.* Soient A et B deux variétés abéliennes sur $\mathbf{F}_q$, et soit ψ la flèche

$$\psi\colon \mathrm{Hom}(A,B)\to \mathrm{Hom}_F(T(A), T(B)).$$

En vertu du théorème de Tate [7] et de (3.1), la flèche

$$\psi_l\colon \mathrm{Hom}(A,B)\otimes\mathbf{Z}_l\to \mathrm{Hom}_F(T(A), T(B))\otimes\mathbf{Z}_l$$

est un isomorphisme pour $(l,p)=1$, de sorte que $\psi\otimes\mathbf{Q}$ est un isomorphisme. On sait que $\mathrm{Hom}(A,B)$ est sans torsion, donc ψ injectif. Soit $u\colon A\to B$ un morphisme tel que $T(u)$ soit divisible par n. Le morphisme induit $u_{\mathbf{C}}\colon \bar{A}_{\mathbf{C}}\to\bar{B}_{\mathbf{C}}$ est alors divisible par n, donc aussi $\tilde{u}\colon \tilde{A}\to\tilde{B}$ au point générique de W. Le noyau de la multiplication par n est plat sur W; $\tilde{u}$ s'annule donc sur ce noyau, $\tilde{u}$ et u sont divisibles par n, et ψ est bijectif.

(C) *Nécessité.* Que $(T(A), F)$ vérifie (a) résulte de Weil; la condition (d), qui implique (b) et (c), résulte de 6.

(D) *Isogénies.* Soient (T_0, F) vérifiant (a) (d) et T un réseau dans $T_0 \otimes Q$, stable par F, vérifiant encore (d). Supposons que (T_0, F) soit l'image d'une variété abélienne A sur $\mathbf{F}_q$ et prouvons que (T, F) provient d'une variété abélienne isogène. Remplaçant T par $\frac{1}{k}T$, qui lui est isomorphe, on peut supposer que $T \supset T_0$. La condition (d) implique que T vérifie (4.1) et T définit un sous-groupe H de $\bar{A}$, qui est défini sur $\mathbf{F}_q$, et $(T, F) = T(A/H)$.

(E) *Surjectivité.* Le foncteur T induit un foncteur $T_{\mathbf{Q}}$ de la catégorie des variétés abéliennes ordinaires à isogénie près sur $\mathbf{F}_q$ dans la catégorie des $\mathbf{Q}$-espaces vectoriels de rang fini, munis d'un automorphisme F vérifiant (a) (b). En vertu de (D), il suffit de prouver que ce foncteur $T_{\mathbf{Q}}$ est essentiellement surjectif. Il suffit même de montrer que tout objet simple (V, F) de la catégorie image est atteint. D'après Honda [1] (voir aussi [6]), il existe une variété abélienne A sur $\mathbf{F}_q$, telle que le polynôme caractéristique du Frobenius F_A de A soit une puissance de celui de F. La troisième caractérisation 1. des variétés abéliennes ordinaires montre que A est ordinaire. De plus, $(T(A) \otimes \mathbf{Q}, F)$ est somme de copies de (V, F), donc, d'après (B), la variété abélienne à isogènie près $A \otimes \mathbf{Q}$ est somme de copies d'une variété abélienne B vérifiant $T(B) \otimes \mathbf{Q} = (V, F)$.

8. Soit (T, F) un couple vérifiant les hypothèses du théorème, $2g$ le rang de T, A la variété abélienne sur $\mathbf{F}_q$ correspondante et $A_{\mathbf{C}}$ la variété abélienne complexe qui s'en déduit (3.). On a

$$T = H_1(A_{\mathbf{C}})$$

de sorte que $T \otimes \mathbf{R}$ s'identifie à l'algèbre de Lie de $A_{\mathbf{C}}$ et est en tant que tel muni d'une structure complexe. Voici, d'après J.-P. Serre, comment reconstruire cette structure complexe en terme de T, F et de la restriction de φ à $W_0(\mathbf{F}_p)$.

Proposition. *La structure complexe définie plus haut sur* $T \otimes \mathbf{R}$ est *caractérisée par les propriétés suivantes:*

(I) *L'endomorphisme* F *est* $\mathbf{C}$*-linéaire.*

(II) *Si* v *est la valuation de la clôture algébrique* $\bar{\mathbf{Q}}$ *de* $\mathbf{Q}$ *dans* $\mathbf{C}$ *prolongeant la valuation de* $W_0(\mathbf{F}_p)$, *les valuations des* g *valeurs propres de cet endomorphisme sont strictement positives.*

La condition (I) est évidente, et la condition (II) résulte de ce que l'action de F sur l'algèbre de Lie de A est congrue à zéro mod p. L'unicité de la structure complexe vérifiant (I) et (II) résulte aisément de la condition (b) vérifiée par (T, F).

Bibliographie

1. Honda, T.: Isogeny classes of abelian varieties over finite fields. J. Math. Soc. Jap. **20**, 83–95 (1968).
2. Ihara, Y.: On congruence monodromy problems, vol. I. University of Tokyo, 1968.
3. – The congruence monodromy problems. J. Math. Soc. Jap. **20**, 107–121 (1968).
4. Lubin, J., J.-P. Serre, and J. Tate: Elliptic curves and formal groups. Woods Hole Summer Institute 1964 (polycopié, tiré à un nombre restreint d'exemplaires).
5. Serre, J.-P.: Groupes p-divisibles (d'après J. Tate). Séminaire Bourbaki 318, Novembre 1966.
6. Tate, J.: Classes d'isogénies de variétés abéliennes sur un corps fini (d'après T. Honda). Séminaire Bourbaki 352, Novembre 1968.
7. – Endomorphisms of abelian varieties over finite fields. Inventiones Math. **2**, 134–144 (1966).

Pierre Deligne
I.H.E.S.
91, Bures-sur-Yvette, France

(Reçu le 3 juillet 1969)