Conducteur d'une variété abélienne et cas particulier des courbes elliptiques

Exposé au séminaire des doctorants en théorie des nombres de Chevaleret

Nicolas Ratazzi

18 Juin 2002

Résumé : Dans cet exposé on introduit et on explique la notion de conducteur d'une variété abélienne. Après un intermède sur les différents modèles d'une courbe elliptique, on revient sur le conducteur d'une courbe elliptique en parlant de la conjecture de Szpiro et de la formule d'Ogg.

Table des matières

Email address : ratazzi@math.jussieu.fr

Dans toute la suite, on appellera *K-variété*, tout K-schéma X, de type fini, géométriquement intègre. Si X est une K-variété, et si L est une extension de K, on notera X_L la variété sur L déduite de X par extension des scalaires.

Définition 0.1 On dit que A/K est *une variété abélienne (sur K)* si A est une K-variété propre munie d'une structure de K-schéma en groupes.

Remarque 0.1 Une variété abélienne A/K est automatiquement un K-schéma en groupes, commutatif et lisse.

1 Conducteur d'une variété abélienne

1.1 Notations

Dans toute la suite on utilisera les notations suivantes :

p désigne un nombre premier, et l un nombre premier différent de p,

$K_\mathfrak{p}$ est un corps local (donc parfait), d'uniformisante π_K, de corps résiduel (nécessairement parfait) de caractéristique p.

$A/K_\mathfrak{p}$ est une variété abélienne, de dimension d,

$V_l(A) = T_l(A) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ est le $\mathbb{Q}_l$-vectoriel déduit du module de Tate l-adique $T_l(A) = \varprojlim A[l^n]$,

$I(\overline{K_\mathfrak{p}}/K_\mathfrak{p})$ est le groupe d'inertie de $\overline{K_\mathfrak{p}}/K_\mathfrak{p}$,

$L_\mathfrak{p} = K_\mathfrak{p}\left(A\left[l\right]\right)$ est l'extension engendrée par les points de l-torsion, d'uniformisante π_L,

$G = \mathrm{Gal}(L_\mathfrak{p}/K_\mathfrak{p})$ de cardinal g, et G_i est le $i^{\text{ème}}$ groupe de ramification supérieure de cardinal g_i, *i.e.*, le groupe

$$G_i = \left\{\sigma \in G \ / \ v_L(\sigma\pi_L - \pi_L) \geq i+1\right\}.$$

1.2 Définitions

On pose

$$\varepsilon(A/K_\mathfrak{p}) = \dim_{\mathbb{Q}_l}\left(\frac{V_l(A)}{V_l(A)^{I(\overline{K_\mathfrak{p}}/K_\mathfrak{p})}}\right), \quad \text{et} \quad \delta(A/K_\mathfrak{p}) = \sum_{i\geq 1}\frac{g_i}{g}\dim_{\mathbb{F}_l}\left(\frac{A[l]}{A[l]^{G_i}}\right).$$

Définition 1.1 Les termes $\varepsilon(A/K_\mathfrak{p})$ et $\delta(A/K_\mathfrak{p})$ sont appelés respectivement *partie modérée* de l'exposant du conducteur et *partie sauvage* de l'exposant du conducteur.

Définition 1.2 Le *conducteur de la variété abélienne* $A/K_\mathfrak{p}$ est l'entier $\mathfrak{p}^{f(A/K_\mathfrak{p})}$ où

$$f(A/K_\mathfrak{p}) = \varepsilon(A/K_\mathfrak{p}) + \delta(A/K_\mathfrak{p}) \ \text{ est } \textit{l'exposant du conducteur.}$$

Remarque 1.1 Notons que les définitions et notations précédentes contiennent de manière implicite le théorème non-trivial suivant :

Théorème 1.1 *Les entiers $\varepsilon(A/K_\mathfrak{p})$ et $\delta(A/K_\mathfrak{p})$ sont indépendants de $l \neq p$.*

Définition 1.3 Si $K/\mathbb{Q}$ est un corps de nombres et si A/K est une variété abélienne, on définit le *conducteur de A/K* comme étant le nombre

$$\mathfrak{c}(A/K) = \prod_\mathfrak{p} \mathfrak{p}^{f(A/K_\mathfrak{p})}.$$

1.3 Résultats généraux

On commence par rappeler un lemme regroupant les propriétés des groupes de ramification dont nous aurons besoin. On renvoie au livre *Corps Locaux* [Ser70] pour une preuve du lemme.

Lemme 1.1 *Soit L/K une extension de corps locaux.*
(i) $G_0(L/K)$ est le groupe d'inertie de L/K.
(ii) L/K est sauvagement ramifiée $\iff$ $G_1(L/K) \neq 1$.

Remarque 1.2 La propriété (ii) du lemme explique pourquoi $\delta(A/K_\mathfrak{p})$ s'appelle la partie sauvage et $\varepsilon(A/K_\mathfrak{p})$ la partie modérée :

$$\delta(A/K_\mathfrak{p}) \neq 0 \iff L_\mathfrak{p}/K_\mathfrak{p} \text{ est sauvagement ramifiée.}$$

Ainsi,

$$f(A/K_\mathfrak{p}) = \varepsilon(A/K_\mathfrak{p}) \quad \iff \quad L_\mathfrak{p}/K_\mathfrak{p} \text{ est modérément ramifiée.}$$

De plus,

$$\begin{aligned}
\varepsilon(A/K_\mathfrak{p}) = 0 \quad &\iff \quad V_l(A)^{I(\overline{K_\mathfrak{p}}/K_\mathfrak{p})} = V_l(A), \\
&\iff \quad I(\overline{K_\mathfrak{p}}/K_\mathfrak{p}) \text{ agit trivialement sur } T_l(A), \\
&\iff \quad T_l(A) \text{ est non-ramifié}, \\
&\implies \quad L_\mathfrak{p}/K_\mathfrak{p} \text{ est non-ramifiée.}
\end{aligned}$$

Le résultat principal découle de la théorie de Serre-Tate [ST68] :

Théorème 1.2 *Soit A/K une variété abélienne sur un corps K, et soit v une valuation discrète de K, de corps résiduel k_v de caractéristique p. Soit l un nombre premier distinct de p. Alors les propriétés suivantes sont équivalentes :*

(i) A a bonne réduction en v.

(ii) pour tout premier $m \neq p$, l'extension $K(A[m])/K$ est non-ramifiée en v.

(iii) $T_l(A)$ est non-ramifié en v (critère de Néron-Ogg-Schafarevitch).

Démonstration : Cf [ST68] Theorem 1. p. 493. □

Corollaire 1.1 *Soit $A/K_\mathfrak{p}$ une variété abélienne. Alors,*

$$\varepsilon(A/K_\mathfrak{p}) = 0 \iff A/K_\mathfrak{p} \text{ a bonne réduction.}$$

Démonstration : La remarque précédente alliée à l'équivalence entre (i) et (iii) dans le théorème 1.2 donne le résultat. □

Corollaire 1.2 *Soit $A/K_\mathfrak{p}$ comme précédemment. Si $A/K_\mathfrak{p}$ a bonne réduction, alors*

$$f(A/K_\mathfrak{p}) = 0.$$

Démonstration : Si $A/K_\mathfrak{p}$ a bonne réduction, alors, $L_\mathfrak{p}/K_\mathfrak{p}$ est non-ramifiée (propriété (ii) du théorème 1.2). Donc le groupe d'inertie $G_0(L_\mathfrak{p}/K_\mathfrak{p})$ est trivial. Par définition de la partie sauvage $\delta(A/K_\mathfrak{p})$, et par le corollaire précédent on en déduit le résultat. □

Remarque 1.3 Si $p > 2d+1$, alors on peut voir que $\delta(A/K_\mathfrak{p}) = 0$ et que $f(A/K_\mathfrak{p}) \leq 2d$. Dans le cas général, on a la majoration suivante :

Théorème 1.3 $f(A/K_\mathfrak{p}) \leq 12d^2 v_{K_\mathfrak{p}}(p)$.

Démonstration : Cf. [LRS93] où un énoncé plus précis (et même optimal) est prouvé. □

Le corollaire 1.2, la remarque 1.3 et le théorème 1.3 indiquent que, tant donnée une variété abélienne A/K sur un corps de nombre K, on sait borner explicitement (en fonction de la dimension et des places de mauvaise réduction) le conducteur $f(A/K)$.

2 Intermède : modèles de courbes elliptiques E sur R

Soient R un anneau de Dedekind et K =Frac(R). On suppose que tous les corps résiduels sont parfaits.

Définition 2.1 On dit que E est *une courbe elliptique (sur K)* si E/K est une variété abélienne de dimension 1.

Proposition 2.1 *Toute courbe elliptique sur K peut-être définie par une équation de Weierstrass à coefficients dans R :*

$$E \ : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Dans ce paragraphe on s'intéresse aux différents modèles sur R "naturels et intéressants" que l'on peut définir pour une courbe elliptique E/K. Il y en a trois : le modèle défini par une équation de Weierstrass, le modèle minimal et le modèle de Néron. On commence par définir ces objets ainsi que leurs propriétés essentielles, puis on indique les liens qui existent entre eux trois.

2.1 Le modèle défini par une équation de Weierstrass

On suppose E/K donnée par une équation de Weierstrass à coefficients dans R. On pose $\mathcal{W}$ le sous-schéma de $\mathbb{P}^2_R$ défini par cette équation. C'est un modèle de E sur R. C'est ce modèle qui donne la réduction naïve de E modulo $\mathfrak{p}$, i.e., obtenue en réduisant les coefficients de l'équation de Weierstrass modulo $\mathfrak{p}$.

Attention : en général ce modèle n'est pas lisse sur R, ni même régulier (en fait, il est lisse si et seulement si E a bonne réduction en toute place de R).

Si $\mathcal{W}$ n'est pas lisse, on pose $\mathcal{W}^0$ le plus grand sous-schéma de $\mathcal{W}$ lisse sur R. C'est encore un modèle de E. En effet, on passe de $\mathcal{W}$ à $\mathcal{W}^0$ en enlevant éventuellement un point (le point singulier) sur chaque fibre spéciale (les "réduites modulo $\mathfrak{p}$"). On ne touche donc pas à la fibre générique.

Proposition 2.2 *(i) On a une bijection entre $E(K)$ et $\mathcal{W}(R)$. De plus, si $\mathcal{W}$ est régulier, alors $\mathcal{W}^0(R)$ est aussi en bijection avec $E(K)$.*
(ii) Si R est de valuation discrète, la structure de groupe de E s'étend en une structure de R-schéma en groupe sur $\mathcal{W}^0$.

2.2 Le modèle minimal

On commence par rappeler la notion de modèle minimal d'une courbe de genre $g \geq 1$.

Définition 2.2 Soient C/K une courbe projective lisse de g et $\mathcal{C}/R$ un modèle de C/K. On dit que c'est un *modèle propre-régulier de C/K* s'il est propre, de type fini et plat, irréductible et régulier.

Définition 2.3 Soient C/K une courbe projective lisse de $g \geq 1$ et $\mathcal{C}^{min}/R$ un modèle propre-régulier de C/K. On dit que c'est un *modèle propre-régulier relativement-minimal de C/K* s'il vérifie la propriété de minimalité suivante : soit $\mathcal{C}/R$ un autre modèle propre-régulier de C/K. Si on a un morphisme birationnel de $\mathcal{C}^{min}$ dans $\mathcal{C}$, alors, c'est un isomorphisme.

Définition 2.4 Soient C/K une courbe projective lisse de $g \geq 1$ et $\mathcal{C}^{min}/R$ un modèle propre-régulier relativement minimal de C/K. On dit que c'est un *modèle propre-régulier minimal de* C/K s'il vérifie la propriété de minimalité suivante : $\mathcal{C}^{min}$ est le seul modèle propre-régulier relativement minimal dans sa classe d'équivalence birationnelle.

Théorème 2.1 *Soit C/K une courbe projective lisse de genre $g \geq 1$. Alors il existe un modèle propre-régulier minimal $\mathcal{C}/R$.*

Démonstration : Elle est dure...cela repose sur plein de chose, notamment (mais pas uniquement) la résolution des singularités pour des surfaces arithmétiques. □

Attention : un tel modèle est régulier mais n'est pas, en général, lisse sur R (lisse sur R signifie que C et tout les $\mathcal{C}_\mathfrak{p}$ sont réguliers). Par contre il est propre et irréductible.

2.3 Le modèle de Néron

Définition 2.5 Avec les notations précédentes, on dit qu'un modèle $\mathcal{E}/R$ de E/K est un modèle de Néron de E si c'est un R-schéma en groupes, lisse et vérifiant la propriété universelle suivante : soient $\mathfrak{X}/R$ un R-schéma lisse de fibre générique X/K et $\varphi : X \to E$ un K-morphisme. Alors le morphisme φ se prolonge de manière unique en un R-morphisme de $\mathfrak{X}$ dans $\mathcal{E}$.

Proposition 2.3 *(i) On a une bijection entre $\mathcal{E}(R)$ et $E(K)$.*
(ii) Le modèle de Néron commute au passage au complété, i.e., si $E_\mathfrak{p} = E \times_K K_\mathfrak{p}$, et si $\mathcal{E}_{R_\mathfrak{p}}$ est le modèle de Néron de $E_\mathfrak{p}$ sur $R_\mathfrak{p}$, on a

$$\mathcal{E}_{R_\mathfrak{p}} \simeq \mathcal{E} \times_R R_\mathfrak{p}.$$

Démonstration : Le point (i) résulte de la propriété universelle définissant le modèle de Néron : "si X/K est lisse, de modèle $\mathfrak{X}/R$, alors, tout K-morphisme de X vers E se prolonge de manière unique en un R-morphisme de $\mathfrak{X}$ vers $\mathcal{E}$." On applique cette propriété à $X = K$ et $\mathfrak{X} = R$ et on en déduit que l'application naturelle $\mathcal{E}(R) \to E(K)$ est une bijection. Le point (ii) est facile, il suffit de l'écrire. □

Théorème 2.2 *Le modèle de Néron d'une courbe elliptique E/K (et même d'une variété abélienne A/K) existe et est unique à unique isomorphisme près.*

Démonstration : L'unicité découle trivialement de la propriété universelle, l'existence est très hautement non triviale... □

Attention : Le modèle de Néron n'est pas propre ni irréductible en général.

2.4 Liens entre $\mathcal{W}$, $\mathcal{C}$ et $\mathcal{E}$

Avant d'indiquer les liens, faisons un petit récapitulatif sur les 3 modèles présentés :

• Le modèle $\mathcal{W}/R$: il n'est pas lisse, ni même régulier, mais il est propre (et même projectif) et a "presque" une structure de groupe.

• Le modèle $\mathcal{C}/R$: il n'est pas lisse, n'a pas de structure de groupe, mais il est propre, irréductible et régulier.

• Le modèle $\mathcal{E}/R$: il n'est pas propre ni irréductible, mais il est lisse et admet une structure de groupe et il vérifie une propriété de prolongement de morphismes très forte.

On donne maintenant les liens qui relie ces objets.

Théorème 2.3 *Le modèle de Néron $\mathcal{E}/R$ est le plus grand sous-schéma de $\mathcal{C}$ lisse sur R.*

Théorème 2.4 *Si $\mathcal{W}/R$ est lisse, alors $\mathcal{W}$ est le modèle de Néron de E/K.*

Démonstration : Le modèle $\mathcal{W}$ est lisse, donc par le (ii) de la proposition 2.2, on en déduit que pour tout $\mathfrak{p} \in \operatorname{Spec} R$, $\mathcal{W}_{\mathfrak{p}} = \mathcal{W} \times R_{\mathfrak{p}}$ est muni d'une structure de $R_{\mathfrak{p}}$-schéma en groupes. Ces lois de groupe sont toutes données par la même équation. Elles se recollent donc pour munir $\mathcal{W}$ d'une structure de schéma en groupes sur R. Il reste pour conclure, à vérifier la propriété universelle du modèle de Néron. Soient donc $\mathfrak{X}$ un R-schéma lisse, de fibre générique X/K et φ un K-morphisme de X dans E. Ce morphisme induit une application rationelle $\Phi : \mathfrak{X} \to \mathcal{W}$. Or $\mathcal{W}$ est projectif, donc propre et $\mathfrak{X}/R$ est lisse. Sous ces hypothèses, on sait par un théorème de Weil que l'application Φ s'étend naturellement en un R-morphisme. Ceci permet de conclure par unicité du modèle de Néron. □

Plus généralement, on a

Théorème 2.5 *Si $\mathcal{E}^0$ dénote la composante connexe de l'identité du modèle de Néron, alors, $\mathcal{W}^0 \simeq \mathcal{E}^0$.*

Remarque 2.1 Notons que ceci implique notamment que si on se donne une équation (minimale) de $E/K_{\mathfrak{p}}$, alors la réduction modulo $\mathfrak{p}$ de E (au sens de la fibre spéciale de son modèle de Néron) est bien ce qu'on croit (i.e. définie par la réduction mod $\mathfrak{p}$ des coefficients de l'équation), au moins dans le cas de bonne réduction.

3 Retour au conducteur : cas particulier des courbes elliptiques

Dans ce paragraphe on reprend les notations précédant l'intermède, à l'exception notable mais classique, de la courbe elliptique que l'on notera E plutôt que A.

On va maintenant voir, dans le cas des courbes elliptiques, ce que l'on peut dire de plus, notamment dans le cas de mauvaise réduction. On s'intéressera également au lien entre le conducteur et le discriminant minimal d'une courbe elliptique. On introduit auparavant quelques notations supplémentaires, et on fait quelques rappels sur les différents types de réduction d'une courbe elliptique.

3.1 Rappel sur la réduction d'une courbe elliptique

Soient $E/K_\mathfrak{p}$ une courbe elliptique, $k_\mathfrak{p}$ le corps résiduel de $K_\mathfrak{p}$, R l'anneau de valuation discrète associé à $K_\mathfrak{p}$, $\mathcal{W}/R$ le modèle défini par une équation de Weierstrass de $E/K_\mathfrak{p}$, et $\widetilde{E}_\mathfrak{p}/k_\mathfrak{p}$ la réduction de E modulo $\mathfrak{p}$, i.e., $\widetilde{E}_\mathfrak{p} = \mathcal{W} \times_R k_\mathfrak{p}$.

Définition 3.1 Soient $E/K_\mathfrak{p}$ une courbe elliptique, et $\widetilde{E}_\mathfrak{p}/k_\mathfrak{p}$ sa réduction modulo $\mathfrak{p}$. Il y a 3 possibilités :

(i) Si $\widetilde{E}_\mathfrak{p}/k_\mathfrak{p}$ est lisse, on dit que E a *bonne réduction*. Dans ce cas, $\widetilde{E}_\mathfrak{p}/k_\mathfrak{p}$ est encore une courbe elliptique.

(ii) Si $\widetilde{E}_\mathfrak{p}/k_\mathfrak{p}$ a un noeud, on dit que E a *réduction multiplicative*.

(iii) Si $\widetilde{E}_\mathfrak{p}/k_\mathfrak{p}$ a une pointe, on dit que E a *réduction additive*.

On peut montrer que seules ces 3 possibilités existent. Par ailleurs, on peut justifier le nom des différents cas. C'est l'objet de la propositon suivante :

Proposition 3.1 *Soit $E/K_\mathfrak{p}$ une courbe elliptique, et $\widetilde{E}_\mathfrak{p}/k_\mathfrak{p}$ sa réduction modulo $\mathfrak{p}$, et $\widetilde{E}^0_\mathfrak{p}$ le lieu des points réguliers.*

Si E a réduction multiplicative alors, $\widetilde{E}^0_\mathfrak{p}(\overline{k_\mathfrak{p}}) \simeq \overline{k_\mathfrak{p}}^\times$ est le groupe multiplicatif.

Si E a réduction additive, alors, $\widetilde{E}^0_\mathfrak{p} \simeq \mathbb{G}_a$ est le groupe additif.

Remarque 3.1 Il se trouve que, d'après le théorème 2.5, $\mathcal{W}^0$ est bien la composante connexe de l'identité du modèle de Néron $\mathcal{E}$, et de même à fortiori pour la réduction modulo $\mathfrak{p}$, $\widetilde{E}^0_\mathfrak{p}$, d'où la notation. On pose également :

$$E_0(K_\mathfrak{p}) = \left\{ P \in E(K_\mathfrak{p}) \ / \ \widetilde{P} \in \widetilde{E}^0_\mathfrak{p}(k_\mathfrak{p}) \right\}, \text{ et, } E_1(K_\mathfrak{p}) = \left\{ P \in E(K_\mathfrak{p}) \ / \ \widetilde{P} = 0 \right\}.$$

Proposition 3.2 *(i) On a les identités :* $E(K_\mathfrak{p}) = \mathcal{E}(R)$, et, $E_0(K_\mathfrak{p}) = \mathcal{E}^0(R)$.
(ii) Le groupe $E(K_\mathfrak{p}^{nr})/E_0(K_\mathfrak{p}^{nr})$ *est isomorphe au groupe* $\mathcal{E}_\mathfrak{p}(R^{nr})/\mathcal{E}_\mathfrak{p}^0(R^{nr})$. *En particulier, c'est un groupe fini.*

Démonstration : Le point (i) résulte de la proposition 2.3. Le point (ii) suit facilement. □

3.2 "Définition" alternative du conducteur

On va donner un théorème qui donne une définition géométrique du conducteur d'une courbe $E/K_\mathfrak{p}$, au moins pour $p > 3$. C'est une généralisation du critère de Néron-Ogg-Schafarevitch (propriété (iii) du théorème 1.2).

Lemme 3.1 *Soit A un groupe abélien, et l un nombre premier. On définit comme d'habitude* $T_l(A) = \varprojlim A[l^n]$ *et* $V_l(A) = T_l(A) \otimes \mathbb{Q}_l$. *Si A est un groupe fini ou sans l-torsion, alors,* $V_l(A) = 0$.

Démonstration : Si A n'a pas de l-torsion, alors on fait une limite projective de $\{0\}$ et on obtient donc $\{0\}$. Si A est fini, alors pour n suffisamment grand, on a $A[l^n] = A[l^{n+1}]$, donc par définition de la limite projective $T_l(A) = 0$. □

Lemme 3.2 *Le groupe* $E_1(K_\mathfrak{p}^{nr})$ *est un p-groupe.*

Démonstration : Si $\mathcal{M}$ désigne l'idéal maximal de l'anneau de valuation discrète R^{nr} associé à $K_\mathfrak{p}^{nr}$. On montre que le groupe $E_1(K_\mathfrak{p}^{nr})$ est isomorphe (comme groupe) au groupe formel $\widehat{E}(\mathcal{M})$. Or la théorie générale des groupes formels nous indique alors que ce groupe est un p-groupe. □

Théorème 3.1 *(i) Soit $E/K_\mathfrak{p}$ une courbe elliptique.*

$$\varepsilon(E/K_\mathfrak{p}) = \begin{cases} 0 & \text{si } E \text{ a bonne réduction,} \\ 1 & \text{si } E \text{ a réduction multiplicative,} \\ 2 & \text{si } E \text{ a réduction additive.} \end{cases}$$

(ii) Soit $E/K_\mathfrak{p}$ une courbe elliptique à réduction semi-stable, ou si $p > 3$, alors,

$$\delta(E/K_\mathfrak{p}) = 0 \text{ et } f(E/K_\mathfrak{p}) = \begin{cases} 0 & \text{si } E \text{ a bonne réduction,} \\ 1 & \text{si } E \text{ a réduction multiplicative,} \\ 2 & \text{si } E \text{ a réduction additive.} \end{cases}$$

Démonstration : On commence par prouver le point (i) de l'énoncé. Notons $K_{\mathfrak{p}}^{nr}$ l'extension maximale non-ramifiée de $K_{\mathfrak{p}}$. C'est un corps local de corps résiduel $\overline{k_{\mathfrak{p}}}$, clôture algébrique du corps résiduel $k_{\mathfrak{p}}$ de $K_{\mathfrak{p}}$. On considère les deux suites exactes

$$0 \longrightarrow E_0(K_{\mathfrak{p}}^{nr}) \longrightarrow E(K_{\mathfrak{p}}^{nr}) \longrightarrow E(K_{\mathfrak{p}}^{nr})/E_0(K_{\mathfrak{p}}^{nr}) \longrightarrow 0$$

$$0 \longrightarrow E_1(K_{\mathfrak{p}}^{nr}) \longrightarrow E_0(K_{\mathfrak{p}}^{nr}) \longrightarrow \mathcal{E}_{\mathfrak{p}}^0(\overline{k_{\mathfrak{p}}}) \longrightarrow 0$$

On sait par la proposition 3.2 que le groupe $E(K_{\mathfrak{p}}^{nr})/E_0(K_{\mathfrak{p}}^{nr})$ est un groupe fini et on sait par le lemme 3.2 que le groupe $E_1(K_{\mathfrak{p}}^{nr})$ est un p-groupe, donc n'a pas de l-torsion. Ainsi, en appliquant le lemme 3.1, on en déduit que

$$V_l\left(E(K_{\mathfrak{p}}^{nr})/E_0(K_{\mathfrak{p}}^{nr})\right) = 0 \quad \text{et} \quad V_l\left(E_1(K_{\mathfrak{p}}^{nr})\right) = 0.$$

On en déduit ainsi les isomorphismes (le premier est clair, dans le second on utilise le fait que $E_1(K_{\mathfrak{p}}^{nr})$ est un p-groupe)

$$V_l\left(E_0(K_{\mathfrak{p}}^{nr})\right) \simeq V_l\left(E(K_{\mathfrak{p}}^{nr})\right) \quad \text{et} \quad V_l\left(E_0(K_{\mathfrak{p}}^{nr})\right) \simeq V_l\left(\mathcal{E}_{\mathfrak{p}}^0(\overline{k_{\mathfrak{p}}})\right).$$

D'autre part, on a par définition

$$V_l\left(E(K_{\mathfrak{p}}^{nr})\right) = V_l\left(E(\overline{K_{\mathfrak{p}}})\right)^{\mathrm{Gal}(\overline{K_{\mathfrak{p}}}/K_{\mathfrak{p}}^{nr})} = V_l\left(E(\overline{K_{\mathfrak{p}}})\right)^{I(\overline{K_{\mathfrak{p}}}/K_{\mathfrak{p}})}.$$

On en déduit l'isomorphisme

$$V_l\left(\mathcal{E}_{\mathfrak{p}}^0(\overline{k_{\mathfrak{p}}})\right) \simeq V_l\left(E(\overline{K_{\mathfrak{p}}})\right)^{I(\overline{K_{\mathfrak{p}}}/K_{\mathfrak{p}})}.$$

On peut maintenant calculer

$$\begin{aligned} \varepsilon(E/K_{\mathfrak{p}}) &= 2 - \dim_{\mathbb{Q}_l}\left(V_l\left(E(\overline{K_{\mathfrak{p}}})\right)^{I(\overline{K_{\mathfrak{p}}}/K_{\mathfrak{p}})}\right), \text{ car } l \neq p, \quad (1) \\ &= 2 - \dim_{\mathbb{Q}_l}\left(V_l\left(\mathcal{E}_{\mathfrak{p}}^0(\overline{k_{\mathfrak{p}}})\right)\right). \quad (2) \end{aligned}$$

Il ne reste plus qu'à calculer la dimension de l'espace vectoriel $V_l\left(\mathcal{E}_{\mathfrak{p}}^0(\overline{k_{\mathfrak{p}}})\right)$ selon les différents types de réduction de $E/K_{\mathfrak{p}}$ pour conclure. On utilise les rappels du paragraphe précédent concernant la structure du groupe des points lisses de la réduction de E.

Si E a bonne réduction, alors $\mathcal{E} = \mathcal{E}^0$, donc $V_l\left(\mathcal{E}_{\mathfrak{p}}^0(\overline{k_{\mathfrak{p}}})\right) = V_l\left(\mathcal{E}_{\mathfrak{p}}\right) \simeq \mathbb{Q}_l^2$.

Si E a réduction multiplicative, alors $V_l\left(\mathcal{E}_{\mathfrak{p}}^0(\overline{k_{\mathfrak{p}}})\right) \simeq V_l\left(\overline{k_{\mathfrak{p}}}^{\times}\right) \simeq \mathbb{Q}_l$.

Si E a réduction additive, alors $V_l\left(\mathcal{E}_{\mathfrak{p}}^0(\overline{k_{\mathfrak{p}}})\right) \simeq V_l\left(\overline{k_{\mathfrak{p}}}^{+}\right) \simeq 0$.

On passe maintenant au point (ii) : Si E a bonne réduction, c'est le corollaire 1.2. Sinon, le résultat est vrai mais on l'admet (cf. [Sil94] p.384-385). □

Finalement, dans le cas des courbes elliptiques et pourvu que p soit supérieur à 4, on a une description géométrique explicite particulierement simple du conducteur. A-t-on une "belle formule" qui marche même en caractéristique 2 et 3 ? La réponse est oui : c'est la *formule d'Ogg*. Si $K_\mathfrak{p}/\mathbb{Q}_p$ est un corps local, cette formule donne explicitement, en fonction du discriminant minimal $\mathcal{D}_{E/K_\mathfrak{p}}$ de $E/K_\mathfrak{p}$ et du nombre de composantes $m(E/K)$ de la fibre spéciale de $E/K_\mathfrak{p}$, l'exposant du conducteur de E. Or $\mathcal{D}_{E/K_\mathfrak{p}}$ et $m(E/K_\mathfrak{p})$ peuvent être calculés par un algorithme dû à Tate. Ainsi, en caractéristique 2 et 3 on utilise la formule de Ogg pour calculer l'exposant du conducteur, et en caractéristique supérieure à 4 on utilise la description géométrique précédente.

Dans la formule suivante, on note :

$m(E/K)$ le nombre de composantes, définies sur $\overline{k}_\mathfrak{p}$ et comptées sans multiplicité, de la fibre spéciale $\widetilde{\mathcal{C}}_\mathfrak{p}$ du modèle minimal de $E/K_\mathfrak{p}$.

$v\left(\mathcal{D}_{E/K_\mathfrak{p}}\right)$ la valuation du discriminant minimal de $E/K_\mathfrak{p}$.

Théorème 3.2 (Formule d'Ogg) $v\left(\mathcal{D}_{E/K_\mathfrak{p}}\right) = f(E/K_\mathfrak{p}) + m(E/K_\mathfrak{p}) - 1$.

3.3 Discriminant et conjecture de Szpiro

Soient $K/\mathbb{Q}$ un corps de nombres et E/K une courbe elliptique semi-stable. Alors, la description géométrique du conducteur nous donne imédiatement :

$$\mathfrak{f}(E/K) = \prod_{\mathfrak{p}|\mathcal{D}_{E/K}} \mathfrak{p}.$$

Notamment, on a dans ce cas l'inégalité $\mathfrak{f}(E/K) \leq \mathcal{D}_{E/K}$. En fait, cette inégalité est vraie sans hypothèse de semi-stabilité : c'est un corollaire de la formule d'Ogg.

Proposition 3.3 *Soient $K_\mathfrak{p}/\mathbb{Q}_p$ un corps local et $E/K_\mathfrak{p}$ une courbe elliptique, alors*

$$f(E/K_\mathfrak{p}) \leq v\left(\mathcal{D}_{E/K_\mathfrak{p}}\right).$$

Démonstration : Par la formule d'Ogg on sait que $f(E/K_\mathfrak{p}) = 1 - m(E/K_\mathfrak{p}) + v\left(\mathcal{D}_{E/K_\mathfrak{p}}\right)$. Or le nombre de composantes irréductibles est nécessairement supérieur à 1. □

Si E/K est une courbe elliptique sur un corps de nombres et si $N_\mathbb{Q}^K$ est la norme de K à $\mathbb{Q}$, alors on déduit de la proposition précédente l'inégalité

$$N_\mathbb{Q}^K\left(\mathfrak{f}(E/K)\right) \leq N_\mathbb{Q}^K\left(\mathcal{D}_{E/K}\right).$$

On peut se demander si une inégalité (avec des exposants) dans l'autre sens existe. Conjecturalement la réponse est oui : c'est la *conjecture de Szpiro*.

Conjecture 3.1 (Szpiro) *Soient K un corps de nombres et $\varepsilon > 0$. Il existe une constante $C(K, \varepsilon)$ telle que pour toute courbe elliptique E/K on a*

$$N_{\mathbb{Q}}^{K}\left(\mathcal{D}_{E/K}\right) \leq C(K,\varepsilon) N_{\mathbb{Q}}^{K}\left(\mathfrak{f}(E/K)\right)^{6+\varepsilon}.$$

Dans l'article [HS88], Hindry-Silverman ont montré que cette conjecture entraine une conjecture de Lang sur la minoration de la hauteur des points d'une courbe elliptique :

Conjecture 3.2 (Lang) *Soit K un corps de nombres. Il existe une constante strictement positive $c(K)$ telle que pour toute courbe elliptique E/K et pour tout point $P \in E(K)\backslash E_{\mathrm{tors}}$, on a*

$$\widehat{h}(P) \geq c \max\left\{h(j_E), \log N_{\mathbb{Q}}^{K}\left(\mathcal{D}_{E/K}\right)\right\}.$$

En particulier on en déduit que cette conjecture est vraie quand on se restreint aux courbes elliptiques ayant potentiellement bonne réduction.

Références

[HS88] M. Hindry and J. Silverman. Canonical heights and integral points on elliptic curves. In *Invent. Math.*, volume 93, pages 419–450, 1988.

[HS00] M. Hindry and J. Silverman. *Diophantine Geometry : An introduction.* GTM 200. Springer, 2000.

[LRS93] P. Lockhart, P. Rosen, and J. Silverman. An upper bound for the conductor of an abelian variety. In *J. Alg. Geo*, volume 2, pages 569–601, 1993.

[Ser70] J.-P. Serre. *Corps locaux.* Hermann, 1970.

[Sil86] J. Silvermann. *The Arithmetic of Elliptic Curves.* GTM 106. Springer, 1986.

[Sil94] J. Silvermann. *Advanced Topics in the Arithmetic of Elliptic Curves.* GTM 151. Springer, 1994.

[ST68] J.-P. Serre and J. Tate. Good reduction of abelian varieties. In *Ann. of Math.*, volume 88, pages 492–517, 1968.