

Courbes sur une variété abélienne et points de torsion

M. Raynaud*

Mathématiques, Bât. 425, Université Paris-Sud, F-91405 Orsay, France

Soient A une variété abélienne définie sur le corps \mathbb{C} des nombres complexes, T le sous-groupe de torsion de $A(\mathbb{C})$ et X une courbe de A propre, intègre, qui n'est pas une courbe elliptique.

Théorème I. *L'ensemble $T \cap X(\mathbb{C})$ des points de torsion de X est finie.*

Rappelons que l'analogie de cet énoncé, dans lequel on remplace T par sa composante n -primaire (n entier > 1), a été établi par Bogomolov ([1], Th. 3).

Indiquons le principe de la démonstration.

Supposons pour simplifier que X est lisse et que X et A sont définies sur un corps de nombres L . Soit \mathcal{O} l'anneau des entiers de L . Soit U un ouvert non vide de $\text{Spec}(\mathcal{O})$ tel qu'il existe un U -schéma abélien \mathcal{A} de fibre générique A et une courbe \mathcal{X} de \mathcal{A} , propre et lisse sur U , de fibre générique X . Notons \mathcal{J} la jacobienne relative de \mathcal{X} sur U et $a: \mathcal{J} \rightarrow \mathcal{A}$ le morphisme d'Albanese associé à l'immersion de \mathcal{X} dans \mathcal{A} . Quitte à restreindre U , on suppose de plus que les conditions suivantes sont réalisées:

i) U est non ramifié sur $\text{Spec}(\mathbb{Z})$.

ii) $\text{Ker}(a)$ est lisse sur U et le nombre n des composantes connexes des fibres géométriques de $\text{Ker}(a)$ est inversible sur U .

Soit alors v un point fermé de U au-dessus d'un nombre premier p et soit \mathcal{O}_v le complété de l'anneau local de v dans U . Par passage à l'extension maximale non ramifiée de \mathcal{O}_v , puis complétion, on obtient un anneau de valuation discrète complet R , à corps résiduel k algébriquement clos de caractéristique p et à corps des fractions K extension de L . Le point essentiel, dans notre démonstration est le résultat local suivant:

Théorème II. *Pour tout $a \in \mathcal{A}(R)$ les points de $(\mathcal{X} + a)(k)$ qui se relèvent en points de $(\mathcal{X} + a)(R) \cap p\mathcal{A}(R)$ sont en nombre fini, borné uniformément par rapport à a .*

Cet énoncé entraîne immédiatement une partie significative du théorème I: les points de torsion de $\mathcal{X} + a$, d'ordre premier à p (ce que nous appellerons la p' -torsion), sont en nombre fini, borné indépendamment de $a \in \mathcal{A}(R)$.

* Université de Paris-Sud Orsay, ERA 653. Ce travail a été préparé sur un crédit NSF, à l'Institute for Advanced Study de Princeton

Changeant de point v dans U , on en déduit un résultat analogue pour la torsion p -primaire. A partir de la finitude de la p '-torsion et de la finitude uniforme après translation de la torsion p -primaire, il est facile d'en déduire le théorème I (cf. 7.4).

Quant au théorème II, il se démontre à l'aide d'un calcul différentiel modulo p^2 , dont nous allons donner l'idée. Changeant de notations, on désigne par A et X les images réciproques de \mathcal{A} et \mathcal{X} par le changement de base $\text{Spec}(R) \rightarrow U$ associé au choix du point v . Notons A_0 et X_0 les fibres spéciales de A et X au-dessus de $R/pR = k$ et soient A_1 et X_1 les restrictions de A et X au-dessus de $\text{Spec}(R_1)$, où $R_1 = R/p^2R$. Désignons par \mathcal{S}_0 le faisceau d'idéaux qui définit X_0 dans A_0 et soit $\mathcal{N}_0 = \mathcal{S}_0/\mathcal{S}_0^2$ vu comme fibré vectoriel sur X_0 .

Pour établir le théorème II, nous sommes amenés à étudier l'image de $X_1(R_1) \cap pA_1(R_1)$ dans $X_0(k)$. Pour cela considérons l'éclatement E de X_0 dans A , sa fibre spéciale E_0 et soit V_0 l'ouvert de lissité de E_0 au-dessus de X_0 . En fait V_0 est un espace affine associé au fibré vectoriel \mathcal{N}_0 : c'est l'espace affine qui contrôle les divers relèvements de X_0 dans A_1 . Localement on peut choisir des coordonnées x, y_1, \dots, y_n sur A , de façon que X_0 ait pour équations $p=0, y_1 = \dots = y_n = 0$; alors V a pour coordonnées x, z_1, \dots, z_n avec $pz_i = y_i$. Soit $h_0: V_0 \rightarrow X_0$ la projection canonique. Désignons par $(A_1, X_0)(R_1)$ le sous-ensemble de $A_1(R_1)$ formé des points qui se réduisent modulo p en des points de $X_0(k)$. On définit une application de relèvement τ qui rend commutatif le diagramme:

$$\begin{array}{ccc}
 (A_1, X_0)(R_1) & \xrightarrow{\tau} & V_0(k) \\
 \text{can.} \searrow & & \swarrow h_0 \\
 & & X_0(k).
 \end{array}$$

L'image par τ de $X_1(R_1)$ (resp. $(A_1, X_0) \cap pA_1(R_1)$) consiste en les points rationnels d'une courbe intègre X'_0 (resp. Y'_0) de V_0 . Pour montrer que l'image de $X_1(R_1) \cap pA_1(R_1)$ dans $X_0(k)$ est finie, il suffit alors de montrer que $X'_0 \cap Y'_0$ est fini, c'est-à-dire que X'_0 et Y'_0 sont distinctes. Or h_0 induit un isomorphisme $X'_0 \xrightarrow{\sim} X_0$ (X'_0 est la trivialisaton du fibré V_0 associée au relèvement X_1 de X_0 dans A_1), tandis que l'on montre que le degré radiciel de la projection $Y'_0 \rightarrow X_0$ est > 1 .

L'étude des diverses propriétés de relèvement utilisées de $h_0: V_0 \rightarrow X_0$ occupe les numéros 2 et 3. Au numéro 2, on définit l'application τ qui est de nature élémentaire. Au numéro 3, on étudie une propriété de relèvement liée à la caractéristique $p > 0$ et utile pour analyser Y'_0 ; c'est elle qui justifie l'introduction de V_0 . En effet, pour étudier des ensembles de points du type $pA_1(R_1) \cap (A_1, X_0)(R_1)$, on aurait pu penser à travailler avec le foncteur de Greenberg; mais celui-ci masque certains phénomènes radiciels, essentiels pour nous, qui sont mis en valeur par l'utilisation de V_0 .

Le calcul du degré radiciel de $Y'_0 \rightarrow X_0$ est fait au numéro 4 et est préparé au numéro 1. Le théorème II est démontré dans 4.4.1 et 6.6.1. Notons que la démonstration fournit en principe une majoration du cardinal de l'image de $(\mathcal{X} + a)(R) \cap p\mathcal{A}(R)$ en fonction du fibré vectoriel \mathcal{N}_0 , mais cette borne n'est très accessible que lorsque A est une surface abélienne.

La méthode présentée ici a le défaut de traiter séparément la p' -torsion et la torsion p -primaire. Récemment, Coleman a proposé une autre approche, p -adique elle aussi, qui évite cette distinction. Elle devrait conduire à une nouvelle démonstration du théorème I, et a permis, dès à présent, de déterminer exactement les points de torsion situés sur certaines courbes de Fermat.

Revenons aux données initiales X et A sur \mathbb{C} . Dans [6] Serge Lang a soulevé le problème suivant: étant donné un sous-groupe de type fini Γ de $A(\mathbb{C})$, et le groupe $\bar{\Gamma}$ des points de division de Γ , $\bar{\Gamma} \cap X$ est-il fini?

Le théorème I fournit une réponse positive à cette question dans le cas où $\Gamma = 0$; une réponse positive en général est, a priori, un résultat plus fort que la conjecture de Mordell. Comme autre application du théorème II, nous montrons qu'en fait la conjecture de Mordell entraîne la conjecture de Lang (pour des énoncés plus précis cf. 9.2.1 et 9.2.2).

Signalons pour terminer que le théorème I présente des extensions naturelles au cas où l'on remplace la courbe X par une sous-variété quelconque de A . Nous étudierons ces généralisations dans un article ultérieur.

1. Courbes plongées dans une variété abélienne en caractéristique $p > 0$.

1.0. Dans ce numéro, k est un corps algébriquement clos de caractéristique $p > 0$. Soit S un k -schéma. On note Ω_S le faisceau des formes différentielles de degré 1 sur S . Pour tout entier $m \in \mathbb{Z}$, on note $\sigma^m: \text{Spec}(k) \rightarrow \text{Spec}(k)$ le morphisme qui envoie $a \in k$ sur a^{p^m} et on note $S^{(m)}$ le k -schéma déduit du k -schéma S par le changement de base σ^m (autrement dit, si S est affine, défini par des équations $f_i = 0$ dans l'anneau de polynômes $k[T_\lambda]$, $S^{(m)}$ est défini par les équations déduites des f_i en élevant les coefficients à la puissance p^m). On dispose alors d'un morphisme de Frobenius relatif:

$$F: S^{(m)} \rightarrow S^{(m+1)},$$

qui est un k -morphisme radiciel; par itération, pour tout entier $n \geq 0$ on a un k -morphisme $F^n: S^{(m)} \rightarrow S^{(m+n)}$. En particulier on a les k -morphisms $F^n: S^{(-n)} \rightarrow S$ et $F^n: S \rightarrow S^{(n)}$.

1.1.1. Soient A une k -variété abélienne et $i: X \rightarrow A$ une immersion d'une k -courbe propre, intègre. Notons $\alpha: \tilde{X} \rightarrow X$ le morphisme de normalisation et $\tilde{i} = i\alpha: \tilde{X} \rightarrow A$ l'application composée. Soit $J_{\tilde{X}}$ la jacobienne de \tilde{X} et $a: J_{\tilde{X}} \rightarrow A$ l'application d'Albanese associée à \tilde{i} .

Définition 1.1.2. Nous dirons que l'immersion $i: X \hookrightarrow A$ satisfait à la propriété (*) si les conditions suivantes sont réalisées:

- i) Le morphisme $a: J_{\tilde{X}} \rightarrow A$ est surjectif et son noyau N est lisse sur k .
- ii) Le groupe des composantes connexes N/N^0 de N est d'ordre premier à p .

Remarques 1.1.3. i) La condition (*) est évidemment satisfaite si a est un isomorphisme, en particulier si X est lisse et si $i: X \hookrightarrow A$ est un plongement usuel de X dans sa jacobienne.

ii) Notons que la partie i) de (*) équivaut au fait que l'application sur les formes différentielles:

$$H^0(A, \Omega_A) \rightarrow H^0(\tilde{X}, \Omega_{\tilde{X}}),$$

déduite de \tilde{i} , est injective. La condition (*) elle-même équivaut au fait que l'application

$$H^1_{DR}(A, \Omega_A) \rightarrow H^1_{DR}(\tilde{X}, \Omega_{\tilde{X}})$$

sur les cohomologies de De Rham, est injective (nous n'utiliserons pas ce fait dans la suite).

1.2.1. Soit $u: B \rightarrow A$ une isogénie de variétés abéliennes, de noyau G d'ordre une puissance de p et soit $G = G_{\text{et}} \times G_{\text{inf}}$ la décomposition canonique de G en le produit d'un groupe étale et d'un groupe infinitésimal. L'image réciproque $B \times_A X$, de X par u , n'est pas réduite dès que A est de dimension ≥ 2 . Soit Y la courbe réduite sous-jacente à $B \times_A X$; on note $v: Y \rightarrow X$ le morphisme induit par u . Même si X est lisse, il n'en est plus nécessairement de même de Y ; toutefois la lissité est conservée si G_{inf} est le noyau d'un itéré du Frobenius de B (par exemple, ce sera le cas si les deux conditions suivantes sont réalisées i) $B = A$ et u est la multiplication par p ; ii) ou bien A est ordinaire, ou bien A est le produit de courbes elliptiques supersingulières). On note $\beta: \tilde{Y} \rightarrow Y$ le morphisme de normalisation, $j: Y \hookrightarrow B$ l'immersion canonique, $\tilde{j} = j\beta$ et $\tilde{v}: \tilde{Y} \rightarrow \tilde{X}$ la normalisation de v .

Proposition 1.2.2. *Supposons que $i: X \hookrightarrow A$ vérifie (*) (1.1.2). Alors:*

- i) *La courbe Y est intègre et son degré séparable sur X est le rang de G_{et} .*
- ii) *Le degré radiciel de Y sur X est p^s où s est le plus petit entier tel que F^s annule G_{inf} .*

Le fait que Y soit intègre (ou ce qui revient au même que \tilde{Y} soit connexe) résulte de la partie ii) de la condition (*): en effet, celle-ci entraîne que le produit fibré $B \times_A (J_{\tilde{X}})$ de u et de a est connexe et on est ramené au cas classique où $X = \tilde{X}$ et $A = J_{\tilde{X}}$.

Pour établir ii), on peut, quitte à diviser B par G_{et} , se ramener au cas où $G = G_{\text{inf}}$. Soit p^r le degré radiciel de Y sur X . Comme G est annulé par F^s , on a une factorisation du morphisme F^s issu de B :

$$F^s: B \xrightarrow{u} A \rightarrow B^{(s)},$$

d'où une factorisation du morphisme F^s issu de Y :

$$F^s: Y \xrightarrow{v} X \rightarrow Y^{(s)},$$

donc $r \leq s$.

L'inégalité inverse résulte du lemme plus précis suivant:

Lemme 1.2.3. *Supposons que $u: B \rightarrow A$ soit une isogénie radicielle, que $Y \rightarrow X$ soit de degré p^r et que $i: X \hookrightarrow A$ vérifie la condition (i) de (*). Alors on a une factorisation canonique:*

$$F^r: A^{(-r)} \rightarrow B \xrightarrow{u} A,$$

et en particulier $G = G_{\text{inf}}$ est annulé par F^r .

On peut identifier \tilde{Y} à $\tilde{X}^{(-r)}$ et $\tilde{v}: \tilde{Y} \rightarrow \tilde{X}$ à F^r . La jacobienne de $\tilde{X}^{(-r)}$ est $J_{\tilde{X}^{(-r)}}$. On déduit alors du diagramme commutatif:

$$\begin{array}{ccc} \tilde{X}^{(-r)} & \longrightarrow & Y \\ F^r \downarrow & & \downarrow v \\ \tilde{X} & \longrightarrow & X, \end{array}$$

(où les flèches horizontales sont les normalisations), le diagramme commutatif de morphismes de schémas abéliens suivant:

$$\begin{array}{ccc} J_{\tilde{X}^{(-r)}} & \xrightarrow{a^{(-r)}} & A^{(-r)} \\ \downarrow F^r & \searrow b & \downarrow F^r \\ & B & \\ & \searrow u & \\ J_{\tilde{X}} & \longrightarrow & A \end{array}$$

où b est le morphisme d'albanese de $\tilde{j}: \tilde{X}^{(-r)} = \tilde{Y} \rightarrow B$. Or $\text{Ker } a^{(-r)} = N^{(-r)}$ est un schéma en groupes lisse, donc son image par b est un sous-schéma en groupes lisse de B . Comme d'autre part, cette image est contenue dans $\text{Ker}(u) = G$ qui est supposé radiciel, cette image est nulle et on obtient un morphisme $c: A^{(-r)} \rightarrow B$, telle que $b = ca^{(-r)}$. Mais alors, comme $a^{(-r)}$ est surjectif, $F^r: A^{(-r)} \rightarrow A$ se factorise en uc , d'où le lemme.

1.3.1. Par translation, on identifie l'espace tangent en un point quelconque de A à l'espace tangent à l'origine et on note \mathbb{P}_A l'espace projectif associé. A la courbe X plongée dans A par i est associée une «application de Gauss»: si x est un point lisse de X on lui fait correspondre le point de \mathbb{P}_A défini par la tangente à X en x . On obtient ainsi un morphisme du lieu lisse de X dans \mathbb{P}_A qui s'étend canoniquement en un morphisme $\gamma_X: \tilde{X} \rightarrow \mathbb{P}_A$. Soit \mathcal{I} le faisceau d'idéaux de \mathcal{O}_A qui définit X , de sorte que l'on a une suite exacte:

$$(1) \quad \mathcal{I}/\mathcal{I}^2 \rightarrow \Omega_A|_X \rightarrow \Omega_X \rightarrow 0.$$

Par image réciproque par $\alpha: \tilde{X} \rightarrow X$, on en déduit une suite exacte sur \tilde{X} :

$$\alpha^*(\mathcal{I}/\mathcal{I}^2) \rightarrow \tilde{i}^*(\Omega_A) \rightarrow \alpha^*(\Omega_X) \rightarrow 0.$$

Si l'on divise $\alpha^*(\Omega_X)$ par son sous-faisceau de torsion, on obtient un faisceau inversible $\tilde{\Omega}_X$, quotient de $\tilde{i}^*(\Omega_A)$, qui définit l'application $\gamma_X: \tilde{X} \rightarrow \mathbb{P}_A$. On a donc une suite exacte de faisceaux localement libres sur \tilde{X} :

$$(2) \quad 0 \rightarrow \tilde{\mathcal{N}}_X \rightarrow \tilde{i}^*(\Omega_A) \rightarrow \tilde{\Omega}_X \rightarrow 0$$

où $\tilde{\mathcal{N}}_X$ est le sous-fibré de $\tilde{i}^*(\Omega_A)$ engendré par l'image de $\alpha^*(\mathcal{I}/\mathcal{I}^2)$. Notons que $\tilde{\Omega}_X$ n'est autre que l'image de l'application sur les différentielles $\alpha^*(\Omega_X) \rightarrow \Omega_{\tilde{X}}$ associée à α . En particulier, le degré de γ_X , qui est le degré du faisceau inversible $\tilde{\Omega}_X$, est au plus $2g_{\tilde{X}} - 2$ où $g_{\tilde{X}}$ est le genre de \tilde{X} . Bien sûr, lorsque X est lisse, $\tilde{\Omega}_X = \Omega_X$ et $\tilde{\mathcal{N}}_X = \mathcal{I}/\mathcal{I}^2$ est le fibré normal.

1.3.2. Reprenons la situation de 1.2.1 où l'on a une isogénie $u: B \rightarrow A$. Aux immersions $i: X \hookrightarrow A$ et $j: Y \hookrightarrow B$ correspondent des applications de Gauss: $\gamma_X: \tilde{X} \rightarrow \mathbb{P}_A$ et $\gamma_Y: \tilde{Y} \rightarrow \mathbb{P}_B$.

L'application γ_X est constante si et seulement si $\tilde{\Omega}_X = \mathcal{O}_X$. C'est le cas si X est elliptique ou bien si X est stable par translations par un sous-groupe radiciel de rang p (par exemple, si $i: X \rightarrow A$ vérifie $(*)$ et si on prend pour $u: B \rightarrow A$ une isogénie radicielle de degré p , alors γ_Y est constante). Si $i: X \hookrightarrow A$ vérifie $(*)$, $H^0(X, \tilde{\Omega}_X)$ est un k -vectoriel de dimension au moins égale à la dimension de la variété A , en particulier, γ_X n'est pas constante si \tilde{X} est de genre au moins 2.

Proposition 1.3.3. *Supposons que l'isogénie u soit radicielle, que $i: X \hookrightarrow A$ vérifie $(*)$ (1.1.2) et que \tilde{X} soit de genre ≥ 2 . Alors on a:*

$$\text{degré } \gamma_Y \leq \text{degré } \gamma_X.$$

En effet, si p' est le degré de $Y \rightarrow X$, on a d'après 1.2.3, une factorisation:

$$F^r: A^{(-r)} \xrightarrow{w} B \xrightarrow{u} A.$$

Alors w induit un morphisme birationnel, noté encore $w: X^{(-r)} \rightarrow Y$. Soit $\tilde{X}^{(-r)} = \tilde{Y}$ la normalisée commune de $X^{(-r)}$ et de Y . Alors, avec les notations de 1.3.1, on a les inclusions $\tilde{\Omega}_Y \subset \tilde{\Omega}_{X^{(-r)}} \subset \Omega_{\tilde{X}^{(-r)}}$ et donc $\text{degré } \gamma_Y \leq \text{degré } \gamma_{X^{(-r)}}$. Mais $\text{degré } \gamma_{X^{(-r)}} = \text{degré } \gamma_X$ par transport par l'isomorphisme σ^r (1.0), d'où la proposition.

Corollaire 1.3.4. *Prenons pour isogénie u la multiplication par p dans A , soit p_A . Alors si $i: X \hookrightarrow A$ vérifie $(*)$ et si X est de genre ≥ 2 , les deux applications γ_Y et $\gamma_X \circ p_A$ de Y dans \mathbb{P}_A ne coïncident qu'en un nombre finie de points.*

Comme Y est réduit, il suffit de montrer que l'on a $\gamma_X \circ p_A \neq \gamma_Y$ et, a fortiori, il suffit de montrer que ces deux applications n'ont pas le même degré. Soit $A \xrightarrow{v} B \xrightarrow{u} A$ la factorisation de p_A dans laquelle v est étale et u est radicielle de degré p' . Comme p_A se factorise à travers le Frobenius de A , on a $r \geq 1$. Les deux applications γ_Y et $\gamma_X \circ p_A$ se factorisent à travers v , donc remplaçant p_A par $u: B \rightarrow A$, on est ramené au cas d'une isogénie radicielle. On a alors $\text{deg}(\gamma_Y) \leq \text{deg}(\gamma_X)$ d'après 1.3.3. Mais $\text{deg}(\gamma_X \circ u) = p^r \text{deg}(\gamma_X) > \text{deg}(\gamma_X)$ (puisque $r \geq 1$ et $\text{deg}(\gamma_X) \geq 1$) donc

$$\text{degré}(\gamma_Y) < \text{degré}(\gamma_X \circ u).$$

1.3.5. Terminons ce numéro en reformulant, en termes de faisceaux, le corollaire 1.3.4. On reprend les notations de 1.2.1 avec $u = p_A$.

Soient $\omega_1, \dots, \omega_d$ une base de Ω_A et $[p]: p_A^*(\Omega_A) \xrightarrow{\sim} \Omega_A$ l'isomorphisme de faisceaux libres qui induit l'identité sur les sections globales; donc $[p]p_A^*(\omega_i) = \omega_i$, pour $i=1, \dots, d$. Par image réciproque par $j: Y \hookrightarrow A$ on obtient un isomorphisme $[p]_Y: (iu)^*\Omega_A \xrightarrow{\sim} j^*\Omega_A$ qui s'insère dans un diagramme:

$$(1) \quad \begin{array}{ccccccc} v^*(\mathcal{F}/\mathcal{F}^2) & \longrightarrow & (iu)^*\Omega_A & \longrightarrow & v^*(\Omega_X) & \longrightarrow & 0 \\ & & \downarrow [p]_Y & & & & \\ \mathcal{F}/\mathcal{F}^2 & \longrightarrow & j^*(\Omega_A) & \longrightarrow & \Omega_Y & \longrightarrow & 0 \end{array}$$

dans lequel les lignes sont exactes, la première étant l'image réciproque par v de la suite exacte (1) de 1.3.1 associée à γ_X , et la seconde étant l'analogue de (1) pour γ_Y .

Prenant l'image réciproque de ce diagramme par le morphisme de normalisation $\beta: \tilde{Y} \rightarrow Y$ et remplaçant les suites exactes (1) de 1.3.1 par les suites exactes (2), on obtient le diagramme à lignes exactes:

$$(2) \quad \begin{array}{ccccccc} 0 & \longrightarrow & \tilde{v}^*(\tilde{\mathcal{N}}_X) & \longrightarrow & (\tilde{i}\tilde{u})^*\Omega_A & \longrightarrow & \tilde{u}^*(\tilde{\Omega}_X) \longrightarrow 0 \\ & & & & \downarrow [p]_{\tilde{Y}} \wr & & \\ 0 & \longrightarrow & \tilde{\mathcal{N}}_Y & \longrightarrow & \tilde{j}^*(\Omega_A) & \longrightarrow & \tilde{\Omega}_Y \longrightarrow 0 \end{array}$$

où $[p]_{\tilde{Y}}$ est l'isomorphisme image réciproque de $[p]$ par \tilde{j} .

Par composition, on déduit de ces diagrammes des applications:

$$(3) \quad \gamma: v^*(\mathcal{S}/\mathcal{S}^2) \rightarrow \Omega_Y \quad \text{et} \quad \tilde{\gamma}: \tilde{v}^*(\tilde{\mathcal{N}}_X) \rightarrow \tilde{\Omega}_Y.$$

Bien sûr γ s'identifie à $\tilde{\gamma}$ sur l'ouvert de lissité de Y situé au-dessus de l'ouvert de lissité de X .

Explicitons localement γ . Soient a une section locale de \mathcal{S} et \bar{a} son image dans $\mathcal{S}/\mathcal{S}^2$. Soit $da = \sum_i f_i \omega_i$ la différentielle de a . Alors l'image de \bar{a} dans $\Omega_A|_X$ qui intervient dans 1.3.1 (1) est simplement $da|_X$. D'où

$$(4) \quad \gamma(v^*(\bar{a})) = \sum_i (f_i \circ u) \omega_i|_Y.$$

Corollaire 1.3.6. *Sous les hypothèses de 1.3.4 les applications γ et $\tilde{\gamma}$ ne sont pas nulles.*

Comme $\tilde{\mathcal{N}}_X$ est localement libre et que γ et $\tilde{\gamma}$ coïncident sur un ouvert non vide, il suffit de montrer que $\tilde{\gamma} \neq 0$. Or, si on avait $\tilde{\gamma} = 0$, $[p]_{\tilde{Y}}$ induirait, par passage au quotient dans (2), un isomorphisme $\tilde{v}^*(\tilde{\Omega}_X) \xrightarrow{\sim} \tilde{\Omega}_Y$ et on a déjà remarqué que γ_Y et $\gamma_X p_A$ n'avaient pas le même degré (cf. 1.3.4).

Remarque 1.3.7. Les mêmes considérations de degré montrent que les corollaires 1.3.4 et 1.3.6 restent valables si on suppose X lisse de genre ≥ 2 , même si $i: X \hookrightarrow A$ ne vérifie pas (*). En fait la condition (*) nous sert, d'une part pour traiter le cas X singulier, d'autre part pour calculer explicitement certains degrés (cf. 1.2.2).

2. Compléments sur le fibré normal

2.0. Dans ce numéro, R_1 est un anneau local d'idéal maximal m , de corps résiduel k ; on suppose de plus que m est de carré nul et est un k -espace vectoriel de dimension 1; on choisit un générateur π de m . Dans la suite, R_1 interviendra comme quotient d'un anneau de valuation discrète par le carré de son idéal maximal. On affecte d'un indice zéro les k -schémas; en particulier, si S_1 est un R_1 -schéma, S_0 désigne le k -schéma $S_1 \times_{R_1} k$, déduit de S_1 , par réduction modulo m .

2.0.1. Soit S_1 un R_1 -schéma. La multiplication par π induit un morphisme de \mathcal{O}_{S_0} -Modules $\theta: \mathcal{O}_{S_0} \rightarrow \pi \mathcal{O}_{S_1} = \pi \mathcal{O}_{S_0}$. Nous utiliserons fréquemment dans la suite le fait que S_1 est plat sur R_1 si et seulement si θ est un isomorphisme ([2] chap. III §5 Th. 1). Lorsque cette condition est réalisée, nous noterons parfois « π^{-1} » l'application inverse de θ .

2.1. Soient S un schéma et \mathcal{M} un faisceau quasi-cohérent sur S . Rappelons que le fibré vectoriel $\mathbf{V}(\mathcal{M})$, associé au faisceau \mathcal{M} , est le S -schéma affine défini par l'algèbre symétrique de \mathcal{M} ; il représente le foncteur qui à tout S -schéma $f: T \rightarrow S$, associe l'ensemble des morphismes de \mathcal{O}_T -Modules $u: f^*(\mathcal{M}) \rightarrow \mathcal{O}_T$.

2.2. Dans la suite de ce numéro, on considère un R_1 -schéma A_1 et un sous-schéma fermé X_0 de $A_0 = A_1 \times_{R_1} k$. Soit \mathcal{I} (resp. \mathcal{I}_0) le faisceau d'idéaux de \mathcal{O}_{A_1} (resp. \mathcal{O}_{A_0}) qui définit X_0 . Alors l'image de π dans \mathcal{O}_{A_1} est dans \mathcal{I} et on a des suites exactes:

$$(1) \quad \begin{aligned} \pi \mathcal{O}_{A_0} &\rightarrow \mathcal{I} \rightarrow \mathcal{I}_0 \rightarrow 0, \\ \pi \mathcal{O}_{X_0} &\rightarrow \mathcal{I}/\mathcal{I}^2 \rightarrow \mathcal{I}_0/\mathcal{I}_0^2 \rightarrow 0. \end{aligned}$$

Considérons alors le fibré vectoriel $\mathbf{V}(\mathcal{I})$ au-dessus du schéma A_1 et soit $\mathbf{V}(\mathcal{I})^*$ le sous-schéma de $\mathbf{V}(\mathcal{I})$ qui représente le foncteur suivant: pour tout A_1 -schéma $f: T \rightarrow A_1$, $\mathbf{V}(\mathcal{I})^*(T)$ est le sous-ensemble de $\mathbf{V}(\mathcal{I})(T)$ formé des morphismes $u: f^*(\mathcal{I}) \rightarrow \mathcal{O}_T$ tels que $u(\pi) = 1$ (on note abusivement encore π , l'image canonique de π dans $f^*(\mathcal{I})$).

Si $u: f^*(\mathcal{I}) \rightarrow \mathcal{O}_T$ correspond à un point de $\mathbf{V}(\mathcal{I})^*$, on a donc: $0 = u(\pi^2) = \pi 1$, donc π annule \mathcal{O}_T . De plus $\mathcal{I} \mathcal{O}_T = u(\mathcal{I} \pi) = \pi u(\mathcal{I}) = 0$, donc \mathcal{I} annule \mathcal{O}_T . C'est dire que le morphisme structural $\mathbf{V}(\mathcal{I})^* \rightarrow A_1$ se factorise à travers X_0 ; en particulier on a $\mathbf{V}(\mathcal{I})^* = \mathbf{V}(\mathcal{I}/\mathcal{I}^2)^*$. Désormais on note simplement $V_0^{\mathcal{I}}$, ou même V_0 , le X_0 -schéma $\mathbf{V}(\mathcal{I})^*$ et $h_0: V_0 \rightarrow X_0$ le morphisme structural.

Exemples 2.2.1. i) Si $A_1 = A_0$, on a $\pi = 0$ dans \mathcal{O}_{A_1} et donc V_0 est vide. En fait le cas le plus intéressant est celui où A_1 est plat sur R_1 .

ii) Si A_1 est lisse sur R_1 et si X_0 est lisse sur k , alors $h_0: V_0 \rightarrow X_0$ est lisse. Plus précisément, supposons A_1 affine et X_0 défini dans A_0 par une suite régulière que l'on relève en des éléments t_i de \mathcal{I} . Alors il existe des sections T_i de \mathcal{O}_{A_0} , uniquement déterminées, telles que $t_i = \pi T_i$ (2.0.1) et V_0 est l'espace affine sur X_0 de coordonnées les T_i .

2.2.2. On a une action naturelle de $\mathbf{V}(\mathcal{I}_0/\mathcal{I}_0^2)$ sur $\mathbf{V}(\mathcal{I})^*$. En effet si $f: T \rightarrow A$ est un A -schéma, on déduit de (1) la suite exacte:

$$f^*(\mathcal{O}_{X_0}) \rightarrow f^*(\mathcal{I}/\mathcal{I}^2) \xrightarrow{-\tau} f^*(\mathcal{I}_0/\mathcal{I}_0^2) \rightarrow 0.$$

Alors si $u: f^*(\mathcal{I}/\mathcal{I}^2) \rightarrow \mathcal{O}_T$ envoie π sur 1, tout autre morphisme u' ayant cette propriété s'écrit uniquement $u' = u + v\tau$, pour un unique $v: f^*(\mathcal{I}_0/\mathcal{I}_0^2) \rightarrow \mathcal{O}_T$. Ceci définit l'action de $\mathbf{V}(\mathcal{I}_0/\mathcal{I}_0^2)$ sur $\mathbf{V}(\mathcal{I})^*$ et montre que pour cette action, $\mathbf{V}(\mathcal{I})^*$ est un espace formellement principal homogène ([4] Exp. III p. 13).

2.3. Soient S_1 un R_1 -schéma plat et $u_1: S_1 \rightarrow A_1$ un R_1 -morphisme tel que $u_0: S_0 \rightarrow A_0$ se factorise à travers X_0 . Cette dernière condition signifie que l'on

a $\mathcal{I}\mathcal{O}_{S_1} = \pi\mathcal{O}_{S_1}$. Par ailleurs, la platitude de S_1 entraîne que la multiplication par $\pi: \mathcal{O}_{S_0} \rightarrow \pi\mathcal{O}_{S_1}$ est un isomorphisme (2.0.1), d'où un morphisme de \mathcal{O}_{S_1} -modules $u^*(\mathcal{I}) \xrightarrow{\text{can.}} \mathcal{I}\mathcal{O}_{S_1} = \pi\mathcal{O}_{S_1} \xrightarrow{\langle\pi^{-1}\rangle} \mathcal{O}_{S_0}$ qui envoie $u^*(\pi)$ sur 1. Il lui correspond un k -morphisme $u'_0: S_0 \rightarrow V_0$ et on a $f_0 u'_0 = u_0$. Nous dirons que u'_0 est le relèvement de u à travers V_0 .

Notons $(A_1, X_0)(R_1)$ le sous-ensemble de $A_1(R_1)$ formé des points dont l'image dans $A_0(k)$ appartient à $X_0(k)$. L'opération de relèvement appliquée avec $S_1 = \text{Spec}(R_1)$ fournit alors une application canonique $\tau: (A_1, X_0)(R_1) \rightarrow V_0(k)$, rendant commutatif le diagramme:

$$\begin{array}{ccc} (A_1, X_0)(R_1) & \xrightarrow{\tau} & V_0(k) \\ & \searrow & \nearrow h_0 \\ & & X_0(k). \end{array}$$

Lorsque A_1 est lisse sur R_1 et X_0 lisse sur k , l'application $(A_1, X_0)(R_1) \xrightarrow{\tau} V_0(k)$ est surjective, comme on le voit sur les coordonnées de 2.2.1 ii).

Exemple 2.3.1. Reprenons l'exemple 2.2.1 ii) et les notations t_i, T_i . Si S_1 est un R_1 -schéma plat et $u_1: S_1 \rightarrow A_1$ un R_1 -morphisme tel que u_0 se factorise à travers X_0 , on a $t_i \circ u = \pi f_i$ où les f_i sont des sections uniquement déterminées de \mathcal{O}_{S_0} . Alors le relèvement u'_0 de u_0 est décrit par les relations: $T_i \circ u'_0 = f_i$.

2.4. Soit X_1 un sous-schéma de A_1 , plat sur R_1 tel que $X_1 \times_{B_1} k = X_0$. Notons $j_1: X_1 \hookrightarrow A_1$ l'immersion correspondante et \mathcal{I} le faisceau d'idéaux de \mathcal{O}_{A_1} qui définit X_1 . Le relèvement (2.3) de j_1 est un k -morphisme $j'_0: X_0 \rightarrow V_0$ tel que $h_0 j'_0 = j_0$, donc j'_0 est une section de h_0 . On a $\mathcal{I} \subset \mathcal{I}$ et l'image de \mathcal{I} dans le faisceau quotient $\mathcal{O}_{X_1} = \mathcal{O}_{A_1}/\mathcal{I}$ est $\pi\mathcal{O}_{X_0}$. Si l'on revient à la définition du relèvement, on trouve que j'_0 est associé au morphisme de faisceaux: $\mathcal{I} \rightarrow \pi\mathcal{O}_{X_1} \xrightarrow{\sim} \mathcal{O}_{X_0}$ composé de la surjection canonique et de l'isomorphisme $\langle\pi^{-1}\rangle$. En particulier le noyau de cette application est \mathcal{I} . Réciproquement, si l'on part d'une section j'_0 de h_0 , elle provient d'un morphisme de faisceau $\mathcal{I} \rightarrow \mathcal{O}_{X_0}$ qui envoie π sur 1. Soit \mathcal{I} son noyau. Alors on a une suite exacte de faisceaux:

$$0 \rightarrow \mathcal{O}_{X_0} \xrightarrow{\theta} \mathcal{O}_{A_1}/\mathcal{I} \rightarrow \mathcal{O}_{A_1}/\mathcal{I} \rightarrow 0$$

avec $\mathcal{O}_{A_1}/\mathcal{I} = \mathcal{O}_{X_0}$ et où $\theta(1)$ est l'image de π . Si alors X_1 est le sous-schéma de A_1 défini par \mathcal{I} , on a $X_1 \times_{R_1} k = X_0$ et X_1 est plat sur R_1 (2.0.1). On a donc établi le résultat suivant (bien connu au moins dans le cas où A_0 et X_0 sont lisses sur k ([5] cor. 5.4)).

Proposition 2.4.1. *L'application de relèvement (2.3) fournit une bijection canonique entre les sous-schémas X_1 de A_1 , plats sur R_1 , tels que $X_1 \times_{R_1} k = X_0$ et les sections de $h_0: V_0 \rightarrow X_0$.*

3. Calcul différentiel modulo p^2

3.0. Dans ce numéro, on reprend les notations du numéro précédent, mais on suppose de plus que le corps résiduel k de R_1 est algébriquement clos de

caractéristique $p > 0$ et que le générateur π de m est l'image de p . Autrement dit, R_1 est le quotient, modulo p^2 , d'un anneau de valuation discrète, d'inégales caractéristiques, non ramifié, à corps résiduel algébriquement clos de caractéristique $p > 0$.

3.1. Soit $u_1: B_1 \rightarrow A_1$ un R_1 -morphisme entre schémas lisses, tel que $u_0 = u_1 \times_{R_1} k: B_0 \rightarrow A_0$ ait une différentielle nulle. Soient $i_0: X_0 \hookrightarrow A_0$ une immersion fermée, Y_0 l'image réciproque réduite de X_0 par u_0 et $j_0: Y_0 \hookrightarrow B_0$ l'immersion associée. On note $v_0: Y_0 \rightarrow X_0$, l'application induite par $u_0: B_0 \rightarrow A_0$. Soit \mathcal{I} (resp. \mathcal{I}_0) le faisceau d'idéaux de \mathcal{O}_{A_1} (resp. \mathcal{O}_{A_0}) qui définit X_0 et soit \mathcal{J} (resp. \mathcal{J}_0) le faisceau d'idéaux de \mathcal{O}_{B_1} (resp. \mathcal{O}_{B_0}) qui définit Y_0 . On a $\mathcal{I}\mathcal{O}_{B_1} \subset \mathcal{J}$, $\mathcal{I}_0\mathcal{O}_{B_0} \subset \mathcal{J}_0$.

Si $h_0: V_0 \rightarrow X_0$ est associé à \mathcal{I} comme dans 2.2, on dispose de l'application de relèvement (2.3) $\tau: (A_1, X_0)(R_1) \rightarrow V_0(k)$. Soit de même $(B_1, Y_0)(R_1)$ la partie de $B_1(R_1)$ image réciproque de $Y_0(k)$ par l'application canonique $B_1(R_1) \rightarrow B_0(k)$. Comme la différentielle de u_0 est nulle, l'application $B_1(R_1) \rightarrow A_1(R_1)$ induite par u se factorise à travers $B_0(k)$. A fortiori, l'application $(B_1, Y_0)(R_1) \rightarrow (A_1, X_0)(R_1)$ induite par u se factorise à travers $Y_0(k)$, via une application $\bar{u}: Y_0(k) \rightarrow (A, X_0)(R_1)$. Composant \bar{u} avec τ , on obtient une application ensembliste $Y_0(k) \rightarrow V_0(k)$. Le but de ce numéro est de construire un k -morphisme canonique $v'_0: Y_0 \rightarrow V_0$ qui sur les points réalise $\tau\bar{u}$ et de calculer sa différentielle. Notons que l'on aura alors le diagramme commutatif:

$$(1) \quad \begin{array}{ccccc} (B, Y_0)(R_1) & \xrightarrow{u} & (A, X_0)(R_1) & \xrightarrow{\tau} & V_0(k) \\ \downarrow & \nearrow \bar{u} & \downarrow & \nearrow h_0 & \\ Y_0(k) & \xrightarrow{v_0} & X_0(k) & & \end{array}$$

3.2. Soient a et b des sections de \mathcal{O}_{A_1} sur un ouvert U , a_0, b_0 (resp. $\underline{a}, \underline{b}$, resp. $\underline{a}_0, \underline{b}_0$) leurs images dans \mathcal{O}_{A_0} (resp. \mathcal{O}_{B_1} , resp. \mathcal{O}_{B_0}). Comme k est parfait, B_0 lisse et la différentielle de u_0 nulle, \underline{a}_0 et \underline{b}_0 sont des puissances p -èmes dans \mathcal{O}_{B_0} : $\underline{a}_0 = \alpha_0^p, \underline{b}_0 = \beta_0^p$. Soient α et β des relèvements de α_0 et de β_0 dans \mathcal{O}_{B_1} . Alors α^p est l'unique relèvement de \underline{a}_0 dans \mathcal{O}_{B_1} qui est une puissance p -ème; c'est le «relèvement de Teichmüller» de \underline{a}_0 noté \underline{a}_0^* . Soit de même $\underline{b}_0^* = \beta^p$. On a les relations:

$$(2) \quad (\underline{a}\underline{b})_0^* = \underline{a}_0^* \underline{b}_0^*; \quad (\underline{a} + \underline{b})_0^* - \underline{a}_0^* + \underline{b}_0^* + pS(\alpha_0, \beta_0)$$

où $S(U, V)$ est le polynôme homogène de degré p dans $\mathbb{Z}[U, V]$, tel que:

$$S(U, V) = [(U + V)^p - U^p - V^p]/p.$$

Comme B_1 est R_1 -plat et que \underline{a} et \underline{a}_0^* sont deux relèvements de \underline{a}_0 , il existe d'après 2.0.1 une unique section $\Phi(\underline{a})$ dans \mathcal{O}_{B_0} , telle que:

$$(3) \quad \underline{a} = \underline{a}_0^* + p\Phi(\underline{a}).$$

De (2) on déduit les identités:

$$\begin{aligned}
 \Phi(a+b) &= \Phi(a) + \Phi(b) + S(\alpha_0, \beta_0) \\
 \Phi(ab) &= \underline{a}_0 \Phi(b) + \underline{b}_0 \Phi(a) \\
 \Phi(p) &= 1.
 \end{aligned}
 \tag{4}$$

Supposons que $a \in \mathcal{I}$, alors $\underline{a}_0 = \alpha_0^p \in \mathcal{I}_0$ et comme Y_0 est réduit, $\alpha_0 \in \mathcal{I}_0$ et donc $\underline{a}_0 \in \mathcal{I}_0^p$. Les formules (4) montrent alors que Φ est linéaire modulo \mathcal{I}_0^p et, a fortiori, définit un morphisme de faisceaux: $u^*(\mathcal{I}) \rightarrow \mathcal{O}_{B_0}/\mathcal{I}_0$ qui envoie p sur 1. Par définition de V_0 (2.2), il lui correspond un k -morphisme $v'_0: Y_0 \rightarrow V_0$. Montrons que l'application ensembliste $\tau \bar{u}: Y_0(k) \rightarrow V_0(k)$ est induite par v'_0 (ce qui suffit à la caractériser, Y_0 étant réduit et k étant algébriquement clos). Pour cela notons que si $f_1: C_1 \rightarrow B_1$ est un R_1 -morphisme avec C_1 lisse sur R_1 , et si Z_0 est l'image réciproque réduite de Y_0 par f_0 , alors la construction précédente de v'_0 est fonctorielle par rapport à f , c'est-à-dire associée à u le morphisme $v'_0 f_0: Z_0 \rightarrow V_0$. Appliquons cette remarque en prenant $C_1 = \text{Spec}(R_1)$ et pour $f_1: \text{Spec}(R_1) \rightarrow B_1$ un point de $(B_1, Y_0)(R_1)$. Alors $Z_0 = \text{Spec}(k)$, et la construction ci-dessus associée à u l'unique application linéaire: $I \xrightarrow{\text{can}} m \xrightarrow{\sim} k$, donc correspond bien au relèvement de u au sens de 2.3.

3.3. Pour terminer ce numéro, calculons la différentielle de v'_0 . La définition de $V_0 = \mathbf{V}(\mathcal{I})^*$ (2.2) entraîne que le faisceau Ω_{V_0/X_0} des différentielles de V_0 relativement à X_0 est canoniquement isomorphe à $h_0^*(\mathcal{I}_0/\mathcal{I}_0^2)$, d'où une suite exacte:

$$h_0^*(\Omega_{X_0}) \rightarrow \Omega_{V_0} \rightarrow h_0^*(\mathcal{I}_0/\mathcal{I}_0^2) \rightarrow 0.
 \tag{5}$$

Comme la différentielle de u_0 est nulle, la différentielle de v'_0 provient, par passage au quotient, d'une application:

$$\delta: v_0^*(\Omega_{V_0/X_0}) = v_0^*(\mathcal{I}_0/\mathcal{I}_0^2) \rightarrow \Omega_{Y_0}
 \tag{6}$$

que nous allons déterminer.

Soit \bar{a}_0 une section locale de $\mathcal{I}_0/\mathcal{I}_0^2$ image d'une section locale a de \mathcal{I} . Avec les notations de 3.2, on a:

$$\delta v_0^*(\bar{a}_0) = d\Phi(a)|_{Y_0}.$$

Or d'après (3), on a:

$$du_1^*(a) = u_1^*(da) = p(dx_0 + d\Phi(a)).$$

Donc $u_1^*(da) = p\Psi(a)$ où $\Psi(a)$ est l'unique section locale de Ω_{B_0} telle que

$$\Psi(a) = dx_0 + d\Phi(a).$$

Comme $\alpha_0 \in \mathcal{I}_0$, on a $\Psi(a)|_{Y_0} = d\Phi(a)|_{Y_0}$ donc est égale à $\delta v_0^*(\bar{a}_0)$.

En résumé, on a obtenu le résultat suivant:

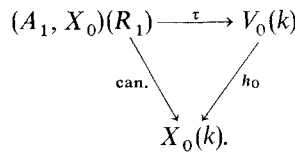
Proposition 3.3.1. *Sous les hypothèses de 3.1, il existe un unique k -morphisme $v'_0: Y_0 \rightarrow V_0$, tel que $h_0 v'_0 = v_0$ et qui sur les points rationnels induit l'application*

$\tau \bar{u}: Y_0(k) \rightarrow V_0(k)$. L'application δ (6) qui décrit la différentielle de v'_0 , se calcule comme suit: soit a une section locale de \mathcal{S} , d'image \bar{a}_0 dans $\mathcal{S}_0/\mathcal{S}_0^2$. Alors $\delta v_0^*(\bar{a}_0) = \Psi(a)|_{Y_0}$, où $\Psi(a)$ est l'unique section locale de Ω_{B_0} telle que $u_1^*(da) = p\Psi(a)$.

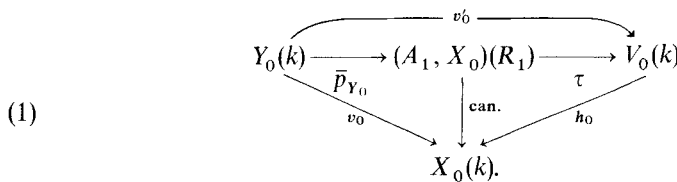
4. Application aux schémas abéliens: étude modulo p^2

4.0. Dans ce numéro, R_1 est un anneau local du type considéré dans 3.0.

Soient A_1 un R_1 -schéma abélien, $i_0: X_0 \hookrightarrow A_0 = A_1 \times_{R_1} k$ une immersion d'une courbe propre et intègre, définie par un faisceau d'idéaux \mathcal{S} (resp. \mathcal{S}_0) dans A_1 (resp. A_0). On note $h_0: V_0 \rightarrow X_0$ le X_0 -schéma $\mathbb{V}(\mathcal{S})^*$ considéré dans 2.2. Soit $(A_1, X_0)(R_1)$ l'image réciproque dans $A_1(R_1)$ de $X_0(k)$ par l'application de réduction mod. $p: A_1(R_1) \rightarrow A(k)$. Alors l'opération de relèvement (2.3) fournit une application canonique τ qui rend commutatif le diagramme:



4.1. Soit p_{A_1} (resp. p_{A_0}) le morphisme de multiplication par p dans A_1 (resp. A_0). Comme la différentielle de p_{A_0} est nulle, on peut appliquer les considérations du numéro précédent en prenant $B_1 = A_1$ et $u_1 = p_{A_1}$. Soient donc Y_0 l'image réciproque réduite de X_0 par p_{A_0} et $v_0: Y_0 \rightarrow X_0$ le morphisme induit par p_{A_0} . La multiplication par $p: A_1(R_1) \rightarrow A_1(R_1)$ définit par passage au quotient une application $\bar{p}: A(k) \rightarrow A_1(R_1)$; celle-ci induit une application $\bar{p}_{Y_0}: Y_0(k) \rightarrow (A_1, X_0)(R_1)$. L'image de \bar{p}_{Y_0} est formée des points de $pA_1(R_1)$ qui relèvent des points de $X_0(k)$. D'après 3.3.1, il existe un k -morphisme canonique $v'_0: Y_0 \rightarrow V_0$, tel que $h_0 v'_0 = v_0$ qui, sur les points à valeur dans k , coïncide avec $\tau \bar{p}_{Y_0}$. On a donc un diagramme commutatif:



Reprenons les considérations et les notations du N° 1, mis à part que les k -schémas et k -morphisms sont maintenant affectés d'un indice «0». Aux immersions $X_0 \hookrightarrow A_0$ et $Y_0 \hookrightarrow A_0$ correspondent des applications de Gauss (1.3.2) γ_{X_0} et γ_{Y_0} et un morphisme de faisceaux $\gamma: v_0^*(\mathcal{S}_0/\mathcal{S}_0^2) \rightarrow \Omega_{Y_0}$ (1.3.5 (3)) qui mesure «la différence» entre $\gamma_{X_0} v_0$ et γ_{Y_0} . Par ailleurs, comme v_0 a une différentielle nulle, la différentielle de v'_0 provient d'une application $\delta: v_0^*(\mathcal{S}_0/\mathcal{S}_0^2) \rightarrow \Omega_{Y_0}$ (3.3 (5)).

Lemme 4.1.1. *Les applications γ et $\delta: v_0^*(\mathcal{F}_0/\mathcal{F}_0^2) \rightarrow \Omega_{Y_0}$ coïncident.*

En effet, soient $\omega_1, \dots, \omega_d$ une base de Ω_A et a une section locale de \mathcal{F} d'image \bar{a}_0 dans $\mathcal{F}_0/\mathcal{F}_0^2$ et soit $da = \sum_i f_i \omega_i$ la différentielle de a . Alors, d'après la formule (4) de 1.3.5, on a :

$$\gamma(v_0^*(\bar{a}_0)) = \sum_i (f_i \circ v_0) \omega_i|_{Y_0}.$$

Par ailleurs, on a $p_{A_1}^*(\omega_i) = p\omega_i$, donc $p_{A_1}^*(da) = p(\sum_i (f_i \circ p_{A_0}) \omega_i)$ et par suite, avec les notations de 3.3.1, $\psi(a) = \sum_i (f_i \circ p_{A_0}) \omega_i|_{A_0}$. On déduit alors de 3.3.1 que l'on a :

$$\delta(v_0^*(\bar{a}_0)) = \sum_i (f_i \circ v_0) \omega_i|_{Y_0},$$

d'où le lemme.

Soient alors Y'_0 l'image schématique de Y_0 par v'_0 et $h'_0: Y'_0 \rightarrow X_0$ la restriction de h_0 à Y'_0 . Comme v_0 est fini, h'_0 est fini.

Proposition 4.1.2. *Supposons que $i_0: X_0 \hookrightarrow A_0$ vérifie (*) (1.1.2) et que la courbe \tilde{X}_0 , normalisée de X_0 , soit de genre ≥ 2 . Alors l'application $Y_0 \rightarrow Y'_0$ déduite de v'_0 est génériquement étale.*

Notons d'abord que la propriété (*) entraîne que Y_0 , et donc aussi Y'_0 , sont intègres (1.2.2). Par ailleurs, d'après 1.3.6, on peut trouver un ouvert non vide U_0 de X_0 au-dessus duquel X_0 et Y_0 sont lisses et γ surjective. D'après 4.1.1 v'_0 est non ramifiée au-dessus de U_0 . Si alors on restreint U_0 pour que Y'_0 soit également lisse au-dessus de U_0 , $Y_0 \rightarrow Y'_0$ est étale au-dessus de U_0 .

4.2. Soit G_1 (resp. G_0) le noyau de p_{A_1} (resp. p_{A_0}). Alors G_0 est produit de sa composante neutre $(G_0)_{\text{inf}}$ et de sa composante étale $(G_0)_{\text{et}}$. Par contre, sur R_1 on a seulement une suite exacte de schémas en groupes plats :

$$(1) \quad 0 \rightarrow (G_1)_{\text{inf}} \rightarrow G_1 \rightarrow (G_1)_{\text{et}} \rightarrow 0,$$

où $(G_1)_{\text{inf}}$ relève $(G_0)_{\text{inf}}$ et $(G_1)_{\text{et}}$ relève $(G_0)_{\text{et}}$.

La proposition 4.1.2 entraîne que le degré radiciel de $h'_0: Y'_0 \rightarrow X_0$ est égal à celui de $v_0: Y_0 \rightarrow X_0$, d'où d'après 1.2.2 :

Corollaire 4.2.1. *Sous les hypothèses de 4.1.2, le degré radiciel de h'_0 est p^s , où s est le plus petit entier tel que F^s annule $(G_0)_{\text{inf}}$; en particulier on a $s \geq 1$.*

Remarque 4.2.2. Que peut-on dire sur le degré séparable de v'_0 ? Bien sûr celui-ci est majoré par le degré séparable de v_0 qui est aussi le rang de $(G_0)_{\text{et}}$. On peut affiner cette majoration en tenant compte du choix du relèvement A_1 de A_0 . En effet, on voit facilement qu'il existe un unique sous-groupe étale maximal H de $(G_1)_{\text{et}}$, au-dessus duquel la suite exacte (1) ci-dessus est scindable. Choisissons alors un sous-schéma en groupes étale H_1 de G_1 qui relève H et soit B_1 le quotient A_1/H_1 . On a une factorisation de p_{A_1} en :

$$A_1 \xrightarrow{w_1} B_1 \xrightarrow{u_1} A_1.$$

Nous pouvons appliquer la construction du N° 3 avec u_1 à la place de p_{A_1} . On en déduit que si Z_0 est l'image réciproque réduite de X_0 dans B_0 , le morphisme $v'_0: Y_0 \rightarrow Y'_0$ se factorise à travers Z_0 . Ainsi le degré séparable de v'_0 est au plus le degré séparable de $u_0: B_0 \rightarrow A_0$ égal au rang de $(G_1)_{\text{ét}}/H$.

Exemple 4.2.3. Supposons que A_0 soit une variété abélienne ordinaire. Alors on a $H=(G_1)_{\text{ét}}$ si et seulement si la suite exacte (1) est scindable, c'est-à-dire si et seulement si A_1 est un relèvement canonique de A_0 au sens de Serre-Tate ([10] § 5). Dans ce cas le degré de h'_0 est égal à son degré radiciel qui est $p^s = p$.

4.3. Soient X_1 une courbe plate définie sur R_1 qui relève X_0 et $i_1: X_1 \hookrightarrow A_1$ une immersion qui prolonge i_0 . A la donnée de i_1 correspond par 2.4.1 une section i'_0 de $h_0: V_0 \rightarrow X_0$, en partilier, V_0 est maintenant un espace principal homogène sous $\mathbf{V}(\mathcal{I}_0/\mathcal{I}_0^2)$ (2.2.2) trivialisé par i'_0 . On note X'_0 la courbe image de i'_0 , donc h_0 induit un isomorphisme $X'_0 \xrightarrow{\sim} X_0$.

Soit $x \in pA_1(R_1) \cap X_1(R_1)$ et soit $\tau(x) \in V_0(k)$ le relèvement de x (2.2.2). Alors $\tau(x) \in X'_0(k)$ et d'après (4.1), $\tau(x)$ est aussi dans l'image de v'_0 , donc est dans $Y'_0(k)$. On obtient ainsi un diagramme commutatif:

$$\begin{array}{ccc}
 pA_1(R_1) \cap X_1(R_1) & \xrightarrow{\tau} & X'_0(k) \cap Y'_0(k) \\
 \text{can.} \searrow & & \nearrow h_0|_{X'_0(k)} \\
 & & X_0(k)
 \end{array}$$

Lemme 4.3.1. *L'image de $pA_1(R_1) \cap X_1(R_1)$ dans $X_0(k)$ est contenue dans l'image de $X'_0(k) \cap Y'_0(k)$ et lui est égale au-dessus de l'ouvert de lissité de X_0 .*

La première assertion est claire vu le diagramme précédent. Prouvons la dernière assertion. Soit $\sigma \in X'_0(k) \cap Y'_0(k)$ un point de $V_0(k)$ qui se projette sur un point lisse x_0 de X_0 . Montrons que σ est l'image par τ d'un point de $pA_1(R_1) \cap X_1(R_1)$. Comme $\sigma \in Y'_0(k)$, il existe un point $y_0 \in Y_0(k)$ tel que $v'_0(y_0) = \sigma$. Comme A_1 est lisse sur R_1 , on peut relever y_0 en $y_1 \in A_1(R_1)$. Alors $x = py_1 = \bar{p}y_0$ est un point de $pA_1(R_1)$ qui relève x_0 et l'on a $\tau(x) = \sigma$. Il suffit donc de montrer que $x \in X_1(R_1)$, sachant que $\tau(x) \in X'_0(k)$. Or X_0 est supposée lisse sur k en x_0 , donc X_1 est lisse sur R_1 en x_0 et localement, le faisceau d'idéaux qui définit X_1 dans A_1 est engendré par une suite régulière (t_1, \dots, t_{d-1}) . Au choix des t_i correspondent des coordonnées T_1, \dots, T_{d-1} sur le X_0 -schéma V_0 , telles que, si un point $x \in A_1(R_1)$ envoie t_i sur pf_i , $i=1, \dots, d-1$, $f_i \in k$, alors son relèvement $\tau(x)$ est le point de V_0 , de coordonnées $T_i = f_i$ (2.3.1). Il en résulte que X'_0 a pour équations dans V_0 , $T_i = 0$ pour $i=1, \dots, d-1$. Donc $\tau(x) \in X'_0(k) \Leftrightarrow f_i = 0, i=1, \dots, d-1, \Leftrightarrow x \in X_1(R_1)$.

4.4. Soient \tilde{Y}'_0 la courbe normalisée de Y'_0 et $\tilde{h}'_0: \tilde{Y}'_0 \rightarrow X_0$ le morphisme composé de la normalisation et de la projection h'_0 . Notons \mathcal{M}_0 le fibré vectoriel sur \tilde{Y}'_0 égal au quotient de $\tilde{h}'_0^*(\mathcal{I}_0/\mathcal{I}_0^2)$ par son sous-faisceau de torsion. Par exemple, si X_0 est lisse, ou plus généralement si X_0 est localement intersection complète dans A_0 , on a $\mathcal{M}_0 = \tilde{h}'_0^*(\mathcal{I}_0/\mathcal{I}_0^2)$. Enfin soit \mathcal{M}_0^\vee le dual de \mathcal{M}_0 .

Si $a \in A_1(R_1)$, on note $X_1 + a$ la courbe déduite de X_1 par la translation par a . Nous pouvons alors démontrer le point essentiel dans la preuve du théorème II de l'introduction.

Théorème 4.4.1. *Supposons que $i_0: X_0 \hookrightarrow A_0$ vérifie (*) (1.1.2) et que la normalisée de X_0 soit de genre ≥ 2 . Alors, pour tout $a \in A_1(R_1)$, l'image de $pA_1(R_1) \cap (X_1 + a)(R_1)$ dans $(X_0 + a)(k)$ est finie, et son cardinal est majoré par le degré maximum μ_0 des sous-faisceaux inversibles de \mathcal{M}_0^\vee .*

Examinons d'abord le cas $a=0$. Soit E l'image de $pA_1(R_1) \cap X_1(R_1)$ dans $X_0(k)$ et montrons que E est finie. Si l'on identifie X_0 à X'_0 par la projection h_0 , il résulte de 4.3.1 que E est contenu dans $X'_0(k) \cap Y'_0(k)$ (et lui est même égal lorsque E est contenu dans l'ouvert de lissité de X_0). Il suffit donc de montrer que $X'_0 \cap Y'_0$ est fini ou encore que ces deux courbes intègres sont distinctes. Or X'_0 est de degré 1 sur X_0 alors que Y'_0 a un degré radiciel sur X_0 qui est > 1 d'après 4.2.1.

Ceci étant, utilisons la section X'_0 de $h_0: V_0 \rightarrow X_0$ pour identifier le X_0 -schéma V_0 au fibré vectoriel $\mathbb{V}(\mathcal{I}_0/\mathcal{I}_0^2)$ (2.2.2). Alors l'immersion $Y'_0 \rightarrow V_0$ correspond à un morphisme de faisceaux $h'_0{}^*(\mathcal{I}_0/\mathcal{I}_0^2) \rightarrow \mathcal{O}_{Y'_0}$ qui s'annule précisément aux points de $X'_0 \cap Y'_0$. Comme cet ensemble est fini, ce morphisme est non nul et par image réciproque sur \tilde{Y}'_0 , puis passage au quotient par le sous-faisceau de torsion, donne un morphisme non nul

$$\varepsilon: \mathcal{M}_0 \rightarrow \mathcal{O}_{\tilde{Y}'_0}.$$

Alors le dual $\varepsilon^\vee: \mathcal{O}_{\tilde{Y}'_0} \rightarrow \mathcal{M}_0^\vee$ est injectif et son image engendre un sous-fibré inversible $\mathcal{O}_{\tilde{Y}'_0}(\Delta)$ de \mathcal{M}_0^\vee où Δ est un diviseur positif sur \tilde{Y}'_0 ayant pour support l'image réciproque de $Y'_0(k) \cap X'_0(k)$; en particulier le cardinal de cette intersection est majoré par le degré de Δ , donc le cardinal de E est majoré par le degré des sous-fibrés inversibles de \mathcal{M}_0^\vee .

Examinons maintenant le cas général. Un élément a de $A_1(R_1)$ est de la forme $pb + c$ avec b et c dans $A_1(R_1)$ et c dans le noyau de $A_1(R_1) \rightarrow A_0(k)$. Si l'on remplace X_1 par la courbe translatée $X_1 + pb$, E est changé en $E + pb$ et son cardinal n'est pas modifié. Si maintenant on remplace X_1 par $X_1 + c$, V_0 et Y'_0 ne sont pas modifiés, simplement la section X'_0 de h_0 est changée. Autrement dit, avec les notations précédentes, on doit remplacer ε par $\varepsilon + h'_0{}^*(\eta)$ pour un certain $\eta: \mathcal{I}_0/\mathcal{I}_0^2 \rightarrow \mathcal{O}_{X_0}$, ce qui n'affecte pas notre majoration.

Exemples 4.4.2. i) Supposons que A_0 soit une surface abélienne. Alors X_0 est localement intersection complète et V_0 est lisse sur X_0 . Le cardinal de $X'_0(k) \cap Y'_0(k)$ est majoré par la multiplicité d'intersection $X'_0 \cdot Y'_0$ qui n'est autre que le degré de \mathcal{M}_0^\vee . Ce degré est égal à $p^{r+s}(X_0 \cdot X_0)$, où $X_0 \cdot X_0$ est la self-intersection de X_0 dans A_0 , p^{r+s} est le degré de h'_0 et se décompose comme suit:

- p^s est le degré radiciel de h'_0 donné par 4.2.1
- p^r est le degré séparable de h'_0 majoré dans 4.2.2.

Comme X_0 n'est pas une courbe elliptique, on a $X_0 \cdot X_0 > 0$ et il résulte de 4.3.1 que si X_0 est lisse, $X_1(R_1)$ contient toujours au moins un point de $pA_1(R_1)$.

ii) Supposons que A_0 soit de dimension $d \geq 3$ et que X_0 soit lisse. Alors si c est un point assez général de $\text{Ker } A_1(R_1) \rightarrow A(k)$, $(X_1 + c)(R_1)$ ne rencontre pas $pA_1(R_1)$. En effet, identifions $\text{Ker } A_1(R_1) \rightarrow A(k)$ à l'algèbre de Lie L de A_0 . Alors pour tout $y \in V_0(k)$, les points c de L tels que la section de $h_0: V_0 \rightarrow X_0$ associée à $(X_1 + c)$ (cf. 2.4) passe par y , sont les points d'une courbe algébrique L_y de L . La réunion des courbes L_y , $y \in Y'_0(k)$, est une partie constructible de L de dimension ≤ 2 , donc distincte de L et il suffit de choisir c dans son complémentaire.

Remarque 4.4.3. Sous les hypothèses de 4.4.1, $pA_1(R_1) \cap X_1(R_1)$ est fini comme il résulte de 4.4.1 et du fait que le noyau de l'application $pA_1(R_1) \rightarrow A_0(k)$, donné par la réduction modulo p , est fini (par exemple c'est un quotient du noyau de la multiplication par p dans $A_0(k)$).

5. Torsion rationnelle et torsion ramifiée (cas local)

5.0. Dans ce numéro, R désigne un anneau de valuation discrète complet, de corps des fractions K de caractéristique 0, de corps résiduel k algébriquement clos de caractéristique $p > 0$. On suppose que le groupe des valeurs de la valuation de K est \mathbb{Z} et on note e la valuation de p (e est l'indice de ramification absolue de R).

Soient \bar{K} une clôture algébrique de K et G le groupe de Galois de \bar{K} sur K .

5.1. Soient A un R -schéma abélien, A_K sa fibre générique, A_0 sa fibre spéciale et T le groupe des points de torsion de $A(\bar{K})$, muni de l'action naturelle de G . On a $T = T_p \oplus T_{p'}$, où T_p est la composante p -primaire de T et $T_{p'}$ est la composante formée des éléments d'ordre premiers à p . Comme A est un R -schéma abélien et que le corps k est algébriquement clos, on a $T_{p'} \subset A(K) = A(R)$ et en particulier G opère trivialement sur $T_{p'}$.

5.2. Soit A_{p^∞} le R -groupe p -divisible construit à partir des noyaux des multiplications par les puissances de p dans A . On a une suite exacte de R -groupes p -divisibles:

$$(1) \quad 0 \rightarrow (A_{p^\infty})_{\text{inf}} \rightarrow (A_{p^\infty}) \rightarrow (A_{p^\infty})_{\text{ét}} \rightarrow 0,$$

où $(A_{p^\infty})_{\text{inf}}$ est le groupe p -divisible associé au R -groupe formel obtenu par complétion de A le long de la section 0, et $(A_{p^\infty})_{\text{ét}}$ est étale, isomorphe à $(\mathbb{Q}_p/\mathbb{Z}_p)^h$, où h est le p -rang de A_0 .

A la suite exacte (1), correspond sur les points de torsion à valeurs dans \bar{K} une suite exacte de G -modules:

$$(2) \quad 0 \rightarrow T_{\text{inf}} \rightarrow T_p \rightarrow (T_p)_{\text{ét}} \rightarrow 0.$$

Notons T'_p le sous-groupe divisible maximal de $T_p(K)$.

Lemme 5.2.1. *Supposons que l'indice de ramification e de R soit $< p - 1$. Alors T'_p est un facteur direct du G -module T_p .*

En effet, comme T'_p est non ramifié sur R , il résulte du lemme de spécialisation ([7] §1, prop. 1.1) que $T'_p \cap (T_p)_{\text{inf}} = 0$. Donc l'application composée $T'_p \hookrightarrow T_p \rightarrow (T_p)_{\text{et}}$ est injective et comme T'_p est p -divisible son image est un facteur direct du module galoisien trivial $(T_p)_{\text{et}} \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^h$. Soit T_1 un supplémentaire de cette image, alors l'image réciproque de T_1 dans T_p est un supplémentaire de T'_p , stable par l'action de Galois.

Dans la suite de ce numéro, on suppose $e < p - 1$ et on choisit un supplémentaire T'' de T'_p dans T_p , stable par Galois. C'est, par construction, le groupe des points de torsion d'un sous-groupe p -divisible A'' de A_{p^∞} .

Le lemme suivant montre que l'action de G sur $T''(\bar{K})$ est «importante»:

Lemme 5.2.2. *Le cardinal des orbites de G dans $T''(\bar{K})$ tend vers $+\infty$ avec l'ordre des éléments de $T''(\bar{K})$ (autrement dit, $\forall N > 0$, il existe un entier $r > 0$, tel que, si $x \in T''(\bar{K})$ est d'ordre $> p^r$, alors l'orbite de x sous G a un cardinal $> N$).*

En effet, soit $M'' = \text{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, T'')$ le module de Tate associé à T'' . C'est un \mathbb{Z}_p -module libre de rang fini, muni d'une action continue de G . Notons M^* l'ouvert de M (pour la topologie p -adique) formé des éléments d'image non nulle dans M/pM . Un argument immédiat de compacité, montre que le lemme 5.2.2 équivaut au fait que G n'a pas d'orbites finies dans M^* . Soit donc M_1 le plus grand sous- \mathbb{Z}_p -module de M sur lequel G agit à travers un groupe fini et montrons que $M_1 = 0$. Alors $T_1 = \varinjlim_n M_1/p^n M_1$ est un sous-groupe divisible de

T' , sur lequel G agit à travers un groupe fini. Il résulte, par exemple des théorèmes de Tate ([11] cor. 1 p. 181) que $T_1 \cap (T_p)_{\text{inf}}$ est fini. Donc le morphisme composé $T_1 \rightarrow T_p \rightarrow (T_0)_{\text{et}}$ a un noyau fini. Comme G agit trivialement sur $(T_p)_{\text{et}}$ et que T_1 est divisible, G agit trivialement sur T_1 . Donc $T_1 = 0$, vu le caractère maximal de T'_p .

Exemples 5.2.3. i) Si le p -rang h de A_0 est nul, on a $T'_p = 0$, $T'' = T_p = T_{\text{inf}}$.

ii) Si A_0 est ordinaire, on a $T'_p = (T_p)_{\text{et}}$ (et donc $T'' = T_{\text{inf}}$) si et seulement si A est le relèvement canonique de A_0 au sens de Serre-Tate. Au contraire, si A est un relèvement général de A_0 , $T'_p = 0$ et $T'' = T_p$.

5.3. On a une décomposition (non canonique), compatible avec G : $T = T' \oplus T''$ où $T' = T'_p \oplus T''_p$.

Nous dirons (abusivement) que T' est la torsion rationnelle de A et que T'' (défini pour $e < p - 1$) est la torsion ramifiée de A . La torsion rationnelle possède les propriétés suivantes:

- i) L'action de G sur T' est triviale et donc $T' \subset A(K) = A(R)$.
- ii) T' est p -divisible.
- iii) L'application de spécialisation

$$T' \hookrightarrow A(K) \xrightarrow{\sim} A(R) \rightarrow A(k)$$

est injective (en effet on a remarqué que $T' \cap T_{\text{inf}} = T'_p \cap T_{\text{inf}} = 0$).

6. Courbes et torsion rationnelle (cas local)

6.0. On reprend les hypothèses et notations de 5.0 et 5.1. Mais en plus du R -schéma abélien A , on se donne une R -courbe X propre et plate contenue dans A grâce à l'immersion $i: X \hookrightarrow A$ et vérifiant les conditions suivantes:

i) Les fibres géométriques de X sont géométriquement intègres; la normalisée \tilde{X} de X est lisse sur R , à fibres de genre ≥ 2 . En particulier, la fibre spéciale $(\tilde{X})_0$ de \tilde{X} est la normalisée de X_0 .

Soit J la jacobienne de \tilde{X} et $a: J \rightarrow A$ le morphisme d'Albanese associé au morphisme composé $\tilde{X} \rightarrow X \xrightarrow{i} A$.

ii) On suppose que a est surjectif et que le noyau N de a est lisse sur R et que le groupe des composantes connexes de N , N/N^0 est d'ordre premier à p .

On peut remarquer que la condition ii) se teste sur la fibre spéciale et donc équivaut au fait que l'immersion $i_0: X_0 \hookrightarrow A_0$ vérifie la condition (*) de 1.1.2. Par ailleurs, lorsque l'indice de ramification e de R vérifie $e < p - 1$, il résulte de ([7] §1 prop. 1.2) que la condition ii) peut aussi se tester sur la fibre générique.

6.1. Commençons par dégager un corollaire de 4.4.1.

Corollaire 6.1.1. *Supposons que R soit non ramifié (i.e. $e = 1$) et que les conditions de 6.0 soient satisfaites. Alors, pour tout $a \in A(R) = A(K)$, l'image de $(X + a)(R) \cap pA(R)$ dans $(X_0 + a)(k)$ est finie et majorée par μ_0 (4.4.1).*

En effet posons $R_1 = R/p^2R$, $A_1 = A \times_R R_1$, $X_1 = X \times_R R_1$. Alors l'anneau R_1 est du type considéré dans 4.0 et on peut appliquer à A_1 et X_1 le théorème 4.4.1. Comme l'image de $(X + a)(R) \cap pA(R)$ dans $(X_0 + a)(k)$ est contenue dans l'image de $(X + a)(R_1) \cap pA(R_1)$, le corollaire en résulte.

Remarque 6.1.2. En fait, pour $e = 1$, il résulte des propriétés d'intégralité du logarithme et de l'exponentielle relatifs au groupe formel complété de A le long de la section unité, ([8], chap. III) que tout élément de $\text{Ker } A(R) \rightarrow A(R_1)$ est contenu dans $pA(R)$. Par suite l'image de $(X + a)(R) \cap pA(R)$ dans $(X + a)(k)$ est en fait égale à l'image de $(X + a)(R_1) \cap pA(R_1)$.

6.2. Notons p_A la multiplication par p dans A , Y la R -courbe propre et plate image réciproque de X par p_A et \tilde{Y} la normalisée de Y . On voit facilement que, sous les conditions de 6.0 la fibre spéciale $(\tilde{Y})_0$ de \tilde{Y} est irréductible.

Proposition 6.2.1. *Sous les hypothèses de 6.1.1 $(\tilde{Y})_0$ n'est pas réduite (c'est-à-dire apparaît avec une multiplicité > 1).*

En effet, soit $x \in X(R) \cap pA(R)$. Alors, mis à part un nombre fini d'exceptions provenant des points entiers x qui, sur la fibre générique, passent par les points singuliers de X_K , les points de $pA(R) \cap X(R)$ sont exactement les images des points de $\tilde{Y}(R)$. Le corollaire 6.1.1 équivaut donc au fait qu'il n'y a qu'un nombre fini de points de $\tilde{Y}(k)$ par lesquels passe un point de $\tilde{Y}(R)$. Cette condition équivaut au fait que $(\tilde{Y})_0$ n'est pas réduit; de plus, lorsque $(\tilde{Y})_0$ n'est pas réduit, les seuls points de $(\tilde{Y})_0$ par lesquels il peut passer des points de $\tilde{Y}(R)$ sont les points y de $(\tilde{Y})_0$ qui sont singuliers dans \tilde{Y} (c'est-à-dire tels l'anneau local $\mathcal{O}_{\tilde{Y}, y}$ ne soit pas régulier).

Remarque 6.2.2. On peut donner une démonstration directe de 6.2.1, valable sous les hypothèses de 6.6 et la condition $e \leq p - 1$, puis en déduire 6.1.1. Nous avons abandonné cette approche pour celle présentée ici qui nous semble plus élémentaire, donne une borne relativement explicite et se prête mieux au remplacement de X par une courbe translatée. Néanmoins, il serait intéressant d'étudier de près les singularités de \tilde{Y} .

6.3. Dans 5.3, on a introduit la torsion rationnelle T' de A .

Théorème 6.3.1. *Sous les hypothèses de 6.1.1, pour tout $a \in A(K)$, $T' \cap (X + a)(K)$ est fini et majoré par μ_0 (4.4.1).*

Cela résulte immédiatement de 6.1.1 et du fait que les points de T' sont dans $pA(R)$ et sont déterminés par leurs réductions dans $A_0(k)$ (5.3).

6.4. Nous allons maintenant étudier $T' \cap (X + a)(\bar{K})$, pour $a \in A(\bar{K}) - A(K)$.

6.4.0. Notons d'abord que X n'étant pas elliptique, le sous-schéma en groupes H_1 de A formé des translations qui laissent X globalement fixe est fini. Soit H le sous-schéma en groupes de H_1 , adhérence schématique dans H_1 , de la fibre générique de H_1 . Alors H est R -plat, opère sur X et cette action s'étend en une action de H sur la courbe lisse \tilde{X} , normalisée de X . Comme \tilde{X} a ses fibres de genre ≥ 2 , \tilde{X} n'a pas d'automorphismes infinitésimaux et par suite H est étale.

Soit $Z \subset A \times A$ l'image réciproque de X par le morphisme

$$A \times A \rightarrow A; \quad (a, b) \mapsto b - a.$$

Considérons $Z \cap (A \times X)$ comme A -schéma via la première projection. Alors la fibre au-dessus d'un point $a \in A(\bar{K})$ est $X \cap X + a$. Le morphisme $Z \cap (A \times X) \rightarrow A$, induit par la première projection, est propre et donc fini au-dessus de $(A - H)_K$. En particulier les fibres au-dessus de $(A - H)(\bar{K})$, ont un cardinal borné. Soit μ_1 un majorant.

Exemple 6.4.1. Si A est de dimension 2 sur R , on peut prendre pour μ_1 la self-intersection $X_0 \cdot X_0$ de X_0 dans A_0 .

Proposition 6.4.2. *Pour tout $a \in A(\bar{K}) - A(K)$, $T' \cap (X + A)$ est fini, de cardinal $\leq \mu_1$.*

Notons tout de suite le corollaire suivant de 6.3.1 et 6.4.2:

Corollaire 6.4.3. *Sous les hypothèses de 6.1.1, pour tout $a \in A(\bar{K})$, $T' \cap (X + a)$ est fini de cardinal $\leq \mu = \text{maximum}(\mu_0, \mu_1)$.*

Démontrons 6.4.2. Soit B le schéma abélien quotient de A par le sous-groupe fini étale H (6.4.0) et soit b l'image de a dans $G(\bar{K})$. Comme H est étale et R complet à corps résiduel algébriquement clos, l'hypothèse $a \in A(\bar{K}) - A(K)$, entraîne $b \in B(\bar{K}) - B(K)$, et par suite, il existe $g \in \text{Gal}(\bar{K}/K)$ tel que $a^g - a \notin H$.

Par ailleurs les points de T' étant rationnels sur K , ceux qui sont contenus dans $X + a$ sont aussi contenus dans $X + a^g$ donc appartiennent à $(X + a) \cap (X + a^g)(\bar{K})$. Par translation par $-a$, cette intersection est en bijection avec $X \cap (X + a^g - a)(\bar{K})$ qui est finie, de cardinal $\leq \mu_1$, puisque $a^g - a \notin H$.

7. Démonstration du théorème 1

7.0. Soient c un corps algébriquement clos de caractéristique 0, A une variété abélienne définie sur c , X une courbe propre intègre non elliptique et $i: X \hookrightarrow A$ une immersion, X et i étant définies sur c . Soit $T \subset A(c)$ le groupe des points de torsion de $A(c)$. Nous devons montrer que $T \cap X$ est fini.

7.1. Soit $B \subset A$ la sous-variété abélienne engendrée par l'ensemble des différences $(x - x')$, $(x, x' \in X(c))$, des points de X . Alors, il existe $a \in A(c)$ tel que X soit contenu dans $B + a$. Si l'image de a dans A/B n'est pas de torsion, $T \cap X = \emptyset$. Sinon, quitte à translater X par un point de torsion, on se ramène au cas où $X \subset B$.

On suppose donc désormais que $B = A$. Soient \tilde{X} la courbe normalisée de X , J la jacobienne de \tilde{X} , $a: J \rightarrow A$ le morphisme d'Albanese associé au morphisme composé $\tilde{X} \rightarrow X \hookrightarrow A$, N son noyau, N^0 la composante neutre de N et h l'ordre de N/N^0 . L'hypothèse que $B = A$ équivaut au fait que a est surjectif.

7.2. Il existe une \mathbb{Z} -algèbre de type fini E contenue dans c , telle que X , A et $i: X \hookrightarrow A$ soient déjà définis sur $S = \text{Spec}(E)$. Quitte à restreindre S à un ouvert non vide, on peut supposer de plus que les conditions suivantes sont réalisées:

i) A est un S -schéma abélien.
 ii) X est une S -courbe propre et plate, à fibres géométriquement intègres et $i: X \hookrightarrow A$ est une immersion.

iii) La normalisée \tilde{X} de X est une S -courbe propre et lisse à fibres géométriques de genre ≥ 2 . Soient J la jacobienne relative de \tilde{X} sur S et $a: J \rightarrow A$ le morphisme d'Albanese associé à l'application composée $\tilde{X} \rightarrow X \hookrightarrow A$. Alors a est surjectif et son noyau N est lisse sur S (noter que N est lisse au point générique η de S qui est en caractéristique zéro). Enfin, si N^0 est la composante neutre de N , N/N^0 est fini étale de rang h .

7.3. Soit s un point fermé de la fibre de S au-dessus de \mathbb{Q} . Notons que le nombre de points de torsion contenu dans une fibre géométrique de X ne peut qu'augmenter par spécialisation en caractéristique 0, en particulier quand on spécialise de η à s . Quitte alors à changer la courbe originelle, on peut remplacer S ci-dessus, par un ouvert de l'adhérence de s dans S . On est donc ramené au cas où S est un ouvert non vide du spectre de l'anneau d'entiers d'un corps de nombre L . Quitte à restreindre S , on peut supposer qu'en plus des conditions de 7.2 on a:

iv) S est non ramifié sur $\text{Spec}(\mathbb{Z})$ et $2h$ est inversible dans S .

Si v est une place finie de S , d'anneau E_v , de complété \hat{E}_v , alors v divise un nombre premier p et si R désigne le complété d'une extension maximale non ramifiée de E_v , R est du type considéré en 5.0 avec $e = 1$. Si on désigne encore X et A les images réciproques de X et A sur R par le changement d'anneaux $E \rightarrow R$, X et A vérifient les conditions de 4.4.1.

Proposition 7.3.1. *Soient l un nombre premier et T_l la composante l -primaire de la torsion de A_L . Alors il existe un entier v_l ayant la propriété suivante: pour toute extension L' de L algébriquement close et tout $a \in A(L)$, $T_l \cap (X + a)(L')$ est fini de cardinal $\leq v_l$.*

En effet, choisissons une place finie v de E qui divise un nombre premier $p \neq l$. On en déduit un anneau local R et soit \bar{K} une clôture algébrique du corps des fractions de R . Alors la composante l -primaire de la torsion T de $A(\bar{K})$ est contenue dans la p -torsion T_p , et a fortiori dans la torsion rationnelle T' relative à R (5.3). D'après 6.4.3, il existe v_i tel que pour tout $a \in A(\bar{K})$, $T_l \cap (X + a)(\bar{K})$ soit fini et majoré par v_i .

Si maintenant L est une extension algébriquement close quelconque de L , quitte à agrandir L , on peut supposer $\bar{K} \subset L$. Soit $a \in A(L)$. Alors a provient de $A(S')$ où S' est le spectre d'une \bar{K} -algèbre de type fini contenue dans L . Soit s' un point de $S'(\bar{K})$. Alors, l'argument de spécialisation déjà utilisé, qui fait passer du point générique de S' , au point s' , nous ramène au cas où $a \in A(\bar{K})$. D'où la proposition.

Remarque 7.3.2. La proposition 7.3.1 peut aussi s'obtenir directement à partir des résultats de Bogomolov [1].

7.4. Pour terminer la démonstration du théorème *I*, on choisit une place finie v de E , d'où un anneau R . On note p la caractéristique résiduelle de R ; \bar{K} est une clôture algébrique du corps des fractions K de R et G est le groupe de Galois de \bar{K}/K .

Comme $e = 1$ et $p \neq 2$, on a $e < p - 1$ et on peut décomposer la torsion T de A_K en $T = T' \oplus T''$ (5.3), où T' est la torsion rationnelle et T'' la torsion ramifiée contenue dans la composante p -primaire de T . Rappelons les résultats de finitude déjà obtenus:

i) Il existe un entier μ , tel que pour tout $a \in A(\bar{K})$, $T' \cap (X + a)(\bar{K})$ soit fini de cardinal $\leq \mu$ (6.4.3).

ii) Il existe un entier v_p tel que $\forall a \in A(\bar{K})$, $T'' \cap (X + a)(\bar{K})$ soit fini majoré par v_p (appliquer 7.3.1 avec $l = p$).

Soit alors $x \in T' \cap (X + a)(\bar{K})$. On a $x = x' + x''$, avec $x' \in T'(K)$, $x'' \in T''(\bar{K})$.

Alors x'' est un point de $T'' \cap (X - x)(\bar{K})$. Comme x' et X sont définis sur K et que T'' est stable sous G , toute l'orbite de x'' sous G est contenue dans $T'' \cap (X - x')(K)$. Donc d'après ii) ci-dessus, cette orbite a au plus v_p éléments. Il résulte alors de 5.2.2 que l'ordre de x'' est borné, indépendamment de x' , C'est dire qu'il n'y a qu'un nombre fini de valeurs possibles pour la composante x'' .

Par ailleurs, pour x'' fixé, $x' \in T' \cap (X - x'')(K)$ donc prend au plus μ valeurs distinctes d'après i) ci-dessus. Au total, il n'y a qu'un nombre fini de valeurs pour $x = x' + x''$.

8. Le système inductif « X_n »

8.0. Dans ce numéro préparatoire à l'étude de la conjecture de Lang; L est un corps de caractéristique 0, A est un L -schéma abélien et X est une courbe propre, géométriquement intègre non elliptique contenue dans A , définie sur L . On note \bar{L} une clôture algébrique de L . On a vu dans 6.3 que seul un sous-groupe fini H de A opérait sur X par translation. Si $B = A/H$ et si Y est la

courbe image de X dans B , alors Y n'est fixe par aucune translation non nulle de B .

8.1. Pour n entier >0 , soient n_A la multiplication par n dans A , ${}_nA$ son noyau, X_n l'image schématique de X par n_A et S_n le lieu singulier de X_n . En particulier $X = X_1$ et S_1 est le lieu singulier de X . Pour $n|n'$, la multiplication dans A par n'/n induit une application $j_n^{n'}: X_n \rightarrow X_{n'}$ de sorte que l'on obtient un système inductif filtrant $(X_n, j_n^{n'})$ indexé par les entiers >0 , munis de la relation d'ordre donnée par la relation de divisibilité.

Proposition 8.1.1. *Supposons que $H=0$ (8.0). Alors, pour tout $n>0$, le morphisme $X \rightarrow X_n$ induit par n_A est birationnel. En particulier, si $x \in X(\bar{L})$ est tel que $nx \in A(L)$, alors, ou bien $x \in X(L)$ ou bien $nx \in S_n(L)$.*

En effet soit Y_n l'image réciproque de X_n par n_A , de sorte que $Y_n \rightarrow X_n$ est étale et que X est une composante irréductible de Y_n . Pour établir le premier point, quitte à remplacer L par \bar{L} on peut supposer L algébriquement clos. Alors $Y_n \rightarrow X_n$ est un revêtement étale galoisien de groupe ${}_nA(L)$; ce groupe opère transitivement sur les composantes irréductibles de Y_n et comme $H=0$ le stabilisateur de la composante X est 0 , donc ${}_nA(L)$ opère aussi librement sur l'ensemble des composantes. Il en résulte que chacune d'elles est de degré 1 sur X_n , d'où la première assertion; la seconde en résulte immédiatement.

Remarque 8.1.2. Les singularités de X_n sont les images des singularités de Y_n , donc consistent d'une part en l'image des singularités S_1 de X et d'autre part en l'image des points de X communs à plusieurs composantes irréductibles de Y_n . Si $x_n \in S_n$ appartient à ce dernier type, l'anneau local \mathcal{O}_{x_n, x_n} n'est pas unibranche (c'est-à-dire son hensélisé strict n'est pas intègre) et la fibre de $X \rightarrow X_n$ au-dessus de x_n a un degré >1 .

Notons le corollaire suivant du théorème I:

Corollaire 8.1.3. *Les fibres de l'application canonique $X(\bar{L}) \rightarrow \varinjlim_n X_n(\bar{L})$ sont finies.*

En effet soit $x \in X(\bar{L})$; quitte à faire la translation par $-nx$ sur les X_n on se ramène au cas où $x=0$. Alors la fibre de $X(\bar{L}) \rightarrow \varinjlim_n X_n(\bar{L})$ contenant 0 est la torsion contenue dans X , donc est finie d'après le théorème I.

8.2. Soient R, K, \bar{K}, G comme dans (5.0) et soient A et X des R -schémas vérifiant les conditions de (6.0).

Proposition 8.2.1. *L'ensemble des $\bar{x} \in X(\bar{K}) - X(K)$ tels qu'il existe n entier >0 avec $n\bar{x} \in A(K)$ est fini.*

Soit H le sous-schéma en groupes étale (6.4.0) de A formé des translations qui laissent stable X et soit Y l'image de X dans $B = A/H$. Comme H est étale et R complet à corps résiduel algébriquement clos, un point de $A(\bar{K})$ a une image dans $B(K)$ si et seulement si ce point est dans $A(K)$. Quitte alors à remplacer X par Y et A par B , on peut pour établir 8.2.1 supposer $H=0$.

Soit $\bar{x} \in X(\bar{K}) - X(K)$ tel que $n\bar{x} \in A(K)$. Ecrivons $n = p^r m$ avec $(m, p) = 1$. Comme la multiplication par m dans A est étale, l'argument précédent montre que $p^r \bar{x} \in A(K)$ et on peut se borner au cas où $n = p^r$.

Reprenons la suite exacte de R -groupes p -divisibles de 5.2 (1) et posons pour simplifier $A'' = (A_{p^\infty})_{\text{inf}}$, $A' = (A_{p^\infty})_{\text{ét}}$. Enfin soient ${}_r A$, ${}_r A'$, ${}_r A''$ les noyaux respectifs de la multiplication par p^r dans A , A' , A'' . On a une suite exacte de R -schémas en groupes finis et plats.

$$0 \rightarrow {}_r A'' \rightarrow {}_r A \rightarrow {}_r A' \rightarrow 0,$$

de sorte que, si $A^{(r)}$ est le R -schéma abélien quotient de A par ${}_r A'$, on a une factorisation de $(p^r)_A: A \xrightarrow{u_r} A^{(r)} \xrightarrow{v_r} A$. Puisque v_r est étale, on a déjà $u_r(\bar{x}) \in A^{(r)}(K)$.

Soit alors v_p un entier > 0 comme dans 7.4 ii) et soit n_0 un entier tel que $p^{n_0} \geq v_p$. Notons n'_0 le plus petit entier tel que, si a' est un point de torsion de $A''(\bar{K})$ d'ordre $> p^{n'_0}$, alors l'orbite de a' sous G a un cardinal $> v_p$ (5.2.2). Posons $m = p^{n_0 + n'_0}$. Nous allons montrer que $m\bar{x} \in A(K)$. Alors, d'après 8.1.1, on aura $m\bar{x} \in S_m(K)$, ce qui ne laisse qu'un nombre fini de possibilités pour \bar{x} .

Notons que la fibre de $u_r: A \rightarrow A^{(r)}$, au-dessus du point rationnel $u_r(\bar{x})$ est un K -torseur P_r sous le schéma en groupes ${}_r A''_K$, fibre générique de ${}_r A''$. Le point $\bar{x} \in P_r(\bar{K})$ a une image x dans le schéma P_r . Soit $K(x)$ le corps résiduel en x . Vu la définition de $v_{p^{n_1}}$ le degré h de $K(x)$ sur K est $\leq v_p$. Ecrivons $h = h_1 p$ avec $(p, h_1) = 1$. On a donc $n_1 \leq n_0$ par définition de n_0 . Il résulte de ([9] prop. 6 p. 127) que le toseur P_r est trivialisé par la multiplication par h et donc par la multiplication par p^{n_1} (puisque ${}_r A''(\bar{K})$ est un p -groupe), donc par la multiplication par p^{n_0} . On obtient ainsi un K -morphisme de P_r dans le toseur trivial ${}_r A''_K$. Soit y l'image de x dans ${}_r A''_K$. On a $(K(y): K) \leq (K(x): K) \leq v_p$. Il résulte alors de la définition de n'_0 que y est un point de ${}_{n_0} A''_K \cap {}_r A''_K$. Finalement l'image de x par la multiplication par $m = p^{n_0 + n'_0}$ est bien un point rationnel.

9. Autour de la conjecture de Serge Lang

9.0. Dans ce numéro, on reprend les notations L, \bar{L}, A, X de 8.0. On note G le groupe de Galois de \bar{L}/L . Soit Γ un sous-groupe de type fini de $A(L)$. On note $\bar{\Gamma}$ le sous-groupe de $A(\bar{L})$ formé des points de division de Γ :

$$\bar{\Gamma} = \{x \in A(\bar{L}), \exists n \text{ entier } \geq 1 \text{ tel que } nx \in \Gamma\}.$$

On a alors une suite exacte de groupes munis d'une action de G :

$$(1) \quad 0 \rightarrow T(\bar{L}) \rightarrow \bar{\Gamma} \rightarrow V \rightarrow 0,$$

où $T(\bar{L})$ est le sous-groupe de torsion de $A(\bar{L})$ et V est le \mathbb{Q} -vectoriel $\Gamma \otimes_{\mathbb{Z}} \mathbb{Q}$ sur lequel G opère trivialement.

Nous allons étudier des propriétés de finitude de $\bar{\Gamma} \cap X(\bar{L})$ et du sous-groupe de $\bar{\Gamma}$ engendré par $\bar{\Gamma} \cap X(\bar{L})$. Nous étudions d'abord le cas où L est un corps local, puis le cas où L est une extension de type fini de \mathbb{Q} .

9.1. Soient R, K, \bar{K}, k comme dans 5.0 et soient A et X satisfaisant aux conditions i) et ii) de 6.0. Enfin soient Γ un sous-groupe de type fini de $A(K) = A(R)$ et $\bar{\Gamma} \subset A(\bar{K})$ le groupe des points de division de Γ . On note Γ' le sous-groupe de $\bar{\Gamma}$ engendré par $\bar{\Gamma} \cap X(\bar{K})$, $\Gamma'(K) = \Gamma' \cap A(K)$ et $\tilde{\Gamma}$ le sous-groupe de $A(K)$ engendré par $\bar{\Gamma} \cap X(K)$. On a donc les inclusions:

$$\tilde{\Gamma} \subset \Gamma'(K) \subset \Gamma'.$$

Théorème 9.1.1. *Sous les hypothèses précédentes, on a les propriétés de finitude suivantes:*

- i) *Le groupe $\Gamma'/\tilde{\Gamma}$ est de type fini.*
- ii) *L'image de $\bar{\Gamma} \cap X(K) = \bar{\Gamma} \cap X(R)$ dans $X(k)$ est finie et l'image de $\Gamma'(K)$ dans $A(k)$ est un groupe de type fini.*
- iii) *Le sous-groupe de torsion de Γ' est fini.*

Prouvons i). Le groupe $\Gamma'/\tilde{\Gamma}$ est engendré par l'image de $\bar{\Gamma} \cap [X(\bar{K}) - X(K)]$, qui est un ensemble fini d'après 8.2.1 donc $\Gamma'/\tilde{\Gamma}$ est de type fini.

Pour établir ii), considérons $\bar{\Gamma}(K) = \bar{\Gamma} \cap A(K)$.

Lemma 9.1.2. *Le groupe $\bar{\Gamma}(K)/p\bar{\Gamma}(K)$ est fini.*

En effet, on a la suite exacte (1) de 9.0:

$$0 \rightarrow T(\bar{K}) \rightarrow \bar{\Gamma} \rightarrow V \rightarrow 0.$$

Prenant les invariants sous le groupe de Galois de \bar{K}/K , on obtient la suite exacte:

$$0 \rightarrow T(K) \rightarrow \bar{\Gamma}(K) \rightarrow W \rightarrow 0,$$

où W est l'image de $\bar{\Gamma}(K)$ dans V .

Pour établir le lemme, il suffit de montrer que $T(K)/pT(K)$ et W/pW sont finis. Or W est un sous-groupe de V , vectoriel de dimension finie sur \mathbf{Q} , donc W/pW est finie. Par ailleurs $T(K)$, groupe des points de torsion de $A(K)$, est somme directe d'un groupe fini et d'un groupe p -divisible (noté T' dans 5.3), donc $T(K)/pT(K)$ est fini.

Soit alors $\gamma_i, i \in I$, une famille finie de représentants dans $\bar{\Gamma}(K)$ des classes $\bar{\Gamma}(K)/p\bar{\Gamma}(K)$. Notons X_i la courbe $X - \gamma_i$ translatée de X par $-\gamma_i$. Alors tout élément de $\bar{\Gamma}(K)$ s'écrit $\gamma = \gamma_i + pa$, pour un choix convenable de i et $a \in A(K)$. Si de plus γ est dans $X(K)$, $pa = \gamma - \gamma_i$ est dans $X_i(K) \cap pA(K) = X_i(R) \cap pA(R)$. D'après 6.1.1, l'image de $X_i(R) \cap pA(R)$ dans $X_i(k)$ est finie, donc l'image de $\bar{\Gamma}(K) \cap X(K)$ dans $X(k)$ est finie. Comme $\bar{\Gamma}(K) \cap X(K) = \tilde{\Gamma} \cap X(K)$, on a établi la première assertion de ii). Comme $\bar{\Gamma} \cap X(K)$ engendre le groupe $\tilde{\Gamma}$ par définition, on en déduit que l'image de $\tilde{\Gamma}$ dans $A(k)$ est un groupe de type fini. Par ailleurs, il résulte de i) que $\Gamma'(K)/\tilde{\Gamma}$ est un groupe de type fini. Combinant ces deux résultats, on en déduit que l'image de $\Gamma'(K)$ dans $A(k)$ est de type fini, d'où ii).

Prouvons iii). Compte tenu de i), il suffit de montrer que le sous-groupe de torsion de $\bar{\Gamma}(K)$ est fini. Or, l'application de spécialisation $A(R) \rightarrow A(k)$, en restriction aux points de torsion, a un noyau fini (et même est injective si $p \neq 2$), donc iii) résulte de ii).

Remarques 9.1.3. i) En considérant la fermeture intégrale \bar{R} de R dans \bar{K} qui est un anneau de valuation (non discrète) de corps résiduel k , on définit une application de spécialisation $A(\bar{K}) \xrightarrow{\sim} A(\bar{R}) \rightarrow A(k)$. Il résulte alors des assertions i) et ii) de 9.1.1 que l'image de \bar{F} dans $A(k)$ est un groupe de type fini, et il résulte de la démonstration de 9.1.1 que l'image de $\bar{F} \cap X(\bar{K})$ dans $X(k)$ est finie.

ii) Sous les hypothèses de 9.1, supposons que la restriction à Γ de l'application de spécialisation $A(K) \rightarrow A(k)$ soit injective, alors 9.1.1 ii) entraîne que $\Gamma \cap X(K)$ est fini. Signalons, sans démonstration, que cette remarque conduit à une nouvelle démonstration de la conjecture de Mordell sur les corps de fonctions en caractéristique 0.

9.2.

Théorème 9.2.1. *Reprenons les hypothèses de 9.0 et supposons de plus que L est de type fini sur \mathbb{Q} , de sorte que $M = A(L)$ est un groupe de type fini. Soit H le sous-schéma en groupes fini de A formé des translations qui laissent X stable (6.3) et posons $B = A/H$, $Y = A/H$, $N = B(L)$. Alors :*

- i) *Le sous-groupe de \bar{M} engendré par $\bar{M} \cap X(\bar{L})$ est de type fini.*
- ii) *$\bar{N} \cap (Y(\bar{L}) - Y(\bar{L}))$ est fini.*
- iii) *$\bar{M} \cap X(\bar{L})$ est fini si et seulement si $Y(L)$ est fini, c'est-à-dire si et seulement si la courbe Y satisfait à la conjecture de Mordell sur le corps L .*
- iv) *Le système inductif $\varinjlim_n S_n(L)$ de (8.1) est stationnaire.*

Notons que l'assertion iii) montre que la conjecture de Serge Lang ([6]) résulte de la conjecture de Mordell pour les courbes. De façon précise on a le résultat suivant :

Corollaire 9.2.2. *Soient c un corps algébriquement clos de caractéristique > 0 , A une variété abélienne définie sur c , X une courbe propre intègre de A qui n'est pas elliptique, Y la courbe X/H , où H est définie comme dans 9.2.1. Soit Γ un sous-groupe de type fini de $A(c)$ et soit L un sous-corps de c , de type fini sur \mathbb{Q} , tel que A et Y soient définies sur L et tel que $\Gamma \subset A(L)$. Alors si $Y(L)$ est fini, $\bar{\Gamma} \cap X(c)$ est fini.*

Prouvons maintenant l'assertion i) de 9.2.1. Soit M' le sous-groupe de \bar{M} engendré par $\bar{M} \cap X(\bar{L})$. Notons que M' n'est pas modifié si l'on remplace L par une extension finie. On peut donc supposer $X(L) \neq \emptyset$. Quitte alors à remplacer A par une sous-variété abélienne, on peut supposer que A est engendré par les différences des points de X .

Soit E une \mathbb{Z} -algèbre de type fini, contenue dans L , de corps des fractions L et soit $S = \text{Spec}(E)$. Quitte à remplacer S par un ouvert non vide, on peut supposer que X et A s'étendent en des S -schémas (notés encore A et X) qui vérifient les conditions i), ii) et iii) de 7.2. Par contre, on ne peut plus nécessairement se ramener, par spécialisation, au cas où L est un corps de nombres. Quitte à restreindre S , on peut supposer que la condition suivante est réalisée :

(iv)' S est lisse sur $\text{Spec}(\mathbb{Z})$ et $2h$ (où h est comme dans 7.1) est inversible sur S .

L'image de S dans $\text{Spec}(\mathbb{Z})$ est un ouvert non vide. Soit alors $p \in \text{Spec}(\mathbb{Z})$ un nombre premier dans l'image de S et soit η le point générique de la fibre de S au-dessus de p . La condition (iv)' entraîne que l'anneau local $\mathcal{O}_{S,\eta}$ de S en η est un anneau de valuation discrète, dont l'idéal maximal est engendré par p . D'après ([3] 0_{III} 10.3.1), on peut étendre $\mathcal{O}_{S,\eta}$ en un anneau de valuation discrète R , de façon que l'idéal maximal de R soit encore engendré par p et que le corps résiduel k de R soit une clôture algébrique du corps résiduel de $\mathcal{O}_{S,\eta}$.

Supposons de plus R complet, alors R est du type considéré dans 5.0 et le corps des fractions K de R est une extension de L . De plus, les images réciproques de A et X par le changement de base $\text{Spec}(R) \rightarrow S$ satisfont aux conditions i) et ii) de 6.0.

On peut alors appliquer 9.1.1 en prenant pour Γ le groupe $A(L) \subset A(K)$. Le groupe noté Γ' dans 9.1.1 est alors égal au groupe M' . Donc d'après 9.1.1 iii), M' a un sous-groupe de torsion qui est fini.

Soit n un entier ≥ 1 qui annule la torsion de M' . Il résulte par exemple de la suite exacte (1) de 9.0 appliquée avec $\Gamma = A(L)$, que nM' s'identifie à un sous-groupe de $A(L)$, donc est de type fini et par suite M' est de type fini.

Prouvons l'assertion ii) de 9.2.1. L'assertion i) appliquée à la courbe Y de B montre que le sous-groupe N' de \bar{N} engendré par $\bar{N} \cap Y(\bar{L})$ est de type fini. Soit n un entier ≥ 1 qui annule la torsion de N' . Comme plus haut on voit que $nN' \subset B(L)$, donc si $y \in Y(\bar{L}) \cap \bar{N}$, $ny \in B(L)$. Comme la courbe Y n'est stable par aucune des translations non nulle de B , il résulte de 8.1.1 que $(Y(\bar{L}) - Y(L)) \cap \bar{N}$ est fini d'où ii).

Prouvons iii). Si $\bar{M} \cap X(\bar{L})$ est fini, il est clair que $Y(L)$ est fini. Réciproquement, si $Y(L)$ est fini, il résulte de ii) que $\bar{N} \cap Y(\bar{L})$ est fini, donc $\bar{M} \cap X(\bar{L})$ (qui est contenu dans l'image réciproque de $\bar{N} \cap Y(\bar{L})$ par la projection $A(\bar{L}) \rightarrow B(\bar{L})$) est aussi fini.

Prouvons iv). Dans l'étude du système inductif $\varinjlim_n S_n(L)$, on peut se borner aux entiers n qui sont des multiples de l'ordre du groupe fini $H(\bar{L})$, ce qui nous permet de remplacer X par Y et donc de supposer $H=0$.

Soit $S_\infty(L) = \varinjlim_n S_n(L)$. D'après 8.1.3, pour voir que le système inductif des

$S_n(L)$ est stationnaire, il suffit de montrer que $S_\infty(L)$ est fini. Notons qu'un point de $S_\infty(L)$ appartient à au moins l'un des trois ensembles suivants:

a) L'image de $\bar{M} \cap (X(\bar{L}) - X(L))$, qui est un ensemble fini d'après 9.2.1 ii) et le fait que $H=0$.

b) L'image de $S_1(L)$ qui est évidemment finie.

c) L'ensemble des images de points $x_n \in S_n(L)$, $n > 1$, tels que la fibre de $X \rightarrow X_n$ au-dessus de x_n contienne des points rationnels x et x' , avec $x' - x$ exactement d'ordre n . Comme le groupe de torsion de $A(L)$ est fini, seuls un nombre fini d'entiers n interviennent, donc ce dernier type ne concerne qu'un nombre fini de points de $S_\infty(L)$.

Ces considérations entraînent que $S_\infty(L)$ est fini et achèvent la démonstration de 9.2.1.

Bibliographie

1. Bogomolov, F.: Sur l'algébricité des représentations l -adiques. C.R. Acad. Sci. Paris **290**, 701–704 (1980)
2. Bourbaki, N.: Algèbre commutative. Hermann
3. Dieudonné, J., Grothendieck, A.: Eléments de géométrie algébrique, chap. III. I.H.E.S., Pub. Math. N° **11** (1961)
4. Grothendieck, A.: Revêtements étales et groupe fondamental (SGA 1). Lecture Notes vol. 224. Berlin-Heidelberg-New York: Springer 1971
5. Grothendieck, A.: Techniques de construction. IV Schémas de Hilbert. Sém. Bourbaki N° **221** (1960–61)
6. Lang, S.: Division points on curves. Annali di matematica pura ed applicata (IV), vol. LXX, pp. 229–234, 1965
7. Mazur, B.: Rational isogenies of prime degree. Invent. Math. **44**, 129–162 (1978)
8. Messing, W.: The crystals associated to Barsotti-Tate groups. Lecture Notes vol. 264. Berlin-Heidelberg-New York: Springer 1972
9. Serre, J-P.: Corps locaux. Hermann 1962
10. Serre, J-P.: Groupes p -divisibles (d'après J. Tate). Sém. Bourbaki N° **318** (1966/67)
11. Tate, J.: p -divisible groups. Local fields, Nuffic summer school, Driebergen: Springer 1966

Oblatum 3-VI-1982