

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 $\mathbb{F}_q$. Le résultat obtenu a été inspiré par Ihara [2], ch. V (voir aussi [3]).

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

$$\mathbb{Z}_\ell(1)(\mathbb{C}) = \varprojlim_n \mu_{\ell^n}(\mathbb{C}).$$

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 valeurs dans $\bar{k}$.

(II) La «matrice de Hasse–Witt»

$$F^* : H^1(A^{(p)}, \mathcal{O}_{A^{(p)}}) \longrightarrow H^1(A, \mathcal{O}_A)$$

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 $k = \mathbb{F}_q$, si F est l'endomorphisme de Frobenius de A et $P_{cA}(F; x)$ son polynôme caractéristique, ces conditions équivalent encore à:

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

3. Soit A une variété abélienne ordinaire sur $\overline{\mathbb{F}_p}$. 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 $A_{\mathbb{C}}$ déduite de $\tilde{A}$ et de φ par extension des scalaires de W à $\mathbb{C}$:

$$T(A) = H_1(\tilde{A} \otimes_{\varphi} \mathbb{C}).$$

On sait que $\tilde{A}$ se descend de façon unique à $W_0(\overline{\mathbb{F}_p})$, de sorte que $A_{\mathbb{C}}$ ne dépend que de A et de la restriction de φ à $W_0(\overline{\mathbb{F}_p})$. Le $\mathbb{Z}$ -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

$$T(A) \otimes \mathbb{Z}_\ell = T_\ell(A). \quad (3.1)$$

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

$$T(A) \otimes T(A^*) \longrightarrow \mathbb{Z}(1) \quad (3.2)$$

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

$$T_\ell(A) \otimes T_\ell(A^*) \longrightarrow \mathbb{Z}_\ell(1);$$

un morphisme $\xi : A \rightarrow A^*$ définit une polarisation de A si et seulement si $\xi_{\mathbb{C}} : A_{\mathbb{C}} \rightarrow A_{\mathbb{C}}^*$ définit une polarisation de $A_{\mathbb{C}}$. Posons

$$T'_p(A) = \text{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, A(\overline{\mathbb{F}_p}))$$

et

$$T''_p(A) = \text{Hom}_{\mathbb{Z}_p}(T'_p(A^*), \mathbb{Z}(1) \otimes \mathbb{Z}_p).$$

Ces $\mathbb{Z}_p$ -modules sont des foncteurs covariants de A .

Par définition du relèvement canonique, le groupe p -divisible $T_p(\tilde{A})$ est somme du groupe pro-étale constant $T'_p(A)$ et du dual de Cartier de $T'_p(A^*)$. Pour tout morphisme $u : A \rightarrow B$, le morphisme induit

$$u : T_p(\tilde{A}) \rightarrow T_p(\tilde{B})$$

s'identifie à la somme de $u|_{T'_p(A)} : T'_p(A) \rightarrow T'_p(B)$ et du transposé de Cartier de ${}^t u|_{T'_p(B^*)} : T'_p(B^*) \rightarrow T'_p(A^*)$. Sur $\mathbb{C}$, on a canoniquement $\mathbb{Z}(1)/(p^n) \sim \mu_{p^n}$, d'où un isomorphisme de foncteurs:

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

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

$$0 \longrightarrow H_1(X) \longrightarrow H_1(Y) \longrightarrow \text{Ker}(\varphi) \longrightarrow 0.$$

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

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

Posons

$$V'_p = T'_p(A) \otimes \mathbb{Q}_p, \quad V''_p(A) = T''_p(A) \otimes \mathbb{Q}_p.$$

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 $A_{\mathbb{C}}$ 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 $[R : T(A)]$ 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

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

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

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

6. Soient A une variété abélienne sur $\mathbb{F}_q$ et $F : x \mapsto x^q$ 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 $\mathbb{F}_q$ à $\overline{\mathbb{F}_q}$; l'endomorphisme F de $\bar{A}$ se factorise par le Frobenius relatif

$$\text{Fr}^{(q)} : \bar{A} \longrightarrow \bar{A}^{(q)}$$

et un isomorphisme

$$F' : \overline{A}^{(q)} \longrightarrow \overline{A}.$$

Si A est ordinaire, on désignera par $T(A)$ le $\mathbb{Z}$ -module $T(\overline{A})$ 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

$$F(T'_p(A)) = T'_p(A), \quad (6.1)$$

$$F(T''_p(A)) = qT''_p(A). \quad (6.2)$$

7. Théorème. Le foncteur

$$A \longmapsto (T(A), F)$$

est une équivalence de catégories entre la catégorie des variétés abéliennes ordinaires sur $\mathbb{F}_q$ et la catégorie des $\mathbb{Z}$ -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 $q^{1/2}$.
- (b) La moitié au moins des racines dans $\overline{\mathbb{Q}}_p$ du polynôme caractéristique de F sont des unités p -adiques; en d'autres termes, si T est de rang d , la réduction modulo p du polynôme $P_{cT}(F; x)$ n'est pas divisible par $x^{\lfloor d/2 \rfloor + 1}$.
- (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 $T \otimes \mathbb{Z}_p$ admet une décomposition, stable par F , en deux sous- $\mathbb{Z}_p$ -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 $\pm q^{1/2}$, les valeurs propres de F dans $\mathbb{C}$, donc dans $\overline{\mathbb{Q}}_p$, 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 $\pm q^{1/2}$ n'est pas valeur propre de F , que la moitié des valeurs propres de F dans $\overline{\mathbb{Q}}_p$ est formée d'unités p -adiques, soit $\alpha_1, \dots, \alpha_{d/2}$, et que l'autre moitié est formée de $\beta_1 = q/\alpha_1, \dots, \beta_{d/2} = q/\alpha_{d/2}$. Soient

$$T_{(p)} = T \otimes \mathbb{Z}_p, \quad V_p = T \otimes \mathbb{Q}_p,$$

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 $\mathbb{F}_q$, et soit ψ la flèche

$$\psi : \text{Hom}(A, B) \longrightarrow \text{Hom}_F(T(A), T(B)).$$

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

$$\psi_\ell : \text{Hom}(A, B) \otimes \mathbb{Z}_\ell \longrightarrow \text{Hom}_F(T(A), T(B)) \otimes \mathbb{Z}_\ell$$

est un isomorphisme pour $(\ell, p) = 1$, de sorte que $\psi \otimes \mathbb{Q}$ est un isomorphisme. On sait que $\text{Hom}(A, B)$ est sans torsion, donc ψ injectif. Soit $u : A \rightarrow B$ un morphisme tel que $T(u)$ soit divisible par n . Le morphisme induit

$$u_{\mathbb{C}} : \overline{A}_{\mathbb{C}} \longrightarrow \overline{B}_{\mathbb{C}}$$

est alors divisible par n , donc aussi $\tilde{u} : \tilde{A} \rightarrow \tilde{B}$ 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 $T_0 \otimes \mathbb{Q}$, stable par F , vérifiant encore (d). Supposons que (T_0, F) soit l'image d'une variété abélienne A sur $\mathbb{F}_q$ 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 $\mathbb{F}_q$, et

$$(T, F) = T(A/H).$$

(E) *Surjectivité.* Le foncteur T induit un foncteur $T_{\mathbb{Q}}$ de la catégorie des variétés abéliennes ordinaires à isogénie près sur $\mathbb{F}_q$ dans la catégorie des $\mathbb{Q}$ -espaces vectoriels de rang fini, munis d'un automorphisme F vérifiant (a) (b). En vertu de (D), il suffit de prouver que ce foncteur $T_{\mathbb{Q}}$ 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 $\mathbb{F}_q$, telle que le polynôme caractéristique du Frobenius F_A de A soit une puissance de celui de F . La troisième caractérisation 2.¹ des variétés abéliennes ordinaires montre que A est ordinaire. De plus, $(T(A) \otimes \mathbb{Q}, F)$ est somme de copies de (V, F) , donc, d'après (B), la variété abélienne à isogénie près $A \otimes \mathbb{Q}$ est somme de copies d'une variété abélienne B vérifiant

$$T(B) \otimes \mathbb{Q} = (V, F).$$

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

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

de sorte que $T \otimes \mathbb{R}$ s'identifie à l'algèbre de Lie de $A_{\mathbb{C}}$ 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 $W_0(\overline{\mathbb{F}_p})$.

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

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

(II) Si v est la valuation de la clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$ dans $\mathbb{C}$ prolongeant la valuation de $W_0(\overline{\mathbb{F}_p})$, 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 modulo 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).

¹L'imprimé renvoie ici à 1.; les caractérisations de l'ordinarité sont énoncées en 2., référence rétablie ici.

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

(Reçu le 3 juillet 1969)