SÉMINAIRE N. BOURBAKI

JOHN TATE

# Classes d'isogénie des variétés abéliennes sur un corps fini

*Séminaire N. Bourbaki*, 1968-1969, exp. n° 352, p. 95-110.

<http://www.numdam.org/item?id=SB_1968-1969__11__95_0>

Séminaire BOURBAKI
21e année, 1968/69, n° 352 Novembre 1968

# CLASSES D'ISOGÉNIE DES VARIÉTÉS ABÉLIENNES SUR UN CORPS FINI

(d'après T. HONDA)

par John TATE

## § 1. Enoncé du résultat principal.

La catégorie des variétés abéliennes sur un corps $k$ est une catégorie additive dans laquelle les groupes de morphismes $\mathrm{Hom}_k(A,B)$ sont des $\mathbb{Z}$-modules libres de type fini. On obtient une catégorie abélienne (même $\mathbb{Q}$-linéaire), que nous désignerons par $M(k)$, en gardant les mêmes objets, mais en posant $\mathrm{Hom}_{M(k)}(A,B) = \mathbb{Q} \otimes \mathrm{Hom}_k(A,B)$. Une flèche $f : A \to B$ dans $M(k)$ est un isomorphisme si et seulement si ses multiples non nuls $mf$, qui se trouvent dans $\mathrm{Hom}_k(A,B)$, sont des isogénies. Donc $M(k)$ est la catégorie des variétés abéliennes à isogénie près sur $k$ ; elle est canoniquement équivalente, comme dirait Grothendieck, à la catégorie des " motifs effectifs de poids 1 sur $k$ ".

On sait que $M(k)$ est semi-simple : chacun de ses objets est isomorphe à un produit fini d'objets simples. Donc, pour connaître $M(k)$, on doit classifier ses objets simples à isomorphisme près, et déterminer pour un tel objet $A$ le corps gauche $\mathrm{End}_{M(k)}A$. Nous allons voir comment une telle description de $M(k)$ peut se faire lorsque le corps de base $k$ est fini.

Soit $k$ un corps fini de caractéristique $p$, à $q = p^a$ éléments. Soit $A$ une variété abélienne $k$-simple définie sur $k$, et soit $\pi_A \in \mathrm{End}_k(A)$ son endomorphisme de Frobenius relatif à $k$. D'après Weil, $\pi_A$ est un entier algébrique tel que, pour tout plongement $\varphi : \mathbb{Q}(\pi_A) \to \mathbb{C}$, on ait $|\varphi(\pi_A)| = q^{\frac{1}{2}}$. Appelons

une telle quantité (dans un corps de caractéristique 0 ) un q-nombre de Weil, et disons que deux tels nombres, $\pi_1$ , $\pi_2$ sont conjugués s'ils le sont sur $\mathbb{Q}$ , c'est-à-dire, s'il existe un isomorphisme $\mathbb{Q}(\pi_1) \to \mathbb{Q}(\pi_2)$ qui transforme $\pi_1$ en $\pi_2$ .

THÉORÈME 1.- (i) La flèche $A \mapsto \pi_A$ donne une bijection entre les classes de $M(k)$-isomorphisme des objets simples de $M(k)$ et les classes de conjugaison des q-nombres de Weil.

(ii) Soit $A$ simple dans $M(k)$ , et soit

$$F = \mathbb{Q}(\pi_A) \subset E = \mathrm{End}_{M(k)}(A) .$$

Alors $E$ est un corps gauche de centre $F$ qui ne splitte en aucune place réelle de $F$, qui splitte en chaque place finie première à $p$ , et dont l'invariant en une place $v$ au-dessus de $p$ est donné par la règle

$$(1) \qquad \mathrm{inv}_v(E) \equiv \frac{v(\pi_A)}{v(q)} [F_v:\mathbb{Q}_p] = v(\pi_A)\frac{f_v}{a} \pmod 1 ,$$

où $F_v$ désigne le complété de $F$ en $v$ , et où $f_v$ désigne le degré résiduel absolu de $v$ . On a

$$(2) \qquad 2 \dim A = [E:F]^{\frac{1}{2}}[F:\mathbb{Q}] .$$

Remarques.- 1) Noter que $E$ est défini à isomorphisme près, en termes de $\pi_A$ , par les propriétés indiquées dans (ii).

2) De (2) résulte que, pour $A$ simple, le polynôme caractéristique $f_A$ de $\pi_A$ est la puissance $m$-ième du polynôme minimal de $\pi_A$ sur $\mathbb{Q}$ , où $m$ se calcule en termes de $\pi_A$ par la règle $m = [E:F]^{\frac{1}{2}}$ .

Exemples.- Donnons ici quelques précisions sur la structure de $E$ pour un $q$-nombre de Weil donné $\pi = \pi_A$, et quelques exemples particuliers.

a) Le cas où $\pi$ a un conjugué réel : Alors, on a $\pi^2 = q = p^a$, donc ce cas est très spécial :

Si $a$ est pair, alors $F = \mathbb{Q}$ et $E$ est le corps gauche de degré 4 sur $\mathbb{Q}$ ramifié seulement à l'infini et en $p$. On a $\dim A = 1$ ; $A$ est une courbe elliptique d'invariant de Hasse 0, dont tous les $\bar{k}$-endomorphismes sont définis sur $k$.

Si $a$ est impair, alors $F = \mathbb{Q}(p^{\frac{1}{2}})$ et $E$ est le corps gauche de degré 4 sur $F$ ramifié seulement aux deux places à l'infini. On a $\dim A = 2$ ; sur une extension quadratique de $k$, $A$ devient isogène au produit de deux courbes elliptiques du type qu'on vient de décrire.

b) Le cas où $F = \mathbb{Q}(\pi)$ est totalement imaginaire (cas général). Alors, $F$ est une extension quadratique du corps $F_o = \mathbb{Q}(\pi + q\pi^{-1})$ qui, lui, est totalement réel. Notons par $\alpha \mapsto \bar{\alpha}$ la conjugaison de $F$ sur $F_o$. Le corps gauche $E$ splitte en chaque place $v$ de $F$ qui n'est pas au-dessus de $p$. Pour une place $v$ au-dessus de $p$, on a

$$\text{(3)} \qquad \mathrm{inv}_v(E) + \mathrm{inv}_{\bar{v}}(E) \equiv 0 \pmod 1 ,$$

et même

$$\text{(4)} \qquad \mathrm{inv}_v(E) \equiv 0 \pmod 1 , \quad \text{si } v = \bar{v} .$$

Ces faits résultent de (1) parce que $\pi\bar{\pi} = q$ implique $v(\pi) + \bar{v}(\pi) = v(q)$, et $[F_v : \mathbb{Q}_p]$ est pair si $\bar{v} = v$.

Si $k$ est le corps premier (ou plus généralement si le degré absolu $a$ de

$k$ divise $f_v\, v(\pi)$ pour toute $v$ au-dessus de $p$ ), alors $E$ splitte partout, donc $E = F$ , et $\mathrm{End}_k(A)$ est commutatif.

Un exemple spécial (Problème de Manin). Soient $n$ et $n'$ deux entiers sans diviseur commun, avec $0 \leq n < n'$ , et soit $\pi$ une racine de l'équation $\pi^2 + p^n\pi + p^a = 0$ , où $a = n + n'$ . Alors $\pi$ est un $p^a$-nombre de Weil quadratique imaginaire ; $p$ splitte en deux places $v$ , $\bar{v}$ dans $\mathbb{Q}(\pi)$ , où les invariants de $E$ sont $n/a$ et $n'/a$ . On a $\dim A = a$ ; $A$ reste simple sur une clôture algébrique $\bar{k}$ de $k$ . Les considérations du § 2, ci-dessous, montrent que le groupe formel (ou p-divisible) $A(p)$ associé à $A$ est isogène sur $\bar{k}$ au groupe $G_{n,n'} \times G_{n',n}$ de la théorie de Dieudonné ; ce dernier est donc algébrique. Comme l'exemple $\pi = (-p)^{\frac{1}{2}}$ donne $G_{1,1}$ , ceci résout affirmativement un problème de Manin [5]. Une telle solution a été trouvée indépendamment par Honda et Serre, il y a deux ans.

## § 2. L'unicité de $A$ et la structure de $\mathrm{End}\, A$ .

Rappelons ici brièvement le principe de la démonstration de (ii) et de la moitié de (i) qui dit que $\pi_A$ détermine $A$ à $k$-isogénie près.

Pour chaque nombre premier $\ell$ (y compris $\ell = p$ ), soit $M(k,\ell)$ la catégorie $\mathbb{Q}_\ell$-linéaire des groupes $\ell$-divisibles (voir [8]) à isogénie près sur $k$ , et soit $V_\ell : M(k) \to M(k,\ell)$ le foncteur déduit de celui qui attache à chaque variété abélienne $A$ sur $k$ son groupe $\ell$-divisible $A(\ell)$ . (On a $A(\ell) = \varinjlim (A_{\ell^n})$ , où $A_{\ell^n}$ désigne le noyau de $\ell^n$ dans $A$ , au sens des schémas en groupes sur $k$ .) Pour $\ell \neq p$ , $V_\ell(A)$ est étale, donc peut être

identifié au module galoisien de ses points à valeurs dans une clôture algébrique $\bar{k}$ de $k$ (c'est-à-dire avec l'espace vectoriel $\ell$-adique de Weil, sur lequel opère l'automorphisme de Frobenius de $\bar{k}/k$ ) ; dans ce cas là, tout ce qu'on va esquisser ici se trouve dans [11]. D'autre part, $V_p(A)$ peut être identifié à son module de Dieudonné ; on trouvera, par exemple, dans [5] ou [6] les sorites sur ceux-ci à l'aide desquels le lecteur pourra compléter les détails de la démonstration dans le cas $\ell = p$ , en moins de temps qu'en attendant [12], sans doute.

Soit $A \in M(k)$ (non nécessairement simple). Soit $f_A$ le polynôme caractéristique de l'endomorphisme de Frobenius $\pi_A$ ; c'est aussi celui de l'endomorphisme de $V_\ell(A)$ défini par $\pi_A$ . Du fait que $\pi_A$ agisse de manière semi-simple dans $V_\ell(A)$ , on déduit que $f_A$ détermine $V_\ell(A)$ à un $M(k,\ell)$-isomorphisme près. De là, on montre que les buts des flèches injectives

$$\alpha_\ell : \mathbb{Q}_\ell \otimes_{\mathbb{Q}} \mathrm{End}_{M(k)}(A) \to \mathrm{End}_{M(k,\ell)}(V_\ell(A))$$

ont tous la même dimension ; il en est évidemment de même de leurs sources. Pour un $\ell_o \neq p$ qui splitte complètement dans l'algèbre $\mathbb{Q}(\pi)$ , on montre que la flèche $\alpha_{\ell_o}$ est surjective. (La démonstration est donnée dans [11], p. 137 ; elle utilise essentiellement la finitude des classes de variétés abéliennes sur $k$ de dimension et de degré de polarisation fixés.) Donc $\alpha_\ell$ est bijective pour tout $\ell$. Comme la structure de l'algèbre semi-simple $\mathrm{End}_{M(k)}(A)$ est déterminée par celle de ses localisations, on en déduit qu'elle est déterminée par $f_A$ ; en explicitant cette structure, on trouve (ii) pour $A$ simple.

On trouve aussi, pour $A$ quelconque, que l'algèbre $\mathbb{Q}(\pi_A)$ est le centre de $\mathrm{End}_{M(k)}A$ . En prenant $A = A' \times A''$ avec $A'$ et $A''$ simples, on en déduit que $\pi_{A'}$ conjugué à $\pi_{A''}$ implique bien $A'$ isomorphe à $A''$ .

## § 3. L'existence de A pour un $\pi$ donné.

Soit $\pi$ un q-nombre de Weil. Disons que $\pi$ est effectif s'il est conjugué au Frobenius $\pi_A$ d'un $A$ simple sur $k$. Notre but est de montrer que $\pi$ est effectif ; ce résultat est dû à Honda [2].

LEMME 1.- Soit $N$ un entier $\geq 1$. Si $\pi^N$ est effectif, alors $\pi$ l'est.

Soit $k'$ une extension de $k$ de degré $N$. Soit $A'$ une variété abélienne simple sur $k'$ telle que $\pi^N$ soit conjugué à $\pi_{A'}$. Soit $A$ la variété abélienne sur $k$ déduite de $A'$ par "restriction des scalaires" au sens de Weil (c'est ce que Grothendieck note $A = \prod_{k'/k} A'$). Alors on a

$$f_A(T) = f_{A'}(T^N) . \tag{5}$$

Donc $\pi$ est une racine de $f_A$, ce qui implique que $\pi$ est conjugué au Frobenius $\pi_{A_1}$ d'un des facteurs $k$-simples $A_1$ de $A$. (La formule (5) résulte par exemple du fait que le $\mathrm{Gal}(\bar{k}/k)$-module $V_\ell(A)$ est le module induit du $\mathrm{Gal}(\bar{k}/k')$-module $V_\ell(A')$.)

Soit maintenant $F = \mathbb{Q}(\pi)$, et soit $E$ un corps gauche de centre $F$ déduit de $\pi$ de la manière indiquée dans la partie (ii) du théorème 1. Appelons corps de type CM une extension quadratique $L$ totalement imaginaire d'un corps de nombres $L_o$ totalement réel.

LEMME 2.- Il existe un corps $L$ de type CM contenant $F$ tel que $L$ splitte $E$ et que $[L:F] = [E:F]^{\frac{1}{2}}$.

On utilise les propriétés de $E$ qui ont été explicitées dans les exemples a)

et b) du § 1. Dans le cas a) ( $\pi$ réel), on peut prendre par exemple $L = F((-p)^{\frac{1}{2}})$. Dans le cas b) ( $\pi$ non réel), $F$ est une extension quadratique totalement imaginaire du corps totalement réel $F_o = \mathbb{Q}(\pi + q\pi^{-1})$. Soit $m = [E:F]^{\frac{1}{2}}$, et soit $L_o$ une extension totalement réelle de degré $m$ de $F_o$, dont le degré local en toute place $v_o$ de $F_o$ au-dessus de $p$ est $m$. (Prendre $L_o = F_o(\alpha)$, où $\alpha$ est une racine d'un polynôme de degré $m$ sur $F_o$ qui est assez proche en chaque place $v_o$ au-dessus de $p$ d'un polynôme de degré $m$ irréductible dans le complété $v_o$-adique de $F_o$, et qui, en chaque place réelle, est assez proche d'un polynôme réel à racines réelles simples.) Posons $L = FL_o$. Alors $L$ est évidemment de type CM. Les seules places $v$ de $F$ où $E$ ne splitte pas sont celles au-dessus de $p$ où le complété de $F$ coïncide avec celui de $F_o$. Le degré de $L$ en une telle place est $m$. Donc $L$ splitte $E$.

Si $L$ est un corps de nombres et $A$ une variété abélienne sur un corps $K$, nous dirons que $A$ est <u>de type</u> $(L)$ si elle est munie d'un plongement $i : L \to \mathrm{End}_{M(K)}(A)$ et si $[L:\mathbb{Q}] = 2 \dim A$.

LEMME 3.- <u>Soit</u> $L$ <u>un corps de type</u> CM <u>contenant</u> $F = \mathbb{Q}(\pi)$ <u>tel que</u> $L$ <u>splitte</u> $E$. <u>Alors, il existe une variété abélienne</u> $A$ <u>de type</u> $(L)$ <u>sur une extension finie de</u> $\mathbb{Q}_p$ <u>telle que</u> $A$ <u>ait bonne réduction, et que le Frobenius de sa réduction soit conjugué à une puissance</u> $\pi^N$ <u>de</u> $\pi$.

Nous prouverons ce lemme au § 4. Après ça, la démonstration du théorème 1 sera achevée, parce que les lemmes 1, 2 et 3 entraînent évidemment que $\pi$ est effectif. En même temps, on aura démontré le théorème suivant, qui résout un problème de Honda ([2], p. 92).

THÉORÈME 2.- Soit A une variété abélienne k-simple définie sur k . Sur une extension finie de k , A devient isogène à la réduction d'une variété abélienne en caractéristique 0 de type (L) ; on peut prendre pour L n'importe quel corps de type CM tel que $\mathbb{Q}(\pi_A) \subset L \subset \mathrm{End}_{M(k)}(A)$ et tel que L splitte $\mathrm{End}_{M(k)}(A)$ .

On applique les lemmes 2 et 3 à $\pi = \pi_A$ , et puis on utilise le théorème 1 pour établir l'isogénie voulue sur une extension de degré N de k .

## § 4. Multiplication complexe ; démonstration du lemme 3.

Soit L un corps de type CM . Soit $\rho$ l'automorphisme d'ordre 2 de L qui est induit par la conjugaison complexe pour tout plongement $L \to \mathbb{C}$ . Soit C un corps algébriquement clos de caractéristique 0 , et soit $\Phi$ un sous-ensemble de $\mathrm{Hom}(L,C)$ tel que

(6) $\qquad \Phi \cap \Phi\rho = \emptyset \quad , \qquad$ et $\qquad \Phi \cup \Phi\rho = \mathrm{Hom}(L,C)$ .

On dit qu'un schéma abélien A défini sur un sous-anneau de C est de type $(L,\Phi)$ s'il est de type (L) et si la représentation de L sur l'espace $t_A$ tangent à A à l'origine a $\sum_{\varphi\in\Phi} \varphi$ comme caractère.

LEMME 4.- Il existe un schéma abélien de type $(L,\Phi)$ défini sur l'anneau des entiers d'un corps de nombres contenu dans C .

Ceci résulte de ([10], §§ 6.2 et 12.4) et de ([9], th. 7) : On construit d'abord un tore complexe dans le cas où $C = \mathbb{C}$ , en divisant $L \otimes_{\mathbb{Q}} \mathbb{R}$ (avec la structure de $\mathbb{C}$-algèbre donnée par $\Phi$ ) par un réseau contenu dans L . On cons-

tate que ce tore porte une forme de Riemann non-dégénérée, donc est algébrique. Puis, on montre qu'on peut trouver une telle variété abélienne définie sur un corps de nombres. Finalement, on applique le "critère de Ogg-Néron-Shafaryevitch", dont la démonstration est basée sur la théorie des modèles minimaux de Néron, pour voir qu'une variété abélienne de type (L) sur un corps de nombres a "potentiellement bonne réduction" partout, donc provient d'un schéma sur l'anneau des entiers, après extension finie du corps de base.

Supposons désormais que $C$ soit une clôture algébrique de $\mathbb{Q}_p$. Pour toute place $w$ de $L$ au-dessus de $p$, on désigne par $L_w$ le complété de $L$ en $w$. On identifie $\mathrm{Hom}_{\mathbb{Q}_p}(L_w,C)$ à son image dans $\mathrm{Hom}(L,C)$, qu'on note simplement par $H_w$, et on pose $\Phi_w = \Phi \cap H_w$. On a la décomposition

$$\mathbb{Q}_p \otimes L = \prod_{w|p} L_w \tag{7}$$

et les partitions

$$\mathrm{Hom}(L,C) = \bigcup_{w|p} H_w \tag{8}$$

$$\Phi = \bigcup_{w|p} \Phi_w \,. \tag{9}$$

LEMME 5.- *Soit $A$ un schéma abélien de type $(L,\Phi)$ défini sur l'anneau $\mathcal{O}$ des entiers d'une extension finie de $\mathbb{Q}_p$. Soit $k_o$ le corps résiduel de $\mathcal{O}$, soit $q_o = \mathrm{Card}(k_o)$, et soit $A_o$ la réduction de $A$ modulo l'idéal maximal de $\mathcal{O}$. Il existe alors un élément $\pi_o \in L$ tel que $i(\pi_o) \in \mathrm{End}_{M(\mathcal{O})}(A)$ induise le Frobenius $\pi_{A_o} \in \mathrm{End}_{M(k_o)}(A_o)$, et l'on a*

$$\frac{w(\pi_o)}{w(q_o)} = \frac{\mathrm{Card}(\Phi_w)}{\mathrm{Card}(H_w)} \,, \tag{10}$$

pour chaque place $w$ de $L$ au-dessus de $p$ .

Ce lemme n'est autre que la "décomposition en idéaux premiers du Frobenius" de Shimura-Taniyama, exprimée sous la forme qui nous convient ici. On trouvera une démonstration par voie globale dans ([2], p. 89) ; voir aussi ([9], § 7) et [1]. On va donner au § 5 ci-dessous une autre démonstration, utilisant les groupes p-divisibles.

Prouvons maintenant le lemme 3. Soient $\pi$ , $q$ , $F$ et $E$ comme au § 3, et supposons que $L$ satisfasse à l'hypothèse du lemme 3. Nous allons d'abord montrer qu'on peut choisir l'ensemble $\Phi$ de telle sorte que l'on ait

$$\frac{w(\pi)}{w(q)} = \frac{\mathrm{Card}(\Phi_w)}{\mathrm{Card}(H_w)} \quad , \tag{11}$$

pour chaque place $w$ de $L$ au-dessus de $p$ . Soient $w$ une telle place, et $v$ la place de $F$ en-dessous. Posons :

$$n_w = \frac{w(\pi)}{w(q)} \mathrm{Card}(H_w) = \frac{w(\pi)}{w(q)} [L_w:\mathbb{Q}_p] = \frac{v(\pi)}{v(q)} [L_w:F_v][F_v:\mathbb{Q}_p] .$$

Le fait que $L$ splitte $E$ montre que $n_w$ est un entier pour chaque $w$ (voir (1)). D'autre part, on a évidemment

$$n_w \geq 0 , \tag{12}$$

et de $\pi\pi^\rho = q$ on tire :

$$n_w + n_{\rho w} = \mathrm{Card}\ H_w . \tag{13}$$

Etant donnés des entiers $n_w$ satisfaisant aux conditions (12) et (13) (où $\rho$ est une permutation d'ordre 2 agissant sans point fixe sur la réunion disjointe $\cup H_w$ de telle façon que l'on ait $H_{\rho w} = (H_w)\rho$ ), on voit facilement qu'on peut

choisir des sous-ensembles $\Phi_w \subset H_w$ tels que $\mathrm{Card}(\Phi_w) = n_w$, et tels que leur réunion $\Phi = \bigcup_w \Phi_w$ satisfasse aux conditions (6). (On regarde les $w$ telles que $w = \rho w$ individuellement, et les autres en paires $(w, \rho w)$ en choisissant les $\Phi_w$.) Pour un tel choix de $\Phi$, on aura (11) par construction ; donc, pour un $A$ comme dans le lemme 5 (qui existe d'après le lemme 4), on aura :

$$(14) \qquad \frac{w(\pi)}{w(q)} = \frac{w(\pi_o)}{w(q_o)} \quad , \text{ pour toute place } w \text{ de } L \text{ au-dessus de } p \text{ ,}$$

où $\pi_o$ est un $q_o$-nombre de Weil dans $L$ qui est conjugué au Frobenius de la réduction $A_o$ de $A$.

Si on remplace l'anneau $\mathcal{O}$ du lemme 5 par une extension non ramifiée de degré $N_o$, on remplace $\pi_o$ par $\pi_o^{N_o}$. Donc la démonstration du lemme 3 sera terminée avec :

LEMME 6.- *Soient $\pi$ un $q$-nombre de Weil et $\pi_o$ un $q_o$-nombre de Weil dans $L$ qui satisfassent à (14). Alors, il existe des entiers $N$ et $N_o > 0$ tels que l'on ait $\pi^N = \pi_o^{N_o}$.*

Quitte à remplacer $\pi$ et $\pi_o$ par des puissances, on peut supposer que $q = q_o$, donc $w(\pi) = w(\pi_o)$ pour toute place $w$ de $L$ au-dessus de $p$. En les autres places finies, $\pi$ et $\pi_o$ sont des unités, parce qu'ils divisent une puissance de $p$. En les places à l'infini, $\pi$ et $\pi_o$ ont la même valeur absolue, à savoir $q^{\frac{1}{2}}$. Donc $\pi/\pi_o$ est de valeur absolue 1 en chaque place de $L$, ce qui implique que $\pi/\pi_o$ est une racine de l'unité ; d'où le lemme.

Remarque.- Vu le lemme 6, l'analogue du théorème 1, pour le corps de base $\bar{k}$ (une clôture algébrique du corps premier de caractéristique $p$), peut s'exprimer en termes de classes d'équivalence de " q-idéaux de Weil " au lieu de q-nombres de

Weil ; ce point de vue est développé dans Honda [2].

## § 5. Groupes p-divisibles "à multiplication complexe".

Soient $C$ une clôture algébrique de $\mathbb{Q}_p$ , $K$ une extension finie de $\mathbb{Q}_p$ contenue dans $C$ , et $\mathcal{O}$ l'anneau des entiers de $K$ . Soient $L_*$ une extension finie de $\mathbb{Q}_p$ , $H_* = \mathrm{Hom}_{\mathbb{Q}_p}(L_*, C)$ , et $\Phi_* \subset H_*$ . Rappelons que $M(\mathcal{O}, p)$ désigne la catégorie des groupes p-divisibles à isogénie près sur $\mathcal{O}$ .

DÉFINITION.- Un groupe p-divisible de type $(L_*, \Phi_*)$ sur $\mathcal{O}$ est un groupe p-divisible $V_*$ de hauteur $[L_* : \mathbb{Q}_p]$ défini sur $\mathcal{O}$ , muni d'un plongement $\mathbb{Q}_p$-linéaire $i_* : L_* \to \mathrm{End}_{M(\mathcal{O},p)}(V_*)$ tel que, si $t_*$ désigne l'espace tangent à $V_*$ à l'origine, la représentation de $L_*$ dans $t_* \otimes_{\mathcal{O}} K$ déduite de $i_*$ a comme caractère $\sum_{\varphi \in \Phi_*} \varphi$ .

Remarque.- Ces groupes ont été introduits par Lubin [3], dans le cas de dimension 1 , où $\Phi_*$ est réduit à un seul élément ; voir aussi [4] et ([7], Ch. III, Appendice).

Soit $V_*$ un groupe p-divisible de type $(L_*, \Phi_*)$ sur $\mathcal{O}$ . Posons

$$h_* = \text{hauteur}\ (V_*) = \mathrm{Card}(H_*) \quad \text{et} \quad n_* = \dim(V_*) = \mathrm{Card}(\Phi_*) .$$

Soit $\deg : \mathrm{End}_{M(\mathcal{O},p)}(V_*) \to \mathbb{Q} \cup \{\infty\}$ l'application multiplicative qui attache à chaque élément de $\mathrm{End}_{\mathcal{O}}(V_*)$ son degré. On montre facilement que la valeur absolue normée d'un élément $\alpha \in L_*$ est donnée par

$$|\alpha|_* = (\deg(i_*\alpha))^{-1} .$$

Supposons maintenant que $\pi_o$ soit un élément de $L_*$ tel que $i_*\pi_o$ induise le Frobenius $\pi_{V_{*_o}}$ dans la réduction $V_{*_o}$ de $V_*$ modulo l'idéal maximal de $\mathcal{O}$ .

Alors, si $q_o$ est le nombre d'éléments du corps résiduel $k_o$ de $\mathcal{O}$, on a

$$|\pi_o|_* = (\deg(i_*\pi_o))^{-1} = (\deg(\pi_{V_{*o}}))^{-1} = q_o^{-n_*} ,$$

et

$$|q_o|_* = (\deg(q_o))^{-1} = q_o^{-h_*} .$$

Si $w$ désigne la valuation de $L_*$, on en déduit

$$(10_*) \qquad \frac{w(\pi_o)}{w(q_o)} = \frac{n_*}{h_*} = \frac{\mathrm{Card}(\Phi_*)}{\mathrm{Card}(H_*)} .$$

C'est la version " p-divisible" de la formule (10). La formule (10) en résulte, compte tenu du

THÉORÈME 3.- Soient $L$, $\Phi$, et les $\Phi_w$ comme on l'a expliqué juste avant le lemme 5, et soient $A$ et $\mathcal{O}$ comme dans le lemme 5. Soit $V_p = V_p(A)$ le groupe p-divisible attaché à $A$, et soit

$$(15) \qquad V_p = \prod_{w|p} V_w$$

la décomposition de $V_p$ dans $M(\mathcal{O},p)$ déduite de la décomposition (7). Alors $V_w$, muni de l'action de $L_w$, est de type $(L_w,\Phi_w)$ pour chaque place $w$ de $L$ au-dessus de $p$.

Soit

$$(16) \qquad t_p = \prod_{w|p} t_w$$

la décomposition de l'espace $t_p$ tangent à $V_p$ à l'origine correspondant à (15). Comme $\mathcal{O}$ est complet pour la topologie p-adique, l'espace tangent à $A$ à l'origine s'identifie à $t_p$ (en effet, le complété de $A$ le long de l'origine s'identifie à la composante connexe de $V_p$ à l'origine). On en déduit que

la partition des caractères irréductibles $\varphi$ de $L$ correspondant à la décomposition (16) est donnée par (9), d'où le théorème.

Remarque.- Avec ce théorème, on montre facilement (à l'aide du lemme 4, bien sûr) l'existence d'un groupe p-divisible de type $(L_*, \Phi_*)$ donné (sur une base $\mathcal{O}$ non précisée), comme l'a remarqué Serre dans son cours de l'an dernier.

## § 6. Compléments.

Pour terminer, signalons deux travaux récents qui sont étroitement liés au théorème 1.

1) Dans la situation de la partie (ii) du théorème 1 ; peut-on classifier à isomorphisme près les variétés abéliennes $A'$ sur $k$ qui sont isogènes à $A$ ? L'anneau d'endomorphismes d'un tel $A'$ est un ordre de $E = \mathrm{End}_{M(k)}(A)$ ; quels sont les ordres possibles ? Ces questions semblent très difficiles en général, mais on trouvera des résultats intéressants dans la thèse de Waterhouse [13]. Par exemple, tous les ordres de $E = F$, qui contient $\pi_A$ et $q\pi_A^{-1}$, sont des anneaux d'endomorphismes dans chacun des deux cas suivants :

a) si $q = p$ et si $\pi$ n'est pas réel ;

b) si $A$ est ordinaire, c'est-à-dire, si le rang du groupe $A(\bar{k})_p$ des points sur $A$ tués par $p$ est égal à $\dim A$. (Ce résultat peut être faux pour les $A$ non ordinaires, même si $E$ est commutatif et stable par extension du corps de base.)

2) Soient $A$ et $B$ deux variétés abéliennes sur $k$. Soit $(\alpha_i)$ (resp. $(\beta_j)$) une $\mathbb{Z}$-base pour $\mathrm{Hom}_k(A,B)$ (resp. $\mathrm{Hom}_k(B,A)$). Milne a démontré [6] que le groupe

$\mathrm{Ext}^1_k(A,B)$ est fini, et que le produit de son ordre avec $\det(\mathrm{Tr}(\beta_j\alpha_i))$ se calcule par une belle formule, en termes des polynômes caractéristiques de $\pi_A$ et de $\pi_B$ .

## BIBLIOGRAPHIE


[1] J. GIRAUD - Remarque sur une formule de Taniyama, Invent. Math., vol. 5, fasc. 3, 1968, p. 231-236.

[2] T. HONDA - Isogeny classes of abelian varieties over finite fields, Journ. Math. Soc. Japan, 20, 1968, p. 83-95.

[3] J. LUBIN - One-parameter formal Lie groups over p-adic integer rings, Annals of Maths., 80, 1964, p. 464-484.

[4] J. LUBIN et J. TATE - Formal complex multiplication in local fields, Annals of Maths., 89, 1965, p. 380-387.

[5] J. I. MANIN - La théorie des groupes formels commutatifs sur les corps de caractéristique finie (en russe), Usp. Mat. Nauk, 18, 1963, p. 3-90. [Traduction anglaise : Russian Math. Surv., 18, n° 6, p. 1-83.]

[6] J. S. MILNE - Extensions of abelian varieties defined over a finite field, Invent. Math., 5, 1968, p. 63-84.

[7] J.-P. SERRE - Abelian $\ell$-adic representations and elliptic curves, W. A. Benjamin, Inc., New York, 1968.

[8] J.-P. SERRE - Groupes p-divisible (d'après J. Tate), Sém. Bourbaki, 1966/67, exposé 318.

[9] J.-P. SERRE et J. TATE - Good reduction of abelian varieties, Annals of Maths., à paraître.

[10] G. SHIMURA et Y. TANIYAMA - Complex multiplication of abelian varieties and its applications to number theory, Publ. Math. Soc. Japan, 6, 1961.

[11] J. TATE - Endomorphisms of abelian varieties over finite fields, Invent. Math., 2, 1966, p. 134-144.

[12] J. TATE - Endomorphisms of abelian varieties over finite fields II, Invent. Math., toujours à paraître.

[13] W. C. WATERHOUSE - Abelian varieties over finite fields, Thesis, Harvard University, May 1968.