Reduction de Familles de points CM

Christophe Cornut

17 novembre 2000

Table des matières

Introduction

Une conjecture de Mazur et son contexte

Birch et Swinnerton-Dyer

Soit F un corps de nombres, et $\mathbb{E}_{/F}$ une courbe elliptique.

Il est conjecturé que la fonction L associée à $\mathbb{E}_{/F}$, $L(\mathbb{E}_{/F}, s)$, initialement définie pour $\mathrm{Re}(s) > 3/2$, admet un prolongement analytique sur le plan complexe. Supposant cette première conjecture vérifiée pour $\mathbb{E}_{/F}$, la conjecture de Birch et Swinnerton-Dyer prédit alors notamment que :

$$\mathrm{ord}_{s=1}\left(L(\mathbb{E}_{/F}, s)\right) = \mathrm{rang}\,(\mathbb{E}(F))$$

("le rang analytique est égal au rang géométrique").

Un premier résultat positif dans cette direction, concerne le cas où $\mathbb{E}$ est une courbe elliptique à multiplication complexe. Dans ce cas, l'existence du prolongement analytique est due à Deuring et Weil. Lorsque $F = \mathbb{Q}$ ou le corps de multiplication complexe, J. Coates et A. Wiles démontrèrent que :

$$\mathrm{rang}\,(\mathbb{E}(F)) \geq 1 \Longrightarrow \mathrm{ord}_{s=1}\left(L(\mathbb{E}_{/F}, s)\right) \geq 1.$$

La formule de Gross-Zagier

Le second résultat positif, plus précis, concerne le cas des courbes elliptiques définies sur $\mathbb{Q}$.

Soit donc $\mathbb{E}_{/\mathbb{Q}}$ une courbe elliptique de conducteur N. D'après Wiles-Taylor-Wiles, il existe une paramétrisation modulaire de $\mathbb{E}$, c'est-à-dire un morphisme non constant

$$\pi : X_0(N)_{/\mathbb{Q}} \to \mathbb{E}_{/\mathbb{Q}}.$$

Pour les courbes elliptiques ainsi paramétrées, l'existence du prolongement analytique des fonctions L est due à Eichler et Shimura.

Soit alors $K \subset \mathbb{C}$ un corps quadratique imaginaire, de discriminant $d_K < 0$, et O_K l'anneau des entiers de K. Supposons que l'*hypothèse de Heegner* est vérifiée pour N et K, à savoir :

– Tout facteur premier q de N est décomposé dans K.

Notons que N étant fixé, il existe une infinité de corps quadratiques K vérifiant l'hypothèse de Heegner. Celle-ci garantit qu'il existe un idéal $\mathcal{N}$ de O_K tel que $O_K/\mathcal{N} \simeq \mathbb{Z}/N\mathbb{Z}$. Le morphisme de tores complexes

$$\mathbb{C}/O_K \to \mathbb{C}/\mathcal{N}^{-1}$$

induit par l'inclusion $O_K \subset \mathcal{N}^{-1}$ de réseaux de $\mathbb{C}$, est alors une N-isogénie cyclique, et définit donc un point complexe

$$x_1 = \left[\mathbb{C}/O_K \to \mathbb{C}/\mathcal{N}^{-1}\right] \in X_0(N)(\mathbb{C})$$

La théorie de la multiplication complexe montre que ce point est rationnel sur $K[1]$, le corps de classe de Hilbert de K, c'est-à-dire l'extension abélienne non ramifiée maximale de K. On pose :

$$y_1 = \pi(x_1) \in \mathbb{E}(K[1]).$$

L'hypothèse de Heegner garantit d'autre part que le rang analytique de $\mathbb{E}_{/K}$ est *impair*, et la célèbre formule de B.H. Gross et D. Zagier [7] stipule que

$$L'(\mathbb{E}_{/K}, 1) = \gamma\widehat{h}\left(\mathrm{Tr}_{K[1]/K}(y_1)\right),$$

où γ est une constante non nulle, et $\widehat{h}$ la hauteur canonique. En particulier, cette formule montre que

$$\mathrm{Tr}_{K[1]/K}(y_1) \notin \mathbb{E}(K)_{\mathrm{tors}} \quad \Longleftrightarrow \quad \mathrm{ord}_{s=1}\left(L(\mathbb{E}_{/K}, s)\right) = 1.$$

A fortiori,

$$\mathrm{ord}_{s=1}\left(L(\mathbb{E}_{/K}, s)\right) = 1 \quad \Longrightarrow \quad \mathrm{rang}\left(\mathbb{E}(K)\right) \geq 1.$$

Kolyvagin

Dans un travail ultérieur, V.A. Kolyvagin [11] a d'autre part montré les implications :

$$\begin{aligned} \mathrm{Tr}_{K[1]/K}(y_1) \notin \mathbb{E}(K)_{\mathrm{tors}} \quad &\Longrightarrow \quad \mathrm{rang}\left(\mathbb{E}(K)\right) = 1 \\ &\Longrightarrow \quad \#\mathrm{Sha}(\mathbb{E}(K)) < \infty \end{aligned}$$

Joint à la formule de Gross et Zagier, les résultats de Kolyvagin prouvent en fait l'essentiel de la conjecture de Birch et Swinnerton-Dyer pour $\mathbb{E}_{/K}$... lorsque le *rang analytique* de $\mathbb{E}_{/K}$ est égal à un.

Si en revanche $\mathrm{ord}_{s=1}\left(L(\mathbb{E}_{/F}, s)\right) > 1$, la formule de Gross-Zagier affirme que $\mathrm{Tr}_{K[1]/K}(y_1) \in \mathbb{E}(K)_{\mathrm{tors}}$. On est alors conduit à prendre en considération des points plus généraux de $X_0(N)$, pour étudier l'arithmétique de $\mathbb{E}_{/K}$.

Points CM et points de Heegner

K et N étant fixés, convenons d'appeler *point CM* tout élément $x \in X_0(N)(\mathbb{C})$ correspondant à une N-isogénie cyclique

$$x = [E_1 \to E_2] \in X_0(N)(\mathbb{C}),$$

où E_1 et E_2 sont des courbes elliptiques sur $\mathbb{C}$, à multiplication complexe par K. On dit de x que c'est un *point de Heegner* si de plus

$$\mathrm{End}_{\mathbb{C}}(E_1) = \mathrm{End}_{\mathbb{C}}(E_2).$$

Cet anneau s'identifie à un ordre de K, et est donc de la forme

$$O_c = \mathbb{Z} + cO_K,$$

pour un entier $c \geq 1$ uniquement déterminé, que l'on appelle le *conducteur* de x. La théorie de la multiplication complexe montre qu'un point de Heegner x de conducteur c est rationnel sur $K[c]$, le "ring class field" de conducteur c de K ; c'est une extension abélienne de K, non ramifiée en dehors de c, galoisienne et dihédrale sur $\mathbb{Q}$.

L'hypothèse de Heegner garantit à nouveau l'existence de tels points. Reprenant en effet notre idéal $\mathcal{N}$ de O_K tel que $O_K/\mathcal{N} \approx \mathbb{Z}/N\mathbb{Z}$, posons, pour tout entier $c \geq 1$ premier à N :

$$\mathcal{N}_c = \mathcal{N} \cap O_c.$$

$\mathcal{N}_c$ est alors un O_c-idéal inversible, et $O_c/\mathcal{N}_c \approx \mathbb{Z}/N\mathbb{Z}$, de sorte que l'isogénie de tore complexe

$$\mathbb{C}/O_c \to \mathbb{C}/\mathcal{N}_c^{-1}$$

définit un point de Heegner de conducteur c :

$$x_c = [\mathbb{C}/O_c \to \mathbb{C}/\mathcal{N}_c^{-1}] \in X_0(N)(K[c]).$$

On pose encore $y_c = \pi(x_c) \in \mathbb{E}(K[c])$.

L'ensemble des points CM constitue la généralisation naturelle du point x_1 considéré dans la formule de Gross et Zagier. Cet ensemble est stable sous les correspondances de Hecke de $X_0(N)$, ainsi que sous l'action de $\mathrm{Gal}(\overline{K}/K)$. Il en résulte que les points de son image par π dans $\mathbb{E}$ vérifient un ensemble de relations de nature galoisienne, axiomatisées par Kolyvagin dans le formalisme des systèmes Eulériens. Ces relations font de ce système de points un outil qui se prête à toutes sortes de techniques de descentes galoisiennes. C'est ainsi que, bien qu'ils soient définis sur de "grosses" extensions de K, les points CM peuvent néanmoins "projeter une ombre" sur l'arithmétique de $\mathbb{E}$ sur le corps quadratique K lui-même.

La conjecture de B. Mazur

La théorie d'Iwasawa, et les théorèmes de contrôle dus à B. Mazur, constituent l'une de ces techniques de descentes galoisiennes.

Fixons un nombre premier p ne divisant pas N, et notons H_∞ la $\mathbb{Z}_p$-extension anticyclotomique de K : c'est l'unique $\mathbb{Z}_p$-extension de K galoisienne et dihédrale sur $\mathbb{Q}$. La réunion $K[p^\infty]$ des ring class fields de conducteur p^n, pour tout $n \geq 0$, est une extension *finie* de H_∞.

En réponse aux cas laissés vacants par la formule de Gross et Zagier, et avant même la parution de leur article, B. Mazur émit la conjecture suivante :

Conjecture *[15] Il existe $n \geq 0$ tel que*

$$\mathrm{Tr}_{K[p^\infty]/H_\infty}(y_{p^n}) \notin \mathbb{E}(H_\infty)_{tors}.$$

La démonstration de cette conjecture constitue l'objectif principal du présent travail.

Conséquences

La conjecture de Mazur est donc un résultat de "non-trivialité asymptotique". Quelques auteurs ont utilisé cette conjecture comme une hypothèse de travail pour l'étude de l'arithmétique de $\mathbb{E}_{/K}$ le long de la $\mathbb{Z}_p$-extension anticyclotomique H_∞ de K : elle stipule en effet que les points de Heegner fournissent une donnée initiale *non triviale* pour la théorie d'Iwasawa de la courbe elliptique $\mathbb{E}_{/K}$ le long de cette $\mathbb{Z}_p$-extension. En d'autres termes : lorsque l'hypothèse si fructueuse que $\mathrm{Tr}_{K[1]/K}(y_1) \notin \mathbb{E}(K)_{\mathrm{tors}}$ n'est *pas* vérifiée, (c'est-à-dire lorsque $L'(\mathbb{E}_{/K}, 1) = 0$), la conjecture de Mazur affirme néanmoins qu'une variante anticyclotomique de cette hypothèse est satisfaite.

Notons que pour exploiter convenablement cette donnée initiale, il faut de plus supposer que $\mathbb{E}_{/\mathbb{Q}}$ a (bonne) réduction ordinaire en p. Dans cet esprit, M. Bertolini [2] a par exemple généralisé les techniques de Kolyvagin dans ce contexte de théorie d'Iwasawa, obtenant (sous quelques hypothèses techniques supplémentaires) :

Corollaire *Soit $\Gamma = \mathrm{Gal}(H_\infty/K)$, et $H_n = H_\infty^{\Gamma^{p^n}}$. Posons*

$$\Lambda = \mathbb{Z}_p[[\Gamma]] = \varprojlim \mathbb{Z}_p[\mathrm{Gal}(H_n/K)]$$

et

$$\mathrm{Sel}_{p^\infty}(\mathbb{E}_{/H_\infty}) = \varinjlim(\mathrm{Sel}_{p^\infty}(\mathbb{E}_{/H_n})).$$

Alors le dual de Pontryagin de $\mathrm{Sel}_{p^\infty}(\mathbb{E}_{/H_\infty})$ est un Λ-module de rang 1.

Les théorèmes de contrôle dus à B. Mazur permettent par ailleurs de "descendre" partiellement l'information ainsi obtenue à K. Dans cette direction, mentionnons le résultat de J. Nekovář et N. Schappacher [21] :

Corollaire *Le groupe de Selmer* $\mathrm{Sel}_{p^\infty}(\mathbb{E}_{/K}) = \varinjlim \mathrm{Sel}_{p^n}(\mathbb{E}_{/K})$ *contient une copie de* $\mathbb{Q}_p/\mathbb{Z}_p$ *:*

$$\mathrm{corang}_{\mathbb{Z}_p}\left(\mathrm{Sel}_{p^\infty}\left(\mathbb{E}_{/K}\right)\right) \geq 1.$$

Si la p-partie du groupe de Tate-Šafarevič de $\mathbb{E}_{/K}$ *est finie, alors*

$$\mathrm{rang}(\mathbb{E}(K)) \geq 1.$$

Enfin, J. Nekovář a récemment démontré [22] :

Corollaire *Pour toute courbe elliptique* $\mathbb{E}/\mathbb{Q}$,

$$\mathrm{ord}_{s=1} L(\mathbb{E}, \mathbb{Q}) \equiv \mathrm{ord}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(\mathbb{E}/\mathbb{Q})) \pmod 2.$$

Les grandes lignes de la preuve

Approche brutale

Posons

$$G_0 = \mathrm{Gal}(K[p^\infty]/K)_{\mathrm{tors}},$$

de sorte que G_0 est précisément le groupe de Galois de l'extension finie $K[p^\infty]/H_\infty$ qui nous intéresse. On veut donc montrer :

$$\exists n \geq 0 \quad \text{tel que :} \quad \sum_{\sigma \in G_0} \sigma y_{p^n} \notin \mathbb{E}(H_\infty)_{\mathrm{tors}}.$$

Notons tout d'abord que $\mathbb{E}(H_\infty)_{\mathrm{tors}}$ est un ensemble *fini*. Si t est son cardinal, il nous faut voir que *l'ensemble*

$$\{(\sigma y_{p^n})_{\sigma \in G_0} \mid n \geq 0\} \subset \mathbb{E}\left(K[p^\infty]\right)^{(G_0)}$$

n'est pas inclus dans le noyau du morphisme

$$\mathbb{E}^{(G_0)} \xrightarrow{\Sigma} \mathbb{E} \xrightarrow{\times t} \mathbb{E}.$$

Il faudrait idéalement que cet ensemble soit *dense* pour la topologie de Zariski, ou, ce qui revient au même, que l'ensemble

$$\{(\sigma x_{p^n})_{\sigma \in G_0} \mid n \geq 0\} \subset X_0(N)\left(K[p^\infty]\right)^{(G_0)}$$

soit dense pour la topologie de Zariski. Or ce n'est en général pas le cas !

Une obstruction géométrique

Soit en effet $q \mid d_K$ un nombre premier *ramifié* dans K et différent de p ; si $qO_K = Q^2$, soit

$$\sigma = \mathrm{Frob}_Q(K[p^\infty]/K) \in \mathrm{Gal}(K[p^\infty]/K)$$

le Frobénius de Q dans $K[p^\infty]/K$. On a alors $\sigma^2 = 1$, donc $\sigma \in G_0$. Mais d'autre part, on vérifie aisément que l'adhérence (pour la topologie de Zariski) de l'ensemble

$$\{(x_{p^n}, \sigma x_{p^n}) \mid n \geq 0\} \subset X_0(N)\,(K[p^\infty])^2$$

est exactement l'image du morphisme propre

$$X_0(Nq) \to X_0(N) \times X_0(N)$$

qui est le produit des deux applications de dégénérescence usuelles. A fortiori, cet ensemble n'est certainement pas dense dans $X_0(N)^2$.

Réalisation géométrique d'une partie de la trace

On est donc conduit à isoler une partie de G_0, donc l'action sur les points de Heegner considérés est de nature géométrique. Plus précisément, considérons le sous-groupe G_1 de G_0 engendré par les Frobénius des idéaux premiers de O_K qui sont ramifiés sur $\mathbb{Q}$, et non ramifiés dans $K[p^\infty]$:

$$G_1 =< \mathrm{Frob}_Q(K[p^\infty]/K) \;\mid\; Q \mid q \mid d_K \text{ et } q \neq p >\subset G_0$$

Choisissons également une *base* de cet $\mathbb{F}_2$-espace vectoriel :

$$G_1 = \ll \mathrm{Frob}_{Q_1}, \cdots, \mathrm{Frob}_{Q_g} \gg$$

où, pour $i = 1, \ldots, g$, $Q_i^2 = q_i O_K$, et $p \neq q_i \mid d_K$. Posons enfin $M = q_1 \cdots q_g$.

Il existe alors une famille de *points de Heegner* $x'_{p^n} \in X_0(NM)(K[p^\infty])$, et un morphisme non constant

$$\pi' : X_0(NM)_{/\mathbb{Q}} \to \mathbb{E}_{/\mathbb{Q}},$$

tels que, pour tout $n \geq 0$,

$$\pi'(x'_{p^n}) = \mathrm{Tr}_{G_1}(y_{p^n}) \in \mathbb{E}(K[p^\infty]).$$

Le morphisme π' n'est autre que la somme (dans $\mathbb{E}$) des morphismes que l'on obtient en composant notre paramétrisation initiale π avec *toutes* les applications de dégénérescence $X_0(NM) \to X_0(N)$. Notons par ailleurs que NM ne vérifie plus l'hypothèse de Heegner relativement à K.

Avec cette nouvelle paramétrisation, la conjecture de Mazur devient donc :

$$\exists n \geq 0 \quad \text{tel que :} \quad \sum_{\sigma \in \mathcal{R}} \sigma\pi'(x'_{p^n}) \notin \mathbb{E}(H_\infty)_{\text{tors}}.$$

où l'on a choisi un système de représentants $\mathcal{R} \subset \mathrm{Gal}(K[p^\infty]/H_\infty)$ de G_0/G_1. Il suffirait donc à nouveau de voir que l'ensemble

$$\left\{(\sigma x'_{p^n})_{\sigma \in \mathcal{R}} \mid n \geq 0\right\} \subset X_0(NM)\left(K[p^\infty]\right)^{(\mathcal{R})}$$

est dense, ou en tout cas, "trop gros" pour être contenu dans l'image réciproque de l'ensemble fini $\mathbb{E}(K[p^\infty])_{\text{tors}}$ par le morphisme

$$X_0(NM)^{(\mathcal{R})} \xrightarrow{\pi'} \mathbb{E}^{(\mathcal{R})} \xrightarrow{\sum} \mathbb{E}.$$

Réduction supersingulière

Pour cela, on montre que *la réduction* de cet ensemble en une place convenablement choisie de $K[p^\infty]$ est un ensemble "aussi gros que possible". Plus précisément, fixons un nombre premier auxiliaire $\ell \nmid pN$ *inerte* dans K, et une place v de $K[p^\infty]$ de caractéristique résiduelle ℓ. La théorie du corps de classe montre alors que le corps résiduel k de $K[p^\infty]$ en v est isomorphe à $\mathbb{F}_{\ell^2}$. Il est par ailleurs bien connu que les points CM de $X_0(NM)(K[p^\infty])$ se réduisent (en v) dans le site *supersingulier* $X_0^{\text{ss}}(NM)(k)$ de $X_0(NM)(k)$.

Notant $\mathcal{L}$ l'ensemble des points de $X_0(NM)(K[p^\infty])^{(\mathcal{R})}$ qui sont *conjugués* sous l'action de $\mathrm{Gal}(K[p^\infty]/K)$ à un élément de $\left\{(\sigma x'_{p^n})_{\sigma \in \mathcal{R}} \mid n \geq 0\right\}$, on montre que $\mathcal{L}$ se réduit *surjectivement* sur l'ensemble $X_0^{\text{ss}}(NM)(k)$.

En d'autres termes, les relations "géométriques" entre les points de Heegner considérés que l'on a fait apparaître en isolant le sous-groupe G_1 de G_0, sont en quelque sorte les seules relations "génériques" liant ces points, la "partie restante" G_0/G_1 de G_0 agissant aléatoirement (sans relations) sur l'ensemble des points de Heegner.

Reste à indiquer comment l'on démontre ce résultat de surjectivité pour la partie "chaotique" de G_0.

L'apport de V. Vatsal

Dans un preprint récent (printemps 2000), V. Vatsal établit un résultat de non-trivialité asymptotique pour des valeurs spéciales de fonctions L anticyclotomiques $L(g, \chi, s)$, dans le cas où le signe de l'équation fonctionnelle est égal à un. Sa preuve, s'inspirant des idées de Ferrero et Washington dans l'étude de l'invariant μ *cyclotomique*, repose sur une formule de Gross (analogue à la formule de Gross et Zagier), reliant ces valeurs spéciales de fonctions L à la distribution de certains "points de Gross" (analogues aux points de Heegner) dans les composantes connexes d'une "fausse courbe de Shimura" X, associée à un corps de quaternions sur $\mathbb{Q}$ qui est *ramifié* en ∞.

Pour démontrer cette non-trivialité asymptotique, Vatsal prouve un résultat d'équidistribution pour les points de Gross dans l'ensemble des composantes connexes de X, en utilisant un théorème de Marina Ratner sur l'adhérence des sous-groupes à un paramètre unipotents dans les groupes de Lie p-adique.

V. Vatsal a depuis également prouvé la conjecture de Mazur [38], en utilisant des congruences de Jochnowitz pour relier ses premiers résultats de non-trivialité de valeurs spéciales de fonctions L au comportement des points de Heegner. Sa preuve ne lui permet toutefois pas de s'affranchir de l'hypothèse restrictive, déjà présente dans ses premiers travaux, selon laquelle le discriminant de K doit être un nombre premier. Cette obstruction correspond précisément, dans notre preuve, à ce que l'on a appelé la partie "géométrique" de G_0 : si d_K est un nombre premier, le sous-groupe G_1 de G_0 est en effet trivial.

Notre résultat de surjectivité de la réduction supersingulière simultanée des points de Heegner est l'analogue du résultat d'équidistribution de Vatsal pour les points de Gross dans l'ensemble des composantes connexes de la fausse courbe de Shimura X. Nous aimerions d'ailleurs mieux comprendre ce lien entre les composantes connexes de X (une courbe en caractéristique 0), et les points supersinguliers des courbes modulaires (en caractéristique > 0). Ce phénomène semble lié à l'inversion des invariants qui apparaît dans l'uniformisation p-adique des (vraies) courbes de Shimura, via la théorie du "level-raising" de Ribet (qui intervient dans la preuve de Vatsal).

La partie "chaotique" de G_0

Pour ce qui nous concerne, on commence par réinterpréter la réduction en v de l'ensemble $\mathcal{L}$ en termes adéliques, puis p-adiques, en utilisant pour cela une description bien connue de $X_0^{\mathrm{ss}}(N)(k)$. La difficulté de cette étape est de garder la trace de l'action de Galois. On est ainsi ramené à montrer la surjectivité d'une application :

$$\begin{array}{rcl} PSL_2(\mathbb{Q}_p) & \to & \prod_{\sigma\in\mathcal{R}} \Gamma_\sigma \setminus PSL_2(\mathbb{Q}_p)/PSL_2(\mathbb{Z}_p) \\ x & \mapsto & ([x], ..., [x]) \end{array}$$

où Γ_σ est un sous-groupe discret et cocompact de $PSL_2(\mathbb{Q}_p)$, associé à $\sigma \in \mathcal{R}$. Cette même application apparaît également dans le contexte des points de Gross sur les (fausses) courbes de Shimura, et notre preuve suit alors, à quelques améliorations près, celle de Vatsal : $PSL_2(\mathbb{Z}_p)$ étant ouvert dans $PSL_2(\mathbb{Q}_p)$, il nous suffit de voir que, si Δ est la diagonale de $PSL_2(\mathbb{Q}_p)^{(\mathcal{R})}$, le produit

$$\Delta . \prod_{\sigma\in\mathcal{R}} \Gamma_\sigma$$

est dense dans $PSL_2(\mathbb{Q}_p)^{(\mathcal{R})}$. Le théorème de M. Ratner [25] stipule que l'adhérence de ce produit est de la forme $H.\prod_{\sigma\in\mathcal{R}}\Gamma_\sigma$, pour un certain sous-groupe fermé $H \subset PSL_2(\mathbb{Q}_p)^{(\mathcal{R})}$ contenant Δ. $PSL_2(\mathbb{Q}_p)$ étant un groupe simple, il y a fort peu de tels sous-groupes H : on montre en fait que $H = PSL_2(\mathbb{Q}_p)^{(\mathcal{R})}$ dès lors que les sous-groupes Γ_σ sont deux à deux non-commensurables. Il ne reste plus qu'à vérifier que c'est effectivement le cas.

Variantes

Au demeurant, cette preuve permet de généraliser la conjecture de Mazur dans différentes directions, et met en évidence un résultat intermédiaire sur la réduction supersingulière simultanée de points CM, dont on espère qu'il pourrait avoir d'autres applications. Nous donnons ici les énoncés de nos principaux résultats.

Familles de points CM p-isogènes

Soit $E_{/\mathbb{C}}$ une courbe elliptique à multiplication complexe par K, $N \geq 1$ un entier, $C \subset E(\mathbb{C})$ un sous-groupe cyclique d'ordre N. Soit également p un nombre premier ne divisant pas N, et $i_0 \geq 0$ un entier. Pour tout sous-groupe fini X de $E(\mathbb{C})_{p-\mathrm{tors}}$, le sous-groupe $(X \oplus C)/X$ de $(E/X)(\mathbb{C})$ est cyclique d'ordre N, et définit donc une $\Gamma_0(N)$-structure sur la courbe elliptique (E/X). Si l'on adjoint à cette structure une $\Gamma_0(p^{i_0})$-structure X'/X, on obtient donc un point CM :

$$[E/X \to E/(X' \oplus C)] \in X_0(Np^{i_0})(\mathbb{C}).$$

Notant $\mathcal{L}$ l'ensemble des points ainsi obtenus, il existe un entier c premier à p tel que

$$\mathcal{L} \subset X_0(Np^{i_0})\,(K[cp^\infty])$$

où $K[cp^\infty]$ est la réunion de tous les "ring class fields" $K[cp^n]$, pour $n \geq 0$.

Surjectivité de la réduction supersingulière

Soit d'autre part $\mathrm{Gal}(K[cp^\infty]/K)^{\mathrm{rat}}$ le sous-groupe de $\mathrm{Gal}(K[cp^\infty]/K)$ formé par les éléments σ qui peuvent être représentés, via l'application de réciprocité d'Artin, par un idèle fini $\hat\lambda = (\hat\lambda_q)_q \in \widehat{K}^*$ dont la p-composante est triviale :

$$\sigma = [K[cp^\infty]/K, \hat\lambda] \quad \text{et} \quad \hat\lambda_p = 1.$$

Soit $\mathcal{R}$ un ensemble fini d'éléments de $\mathrm{Gal}(K[cp^\infty]/K)$, *deux à deux distincts modulo* $\mathrm{Gal}(K[cp^\infty]/K)^{\mathrm{rat}}$.

Soit enfin S un ensemble fini de nombres premiers $\ell \nmid pN$, inertes ou ramifiés dans K, et choisissons pour tout $\ell \in S$ une place v_ℓ de $K[cp^\infty]$ dont le corps résiduel $k(\ell)$ soit de caractéristique ℓ. Soit

$$\mathrm{red}_\ell : X_0(Np^{i_0})\,(K[cp^\infty]) \to X_0(Np^{i_0})\,(k(\ell))$$

l'application de réduction en v_ℓ.

Notre résultat optimum de "surjectivité de la réduction" est alors :

Théorème *L'application*

$$\begin{array}{rccc} \mathrm{RED}: & \mathcal{L} & \to & \prod_{\ell \in S} \left(X_0^{ss}(Np^{i_0})(k(\ell))\right)^{\mathcal{R}} \\ & x & \mapsto & \left(\mathrm{red}_\ell(\sigma.x)\right)_{(\sigma,\ell)\in\mathcal{R}\times S}. \end{array}$$

est surjective.

Généralisation de la conjecture de Mazur

Supposons que N satisfait l'hypothèse de Heegner relativement à K, et prenons pour couple (E, C) :

$$E = \mathbb{C}/O_K \quad \text{et} \quad \mathrm{C} = E[\mathcal{N}]$$

où $O_K/\mathcal{N} \approx \mathbb{Z}/N\mathbb{Z}$. On a alors :

$$\mathcal{L} \subset X_0(Np^{i_0})\,(K[p^\infty])$$

(c'est-à-dire, $c = 1$ dans les notations du pénultième paragraphe).

Soit $\alpha : J_0(Np^{i_0})_{/\mathbb{Q}} \to \mathbb{A}_{/\mathbb{Q}}$ un morphisme surjectif de variétés abéliennes dont le noyau soit *connexe*, et

$$\pi : X_0(Np^{i_0}) \to \mathbb{A}$$

le morphisme obtenu en composant α avec l'immersion habituelle $X_0(Np^{i_0}) \to J_0(Np^{i_0})$ qui envoie la pointe ∞ sur 0.

Soit enfin q un nombre premier ne divisant pas $\varphi(Np^{i_0}d_K) = \#\left(\mathbb{Z}/Np^{i_0}d_K\mathbb{Z}\right)^*$, et $\chi : G_0 \to \mathbb{F}_q^*$ un caractère. Remarquons notamment que, N et K étant fixés, on peut prendre $q = p$ si $i_0 = 1$, pour presque tout p. Alors :

Théorème *Le $\mathbb{F}_q$-espace vectoriel engendré par*

$$\sum_{\sigma \in G_0} \chi^{-1}(\sigma)\,(\pi(a) \otimes 1) \in \mathbb{A}\,(K[p^\infty]) \otimes \mathbb{F}_q \qquad a \in \mathcal{L}$$

est de dimension infinie.

On en déduit aisément que, pour tout caractère $\chi : G_0 \to \mathbb{C}^*$,

Théorème *Le $\mathbb{C}$-espace vectoriel engendré par*

$$\sum_{\sigma \in G_0} \chi^{-1}(\sigma)\,(\pi(a) \otimes 1) \in \mathbb{A}\,(K[p^\infty]) \otimes \mathbb{C} \qquad a \in \mathcal{L}$$

est de dimension infinie.

La preuve de ces énoncés diffère légèrement de celle que nous avons indiquée plus haut, en ce sens que pour tirer le meilleur parti de notre résultat de surjectivité de la réduction supersingulière, nous utilisons un théorème d'Ihara. Ceci nous permet de contrôler beaucoup plus finement le passage de l'ensemble des points supersinguliers d'une courbe modulaire en caractéristique ℓ, au groupe des points rationnels sur $\mathbb{F}_{\ell^2}$ de sa Jacobienne.

Description de la thèse

Dans une première partie ("Réseaux dans les corps quadratiques K"), nous avons d'une part collecté les principales propriétés des ordres de K et de leurs idéaux (Chapitre 1), et d'autre part, tenté de donner une représentation graphique des relations existant entre les différents points CM (Chapitre 2).

La seconde partie ("Points CM") débute par un rappel des principaux résultats de la théorie des courbes elliptiques à multiplication complexe (Chapitre 3), et des propriétés des points CM qui en découlent (Chapitre 4). Le Chapitre 5, relativement technique, vise à mettre en place les outils permettant de décrire les familles de points CM et leurs réductions, tandis que le Chapitre 6 est entièrement consacré à la preuve de notre premier résultat principal, sur la surjectivité de la réduction supersingulière.

Dans la troisième partie ("La conjecture de Mazur"), on en déduit une preuve de la conjecture de Mazur (Chapitre 9), en essayant de tirer le meilleur parti du résultat de surjectivité, tant dans la précision des énoncés que dans leur généralité. Si l'utilisation du théorème d'Ihara (Chapitre 7) remplit à cet égard parfaitement son rôle, le Chapitre 8 est en revanche plus décevant : en l'absence de résultats conjecturaux qui eussent guidé nos pas, nous y perdons beaucoup en généralité.

Enfin, nous avons inclus un appendice sur les "$\mathfrak{a}$-transforms", une variation schématique due semble-t'il à J-P. Serre d'une technique de constructions de variétés abéliennes utilisée antérieurement par de nombreux auteurs.

Première partie

Réseaux dans les corps quadratiques

Chapitre 1

Ordres

Soit $K \subset \mathbb{C}$ un corps quadratique imaginaire, d_K son discriminant, O_K l'anneau des entiers de K. Un ordre est un sous-anneau de K, de type fini sur $\mathbb{Z}$ et engendrant K sur $\mathbb{Q}$. L'objet de ce chapitre est d'étudier l'arithmétique de ces ordres.

1.1 Les éléments de K

Pour un élément x de K, on note $\mathrm{N}(x) = x\overline{x}$ la norme de x, et $\mathrm{Tr}(x) = x + \overline{x}$ sa trace. On a donc : $x^2 - \mathrm{Tr}(x)x + \mathrm{N}(x) = 0$, et $\mathrm{Tr}(x), \mathrm{N}(x) \in \mathbb{Q}$.

Si $x \in K \setminus \mathbb{Q}$, $x - \overline{x} \in K \setminus \mathbb{Q}$ et $\mathrm{Tr}(x - \overline{x}) = 0$, donc $(x - \overline{x})^2 = -\mathrm{N}(x - \overline{x})$ est la racine carrée d'un nombre rationnel négatif $-\lambda$, de sorte que $\mathbb{Q}(\sqrt{-\lambda}) \subset K$ et, par comparaison des dimensions, $K = \mathbb{Q}(\sqrt{-\lambda})$. Ecrivant $\lambda = \frac{n_1}{n_2}$ où n_1 et n_2 sont des entiers, on a donc : $K = \mathbb{Q}\left(\sqrt{-\frac{n_1}{n_2}}\right) = \mathbb{Q}(\sqrt{-n_1 n_2})$. On peut donc d'abord supposer que λ est entier, puis enfin, que λ est un entier positif sans facteur carré.

On obtient ainsi une base de K sur $\mathbb{Q}$, à savoir 1 et $\sqrt{-\lambda}$. Si $x = a + b\sqrt{-\lambda}$,

$$\begin{aligned} \mathrm{Tr}(x) &= 2a \\ \mathrm{N}(x) &= a^2 + \lambda b^2 \end{aligned}$$

Pour que x soit entier, il faut et il suffit que $\mathrm{Tr}(x)$ et $\mathrm{N}(x)$ soient des entiers naturels. Cela force déjà : $2a \in \mathbb{Z}$, donc on peut écrire $a = \frac{n}{2}$, puis $4\mathrm{N}(x) = n^2 + 4\lambda b^2$, donc $\lambda(2b)^2 \in \mathbb{Z}$. λ étant premier et sans facteur carré, on obtient : $2b \in \mathbb{Z}$. Ecrivant $b = \frac{m}{2}$, on a alors : $4\mathrm{N}(x) = n^2 + \lambda m^2$. Si λ n'est pas congru à $3 \bmod 4$, cela force : n et m sont pairs, donc a et b sont entiers. Si $\lambda \equiv 3 \bmod 4$, cela force : n et m ont même parité.

Posons :

$$\varpi_K = \begin{cases} \sqrt{-\lambda} & \text{si } \lambda \equiv 1, 2 \bmod 4 \\ \frac{1+\sqrt{-\lambda}}{2} & \text{si } \lambda \equiv 3 \bmod 4 \end{cases}$$

Il résulte des calculs précédents que 1 et ϖ_K forment une $\mathbb{Z}$-base de O_K, ce que l'on note : $O_K = [1, \varpi_K]$. Le discriminant de K est alors le discriminant du polynome minimal de ϖ_K :

$$\text{si } \begin{cases} \lambda \equiv 1,2 \bmod 4 \\ \lambda \equiv 3 \bmod 4 \end{cases} \quad \text{alors} \quad \begin{cases} \varpi_K^2 + \lambda = 0 \\ \varpi_K^2 - \varpi_K + \frac{1+\lambda}{4} = 0 \end{cases} \quad \text{et} \quad d_K = \begin{cases} -4\lambda \\ -\lambda \end{cases}$$

Si $x = a + b\varpi_K$,

$$\mathrm{Tr}(x) = \begin{cases} 2a \\ 2a+b \end{cases} \quad \text{et } \mathrm{N}(x) = \begin{cases} a^2 + \lambda b^2 \\ (a + \frac{1}{2}b)^2 + \frac{\lambda}{4}b^2 \end{cases} \quad \text{selon que} \quad \begin{cases} d_K \equiv 0 \bmod 4 \\ d_K \equiv 1 \bmod 4 \end{cases}$$

1.2 Les ordres de K

Lemme 1.2.1
1) *Les ordres de K sont de la forme*

$$O_c = \mathbb{Z} + cO_K = [1, c\varpi_K]$$

pour un entier $c \geq 1$.
2) *Le discriminant de O_c est égal à $c^2 d_K$.*
3) *$O_K/O_c \simeq \mathbb{Z}/c\mathbb{Z}$.*
4) *$O_c \subset O_{c'} \Leftrightarrow c' \mid c$.*

Preuve: Soit O un ordre de K. O étant de type fini, tout élément de O est entier, donc $O \subset O_K$. O engendrant K sur $\mathbb{Q}$, O et O_K sont deux $\mathbb{Z}$-modules de rang 2, et l'indice $c = \#O_K/O$ est donc fini. Par définition, $cO_K \subset O$ et $\mathbb{Z} \subset O$ donc $O_c = \mathbb{Z} + cO_K \subset O$. Mais $O_c = [1, c\varpi_K]$ a le même indice que O dans O_K, donc $O = O_c$. Inversement, on vérifie facilement que pour tout entier $c \geq 1$, $O_c = \mathbb{Z} + cO_K$ est un ordre de K. Le reste du lemme est évident. □

Lemme 1.2.2 *Soit c et c' deux entiers positifs. Alors :*

$$\begin{aligned} O_c + O_{c'} &= O_{pgcd(c,c')}, \\ O_c O_{c'} &= O_{pgcd(c,c')}, \\ O_c \cap O_{c'} &= O_{ppcm(c,c')}. \end{aligned}$$

Preuve: Seule la deuxième égalité n'est pas tout à fait triviale. Le réseau $O_c O_{c'}$ est stable par O_c, stable par $O_{c'}$, donc stable par $O_c + O_{c'} = O_{\mathrm{pgcd}(c,c')}$. Ainsi, $O_c O_{c'} = O_{\mathrm{pgcd}(c,c')} O_c O_{c'} = O_{\mathrm{pgcd}(c,c')}$. □

1.3 Unités et idéaux premiers

Proposition 1.3.1 *Les unités de l'ordre O_c sont :*

$$O_c^* = \begin{cases} \{\pm 1\} & si\ c \neq 1\ ou\ d_K \neq -3, -4 \\ \{\pm 1, \pm i\} & si\ c = 1\ et\ d_K = -4 \\ \{\pm 1, \pm \varpi_K, \pm \varpi_K^2\} & si\ c = 1\ et\ d_K = -3 \end{cases}$$

Preuve: Si $x \in O_c^*$, on doit avoir $\mathrm{N}(x) = 1$. Le calcul explicite de la norme de $\mathrm{N}(x)$ effectué plus haut donne le résultat. $\square$

Proposition 1.3.2 *Soit p un nombre premier, c un entier positif.*

1. *Si $p \nmid c$ alors :*
   (a) *Si $\left(\frac{d_K}{p}\right) = -1$: p est inerte dans K, $pO_c = P$ est premier, et :*
   $O_c/P^n \approx (\mathbb{Z}/p^n\mathbb{Z})^2$ *comme groupe,*
   $(O_c/P^n)^* \approx (\mathbb{Z}/p^{n-1}\mathbb{Z})^2 \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/(p+1)\mathbb{Z}$ *si* $p \geq 5$.
   (b) $\left(\frac{d_K}{p}\right) = 0$ *: p est ramifié dans K, $pO_c = P^2$ avec P premier, et :*
   $O_c/P^n \approx (\mathbb{Z}/p^{[n/2]}\mathbb{Z}) \times (\mathbb{Z}/p^{n-[n/2]}\mathbb{Z})$ *comme groupe,*
   $(O_c/P^n)^* \approx (\mathbb{Z}/p^{[(n-1)/2]}\mathbb{Z}) \times (\mathbb{Z}/p^{n-1-[(n-1)/2]}\mathbb{Z}) \times \mathbb{Z}/(p-1)\mathbb{Z}$ *si* $p \geq 5$.
   (c) $\left(\frac{d_K}{p}\right) = 1$ *: p est décomposé dans K, $pO_c = P\overline{P}$ avec P et $\overline{P}$ premiers et :*
   $O_c/P^i \simeq \mathbb{Z}/p^i\mathbb{Z}$ *comme anneau.*
2. *Si $p \mid c$, il y a un unique idéal premier $P = pO_{c/p}$ de O_c sur p, qui n'est pas propre pour O_c, et :*
   $O_c/P^n \approx (\mathbb{Z}/p^n\mathbb{Z}) \times (\mathbb{Z}/p^{n-1}\mathbb{Z})$ *comme groupe.*

Preuve: 1) Si $p \nmid c$, $(O_c)_p = (O_K)_p$ et l'on peut donc supposer que $c = 1$. Comme K est de dimension 2 sur $\mathbb{Q}$, les premiers de $\mathbb{Z}$ sont soit inertes, soit décomposés, soit ramifiés. Le dernier cas correspond à $p \mid d_K$. Les deux autres cas se différencient en fonction des corps résiduels en p, et il s'agit alors de savoir si $-\lambda$ (cf. section 1.1) est un carré ou non dans $\mathbb{F}_p$. Comme $d_K = -\lambda$ ou -4λ, et $4 = 2^2$, on a donc : (d_K est un carré modulo p) $\Leftrightarrow$ (p est décomposé), et, (d_K n'est pas un carré modulo p) $\Leftrightarrow$ (p est inerte).

a) Si $pO_K = P$, $(O_K)_P \approx \mathbb{Z}_{p^2}$ et $O_K/P^n = O_K/p^n \approx (\mathbb{Z}/p^n\mathbb{Z})^2$ comme groupe.

b) Si $pO_K = P^2$, $O_K/P^n = O_K/p^{n/2} \approx (\mathbb{Z}/p^{n/2}\mathbb{Z})^2$ si n est pair. Si n est impair, O_K/P^n est d'ordre p^n, admet un quotient isomorphe à $(\mathbb{Z}/p^{[n/2]}\mathbb{Z})^2$, et est engendré par deux éléments. La classification des groupes abéliens permet alors d'affirmer que $O_c/P^n \approx (\mathbb{Z}/p^{[n/2]}) \times (\mathbb{Z}/p^{n-[n/2]})$.

c) Si $pO_K = P\overline{P}$, $(O_K)_P \simeq \mathbb{Z}_p$ et donc $O_K/P^n \simeq \mathbb{Z}/p^n\mathbb{Z}$ comme anneau.

Pour calculer le groupe multiplicatif de $O_K/P^n \simeq (O_K)_P/P^n$ lorsque $p \geq 5$, on utilise les suites exactes

$$1 \to 1 + P^i(O_K)_P \to (O_K)_P^* \to (O_K/P^i)^* \to 1$$

et l'application exponentielle, un isomorphisme de groupe $P^iO_K \xrightarrow{\simeq} 1+P^i(O_K)_P$.

2) Si $p \mid c$, $pO_{c/p} \subset O_c$ est un idéal de O_c, non propre, et d'indice p dans O_c. C'est donc un idéal premier P de O_c. De plus, $P^2 + pO_c = p^2O_{c/p} + pO_c \subset pO_c$, donc l'anneau O_c/pO_c est local, d'idéal maximal P/pO_c, et P est l'unique idéal premier de O_c sur p. Enfin, $P^n = p^nO_{c/p}$, donc $O_c/P^n \approx (\mathbb{Z}/p^n\mathbb{Z}) \times (\mathbb{Z}/p^{n-1}\mathbb{Z})$ comme groupe. $\square$

Corollaire 1.3.3 *Pour $d, c \geq 1$,*

$$\#(O_c/dO_c)^* = d^2 \times \prod_{q|d} q^{-2}(q-1)\left(q - \left(\frac{d_K c^2}{q}\right)\right). \tag{1.1}$$

Nous aurons besoin du lemme suivant.

Lemme 1.3.4 *Supposons p ramifié dans O_K, $pO_K = P^2$. Pour un entier $c \geq 1$ premier à p, posons $P_c = P \cap O_c$. C'est un idéal propre de O_c sur p, et*

$$P_c \text{ est principal} \quad \Leftrightarrow \quad (c = 1 \text{ et } d_K = -4p) \text{ ou } (c = 1, 2 \text{ et } d_K = -p).$$

Preuve: Supposons que $P_c = O_c x$, avec $x \in O_c = [1, c\varpi_K]$ (notations de 1.1), et écrivons $x = a + bc\varpi_K$ où $a, b \in \mathbb{Z}$. On a alors : si $d_K \equiv 0 \bmod 4$, $\mathrm{N}(x) = p = a^2 + \lambda b^2 c^2$, avec $p \mid d_K = -4\lambda$. Cela force donc : $a = 0$, $b = c = 1$ et $\lambda = p \equiv 0, 1, 2 \bmod 4$, donc $K = \mathbb{Q}(\sqrt{-p})$. Si $d_K \equiv 1 \bmod 4$, alors $\mathrm{N}(x) = (a + \frac{1}{2}bc)^2 + \frac{\lambda}{4}b^2c^2 = p$, avec $p \mid d_K = -\lambda$, et $\lambda \equiv 3 \bmod 4$. Cela force $c = 1$ ou 2, et $d_K = -p$. La réciproque est immédiate. □

1.4 La propriété de Gorenstein

Un *idéal fractionnaire* de O est un sous-O-module de type fini de K, différent de zéro. On utilisera par abus le mot "idéal" pour désigner les idéaux fractionnaires, désignant par *idéal entier* les idéaux (fractionnaires) *contenus* dans O. Tout idéal étant également de type fini sur $\mathbb{Z}$ et engendrant K sur $\mathbb{Q}$ est un réseau, donc libre de rang 2 sur $\mathbb{Z}$. De plus, un O-idéal est *indécomposable* comme O-module.

Lemme 1.4.1 *Tout ordre de K est un anneau de Gorenstein.*

Preuve: O étant fini et plat sur $\mathbb{Z}$, est de dimension de Krull égale à un. Si I est un O-idéal, notons (temporairement) $I^{-1} = \{x \in K \mid xI \subset O\}$. On vérifie facilement que I^{-1} est encore un O-idéal, et est donc engendré sur O par moins de deux éléments. Il résulte alors de [1, 6.3] que O est un anneau de Gorenstein. □

Corollaire 1.4.2 *K et K/O sont des O-modules injectifs.*

Preuve: [1, 6.2]. □

Corollaire 1.4.3 *Tout O-module $N \neq 0$ sans torsion, de type fini et indécomposable, est isomorphe à un O-idéal, et est projectif sur $\mathrm{End}_O(N)$.*

Preuve: [1, 7.3]. □

Corollaire 1.4.4 *Tout O-module de type fini sans torsion est isomorphe à une somme directe finie de O-idéaux.*

On affinera ces résultats plus loin.

1.5 Les idéaux propres

Définition *On dit qu'un O-idéal I (fractionnaire) est propre pour O s'il vérifie l'une des conditions équivalentes suivantes :*

1. *I est O-projectif.*
2. *I est localement principal.*
3. *Si $I^{-1} = \{x \in O \mid xI \subset O\}$, alors $I^{-1}I = O$.*
4. *Il existe un réseau J tel que $JI = O$.*
5. *Il existe un O-idéal J tel que $JI = O$.*
6. *$O = \{x \in K \mid xI \subset I\}$.*

Preuve: 1) $\Rightarrow$ 2) Si I est O-projectif, et p un nombre premier, le localisé I_p de I est O_p-projectif et de rang 1, donc libre de rang 1 puisque O_p est semi-local. 2) $\Rightarrow$ 3) La formation de I^{-1} commute à la localisation, et si $I_p = O_p x$, alors $I_p^{-1} = O_p x^{-1}$ donc $(I^{-1}I)_p = O_p$. 3) $\Rightarrow$ 4) car I^{-1} est un réseau. 4) $\Rightarrow$ 5) car si $JI = O$, $OJI = O$, 5) $\Rightarrow$ 6) car si $xI \subset I$ alors $xIJ = xO \subset IJ = O$, donc $x \in O$. Enfin, 6) $\Rightarrow$ 1) car I est toujours projectif sur $\mathrm{End}_O(I) \simeq \{x \in K \mid xI = I\}$ d'après (1.4.3). □

Partant d'un réseau complet I de K, on peut former l'ensemble

$$O(I) = \{x \in K \mid xI \subset I\}.$$

C'est un sous-anneau de K, agissant fidèlement sur I, donc de type fini sur $\mathbb{Z}$: $O(I)$ est donc un ordre de K. On dit que $O(I)$ est l'ordre de I, et l'on note $c(I)$ son conducteur. Par définition, I est un $O(I)$-idéal propre. On définit encore

$$I^{-1} = \{x \in K \mid xI \subset O(I)\},$$

de sorte que $II^{-1} = O(I)$.

Comment calculer $c(I)$? Partant d'un $\mathbb{Z}$-base de I, disons $I = [\varpi_1, \varpi_2]$, on commence par remplacer I par $\varpi_1^{-1}I$, de sorte que l'on obtient une base de la forme $[1, \tau]$, avec $\tau \in K \setminus \mathbb{Q}$. τ satisfait alors à une équation de degré deux que l'on peut écrire uniquement sous la forme

$$A\tau^2 + B\tau + C = 0,$$

où $\mathrm{pgcd}(A, B, C) = 1$, et $A > 0$. On vérifie alors aisément que l'ordre de I est égal à :

$$O(I) = [1, A\tau].$$

C'est un ordre de discriminant $B^2 - 4AC$. Donc :

$$c(I)^2 = \frac{B^2 - AC}{d_K}.$$

.

Lemme 1.5.1 *Soit I et J deux réseaux de K. Alors*

$$\begin{aligned} c(IJ) &= \mathrm{pgcd}(c(I), c(J)), \\ c(I^{-1}) &= c(I). \end{aligned}$$

Preuve: IJ est stable par $O_{c(I)}$ et $O_{c(J)}$, donc stable par $O_{c(I)} + O_{c(J)} = O_{\mathrm{pgcd}(c(I),c(J))}$. De plus, $I^{-1}J^{-1}IJ = O_{c(I)}O_{c(J)} = O_{\mathrm{pgcd}(c(I),c(J)}$ donc $c(IJ) = \mathrm{pgcd}(c(I), c(J))$. De même, I^{-1} est stable sous $O_{c(I)}$ et $II^{-1} = O_{c(I)}$ donc $c(I^{-1}) = c(I)$. □

Mentionnons également :

Proposition 1.5.2 *Soit $I \subset L$ et $J \subset L$ trois réseaux de K, avec $\#L/I = n$ premier à $\#L/J = m$. Soit i, j, l les conducteurs respectifs de I, J, L. Alors : $L = I + J$ $I/I \cap J \simeq L/J$, $J/I \cap J \simeq L/I$ et $I \cap J$ est de conducteur $\frac{ij}{l}$.*

Preuve: $I \cap J$ est stable sous $O_i \cap O_j = O_{\mathrm{ppcm}(i,j)}$. Soit $c \mid \mathrm{ppcm}(i,j)$ son conducteur. $I + J \subset L$ est d'indice divisant m et n donc $I + J = L$. Donc $I/I \cap J \to L/J$ et $J/I \cap J \to L/I$ sont des isomorphismes, et $n = \#J/I \cap J$, $m = \#I/I \cap J$.

Supposons d'abord $n = p$ et $m = q$ *premiers*. Nous verrons plus bas que les différentes possibilités pour i, j, l, c sont alors les suivantes : $i = lp$, l ou l/p ; $j = lq$, l ou l/q ; et enfin, $c = iq$, i ou i/q d'une part, $c = jp$, j ou j/p d'autre part. On vérifie que cela donne nécessairement : $c = \frac{ij}{l}$.

Supposons ensuite seulement que $n = p$ est premier, et choisissons une filtration maximale de L/J qui nous permet de former :

$$\begin{array}{ccccccccc} J = L_r & \subset & L_{r-1} & \subset \cdots \subset & L_k & \subset & \cdots & \subset & L_0 = L \\ \cup & & \cup & & \cup & & & & \cup \\ I \cap J = I \cap L_r & \subset & I \cap L_{r-1} & \subset \cdots \subset & I \cap L_k & \subset & \cdots & \subset & I \cap L_0 = I \end{array}$$

Chaque "carré" vérifie les hypothèses précédentes. Si l_k est le conducteur de L_k et i_k celui de $I \cap L_k$, on a donc $l_0 = l$, $l_r = j$, $i_0 = i$, $i_r = c$; par ce qui précède, on obtient :

$$i_{k+1} = \frac{i_k l_{k+1}}{l_k}$$

pour tout $0 \leq k \leq r - 1$. Ainsi,

$$c = i_r = i_{r-1}\frac{l_r}{l_{r-1}} = i_{r-2}\frac{l_{r-1}}{l_{r-2}}\frac{l_r}{l_{r-1}} = \cdots = i_0\frac{l_1 \cdots l_r}{l_0 \cdots l_{r-1}} = \frac{ij}{l}.$$

La formule est donc encore vraie pour n *premier*, et m *quelconque*. Réitérant le même raisonnement avec des "rectangles", en filtrant cette fois-ci L/I, on obtient le résultat dans le cas général. □

Fait 1.5.3 *Dans un "carré"*

$$\begin{array}{ccc} I & \subset & L \\ \cup & & \cup \\ I \cap J & \subset & J \end{array}$$

dont les côtés sont d'indices relativement premiers, les produits des conducteurs sur les deux diagonales sont égaux :

$$c(I \cap J) \times c(L) = c(I) \times c(J).$$

1.6 Les groupes de Picard : formule des classes

Il résulte de la section précédente que l'ensemble $\mathcal{I}(O_c)$ des idéaux propres pour O_c est un groupe commutatif pour la multiplication des idéaux. L'ensemble $\mathcal{P}(O_c)$ des idéaux O_c-principaux en est évidemment un sous-groupe, et l'on note :

$$\mathrm{Pic}(O_c) = \mathcal{I}(O_c)/\mathcal{P}(O_c)$$

le groupe quotient. Tout O_c-idéal propre étant localement principal, l'action de $\widehat{K}^*$ sur les O_c-idéaux propres est transitive, et l'on a donc un isomorphisme :

$$\begin{array}{rcl} \widehat{K}^*/\widehat{O}_c^* & \stackrel{\simeq}{\longrightarrow} & \mathcal{I}(O_c) \\ [\hat{\lambda}] & \longmapsto & O_c.\hat{\lambda} \end{array}$$

qui induit à son tour un isomorphisme :

$$\begin{array}{rcl} \widehat{K}^*/K^*\widehat{O}_c^* & \stackrel{\simeq}{\longrightarrow} & \mathrm{Pic}(O_c) \\ [\hat{\lambda}] & \longmapsto & [O_c.\hat{\lambda}] \end{array}$$

Si $c \mid c'$, l'application

$$\begin{array}{rcl} \mathcal{I}(O_{c'}) & \to & \mathcal{I}(O_c) \\ I & \mapsto & O_c I \end{array}$$

est un morphisme de groupe, correspondant au quotient $\widehat{K}^*/\widehat{O}_{c'}^* \to \widehat{K}^*/\widehat{O}_c^*$; ce morphisme est donc surjectif. Il envoie les idéaux principaux (surjectivement) sur les idéaux principaux, et induit par conséquent un morphisme de groupe :

$$\begin{array}{rcl} \mathrm{Pic}(O_{c'}) & \to & \mathrm{Pic}(O_c) \\ [I] & \mapsto & [O_c I] \end{array}$$

Lemme 1.6.1 $\mathrm{Pic}(O_c)$ *est le groupe de Picard de* O_c, *c'est-à-dire le groupe des classes de faisceaux inversibles sur* $\mathrm{Spec}(O_c)$.

Preuve: Une quasi-tautologie : tout O-module projectif de rang 1 est isomorphe à un O-idéal propre. Deux O-idéaux I et J sont isomorphes si, et seulement si, il existe $x \in K^*$ tel que $Ix = J$. □

On peut également reformuler le fait que tout idéal propre pour O_c soit localement principal dans les termes suivants : la localisation induit un isomorphisme

$$\mathcal{I}(O_c) \stackrel{\simeq}{\longrightarrow} \bigoplus_q \mathcal{P}\left((O_c)_q\right).$$

Il en résulte une suite exacte :

$$1 \to \mathcal{P}(O_c) \to \bigoplus_q \mathcal{P}\left((O_c)_q\right) \to \mathrm{Pic}(O_c) \to 1.$$

De plus :

$$\begin{aligned} \mathcal{P}(O_c) &= K^*/O_c^*, \\ \mathcal{P}\left((O_c)_q\right) &= K_q^*/(O_c)_q^*. \end{aligned}$$

Si $c \mid c'$, on a donc un diagramme :

$$\begin{array}{ccccccccc} 1 & \to & \mathcal{P}(O_{c'}) & \to & \bigoplus_q \mathcal{P}\left((O_{c'})_q\right) & \to & \mathrm{Pic}(O_{c'}) & \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & \mathcal{P}(O_c) & \to & \bigoplus_q \mathcal{P}\left((O_c)_q\right) & \to & \mathrm{Pic}(O_c) & \to & 1 \end{array}$$

Les deux premières flèches verticales sont évidemment surjectives et le lemme du serpent nous donne alors une suite exacte :

$$1 \to O_c^*/O_{c'}^* \to \bigoplus_{q \mid \frac{c'}{c}} (O_c)_q^*/(O_{c'})_q^* \to \mathrm{Pic}(O_{c'}) \to \mathrm{Pic}(O_c) \to 1.$$

Pour calculer le second terme, posons $d = \frac{c'}{c}$. De $O_{c'} = \mathbb{Z} + dO_c$, on déduit que pour tout $q \mid d$, $(O_{c'})_q = \mathbb{Z}_q + d(O_c)_q$. En particulier, $1 + d(O_c)_q \subset (O_{c'})_q^*$, et on a donc une surjection :

$$\left((O_c)_q/d(O_c)_q\right)^* = (O_c)_q^*/\left(1 + d(O_c)_q\right) \to (O_c)_q^*/(O_{c'})_q^* \to 1.$$

Le noyau est $\left((O_{c'})_q/d(O_c)_q\right)^*$. Finalement, comme

$$\begin{aligned} O_c/dO_c &\simeq \bigoplus_{q \mid d} (O_c)_q/d(O_c)_q, \\ O_{c'}/dO_c &\simeq \bigoplus_{q \mid d} (O_{c'})_q/d(O_c)_q, \end{aligned}$$

on obtient

$$(O_c/dO_c)^*/(O_{c'}/dO_c)^* = \bigoplus_{q \mid d} (O_c)_q^*/(O_{c'})_q^*,$$

et une suite exacte :

$$1 \to O_c^*/O_{c'}^* \to (O_c/dO_c)^*/(O_{c'}/dO_c)^* \to \mathrm{Pic}(O_{c'}) \to \mathrm{Pic}(O_c) \to 1.$$

Enfin, il est clair que l'anneau $O_{c'}/dO_c$ n'est autre que $\mathbb{Z}/d\mathbb{Z}$. Son groupe multiplicatif est donc de cardinal

$$d \times \prod_{q \mid d} (1 - q^{-1}).$$

Comparant avec la formule (1.1) du corollaire 1.3.3, on trouve finalement :

$$\#\mathrm{Pic}(O_{c'}) = \frac{\#\mathrm{Pic}(O_c) \times [O_c : O_{c'}]}{[O_c^* : O_{c'}^*]} \prod_{q \mid [O_c : O_{c'}]} \left(1 - \left(\frac{d_K c^2}{q}\right) q^{-1}\right).$$

En particulier :

$$\#\mathrm{Pic}(O_c) = \frac{\#\mathrm{Pic}(O_K) \times c}{[O_K^* : O_c^*]} \prod_{q \mid c} \left(1 - \left(\frac{d_K}{q}\right) q^{-1}\right).$$

1.7 Factorisation et approximation

On dit d'un O_c idéal I qu'il est premier à un entier n si pour tout facteur premier q de n, $I_q = (O_c)_q$.

Proposition 1.7.1 *Soit n un entier.*

1. *Les idéaux propres premiers à n forment un sous-groupe de $\mathcal{I}(O_c)$*
2. *Tout O_c-idéal propre est isomorphe à un O_c-idéal premier à n.*
3. *Tout O_c-idéal premier à c est propre.*
4. *Le groupe des O_c-idéaux premiers à c est le groupe libre engendré par les idéaux premiers de O_c qui sont premiers à c.*

Preuve: Tout idéal propre pour O_c est localement principal, de sorte que la localisation induit un isomorphisme :

$$\mathcal{I}(O_c) \xrightarrow{\simeq} \bigoplus_q \mathcal{P}\left((O_c)_q\right),$$

où $\mathcal{P}\left((O_c)_q\right)$ est le groupe des $(O_c)_q$-idéaux principaux inversibles, c'est-à-dire $\mathcal{P}\left((O_c)_q\right) \simeq K_q^*/(O_c)_q^*$. 1) est donc clair, et 2) résulte du théorème d'approximation forte. Si q est un entier premier à c, le localisé $(O_c)_q = (O_K)_q$ est un anneau de valuation discrète, ou le produit de deux anneaux de valuation discrète, et en particulier, tout O_c-idéal est localement principal en q, d'où 3). Enfin, 4) résulte de ce que $\mathcal{P}(R) \simeq \mathbb{Z}$ pour tout anneau de valuation discrète R. $\square$

Corollaire 1.7.2 *Soit $M \neq 0$ un O_c-module de type fini et sans torsion.*

1. *Il existe une décomposition de M :*

$$M = \bigoplus_{d \mid c} M_d,$$

où pour $d \mid c$, M_d est un sous O_c-module de M qui est un O_d-module projectif.

2. *Si M est O_c-projectif, $M_d = 0$ si $d \neq c$, et M est isomorphe à un module de la forme :*

$$O^{r-1} \oplus I,$$

où I est un idéal propre de O_c, et r est le rang de M. De plus : $I \simeq \Lambda^r_{O_c} M$.

Preuve: On décompose d'abord M en somme directe de sous-modules indécomposables : $M = \oplus M_i$. Chaque M_i est isomorphe à un O-idéal, et donc O_{d_i}-projectif de rang 1 pour un certain diviseur d_i de c. Regroupant les termes, on obtient 1). Si de plus M est O-projectif, chacun de ses facteurs directs M_i l'est également, donc $d = c$. Pour conclure 2), il suffit de montrer que si I et J sont deux idéaux propres pour O_c, alors

$$I \oplus J \approx O_c \oplus IJ.$$

Pour cela, on peut d'abord supposer que $I \subset O_c$; soit n_I son indice. On peut ensuite supposer que J est premier à n_I par la proposition précédente, puis également que $J \subset O_c$, avec un indice n_J premier à n_I. L'idéal $n_J I + n_I J$ contient IJ, est inclus dans $I \cap J$, et on vérifie place par place que $IJ = I \cap J$, donc $n_J I + n_I J = IJ$. L'application O_c-linéaire :

$$\begin{array}{rccc} f: & I \oplus J & \to & IJ \\ & x \oplus y & \mapsto & n_J x + n_I y \end{array}$$

est surjective, et IJ est O_c-projectif, donc $I \oplus J \simeq IJ \oplus \ker(f)$. $\ker(f)$ est de rang 1, sans torsion, et facteur direct du O_c-module projectif $I \oplus J$, donc isomorphe à un O_c-idéal propre L de K. On calcule alors :

$$IJ \simeq \Lambda^2(I \oplus J) \simeq \Lambda^2(IJ \oplus L) \simeq IJL,$$

donc $L \simeq O_c$. □

1.8 Ring class fields

Soit $K^{\mathrm{ab}} \subset \mathbb{C}$ l'extension abélienne maximale de K. La théorie du corps de classe établit un isomorphisme :

$$C_K^{\mathrm{comp}} \xrightarrow{\simeq} \mathrm{Gal}(K^{\mathrm{ab}}/K),$$

où $C_K^{\mathrm{comp}} = \varprojlim C_K/N$, N décrivant les sous-groupes ouverts d'indice fini de $C_K = J_K/K^*$, et J_K est le groupe des idèles de K : $J_K = \widehat{K}^* \times \mathbb{C}$ ([36, 5.1]). De plus, tout sous-groupe ouvert d'indice fini N de C_K est le groupe des normes d'une extension abélienne finie L de K : $N = \mathrm{N}_{L/K} C_L$. Comme L/K est non ramifiée en l'unique place ∞ de K, on peut se borner aux seuls idèles finis, et réécrire l'isomorphisme ci-dessus :

$$\left(\widehat{K}^*/K^*\right)^{\mathrm{comp}} \xrightarrow{\simeq} \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

Si c est un entier, $\widehat{K}^*/\widehat{O}_c^* K^*$ est fini. Il en résulte d'abord que $\widehat{K}^*/K^*$ est compact dans la topologie quotient, puisqu'il contient un sous-groupe d'indice fini et compact, à savoir $\widehat{O}_c^* K^*$. Tout sous-groupe ouvert est donc d'indice fini, de sorte que $\widehat{K}^*/K^* = \left(\widehat{K}^*/K\right)^{\mathrm{comp}}$ et notre isomorphisme devient :

$$\begin{array}{rccc} [K^{\mathrm{ab}}/K, \star]: & \widehat{K}^*/K^* & \xrightarrow{\simeq} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \\ & \hat{\lambda} & \mapsto & [K^{\mathrm{ab}}/K, \hat{\lambda}] \end{array}$$

Le sous-groupe $\widehat{O}_c^* K^*$ de $\widehat{K}^*$ définit un sous-groupe ouvert (car fermé d'indice fini) de $\mathrm{Gal}(K^{\mathrm{ab}}/K)$, et donc une extension abélienne finie de K, que l'on note $K[c]$: c'est le *ring class field* de conducteur c de K. Par construction, $K[c]/K$ est non ramifiée en dehors de c, et son groupe de Galois est canoniquement isomorphe à $\mathrm{Pic}(O_c)$. On note cet isomorphisme

$$\begin{array}{rccc} \left(\frac{K[c]/K}{\star}\right): & \mathrm{Pic}(O_c) & \xrightarrow{\simeq} & \mathrm{Gal}(K[c]/K) \\ & [I] & \mapsto & \left(\frac{K[c]/K}{I}\right) \end{array}$$

de sorte que, pour $\hat{\lambda} \in \widehat{K}^*$,

$$\left(\frac{K[c]/K}{O_c.\hat{\lambda}}\right) = [K[c]/K, \hat{\lambda}] \in \mathrm{Gal}(K[c]/K).$$

L'action de la conjugaison complexe par conjugaison sur $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ correspond, dans $\widehat{K}^*/K^*$, à l'action de la conjugaison complexe. Le groupe de norme $\widehat{O}_c^* K^*/K^*$ étant stable sous cette action, $K[c]$ est une extension galoisienne sur $\mathbb{Q}$. De plus, si $\hat{\lambda} \in \widehat{K}^*$, comme $\hat{\lambda}^{-1} = \mathrm{Norme}(\hat{\lambda})^{-1}\overline{\hat{\lambda}}$ avec $\mathrm{Norme}(\hat{\lambda}) \in \widehat{\mathbb{Q}}^* \subset \widehat{O}_c K^*$, $[\hat{\lambda}]^{-1} = \overline{[\hat{\lambda}]}$ dans $\widehat{K}^*/\widehat{O}_c^* K^*$. Il en résulte que l'extension $K[c]/\mathbb{Q}$ est dihédrale.

Si $c \mid c'$, alors $K[c] \subset K[c']$, et le groupe de Galois de $K[c']/K[c]$ est isomorphe au noyau de $\mathrm{Pic}(O_{c'}) \to \mathrm{Pic}(O_c)$. On note $K[\infty]$ l'union de tous les $K[c]$, $c \geq 1$. Si p est un nombre premier et c un entier premier à p, on note de même $K[cp^\infty]$ l'union de tous les $K[cp^i]$, pour $i \geq 0$.

Proposition 1.8.1 *Le groupe* $\mathrm{Gal}(K[cp^\infty]/K)_{\mathrm{tors}}$ *est fini et*

$$\mathrm{Gal}(K[cp^\infty]/K)/\mathrm{Gal}(K[cp^\infty]/K)_{\mathrm{tors}} \approx \mathbb{Z}_p.$$

Preuve: Considérons la suite exacte :

$$0 \to \mathrm{Gal}(K[cp^\infty]/K[c]) \to \mathrm{Gal}(K[cp^\infty]/K) \to \mathrm{Gal}(K[c]/K) \to 0. \tag{1.2}$$

Le premier terme est égal à la limite projective :

$$\begin{aligned} \mathrm{Gal}(K[cp^\infty]/K[c]) &= \varprojlim \mathrm{Gal}(K[cp^n]/K[c]) \\ &= \varprojlim \ker\left(\mathrm{Pic}(O_{cp^n}) \to \mathrm{Pic}(O_c)\right) \end{aligned}$$

On a calculé ce genre de noyau dans la section 1.6 : il s'insère dans une suite exacte

$$\begin{aligned} &1 \to (\mathbb{Z}/p^n\mathbb{Z})^* = (O_{cp^n})_p^* / \left(1 + p^n (O_K)_p\right) \to \\ &\quad \to (O_K)_p^* / \left(1 + p^n (O_K)_p\right) \to \ker\left(\mathrm{Pic}(O_{cp^n}) \to \mathrm{Pic}(O_c)\right) \to 1. \end{aligned}$$

Passant à la limite projective, on obtient donc une suite exacte

$$1 \to \mathbb{Z}_p^* \to (O_K)_p^* \to \mathrm{Gal}(K[cp^\infty]/K[c]) \to 1. \tag{1.3}$$

Or $(O_K)_p^* \simeq \mu(K_p) \times \mathbb{Z}_p^2$, où $\mu(K_p)$ est le groupe *fini* des racines de l'unité de K_p. Il résulte de (1.3) que le pro-p-sous-groupe de $\mathrm{Gal}(K[cp^\infty]/K)$ est de type fini et de rang 1 sur $\mathbb{Z}_p$, et facteur direct d'indice fini de $\mathrm{Gal}(K[cp^\infty]/K)$. Puis (1.2) donne de même que le pro-p-sous-groupe de $\mathrm{Gal}(K[cp^\infty]/K)$ est facteur direct d'indice fini dans $\mathrm{Gal}(K[cp^\infty]/K)$, de type fini et de rang 1 sur $\mathbb{Z}_p$. La proposition en découle. $\square$

Remarque: Dans le cas où $p \geq 5$, les suites exactes de (1.6) et la proposition 1.3.2 montrent directement que $\mathrm{Gal}(K[cp^\infty]/K[cp]) \approx \mathbb{Z}_p$.

Il en résulte que le sous-corps H_{p^∞} de $K[cp^\infty]$ fixé par $\mathrm{Gal}(K[cp^\infty]/K)_{\mathrm{tors}}$ est une $\mathbb{Z}_p$-extension de K, et est même l'unique $\mathbb{Z}_p$-extension de K contenue dans $K[cp^\infty]$, donc ne dépend pas de c.

Définition *La* $\mathbb{Z}_p$-extension anticyclotomique de K *est*

$$H_{p^\infty} = K[cp^\infty]^{\mathrm{Gal}(K[cp^\infty]/K)_{\mathrm{tors}}},$$

où c est n'importe quel entier premier à p.

Chapitre 2

Le graphe des p-isogénies

On fixe dans toute cette section un nombre premier p. Pour tout entier $n \geq 1$, on appelle “inclusion n-cyclique”, ou “n-inclusion”, et l'on note $I \subset_n J$, tout couple de réseaux (I, J) de K tel que $I \subset J$ et $J/I \approx \mathbb{Z}/n\mathbb{Z}$.

2.1 Définition

$\mathbb{Q}^*$ et K^* agissent sur l'ensemble des p-inclusions, et l'on définit :

$$\begin{aligned} \mathcal{T} &= \{\text{réseaux de } K\}/\mathbb{Q}^*, \\ \mathcal{E} &= \{\text{réseaux de } K\}/K^*, \\ \text{Arêtes}(\mathcal{T}) &= \{p-\text{inclusions}\}/\mathbb{Q}^*, \\ \text{Arêtes}(\mathcal{E}) &= \{p-\text{inclusions}\}/K^*. \end{aligned}$$

Soit également :

$$s,\, b : \text{Arêtes}(\mathcal{T}) \to \mathcal{T},$$

les applications “source” et “but”, définies respectivement par $s([I \subset_p J]) = [I]$ et $b([I \subset_p J]) = [J]$. On définit de même les applications “source” et “but” :

$$s,\, b : \text{Arêtes}(\mathcal{E}) \to \mathcal{E}.$$

Soit enfin

$$\begin{aligned} i : \text{Arêtes}(\mathcal{T}) &\to \text{Arêtes}(\mathcal{T}), \\ i : \text{Arêtes}(\mathcal{E}) &\to \text{Arêtes}(\mathcal{E}), \end{aligned}$$

les applications définies par :

$$\begin{aligned} i([I \subset_p J]) &= [J \subset_p p^{-1}I] \\ &= [pJ \subset_p I] \end{aligned}$$

de sorte que $s \circ i = b$, $b \circ i = s$ et $i^2 = 1$. On a ainsi défini deux graphes : $(\mathcal{T}, \text{Arêtes}(\mathcal{T}), s, b, i)$ est bien connu, et $(\mathcal{E}, \text{Arêtes}(\mathcal{E}), s, b, i)$ en est un quotient. Notons que dans $\mathcal{E}$, un sommet peut être voisin de lui-même, et une arête égale à son inverse.

L'application qui à un réseau I associe son conducteur $c(I)$ passe au quotient :

$$c : \mathcal{E} \to \mathbb{Z}.$$

Par définition, les fibres de $c(\star)$ sont les *groupes de Picard.*

Le groupe de Galois $\text{Gal}(K[\infty]/K)$ agit sur le graphe $\mathcal{E}$ muni de cette fibration, c'est-à-dire qu'il agit sur les sommets, respecte les arêtes, et est compatible avec l'application conducteur. On peut définir cette action de deux manières :

- en utilisant la fibration c : $\text{Gal}(K[\infty]/K)$ agit sur les $c^{-1}(c_0) = \text{Pic}(O_{c_0})$ par translation, via son quotient $\text{Gal}(K[c_0]/K) \simeq \text{Pic}(O_{c_0})$.
- en utilisant l'application de réciprocité d'Artin : si $\sigma = [K[\infty]/K, \hat{\lambda}]$ et $x = [I]$, alors $\sigma x = [\hat{\lambda}.I]$.

Le but de cette section est essentiellement d'étudier la structure du graphe $\mathcal{E}$, d'une part en tant que graphe quotient de $\mathcal{T}$, et d'autre part en tant que graphe muni de la "fibration en groupes finis" donnée par c.

2.2 Les arêtes

Soit I un réseau de K. On pose $c = c(I)$, et on choisit un O_c-idéal premier P sur p. On sait qu'il y a exactement $p+1$ sous-réseaux distincts J de I d'indice p. Leurs conducteurs respectifs sont donnés par la règle suivante.

Proposition 2.2.1 *La liste des conducteurs des sous-réseaux d'indice p de I contient exactement :*

1. *Si $p \nmid c$, et*
   (a) $\left(\frac{d_K}{p}\right) = -1$ *: $p+1$ fois cp.*
   (b) $\left(\frac{d_K}{p}\right) = 0$ *: p fois cp, et une fois c, correspondant au sous-réseau PI.*
   (c) $\left(\frac{d_K}{p}\right) = 1$ *: $p-1$ fois cp, et deux fois c, correspondant aux sous-réseaux PI et $\overline{P}I$.*
2. *Si $p \mid c$: p fois cp, et une fois c/p, correspondant à $PI = pO_{c/p}I$.*

Preuve: Soit $J \subset_p I$. Localisant en $q \neq p$, on voit déjà que $O(I)_q = O(J)_q$, donc $c(J)$ est déjà égal à c à une puissance de p près. De plus,

$$pO(I)J \subset pO(I)I \subset pI \subset J \quad \text{et} \quad pO(J)I = O(J)pI \subset O(J)J \subset J \subset I,$$

donc $pO(I) \subset O(J) \subset p^{-1}O(I)$, de sorte que $c(J)$ diffère de c au plus d'un facteur p.

Si $c(J) = c$, alors $L = I^{-1}J \subset_p O_c$ est un idéal premier de O_c d'indice p. Inversement, un tel L donne le sous-réseau $J = LI$ de I, d'indice p dans I et tel que $c(J) = c$. Compte-tenu de (1.3.2), la liste de ces sous-réseaux est bien celle indiquée par la proposition. Si $p \nmid c$, les *autres* sous-réseaux ont donc cp pour conducteur, tandis que si $p \mid c$, les seules possibilités pour $c(J)$ sont cp et c/p. Mais, si J est un sous-réseau de I stable sous $O_{c/p}$, alors

$$O_{c/p}I \subset O_{c/p}p^{-1}J = p^{-1}J;$$

comme $[O_{c/p}I : I] = p = [p^{-1}J : I]$, on a donc $p^{-1}J = O_{c/p}I$, d'où $J = O_{c/p}I$. □

Corollaire 2.2.2

1. *Si $O_c^* = \{\pm 1\}$, il y a exactement $p+1$ arêtes distinctes partant de $[I]$, et les sommets correspondants sont distribués selon la règle suivante :*
   (a) *Si $p \mid c$: $[I]$ a exactement $p+1$ voisins, p ont pour conducteur cp et 1 a pour conducteur c/p.*
   (b) *Si $p \nmid c$ et :*
      i. *$\left(\frac{d_K}{p}\right) = -1$: $[I]$ a exactement $p+1$ voisins, tous de conducteur cp.*
      ii. *$\left(\frac{d_K}{p}\right) = 0$: $[I]$ a exactement $p+1$ voisins, dont p de conducteur cp et 1 de conducteur c.*
      iii. *$\left(\frac{d_K}{p}\right) = 1$: $[I]$ a exactement $p-1$ voisins de conducteur cp, et un ou deux voisins de conducteur c, selon que P^2 est O_c-principal ou non.*
2. *Sinon, $c = 1$ et $d_K = -3$ ou -4. Soit $u = \#O_K^*/\{\pm 1\}$. Alors :*
   (a) *$\left(\frac{d_K}{p}\right) = -1$: Il y a exactement $(p+1)/u$ arêtes partant de $[I]$, vers autant de voisins distincts, tous de conducteurs p.*
   (b) *$\left(\frac{d_K}{p}\right) = 0$: Il y a exactement $(p/u) + 1 = 2$ arêtes partant de $[I]$, vers autant de voisins distincts, l'un de conducteur p et l'autre, égal à $[I]$, de conducteur 1.*
   (c) *$\left(\frac{d_K}{p}\right) = 1$: Il y a exactement $(p-1)/u + 2$ arêtes partant de $[I]$, vers seulement $(p-1)/u + 1$ voisins distincts. Deux de ces arêtes aboutissent à $[I]$, et les $(p-1)/u$ autres arêtes aboutissent à autant de sommets voisins distincts, tous de conducteur p.*

Preuve: Toute arête de but $[I]$ se relève en une inclusion de réseaux $J \subset_p I$, et il y a donc au plus $p+1$ arêtes distinctes de but $[I]$. Il s'agit de déterminer les cas pour lesquels deux inclusions $J \subset_p I$ et $J' \subset_p I$ donnent la même arête, resp. le même sommet voisin.

Supposons d'abord que $O_c^* = \{\pm 1\}$ et que J et J' donnent le même sommet : il existe $\lambda \in K^*$ tel que $J = J'\lambda$. En particulier, J et J' ont le même conducteur. Si ce conducteur est cp, alors $I = O_c J = O_c J'$, donc $I = I\lambda$ et $\lambda \in O_c^* = \{\pm 1\}$, donc $J = J'$. Si ce conducteur est c/p, ou c, alors $J = J'$, sauf éventuellemnt dans le cas : p est décomposé, ne divise pas c et $J = PI$, $J' = \overline{P}I$. On a alors $PI = \overline{P}I\lambda$ donc $P = \overline{P}\lambda$ et $P^2 = O_c p\lambda$ est principal. Inversement, si P^2 est O_c-principal, alors PI et $\overline{P}I$ sont deux sous-réseaux distincts d'indice p dans I, donnant le même sommet dans $\mathcal{E}$. Les deux arêtes correspondantes, en revanche, ne sont pas égales : s'il existait μ tel que $(PI \subset_p I) = (\overline{P}I \subset_p I)\mu$, on aurait $\mu I = I$ donc $\mu = \pm 1$ et $PI = \overline{P}I$, d'où $P = \overline{P}$, une contradiction.

Supposons ensuite que $O_c^* \neq \{\pm 1\}$, de sorte que $c = 1$ et $d_K = -3$ ou -4 et tout O_c-idéal est *principal*. Si J et J' donnent le même sommet, J et J' ont le même conducteur 1 ou p. Si ce conducteur est 1, $J = J'$ sauf si p est décomposé et $J = PI$, $J' = \overline{P}I$. Dans ce cas : J et J' donnent effectivement le même sommet (puisque P est principal) mais pas la même arête : si $(PI \subset_p I) = (\overline{P}I \subset_p I).\mu$, alors $\mu \in O_K^*$ donc $PI\mu = \overline{P}I\mu$ et $P = \overline{P}$, contradiction. Si enfin ce conducteur commun est p, alors $J = \lambda J'$ implique que $I = O_K J = O_K J' = \lambda I$, donc $\lambda \in O_K^*$. Inversement, $O_K^*/\{\pm 1\}$ agit fidèlement sur les sous-réseaux de I d'indice p et de conducteur p, et si J et J' sont dans la même orbite pour cette action, alors J et J' définissent le même sommet voisin de $[I]$, ainsi que la même arête. □

Corollaire 2.2.3 *(p et K étant fixés) : Si $c \gg 0$, exactement $p+1$ arêtes partent de $[I]$ vers $p+1$ sommets distincts.*

Preuve: Il faut voir que pour p décomposé dans K, l'ensemble Z des conducteurs c premiers à p pour lesquels il existe un idéal P_c de O_c sur p tel que P_c^2 est principal, est fini. Soit X l'ensemble des générateurs des carrés des deux idéaux premiers de O_K sur p. Alors X est fini et ne contient aucun élément de $\mathbb{Q}$, donc l'ensemble Y des conducteurs c tels que $X \cap O_c \neq \emptyset$ est *fini.* Si $c \in Z$, et P_c est un idéal de O_c sur p tel que P_c^2 est principal, il existe $\lambda \in O_c$ tel que $P_c^2 = O_c\lambda$, donc $(P_c O_K)^2 = O_K\lambda$ et $\lambda \in X \cap O_c$. Ainsi, $Z \subset Y$ est fini. □

2.3 Les chemins sans aller-retour

Lemme 2.3.1 *Tout chemin $x_0 \to x_1 \to \cdots \to x_{n-1} \to x_n = [J]$ (resp. $[I] = x_0 \to x_1 \to \cdots \to x_{n-1} \to x_n$) de $\mathcal{E}$ ou $\mathcal{T}$ se relève en un "chemin de réseaux" : $I = I_0 \subset_p I_1 \subset_p \cdots \subset_p I_n = J$. Si le chemin de départ est sans* aller-retour*, alors $I \subset_{p^n} J$.*

Preuve: Il est clair que tout chemin se relève. Il est bien connu que tout relèvement d'un chemin sans aller-retour de longueur n dans $\mathcal{T}$ "est" une inclusion p^n-cyclique. Il en est donc à fortiori de même pour les relèvements des chemins sans aller-retour dans le graphe quotient $\mathcal{E}$. □

Inversement :

Proposition 2.3.2 *Soit $I_0 \subset_{p^n} I_n$ une p^n-inclusion de réseaux de K, et posons $c(I_0) = cp^{h_0}$, avec c premier à p, $h_0 \geq 0$. Alors :*

1. $p^{n-i}I_n + I_0 = (p^{-i}I_0) \cap I_n =: I_i$, *et* $I_0 \subset_p I_1 \subset_p \cdots \subset_p I_n$.
2. *Pour tout* i, *il existe un entier* $h_i \geq 0$ *tel que* $c(I_i) = cp^{h_i}$.
3. *La fonction* $i \in [0 \cdots n] \mapsto h_i \in \mathbb{N}$ *est convexe.*
4. $\delta_i = h_{i+1} - h_i \in \{-1, 0, 1\}$. *De plus :*
   (a) *Si* $\delta_i = -1$, $I_{i+1} = O_{cp^{h_{i+1}}} I_i$.
   (b) *Si* $\delta_i = +1$, $I_i = pO_{cp^{h_i}} I_{i+1}$.
   (c) *Si* $\delta_i = 0$, $h_i = 0 = h_{i+1}$.
5. *S'il existe* i *tel que* $h_i = 0$, *posons* $\{i \mid h_i = 0\} = [i_0, \cdots, i_r]$. *Alors :*
   (a) *Si* p *est inerte dans* K, $r = 0$.
   (b) *Si* p *est ramifié dans* K, $r = 0$ *ou* 1.
   (c) *Si* p *est décomposé dans* K, *il existe un idéal premier* P *de* O_c *sur* p *tel que pour tout* $j \in [0, \cdots, r]$, $I_{i_j} = P^{-j} I_{i_0}$.
6. *Si* $O_c^* = \{\pm 1\}$, *le chemin* $[I_0] \to [I_1] \to \cdots \to [I_n]$ *de* $\mathcal{E}$ *est sans aller-retour. Dans le cas général, il y a au plus un aller-retour* $([I_{i-1}] \to [I_i] \to [I_{i+1}])$, *et alors :* $c = 1$, $h_i = 0$, $d_K = -3$ *ou* -4, *et* $h_{i-1} = h_{i+1} = 1$.

Preuve: 1) Comme $I_n/I_0 \approx \mathbb{Z}/p^n\mathbb{Z}$, il existe un unique sous-réseau intermédiaire $I_0 \subset_{p^i} I_i \subset_{p^{n-i}} I_n$ et

$$\begin{array}{rcl} I_i/I_0 & = & p^{n-i}(I_n/I_0) \\ & = & \left(p^{n-i}I_n + I_0\right)/I_0 \end{array} \quad \text{et} \quad \begin{array}{rcl} I_i/I_0 & = & (I_n/I_0)[p^i] \\ & = & \left(I_n \cap p^{-i}I_0\right)/I_0 \end{array}$$

2) et 4) résultent de la proposition 2.2.1.

3) Il faut voir que $i \mapsto \delta_i$ est croissante. Or, si $\delta_{i+1} < \delta_i$, on a :

Si $\delta_i = 0$, $\delta_{i+1} = -1$ et $h_i = h_{i+1} = h_{i+2} + 1$, ce qui est impossible puisque $\delta_i = 0$ donc $h_i = 0$.

Si $\delta_i = 1$ et $\delta_{i+1} = 0$, $h_i + 1 = h_{i+1} = h_{i+2}$, ce qui est à nouveau impossible puisque $\delta_{i+1} = 0$ donc $h_{i+1} = 0$.

Si enfin $\delta_i = 1$ et $\delta_{i+1} = -1$, alors $I_i = pO_{cp^{h_i}} I_{i+1}$ et $I_{i+2} = O_{cp^{h_{i+2}} I_{i+1}}$, mais $h_i = h_{i+1} - 1 = h_{i+2}$, donc $I_i = pI_{i+2}$ et I_{i+2}/I_i est un sous-quotient *non* cyclique de I_n/I_0 : contradiction.

Il en résulte que $i \mapsto \delta_i$ est croissante.

5) Comme $I_{i_0} \subset_{p^n} I_{i_r}$ sont deux idéaux propres pour O_c, $I_{i_0} I_{i_r}^{-1} = L \subset_{p^r} O_c$: cela se voit par exemple en localisant. Donc $I_{i_0} = LI_{i_r}$, pour un idéal propre L de O_c tel que $L \subset_{p^r} O_c$. Le résultat découle alors des calculs de la proposition 1.3.2.

6) Supposons que l'arête $([I_i] \to [I_{i+1}])$ soit l'inverse de $([I_{i-1}] \to [I_i])$, c'est-à-dire que :

$$[I_{i-1} \subset I_i] = [pI_{i+1} \subset I_i].$$

Il existe donc $\lambda \in K^*$ tel que $(I_{i-1} \subset I_i) = (pI_{i+1} \subset I_i)\lambda$, d'où $\lambda \in O^*_{cp^{h_i}}$. Si $O^*_{cp^{h_i}} = \{\pm 1\}$, cela implique évidemment que $I_{i-1} = pI_{i+1}$, ce qui n'est pas possible puisque I_{i+1}/I_{i-1} est cyclique. Sinon, $cp^{h_i} = 1$ donc $c = 1$, $h_i = 0$ et

$d_K = -3$ ou -4, et $I_{i-1} = p\lambda I_{i+1}$ donc I_{i-1} et I_{i+1} ont le même conducteur 1 ou p. Si ce conducteur est 1, $\delta_{i-1} = \delta_i = 0$ donc p est décomposé, et $I_{i-1} = P^2 I_{i+1}$ pour un idéal premier P de O_K sur p. Mais alors $P^2 = p\lambda O_K = pO_k$, contradiction. Donc le conducteur est p. $\square$

2.4 Les cycles

Soit $x = [I] \in \mathcal{E}$, et écrivons $c(x) = cp^h$ pour un entier $c \geq 1$ premier à p. La classe d'équivalence de $O_c I$ est alors uniquement déterminée par la classe d'équivalence de I, et l'on pose : $\mathrm{ecr}(x) = [O_c I] \in \mathcal{E}$. Le chemin de réseaux

$$I \subset_p O_{cp^{h-1}} I \subset_p O_{cp^{h-2}} I \subset_p \cdots \subset_p O_{cp} I \subset_p O_c I$$

induit un chemin de longueur h de x vers $\mathrm{ecr}(x)$, qui est sans aller-retour, et uniquement déterminé par la classe d'équivalence de x. On note

$$\mathrm{desc}(x) : x \longrightarrow \mathrm{ecr}(x)$$

ce chemin, et

$$\mathrm{mont}(x) : \mathrm{ecr}(x) \longrightarrow x$$

le chemin inverse.

On appelle *cycles* les chemins (non triviaux) de x vers x. On dit d'un cycle $x = x_0 \to x_1 \to \cdots \to x_{n-1} \to x_n = x$ qu'il est *minimal* s'il est de longueur minimale, qu'il est *primaire* s'il ne contient pas de sous-cycle $x_i \to x_{i+1} \to \cdots \to x_j = x_i$. En particulier, un cycle minimal ou primaire est sans aller-retour.

Proposition 2.4.1

1. *Tout cycle $C : x \longrightarrow x$ sans aller-retour se factorise uniquement en*

$$x \xrightarrow{\mathrm{desc}(x)} \mathrm{ecr}(x) \xrightarrow{C_0^r} \mathrm{ecr}(x) \xrightarrow{\mathrm{mont}(x)} x,$$

où C_0 est un cycle primaire et $r \geq 1$. De plus, on a alors :

   (a) *C est un cycle minimal si et seulement si $r = 1$.*

   (b) *C est un cycle primaire si et seulement si $C = C_0$ (et en particulier, $h = 0$).*

2. *Enfin :*

   (a) *Si p est inerte, il n'y a pas de cycle.*

   (b) *Si p est ramifié, il n'y a qu'un cycle sans aller-retour C, il est minimal ($r = 1$), et C_0 est de longueur 1.*

   (c) *Si p est décomposé, il y a une infinité de cycles C. Exactement deux d'entre eux sont minimaux.*

Preuve: Ecrivons $C = (x = x_0 \to x_1 \to \cdots \to x_{n-1} \to x_n = x)$, $c(x_i) = cp^{h_i}$, $\delta_i = h_{i+1} - h_i$. La fonction $i \mapsto h_i$ est convexe et $\delta_i \in \{-1, 0, 1\}$ par la proposition 2.3.2. Comme $h_0 = h_n = h$, il existe un plus petit indice i_0 et un plus grand indice i_1 tel que $h_0 = h_{i_0} = h_{i_1}$ soit minimal. On a alors : $\delta_j = -1$ si $j < i_0$, $\delta_j = 0$ si $i_0 \leq j < i_1$, et $\delta_j = 1$ si $j \geq i_1$. Si $x = [I]$, on a donc : $x_{i_0} = [O_{cp^{h_0}} I]$ et $x_{i_1} = [p^{h-h_0} O_{cp^{h_0}} I]$, donc $x_{i_0} = x_{i_1}$.

On sait que δ_i ne peut être nul que si $h_i = h_{i+1} = 0$. En particulier, si $h \neq 0$, $\delta_0 = -1$ et $\delta_{n-1} = +1$, donc $0 < i_0 \leq i_1 < n$. Si $i_0 = i_1$, on a alors : $x_{i_0-1} = [O_{cp^{h_0+1}} I]$ et $x_{i_0+1} = x_{i_1+1} = [p^{h-h_0-1} O_{cp^{h_0+1}} I]$, de sorte que par le corollaire 2.2.2, $x_{i_0-1} \to x_{i_0} \to x_{i_0+1}$ est un aller retour, contradiction. On a donc finalement : $0 < i_0 < i_1 < n$. En particulier, $\delta_{i_0} = 0$, donc $h_0 = 0$, $x_{i_0} = x_{i_1} = \mathrm{ecr}(x)$ et C se factorise déjà en :

$$x \overset{\mathrm{desc}(x)}{\longrightarrow} \mathrm{ecr}(x) = x_{i_0} \overset{C'}{\longrightarrow} x_{i_1} = \mathrm{ecr}(x) \overset{\mathrm{mont}(x)}{\longrightarrow} x,$$

où C' est un cycle non trivial sans aller-retour.

La proposition 2.3.2 donne alors les résultats suivants : si p est inerte, C' ne peut pas exister ; si p est ramifié, C' est de longueur 1. Si p est décomposé, $pO_c = P\overline{P}$ et $x_{i_1} = [J]$, $C' : x_{i_0} \longrightarrow x_{i_1}$ se relève en $P^{i_1-i_0} J \subset J$ ou en $\overline{P}^{i_1-i_0} J \subset J$. Dans les deux cas, comme $x_{i_0} = x_{i_1}$, $P^{i_1-i_0}$ est *principal*, donc $i_1 - i_0$ divise l'ordre $\mathrm{ord}([P])$ de $[P] \in \mathrm{Pic}(O_c)$. On pose $i_1 - i_0 = r \times \mathrm{ord}([P])$, et on prend pour C_0 le cycle évident, de sorte que $C_0^r = C'$.

Le reste de la proposition est plus ou moins évident. Le fait que, dans le cas où p est décomposé, les deux cycles primaires possibles soient distincts résulte du corollaire 2.2.2. □

2.5 Orientations

Fixons un idéal premier P de O_K sur p : si p est inerte ou ramifié, il n'y a évidemment aucun choix à faire, tandis que si p est décomposé, il y a deux choix possibles pour p. Pour tout entier c premier à p, posons $P_c = P \cap O_c$: c'est alors un idéal propre de O_c sur P. Ceci va nous permettre de définir une *orientation* sur l'ensemble des arêtes de $\mathcal{E}$, c'est à dire une application :

$$\mathrm{or} : \mathrm{Arêtes}(\mathcal{E}) \to \{\pm 1\}.$$

On procède de la manière suivante. Soit $x_0 \to x_1$ une arête de $\mathcal{E}$, et $I \subset_p J$ un relèvement de cette arête.

- Si x_0 et x_1 n'ont pas le même conducteur, on pose $\mathrm{or}(x_0 \to x_1) = 1$ si $c(x_1) < c(x_0)$, -1 sinon.
- Si x_0 et x_1 ont le même conducteur c, alors c est premier à p et $I = P_c J$ ou $\overline{P}_c J$: on pose $\mathrm{or}(x_0 \to x_1) = 1$ si $I = P_c J$, et -1 sinon.

Notons que ce second cas ne peut se produire que lorsque p est ramifié ou décomposé dans K. De plus, si p est ramifié, $P_c = \overline{P}_c$. Dans ce cas, on a donc $\mathrm{or}(x_0 \to x_1) = 1$, mais également $\mathrm{or}(i(x_0 \to x_1)) = 1$. C'est d'ailleurs le seul cas où une arête et son arête opposée ont la même orientation. Compte-tenu du corollaire 2.2.2 :

Proposition 2.5.1 *Pour tout $x \in \mathcal{E}$, il y a au plus une arête $x \to y$ d'origine x orienté positivement ($or(x \to y) = 1$). Il n'y en a pas si et seulement si p est inerte et $c(x)$ premier à p.*

2.6 Les composantes connexes

Proposition 2.6.1 *Pour tout entier c premier à p, soit $Fr(c)$ le sous-groupe de $Pic(O_c)$ engendré par un idéal premier de O_c sur p. Pour tout $x \in \mathcal{E}$, soit $bc(x) = c(desc(x))$, de sorte que $c(x) = bc(x)p^n$ pour un certain n, et $bc(x)$ est premier à p. Alors, pour tout couple $x, y \in \mathcal{E}$, x et y sont dans la même composante connexe du graphe $\mathcal{E}$ si, et seulement si :*

$$bc(x) = bc(y) \quad et \quad desc(x) \equiv desc(y) \ mod \ Fr(bc(x)).$$

Preuve: La condition est clairement suffisante. Elle est nécessaire d'après la proposition 2.3.2. $\square$

On dit de $\mathrm{bc}(x)$ que c'est le *conducteur de base* de x, ou de la composante connexe de x.

2.7 Demi-droites, directions et interprétation galoisienne

Une *demi-droite* dans $\mathcal{E}$ est une séquence infinie sans aller-retour de sommets adjacents : $x_0 \to x_1 \to x_2 \to \cdots \to x_n \to \cdots$. Tous les sommets d'une même demi-droite sont inclus dans une même composante connexe, et on dit du conducteur de base de celle-ci que c'est le *conducteur de base* de la demi-droite.

Proposition 2.7.1 *Soit $x_0 \to x_1 \to x_2 \to \cdots \to x_n \to \cdots$ une demi-droite, et posons $c(x_i) = cp^{h_i}$, avec c premier à p. Alors :*

1. *La suite $i \mapsto h_i$ est soit stationnaire égale à 0, soit affine de pente 1 à partir d'un certain rang.*
2. *Le premier cas ne peut se produire que si p est décomposé dans K ; $(x_i)_{i \geq 0}$ est alors cyclique à partir de la première valeur de i pour laquelle $h_i = 0$.*

Preuve: Cela résulte de la proposition 2.3.2. $\square$

Dans le deuxième cas, on dit que la demi-droite est *non bornée*. Un exemple en est donné par la suite :

$$[O_K] \to [O_p] \to [O_{p^2}] \to \cdots \to [O_{p^n}] \to \cdots$$

Plus généralement, si $a \subset O_K$ est un sous-réseau d'indice premier à p, posons $a_i = a \cap O_{p^i}$, de sorte que l'on a un diagramme :

$$\begin{array}{ccc} a & \subset & O_K \\ \cup & & \cup \\ a_i & \subset & O_{p^i} \end{array}$$

et $c(a_i) = p^i c(a)$ d'après la proposition 1.5.2. On note $D(a)$ la demi-droite ainsi définie, et on dit d'une telle demi-droite qu'elle est *rationnelle.*

Une *direction* est une classe d'équivalence de demi-droites pour la relation d'équivalence : $(x_i) \sim (x'_i) \Leftrightarrow$ il existe une constante i_0 telle que $x_i = x_{i+i_0}$ pour tout $i \gg 0$. Une *direction infinie* est la classe d'équivalence d'une demi-droite infinie. Une direction *rationnelle* est de même la calsse d'équivalence d'une demi-droite rationnel. D'après la proposition précédante : deux demi-droites infinies sont équivalentes si et seulement si elles ont le même support, à un nombre fini de points près. Chaque direction infinie contient une unique demi-droite telle que $h_i = i$, et deux demi-droites équivalentes sont évidemment dans la même composante connexe de $\mathcal{E}$: on dit du conducteur de base de cette composante connexe que c'est le *conducteur de base* de la direction.

Proposition 2.7.2 *Soit c un entier premier à p. Les directions infinies de conducteur de base c sont en bijection avec les éléments de* $\mathrm{Gal}(K[cp^\infty]/K)$. *Dans cette bijection, les directions rationnelles de conducteur de base c ont pour image un sous-groupe* $\mathrm{Gal}(K[cp^\infty]/K)^{\mathrm{rat}}$, *qui est dénombrable et dense dans* $\mathrm{Gal}(K[cp^\infty]/K)$. *Ce sous-groupe est précisément*

$$\mathrm{Gal}(K[cp^\infty]/K)^{\mathrm{rat}} = [K[cp^\infty]/K, \widehat{K}^{(p)*}],$$

où $\widehat{K}^{(p)*}$ est le sous-groupe de $\widehat{K}^*$ formé des éléments dont la p-composante est triviale.

Preuve: Se donner une direction infinie revient, d'après ce qui précède, à se donner pour tout entier $i \geq 0$ un élément x_i tel que $c(x_i) = cp^i$, de telle sorte que si $x_i = [I]$, alors $x_{i-1} = [O_{cp^{i-1}} I]$. Autrement dit, il revient au même de se donner un élément de la limite projective des groupes $\mathrm{Pic}(O_{cp^i})$, c'est-à-dire un élément de $\mathrm{Gal}(K[cp^\infty]/K)$. Si $\hat{\lambda} \in \widehat{K}^*$, la droite correspondant à $\sigma = [K[cp^\infty]/K, \hat{\lambda}] \in \mathrm{Gal}(K[cp^\infty]/K)$ est donnée par :

$$D(\sigma) = \Big([O_c \hat{\lambda}] \to [O_{cp} \hat{\lambda}] \to [O_{cp^2} \hat{\lambda}] \to \cdots \to [O_{cp^n} \hat{\lambda}] \to \cdots \Big).$$

Si $a \subset O_K$ est un sous-réseau d'indice premier à p et de conducteur c, il existe $\hat{\lambda} \in \widehat{K}^{(p)*}$ tel que $a = O_c \hat{\lambda}$. On a alors, pour tout $i \geq 0$, $a_i = a \cap O_{p^i} = O_{cp^i} \hat{\lambda}$: on vérifie en effet que les localisés des deux termes sont égaux. Inversement, si $\hat{\lambda} \in \widehat{K}^{(p)*}$, il existe un entier n premier à p tel que $a = O_c \hat{\lambda} n \subset O_K$ soit d'indice premier à p, et alors pour tout $i \geq 0$, $a_i = a \cap O_{p^i} = O_{cp^i} \hat{\lambda} n$. Ainsi, les droites rationnelles correspondent exactement aux éléments de $\mathrm{Gal}(K[cp^\infty]/K)^{\mathrm{rat}}$.

L'ensemble des sous-réseaux d'indice premier à p de O_K et de conducteur c étant dénombrable, $\mathrm{Gal}(K[cp^\infty]/K)^{\mathrm{rat}}$ est dénombrable. Enfin, il résulte aisément de la proposition 1.7.1 que pour tout $i \geq 0$, l'application

$$\mathrm{Gal}(K[cp^\infty]/K)^{\mathrm{rat}} \to \mathrm{Gal}(K[cp^i]/K)$$

est surjective. Le sous-groupe $\mathrm{Gal}(K[cp^\infty]/K)^{\mathrm{rat}}$ de $\mathrm{Gal}(K[cp^\infty]/K)$ est donc dense. $\square$

2.8 Sous-graphes

On se donne un ensemble *fini* S de nombres premiers ne contenant pas p, et un réseau I_0 de K de conducteur c_0. Soit $\mathcal{R}_S^0$ l'ensemble des réseaux I de K tels que $I_\ell = (I_0)_\ell$ pour tout $\ell \in S$, $\mathbb{Q}_S^*$ l'ensemble des rationnels premiers à S, K_S l'ensemble des éléments λ de K tels que $\lambda \in (O_{c_0})_\ell^*$ pour tout $\ell \in S$. On définit alors :

$$\begin{array}{rcl} \mathcal{T}_S^0 & = & \mathcal{R}_S^0/\mathbb{Q}_S^*, \\ \mathcal{E}_S^0 & = & \mathcal{R}_S^0/K_S^*, \\ \text{Arêtes}(\mathcal{T}_S^0) & = & \{p-\text{inclusions de } \mathcal{R}_S^0\}/\mathbb{Q}_S^*, \\ \text{Arêtes}(\mathcal{E}_S^0) & = & \{p-\text{inclusions de } \mathcal{R}_S^0\}/K_S^*. \end{array}$$

Comme dans la section 2.1, ces ensembles définissent des graphes.

Proposition 2.8.1 *Les applications naturelles :*

$$\begin{array}{rcl} \mathcal{E}_S^0 & \to & \mathcal{E}, \\ \mathit{Arêtes}(\mathcal{E}_S^0) & \to & \mathit{Arêtes}(\mathcal{E}), \end{array}$$

sont injectives, et identifient le graphe $\mathcal{E}_S^0$ au sous-graphe de $\mathcal{E}$ qui est la réunion des composantes connexes dont le conducteur de base c vérifie $v_\ell(c) = v_\ell(c_0)$ pour tout $\ell \in S$.

Preuve: 1) Soient $I, I' \in \mathcal{R}_S^0$, et supposons qu'il existe $\lambda \in K^*$ tel que $I = I'\lambda$. Alors pour tout $\ell \in S$, $I_\ell = (I'_\ell)\lambda$ donc $(I_0)_\ell = (I_0)_\ell\lambda$ et $\lambda \in (O_{c_0})_\ell^*$. De même, soient $I \subset_p J$ et $I' \subset_p J'$ des p-inclusions de $\mathcal{R}_S^0$, et supposons qu'il existe λ tel que $(I \subset_p J) = (I' \subset_p J')\lambda$. Alors à fortiori $I = I'\lambda$, donc $\lambda \in (O_{c_0})_\ell^*$ pour tout $\ell \in S$.

2) Soit $x \to y$ une arête de $\mathcal{E}$, telle que $v_\ell(c(x)) = v_\ell(c_0)$, et soit $I \subset_p J$ un relèvement de cette arête. D'après la proposition 1.7.1, il existe $\lambda \in K^*$ tel que $J\lambda$ soit un idéal $O_{c(J)}$-propre *premier* à S. Il est alors clair que $I\lambda \subset_p J\lambda$ est une p-inclusion de $\mathcal{R}_S^0$. $\square$

Soit $\widehat{\mathbb{Z}}^{(S)}$ le complété profini de $\mathbb{Z}$ en dehors de S. Si M est un groupe abélien, on pose $\widehat{M}^{(S)} = M \otimes \widehat{\mathbb{Z}}^{(S)}$. En particulier, $\widehat{K}^{(S)} = K \otimes \widehat{\mathbb{Z}}_S$ est le produit restreint des K_q relativement aux $(I_0)_q$, q parcourant les nombres premiers n'appartenant pas à S. Un *réseau de* $\widehat{K}^{(S)}$ est un sous-$\widehat{\mathbb{Z}}^{(S)}$ module M de $\widehat{K}^{(S)}$ tel qu'il existe un entier n pour lequel nM soit d'indice fini dans $\widehat{I_0}^{(S)} \subset \widehat{\mathbb{Z}}^{(S)}$. On a alors :

Lemme 2.8.2 *L'application*

$$\begin{array}{rcl} \mathcal{R}_S^0 & \to & \{\text{réseaux } \textit{de } \widehat{K}^{(S)}\} \\ I & \mapsto & \widehat{I}^{(S)} \end{array}$$

est bijective.

Preuve: On voit aisément que l'ensemble des réseaux de $\widehat{K}^{(S)}$ est exactement l'ensemble des sous-$\widehat{\mathbb{Z}}^{(S)}$ modules qui se décomposent en

$$M = \prod_{q \notin S} M_q,$$

où chaque M_q est un réseau complet de K_q, et presque tous les M_q sont égaux à $(I_0)_q$. La conclusion résulte alors de [4, §4 n°3]. $\square$

2.9 Application : structures de niveaux "distinguées"

Soit $N \geq 1$ un entier. A tout réseau a de K, on peut associer le tore complexe $\mathbb{C}/a$. On se propose ici de construire, dans la plupart de ces tores, un sous-groupe cyclique d'ordre N. Il revient au même de construire un réseau a_N de K tel que $a \subset_N a_N$. Ce chapitre nous indique la méthode.

Supposons en effet d'abord que N soit une puissance d'un nombre premier p, disons $N = p^r$, et soit a un réseau de K de conducteur $c(a) = cp^n$, avec c premier à p. Si $n \geq r$, on peut prendre $a_N = aO_{cp^{n-r}}$. Sinon, on peut déjà considérer $a \subset_{p^n} O_c a$, et il reste à construire un réseau a_N tel que $O_c a \subset_{p^{n-r}} a_N$ et a_N/a est cyclique. Si p est *inerte* dans K, il n'y a aucune manière "canonique" pour faire cela. Si p est *ramifié*, il y a une manière canonique si $n - r = 1$: on prend $a_N = P^{-1}O_c a$, où P est l'unique idéal propre de O_c sur p. Si enfin p est *décomposé* dans K, il y a deux manières canoniques : on prend $a_N = P^{r-n}O_c a$, où P est l'un des *deux* idéaux propres de O_c sur p. Dans ce cas, le choix de P peut être fait de manière uniforme, indépendamment de a : on choisit l'un des deux idéaux premiers de O_K sur p, disons P, puis pour tout entier c premier à p, on pose $P_c = P \cap O_c$.

En d'autres termes, le choix de P (lorsque p est décomposé) nous permet de définir une orientation sur le graphe $\mathcal{E}$, et on définit a_N à partir de a en suivant les arêtes orientées positivement à partir de la classe $[a]$ (cf. proposition 2.5.1). Si p est inerte, il se peut que l'on arrive sur un sommet d'où ne part aucune arête : la condition $n \geq r$ est là pour exclure ce cas. Si p est ramifié, il se peut qu'en suivant les arêtes orientées positivement, on construise une isogénie non cyclique : la condition $n \geq r - 1$ est là pour exclure ce cas.

Dans le cas d'un entier N plus général, on procède exactement de même, à ceci près qu'il faut traiter chaque facteur premier de N séparément. On commence donc par choisir, pour tout nombre premier $q \mid N$, un idéal premier Q de O_K sur q : on effectue véritablement un choix que lorsque q est décomposé dans K. Pour tout entier c, on pose alors $Q_c = Q \cap O_c$: c'est un idéal premier de O_c sur q, qui est propre si $q \nmid c$. On dit que c'est l'idéal premier "distingué" de O_c sur q.

On définit ensuite un entier $c_{\min}(N)$ divisant N, qui joue le rôle de conducteur minimal pour lequel il existe des structures de niveaux N "distinguées". Précisément, pour tout nombre premier q, la q-valuation de $c_{\min}(N)$ est donnée par :

$$v_q(c_{\min}(N)) = \begin{cases} v_q(N) & \text{si } q \text{ est inerte} \\ v_q(N) - 1 & \text{si } q \text{ est ramifié} \\ 0 & \text{si } q \text{ est décomposé} \end{cases}$$

Pour tout entier c *divisible par* $c_{\min}(N)$, on définit de même un entier $c_N(c)$ *divisant* c par :

$$v_q(c_N(c)) = \begin{cases} v_q(c) - v_q(N) & \text{si } q \mid N \text{ est inerte} \\ \max(v_q(c) - v_q(N), 0) & \text{si } q \mid N \text{ est ramifié} \\ \max(v_q(c) - v_q(N), 0) & \text{si } q \mid N \text{ est décomposé} \\ \max(v_q(c) - v_q(N), 0) & \text{si } q \nmid N \end{cases}$$

On a donc

$$c_{\min}(N) \mid \frac{c}{c_N(c)} \mid N.$$

Enfin, pour $q \mid N$, on pose

$$\delta_q(c) = v_q(N) - v_q(c) + v_q(c_N(c)).$$

de sorte que $\delta_q(c) \geq 0$, $\delta_q(c) = 0$ si $q \mid c_N(c)$ ou si q est inerte, et $\delta_q(c) = 0$ ou 1 si q est ramifié.

L'idéal *distingué* de O_c est alors

$$I_c = O_{c_N(c)} \prod_{q \mid N} Q_{c_N(c)}^{-\delta_q(c)}.$$

Cet idéal est propre pour $O_{c_N(c)}$, et $O_c \subset_N I_c$. Remarquons que $O_c \subset_N I_c$ implique que $O_c \subset_N \overline{I_c}$, donc $N\overline{I_c} \subset_N O_c$.

Pour tout réseau a de K tel que $c_{\min}(N) \mid c(a)$, on pose :

$$\begin{aligned} c_N(a) &= c_N(c(a)), \\ \delta_q(a) &= \delta_q(c(a)), \\ a_N &= I_{c(a)} a, \end{aligned}$$

de sorte que

$$a \subset_N a_N \quad \text{et} \quad c(a_N) = c_N(a).$$

Proposition 2.9.1 *Pour tout réseau a de K tel que $c_{min}(N) \mid c(a)$,*

$$\ker\left(\mathbb{C}/a \to \mathbb{C}/a_N\right) = \left\{x \in \mathbb{C}/a \mid \alpha x = 0 \quad \forall \alpha \in N\overline{I_{c(a)}} \subset O_{c(a)}\right\}.$$

Preuve: 1) On a $\ker(\mathbb{C}/a \to \mathbb{C}/a_N) = a_N/a$.

Posons $c = c(a)$ et $c' = c_N(a)$. Comme $a_N = aI_c$, $N\overline{I_c}a_N = NI_c\overline{I_c}a$. Mais

$$\begin{aligned} I_c\overline{I_c} &= \prod_{q|N_rN_d} Q_{c'}^{-\delta_q(c)}\overline{Q}_{c'}^{-\delta_q(c)} \\ &= \prod_{q|N_rN_d} q^{-\delta_q(c)}O_{c'} \\ &= \frac{c}{Nc'}O_{c'}, \end{aligned}$$

donc

$$N\overline{I_c}a_N = \frac{c}{c'}O_{c'}a \subset_{c/c'} a.$$

Ainsi, $N\overline{I_c} \cdot (a_N/a) = 0$.

2) Inversement, supposons que $N\overline{I_c}x \subset a$ pour $x \in \mathbb{C}$. Si

$$a/N\overline{I_c}x \approx \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/nm\mathbb{Z},$$

on a donc $n^{-1}N\overline{I_c}x \subset_m a$, d'où $a \subset_m m^{-1}n^{-1}N\overline{I_c}x$ et à fortiori,

$$O_{c'}a \subset_{m'} m^{-1}n^{-1}N\overline{I_c}x$$

avec $m' = \frac{mc'}{c}$. Donc $m'm^{-1}n^{-1}N\overline{I_c}x \subset_{m'} O_{c'}a$, c'est-à-dire :

$$N\overline{I_c}x \subset_{m'} n\frac{c}{c'}O_{c'}a \subset \frac{c}{c'}O_{c'}a.$$

Multipliant par I_c, on obtient alors

$$NI_c\overline{I_c}x = \frac{c}{c'}O_{c'}x \subset \frac{c}{c'}O_{c'}aI_c = \frac{c}{c'}a_N.$$

Donc $x \in a_N$. $\square$

Si $a = a'\lambda$, avec $c_{\min}(a) \mid c(a) = c$, alors $aI_c = a'I_c\lambda$, c'est-à-dire : $(a \subset_N a_N) = (a' \subset_N a'_N)\lambda$. Il en résulte que le point complexe

$$H(a) = [\mathbb{C}/a \to \mathbb{C}/a_N] \in X_0(N)(\mathbb{C})$$

ne dépend que de la classe d'équivalence de a dans $\mathcal{E}$. Si $\mathcal{E}_N$ est l'ensemble des sommets de $\mathcal{E}$ dont le conducteur est divisible par $c_{\min}(N)$, on a donc défini une application :

$$H : \mathcal{E}_N \to X_0(N)(\mathbb{C}).$$

Deuxième partie

Points CM

Chapitre 3

Courbes elliptiques à multiplication complexe

3.1 Définition et normalisation

On dit d'une courbe elliptique E sur un corps F qu'elle a multiplication complexe par K si

$$\mathrm{End}^0_{\overline{F}}(E) \approx K.$$

Il y a alors deux tels isomorphismes. Lorsque $K \subset \overline{F}$, par exemple si $F \subset \mathbb{C}$, on *choisit* comme isomorphisme celui qui est donné par l'action de $\mathrm{End}^0_{\overline{F}}(E)$ sur le $\overline{F}$-espace vectoriel de dimension un $\mathrm{Lie}(E)(\overline{F})$. L'anneau $\mathrm{End}_{\overline{F}}(E)$ est alors un ordre O_c dans K, et l'on dit aussi que E a multiplication complexe par O_c, et que c est le conducteur de E. Avec cette normalisation, on a :

$$\begin{aligned} K \subset F \quad &\Leftrightarrow \quad \mathrm{End}^0_F(E) = \mathrm{End}^0_{\overline{F}}(E) \\ &\Leftrightarrow \quad \mathrm{End}_F(E) = \mathrm{End}_{\overline{F}}(E). \end{aligned}$$

On dit dans ce cas que $E_{/F}$ a multiplication complexe par K *sur* F.

Cette normalisation implique notamment que pour toute isogénie $f : E_1 \to E_2$ entre deux courbes elliptiques à mulltiplication complexe par respectivement O_{c_1} et O_{c_2} sur un corps $F \subset \mathbb{C}$, f commute à l'action des éléments de $O_{c_1} \cap O_{c_2}$ sur E_1 et E_2 : on dit que f est K-linéaire.

3.2 Modules de Tate, réseaux et sous-groupes finis

3.2.1 Définition

Le module de Tate d'une variété abélienne A sur un corps F est

$$\hat{T}(A) = \prod_q T_q(A) = \varprojlim A[n](\overline{F}),$$

où q parcourt l'ensemble des nombres premiers. On pose également

$$\hat{V}(A) = \hat{T}(A) \otimes \mathbb{Q}.$$

C'est le produit restreint des

$$\begin{aligned} V_q(A) &= T_q(A) \otimes \mathbb{Q} \\ &= T_q(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \end{aligned}$$

relativement aux $T_q(A)$. Tous ces modules sont d'une part munis d'une action de $\mathrm{End}_{\overline{F}}(A)$, et d'autre part d'une action $\mathrm{End}_F(A)$-linéaire de $\mathrm{Gal}(\overline{F}/F)$.

3.2.2 Réseaux et sous-groupes

Définition *Un* réseau *de $\hat{V}(A)$ est un sous-$\mathbb{Z}$-module T de $\hat{V}(A)$ tel qu'il existe un entier n pour lequel nT soit inclus dans $\hat{T}(A)$ avec un indice fini.*

Si T est un réseau, T se décompose selon les nombres premiers :

$$T = \prod_q T_q,$$

où chaque T_q est un $\mathbb{Z}_q$-réseau (complet) de $V_q(A)$.

La limite *inductive* des isomorphismes

$$n^{-1}\hat{T}(A)/\hat{T}(A) \xrightarrow{\simeq} \hat{T}(A)/n\hat{T}(A) \xrightarrow{\simeq} A[n](\overline{F})$$

est un isomorphisme $\mathrm{Gal}(\overline{F}/F)$-équivariant

$$\hat{V}(A)/\hat{T}(A) \xrightarrow{\simeq} A(\overline{F})_{\mathrm{tors}}.$$

En particulier, il réalise une bijection $\mathrm{Gal}(\overline{F}/F)$-équivariante :

$$\{\text{réseaux } T \supset \hat{T}(A) \text{ de } \hat{V}(A)\} \xrightarrow{\simeq} \{\text{sous} - \text{groupes finis de } A(\overline{F})_{\mathrm{tors}}\}$$

Si T est un réseau de $\hat{V}(A)$ contenant $\hat{T}(A)$, et X le sous-groupe correspondant à $T/\hat{T}(A)$, on a donc

$$\mathrm{Fix}(T) = \{\sigma \in \mathrm{Gal}(\overline{F}/F) \mid \sigma T = T\} = \{\sigma \in \mathrm{Gal}(\overline{F}/F) \mid \sigma X = X\} = \mathrm{Fix}(X).$$

C'est un sous-groupe ouvert de $\mathrm{Gal}(\overline{F}/F)$, et le corps $F' = \overline{F}^{\mathrm{Fix}(X)}$ est une extension finie de F. Le sous-groupe $X \subset A(\overline{F})$ descend en un sous-schéma en groupe fini et étale $X_{/F'}$ de $A_{/F'}$, et l'on peut donc définir le quotient

$$A_{/F'} \to (A_{/F'})/(X_{/F'}).$$

C'est une isogénie étale. Pour simplifier les notations, on la notera seulement :

$$A \to A/X,$$

en disant que cette isogénie est "définie" sur F'.

3.2.3 Cas des courbes elliptiques

On suppose maintenant que $A = E$ est une courbe elliptique. Si $T \supset \hat{T}(E)$ est un sous-réseau de $\hat{V}(E)$, soit $X \subset E(\overline{F})$ le sous-groupe correspondant, $f : E \to E/X$ l'isogénie naturelle, et $g : E/X \to E$ l'isogénie duale de f. Si $d = \#X$, d est donc le degré de f et g, ainsi que l'indice de $\hat{T}(E)$ dans T. De plus :

Lemme 3.2.1 *$\hat{T}(g)(\hat{T}(E/X)) = dT$ dans $\hat{V}(E)$*

Preuve: Par définition,

$$f : E_{\mathrm{tors}}(F^{\mathrm{ab}}) = \hat{V}(E)/\hat{T}(E) \to \hat{V}(E/X)/\hat{T}(E/X) = (E/X)_{\mathrm{tors}}(F^{\mathrm{ab}})$$

a pour noyau $T/\hat{T}(E) = X$, qui est d'ordre d. On a donc : $\hat{V}(f)(T) \subset \hat{T}(E/X)$, donc $\hat{V}(g)\hat{V}(f)(T) = dT \subset \hat{V}(g)(\hat{T}(E/X))$. Inversement, si $t \in \hat{T}(E/X)$, alors $d^{-1}\hat{V}(g)(t) \bmod \hat{T}(E)$ est dans le noyau de f, car

$$\hat{V}(f)(d^{-1}\hat{V}(g)(t)) = t \in \hat{T}(E/X),$$

donc $d^{-1}\hat{V}(g)(\hat{T}(E/X)) \subset T$, et $\hat{V}(g)(\hat{T}(E/X)) = \hat{T}(g)(\hat{T}(E/X)) = dT$. □

Remarque: On n'a pas fait d'hypothèse sur la caractéristique de F !

3.3 Réduction des courbes elliptiques à multiplication complexe

Soit $F \subset \mathbb{C}$ un corps de nombre, $E_{/F}$ une courbe elliptique à multiplication complexe par $O = O_c \subset K$ sur F, de sorte que $K \subset F$. On normalise l'isomorphisme $O \xrightarrow{\simeq} \mathrm{End}_F(E)$ comme expliqué en (3.1).

3.3.1 Modèle de Néron et réduction

La courbe elliptique $E_{/F}$ ayant multiplication complexe, a bonne réduction potentielle à toutes les places de F ([33, Theo 6]). Soit v une place finie de F, A_v l'anneau local correspondant, k le corps résiduel de A_v, et p sa caractéristique. Soit $\mathcal{E}_{/A_v}$ le modèle de Néron de $E_{/F_v}$, et $\widetilde{\mathcal{E}}_{/k}$ sa fibre spéciale. On suppose que $E_{/F}$ a bonne réduction en v, de sorte que $\mathcal{E}_{/A_v}$ est une courbe elliptique (relative).

L'action de O sur $E_{/F}$ s'étend par la propriété universelle du modèle de Néron en une action de O sur $\mathcal{E}_{/A_v}$, puis se restreint à la fibre spéciale en une action de O sur $\widetilde{\mathcal{E}}_{/k}$. Le morphisme $O \to \mathrm{End}_{A_v}(\mathcal{E})$ est un isomorphisme : cela résulte encore de la propriété universelle du modèle de Néron. Le morphisme $O \to \mathrm{End}_k(\widetilde{\mathcal{E}})$ est en revanche à priori seulement *injectif* : cela résulte de ce que $\mathcal{E}_{/A_v}$ étant un schéma abélien, tout morphisme trivial sur une fibre est trivial ([18, Chap 6]). Pour $\lambda \in \mathrm{End}_F(E)$, on note $\widetilde{\lambda}$ la réduction de λ.

$\mathcal{E}_{/A_v}$ étant abélienne, les éléments de $O \setminus \{0\}$ induisent sur $\mathcal{E}$ des isogénies, c'est-à-dire des morphismes plats et finis ([3, 7.3]). Leur noyau est en particulier plat sur A_v, donc de rang constant ; en particulier,

$$\forall \lambda \in O : \quad \deg(\widetilde{\lambda}) = \deg(\lambda) = \mathrm{N}_{K/\mathbb{Q}}(\lambda).$$

Soit $L = \mathrm{Lie}(\mathcal{E})(A_v)$. Pour toute A_v-algèbre B,

$$\mathrm{Lie}(\mathcal{E})(B) \simeq L \otimes_{A_v} B$$

car $\mathcal{E}_{/A_v}$ est lisse ([DG, II §4.1.8]). De plus, L est A_v-projectif de type fini ([DG, II §4.1.8 et 4.3.6]), donc libre de rang un, puisque A_v est local et $L \otimes_{A_v} F \simeq \mathrm{Lie}(E)(F)$ est de dimension un. L'action de O sur L induit donc un morphisme d'anneau $O \to A_v$, et la normalisation que l'on a imposée pour l'action de O sur la fibre générique montre alors que

$$(O \to A_v \to F) = (O \subset K \subset F)\,.$$

Autrement dit, O agit sur le A_v-module L par multiplication scalaire, via l'inclusion $O \subset K \subset F$.

Soit P l'idéal premier de O sous v, de sorte que l'action de O sur le k-espace vectoriel de dimension un $\mathrm{Lie}(\widetilde{\mathcal{E}})(k)$ se factorise par $O/P \hookrightarrow k$.

3.3.2 O-injectivité

Le comportement du schéma en O-module $\mathcal{E}_{/A_v}$ est donné par la proposition suivante (voir l'appendice pour les définitions).

Proposition 3.3.1

1. *$E_{/F}$ est O-injectif : le foncteur $M \mapsto E^M_{/F}$ est exact.*
2. *$\mathcal{E}_{/A_v}$ est O-injectif si et seulement si $p \nmid c$.*

Preuve: 1) Tout schéma en groupe sur un corps de caractéristique 0 est lisse ([23]). D'après le critère de Baer (section 10.4.2), il suffit donc de vérifier que $E(\mathbb{C})$ est un O-module injectif. La théorie analytique des courbes elliptiques à multiplication complexe montre que ce module est isomorphe à $\mathbb{C}/a$, pour un O-idéal *propre* de K. Si $(e_i)_{i\in I}$ est une K-base de $\mathbb{C}$, avec $e_{i_0} \in K$, on a donc un isomorphisme de O_c-module :

$$E(\mathbb{C}) \approx K/a \oplus K^{(I\setminus\{i_0\})}.$$

K est K-injectif (!) donc à fortiori O-injectif, et il reste à voir que K/a est O-injectif. Mais a est O-projectif, donc facteur direct d'un O-module libre O^n, et K/a est donc facteur direct d'un O-module $(K/O)^n$. Ce dernier étant O-injectif par (1.4.2), K/a l'est également.

2) Si $p \nmid c$, O est maximal (et à fortiori héréditaire) en p, donc $\mathcal{E}_{/A_v}$ est O-injectif par le corollaire 11.2.5. D'autre part, $\dim(\mathcal{E}^P_{/A_v}) = 1$ par la proposition 11.2.6, tandis que

$$\begin{aligned} \mathrm{Lie}(\mathcal{E}^P)(k) &= \mathrm{Hom}_O(P, \mathrm{Lie}(\mathcal{E})(k)) \\ &\simeq \mathrm{Hom}_{O/P}(P/P^2, k) \\ &\simeq \mathrm{Hom}_{O/P}(P/P^2, O/P) \otimes_{O/P} k. \end{aligned}$$

Si $p \mid c$, $P = pO_{c/p} \subset_p O_c$ et $O/P \simeq \mathbb{F}_p$, tandis que $P^2 = p^2 O_{c/p} = pP$ et $P/P^2 \simeq \mathbb{F}_p^2$. Dans ce cas, on a donc

$$\dim_k \mathrm{Lie}(\mathcal{E}^P)(k) = 2$$

et $\widetilde{\mathcal{E}}_{/k}$ n'est pas lisse. A fortiori, $\mathcal{E}_{/A_v}$ n'est pas O-injectif. □

Remarque: La proposition implique que si $p \nmid c$, pour tout O-module M sans-torsion de type fini, $\mathcal{E}^M_{/A_v}$ est un schéma abélien. Lorsque $p \mid c$, on peut montrer que $\mathcal{E}^M_{/A_v}$ est abélien si et seulement si M est sans facteur direct $O_{c/p}$-stable.

3.3.3 Réduction ordinaire ou supersingulière ?

Proposition 3.3.2 *$E_{/F}$ a réduction ordinaire en v $\Leftrightarrow$ p est décomposé dans O_K.*

Preuve: Si E a réduction ordinaire en v, alors pour tout entier $n \geq 1$, $\widetilde{\mathcal{E}}[p^n](\overline{k}) \approx \mathbb{Z}/p^n\mathbb{Z}$ est un O-module cyclique, donc de la forme O/I_n. En particulier, O admet des idéaux cycliques de rang p^n avec n arbitrairement grand, donc p est décomposé dans K : cela résulte de la proposition 2.3.2.

Supposons inversement que p soit décomposé dans K, et considérons $E^{O_K}_{/F}$: c'est une courbe elliptique isogène à $E_{/F}$, qui a donc également bonne réduction en v. De plus, $E_{/F}$ et $E^{O_K}_{/F}$ ont simultanément réduction ordinaire ou non ; remplaçant $E_{/F}$ par $E^{O_K}_{/F}$, on peut donc supposer que O est maximal. Soit alors n un entier tel que $\overline{P}^n$ soit principal, disons $\overline{P}^n = O_K\lambda$; comme $\lambda \notin P$, la multiplication par λ dans $\mathrm{Lie}(\mathcal{E})(A_v)$ est bijective. A fortiori, la réduction $\widetilde{\lambda}$ de l'isogénie $\lambda \in \mathrm{End}_F(E)$ induit une bijection sur $\mathrm{Lie}(\mathcal{E})(k) = \mathrm{Lie}(\widetilde{\mathcal{E}})(k)$, et $\widetilde{\lambda}$ est donc séparable (étale), et de degré p^n : il en résulte effectivement que $\widetilde{\mathcal{E}}_{/k}$ est ordinaire. □

3.3.4 Anneau d'endomorphismes et p-torsion de la réduction

Ecrivons $c = c_0 p^n$, avec c_0 premier à p, et soit P le premier de O_{c_0} sous v.

Proposition 3.3.3 (cas ordinaire) *Si p est décomposé dans K, alors :*

1. $\mathrm{End}_k(\widetilde{\mathcal{E}}) = \mathrm{End}_{\overline{k}}(\widetilde{\mathcal{E}}) = O_{c_0}$ *est maximal en p.*
2. $\widetilde{\mathcal{E}}(\overline{k})[p^s] \simeq O_{c_0}/\overline{P}^s$ *pour tout $s \geq 0$.*
3. $\mathrm{Lie}\left(\widetilde{\mathcal{E}}\right)(k) \simeq (O_{c_0}/P) \otimes k$.
4. *Si $\pi \in O_{c_0}$ est le frobenius de $\widetilde{\mathcal{E}}_{/k}$, $O_{c_0}\pi = P^{\deg(\pi)} = P^{\log_p(\#k)}$.*

Preuve: D'après [34, V 3.1], $\mathrm{End}_{\overline{k}}(\widetilde{\mathcal{E}})$ est un ordre dans un corps quadratique imaginaire. $\mathrm{End}_k(\widetilde{\mathcal{E}}) = \mathrm{End}_{\overline{k}}(\widetilde{\mathcal{E}})^{\mathrm{Gal}(\overline{k}/k)}$ en est un $\mathbb{Z}$-facteur direct, et contient O, donc $\mathrm{End}_{\overline{k}}(\widetilde{\mathcal{E}}) = \mathrm{End}_k(\widetilde{\mathcal{E}})$ est un ordre O' de K, de conducteur divisant c. Si $q \neq p$, l'action de $(O')_q$ sur le module de Tate $T_q(\widetilde{\mathcal{E}}) \simeq T_q(E)$ est $(O)_q$-linéaire, et $T_q(E)$ est $(O)_q$-libre de rang un, donc $(O')_q = (O)_q$ et finalement, $O' = O_{c_0p^m}$ pour un entier $m \leq n$.

Soit I_s l'annulateur du O'-module cyclique $\widetilde{\mathcal{E}}(\overline{k})[p^s] \approx \mathbb{Z}/p^s\mathbb{Z}$, de sorte que O'/I_s est cyclique d'ordre p^s, et l'on a une suite infinie d'idéaux de O' :

$$\cdots \subset I_{s+1} \subset_p I_s \subset_p I_{s-1} \subset_p \cdots \subset_p O_{c_0p^m}.$$

Il résulte alors de la proposition 2.3.2 (voir aussi la section 2.7) que $I_s = p^s O_{c_0p^{m-s}}$ pour $s \leq m$, puis : $I_s = p^m P^{s-m}$ pour tout $s \geq m$, ou bien $I_s = p^m \overline{P}^{s-m}$ pour tout $s \geq m$.

Soit π le Frobenius de $\widetilde{\mathcal{E}}_{/k}$, π' son dual, et $\#k = p^r$. π et π' appartiennent donc à O', sont de degré p^r, π est purement inséparable et π' est séparable (étale). En particulier, $\ker(\pi'^i)(\overline{k}) = \widetilde{\mathcal{E}}(\overline{k})[p^{ri}]$ pour tout $i \geq 0$, de sorte que $O'\pi'^i \subset I_{ri}$. Inversement, tout élément de I_{ri} est nul sur le noyau de π'^i, donc divisible par π'^i dans O' : ainsi, $O'\pi'^i = I_{ri}$. Il en résulte que $m = 0$, $O' = O_{c_0}$, et $I_s = P^s$ pour tout s, ou bien $I_s = \overline{P}^s$ pour tout s.

Or π' est non trivial dans $\mathrm{Lie}(\widetilde{\mathcal{E}})(k)$, et l'action de O_{c_0} sur ce k-espace vectoriel se factorise par O_{c_0}/P, donc $\pi' \notin P$, et $I_{ri} = O_{c_0}\pi^i$ est donc égal à $\overline{P}^{ri}$, d'où $I_s = \overline{P}^s$ pour tout s, et $\widetilde{\mathcal{E}}(\overline{k})[p^s] \approx O_{c_0}/\overline{P}^s$. Comme $O_{c_0}\pi\pi' = O_{c_0}p^r = P^r\overline{P}^r$, $O_{c_0}\pi = P^r$. □

Proposition 3.3.4 (cas super-singulier) *Si p est inerte ou ramifié dans K, alors :*

1. $\mathrm{End}_{\overline{k}}(\widetilde{\mathcal{E}})$ *est un ordre maximal dans le corps de quaternions ramifié en p et ∞.*
2. $\mathrm{End}_{\overline{k}}(\widetilde{\mathcal{E}}) \cap K = O_{c_0}$.
3. *Si p est inerte et $O_{c_0}^* = \{\pm 1\}$, alors* $\mathrm{End}_k(\widetilde{\mathcal{E}}) = \mathrm{End}_{\overline{k}}(\widetilde{\mathcal{E}})$
4. *Si p est ramifié, $[k : \mathbb{F}_p]$ est pair et $O_{c_0}^* = \{\pm 1\}$, alors* $\mathrm{End}_k(\widetilde{\mathcal{E}}) = \mathrm{End}_{\overline{k}}(\widetilde{\mathcal{E}})$. *C'est le cas si P n'est pas principal.*

Preuve: Soit $R = \mathrm{End}_{\overline{k}}(\widetilde{\mathcal{E}})$, $\#k = p^r$. D'après [5], R est un ordre *maximal* dans $B = \mathrm{End}^0_{\overline{k}}(\widetilde{\mathcal{E}})$, un corps de quaternions. Ce corps est ramifié en un nombre pair non nul de places, et admet des représentations de dimension 2 sur $\mathbb{Q}_\ell$, pour tout ℓ premier à p, à savoir les modules de Tate $\hat{V}_\ell(\widetilde{\mathcal{E}})$. Il est donc non ramifié en dehors de p et de ∞, et par conséquent, ramifié en p et ∞. D'où 1).

Soit $O' = \mathrm{End}_k(\widetilde{\mathcal{E}}) = (\mathrm{End}_{\overline{k}}(\widetilde{\mathcal{E}}))^{\mathrm{Gal}(\overline{k}/k)}$; c'est un $\mathbb{Z}$-facteur direct de R contenant O, et B contient K. On a donc : $O' \cap K = R \cap K$. Cette intersection contient O, est un ordre de K, et agit (via l'action de R) sur les $(O)_q$-modules libres de rang un $T_q(\widetilde{\mathcal{E}}) \approx T_q(E)$. Comme dans le cas ordinaire, on en déduit que $O' \cap K = R \cap K$ est un ordre de conducteur $c_0 p^m$, pour un certain entier $m \leq n$. Mais $R \cap K$ est aussi un ordre *maximalement plongé dans* R par définition, et il en résulte que $m = 0$ [39, p. 43].

Soit enfin π le Frobenius géométrique de $\widetilde{\mathcal{E}}_{/k}$. L'action du Frobenius galoisien $\sigma \in \mathrm{Gal}(\overline{k}/k)$ sur $\widetilde{\mathcal{E}}_{/k}$ est précisément donnée par π, de sorte que O' *est le commutant* de π dans R. En particulier, π commute à $O \subset O'$, donc π appartient à K, puisque K est un sous-corps commutatif maximal de B. Finalement, $\pi \in R \cap K = O_{c_0}$. π étant de degré p^r,

- Si p est inerte dans K, r est pair et $O_{c_0}\pi = O_{c_0}p^{r/2}$, donc $\pi = up^{r/2}$ pour un $u \in O_{c_0}^*$. Donc si $O_{c_0} = \{\pm 1\}$, $\pi \in \mathbb{Z}$ et $O' = R$.
- Si p est ramifié dans K, alors $O_{c_0}\pi = P^r$. Si r est pair, on obtient à nouveau $\pi = up^r$ avec $u \in O_{c_0}^*$, donc $O' = R$ si $O_{c_0}^* = \{\pm 1\}$
- Si P n'est pas principal, alors r est pair et $d_K \neq -3, -4$, donc $O_{c_0}^* = \pm 1$.

$\square$

3.3.5 Points de torsion

Soit $F_v^{\mathrm{ab/nr}}$ l'extension maximale abélienne non ramifiée en v, $v^{\mathrm{ab/nr}}$ une place de $F^{\mathrm{ab/nr}}$ sur v, $A_v^{\mathrm{ab/nr}} \subset F_v^{\mathrm{ab/nr}}$ l'anneau de valuation correspondant. Son corps résiduel est une clôture algébrique $\overline{k}$ de k.

Proposition 3.3.5 *Pour tout entier n premier à p, on a des isomorphismes :*

$$E[n](F^{ab/nr}) \xleftarrow{\simeq} \mathcal{E}[n](A_v^{ab/nr}) \xrightarrow{\simeq} \widetilde{\mathcal{E}}[n](\overline{k}).$$

Preuve: Commençons par étendre $v^{\mathrm{ab/nr}}$ en une place $\overline{v}$ de $\overline{F}$, soit $F_v^{\mathrm{nr}} \subset \overline{F}$ l'extension maximale non ramifiée en $\overline{v}$, de sorte que $F_v^{\mathrm{ab/nr}} \subset F_v^{\mathrm{nr}}$ est la sous-extension abélienne maximale de F_v^{nr}. D'après [3, 2.3.11], l'anneau local A_v^{nr} de $v^{\mathrm{nr}} = v \mid_{F_v^{\mathrm{nr}}}$ est un hensélisé strict de A_v, et l'inclusion $A_v^{\mathrm{ab/nr}} \subset A_v^{\mathrm{nr}}$ induit donc un isomorphisme sur les corps résiduels. D'autre part, d'après [3, 7.1], le morphisme suivant est bijectif :

$$\mathcal{E}(A_v^{\mathrm{nr}}) \xrightarrow{\simeq} E(F_v^{\mathrm{nr}}).$$

A fortiori,

$$\mathcal{E}[n](A_v^{\mathrm{nr}}) \xrightarrow{\simeq} E[n](F_v^{\mathrm{nr}}).$$

Mais n étant premier à p, $\mathcal{E}[n]_{/A_v}$ est fini étale ([3, 7.3.2]), donc par [EGA, IV 18.5.5] :

$$\mathcal{E}[n](A_v^{\mathrm{nr}}) \xrightarrow{\simeq} E[n](\overline{k}).$$

L'action de $\mathrm{Gal}(\overline{F}/F)$ sur $E(\overline{F})_{\mathrm{tors}}$ est d'autre part abélienne : cela résulte de ce que l'action de $\mathrm{Gal}(\overline{F}/F)$ sur le module $\hat{V}(E)$ est $\widehat{K}$-linéaire, et $\hat{V}(E)$ est libre de rang un sur $\hat{K}$. En particulier :

$$E[n](F_v^{\mathrm{ab/nr}}) \xrightarrow{\simeq} E[n](F_v^{\mathrm{nr}}).$$

Il ne reste plus qu'à combiner ces trois isomorphismes. $\square$

3.4 Action de K et action de Galois sur $\hat{V}(E)$

Soit F un corps de nombre, $E_{/F}$ une courbe elliptique a multiplication complexe par O_c sur F.

3.4.1 L'action de K.

Il est bien connu que le module de Tate $\hat{T}(E)$ est *libre* de rang un sur $\widehat{O}_c$: cela résulte par exemple de la théorie analytique. Choisissant un générateur $\hat{e}$ de $\hat{T}(E)$ sur $\widehat{O}_c$, on obtient donc un isomorphisme :

$$\begin{array}{ccc} \widehat{K} & \xrightarrow{\simeq} & \hat{V}(E) \\ \hat{\lambda} & \mapsto & \hat{\lambda}\hat{e} \end{array}$$

Bien entendu, les réseaux de $\hat{K}$ tels que définis en (2.8) correspondent bijectivement aux réseaux de $\hat{V}(E)$, de sorte qu'en utilisant le lemme 2.8.2, on obtient finalement une bijection :

$$\hat{T} : \{\text{réseaux de } K\} \xrightarrow{\simeq} \{\text{réseaux de } \hat{V}(E)\}$$

Si a est un réseau de K, le réseau correspondant $\hat{T}(a)$ de $\hat{V}(E)$ est défini par :

$$\hat{T}(a)_q = a_q.\hat{e}_q$$

Il est clair que $\hat{T}(a)$ est un $\widehat{O}_{c(a)}$-module libre de rang 1.

L'existence de cette bijection montre tout d'abord que pour tout réseau T de $\hat{V}(E)$, il existe un unique entier c, que l'on appelle encore *le conducteur* de T, tel que :

$$\forall q : \qquad \{x \in K_q \mid xT_q \subset T_q\} = (O_c)_q.$$

T_q est alors $(O_c)_q$-libre, et

$$\begin{array}{rcl} \{x \in \widehat{K} \mid xT \subset T\} & = & \widehat{O}_c, \\ \{x \in K \mid xT \subset T\} & = & O_c. \end{array}$$

On note $c(T)$ le conducteur de T. Si $\hat{T}(E) \subset T$, et X est le sous-groupe correspondant dans $E(\overline{F})$, la courbe elliptique E/X, qui est définie sur une extension finie de F, a multiplication complexe par $c(T)$ sur cette extension : cela résulte de 3.2.1.

L'existence de cette bijection nous permet également de transférer les résultats de la section 2.1 à l'étude des réseaux de $\hat{V}(E)$. Plus précisément, considérons l'opération qui à un réseau a de K et un réseau T de $\hat{V}(E)$ associe le réseau aT de $\hat{V}(E)$. Cette opération est compatible avec les fibrations données par les conducteurs, et permet de munir l'ensemble fibré des réseaux de $\hat{V}(E)$ d'une "action simple et fidèle" du fibré en groupe que constituent les réseaux de K.

3.4.2 L'action de Gal$(\overline{F}/F)$

L'action de $\mathrm{Gal}(\overline{F}/F)$ étant $(O_c)_q$-linéaire, se factorise en un morphisme (continu) :

$$\rho_q : \mathrm{Gal}(F^{\mathrm{ab}}/F) \to (O_c)_q^*.$$

Il en résulte notamment que $E(\overline{F})_{\mathrm{tors}} = E(F^{\mathrm{ab}})_{\mathrm{tors}}$. La théorie du corps de classe permet de réécrire ce morphisme en

$$\rho_q : I_F \to (O_c)_q^*,$$

où I_F est le groupe des idèles de F. Posant $F[c] = FK[c]$ pour tout entier $c \geq 1$, on a :

Proposition 3.4.1 *Supposons que $O_c^* = \{\pm 1\}$, ou que $E_{/F}$ soit (F-)isogène à une courbe elliptique ayant multiplication complexe par un ordre non maximal. Alors pour tout réseau T de $\hat{V}(E)$, T est stable sous* $\mathrm{Gal}(F^{\mathrm{ab}}/F[c(T)])$.

Preuve: Supposons d'abord que $O_c^* = \{\pm 1\}$. Il existe un homomorphisme continu $\varepsilon : I_F \to K^*$ tel que, pour tout nombre premier q,

$$\forall s \in I_F : \qquad \rho_q(s) = \varepsilon(s) N_{F/K}(s_q^{-1}) \in (O_c)_q^*,$$

où s_q est la q-composante de s. C'est précisément [33, Theorem 10] dans le cas où $\mathrm{End}_F(E) = O_K$ ($c = 1$), et le cas général s'en déduit de la manière suivante : soit $C = \{x \in E(\overline{F}) \mid cO_K.x = 0\}$, de sorte que C est un sous-groupe fini de $E(\overline{F})$, défini sur F. E est F-isogène à la courbe elliptique $E' = E/C$, qui a multiplication complexe par O_K ; il suffit alors d'utiliser l'isomorphisme $\mathrm{Gal}(\overline{F}/F)$-équivariant $\hat{V}(E) \to \hat{V}(E/C)$.

Soit $[\star, F] : I_F \to \mathrm{Gal}(F^{\mathrm{ab}}/F)$ l'application de réciprocité d'Artin, et choisissons un élément $s \in I_F$ tel que $[s, F] = \sigma \in \mathrm{Gal}(F^{\mathrm{ab}}/F[c(a)])$. Soit $d(a) = \mathrm{ppcm}(c(a), c)$, de sorte que $F[d(a)] = F[c(a)]$, puisque $K[c] = K[j(E)] \subset F$. Comme

$$\sigma \mid_{K[d(a)]} = 1 = [N_{F/K}(s), K] \mid_{K[d(a)]},$$

$N_{F/K}(s)$ appartient au groupe de normes dans I_K de l'extension abélienne $K[d(a)]/K$, à savoir $K^*.(\widehat{O}^*_{d(a)} \times \mathbb{C}^*)$. On peut donc écrire $N_{F/K}(s) = \lambda.(\hat{x} \times \mu)$, avec $\lambda \in K^*$, $\hat{x} \in \widehat{O}^*_{d(a)} \subset \widehat{O}^*_c$ et $\mu \in \mathbb{C}^*$. Alors :

$$\forall q : \qquad \varepsilon(s)\lambda^{-1} = \rho_q(s).\hat{x}_q.$$

Dans cette égalité, le terme de gauche appartient à K, tandis que le terme de droite appartient à $O^*_{c,q}$, de sorte que finalement $\varepsilon(s)\lambda^{-1}$ appartient à $O^*_c = \{\pm 1\}$. Mais alors $\rho_q(s) = \pm\hat{x}_q^{-1} \in O^*_{c(a),q}$ et $\rho_q(s).\hat{T}_q(a) = \hat{T}_q(a)$ pour tout q, donc $\sigma.\hat{T}(a) = \hat{T}(a)$.

Dans le cas spécial où $O^*_c \neq \{\pm 1\}$ ($d_K = -3$ ou -4 *et* $c = 1$), on travaille d'abord dans le module de Tate d'une courbe elliptique $E'_{/F}$ à multiplication complexe par un ordre non maximal de K, et F-isogène à E. La discussion précédante s'applique alors à E', et la conclusion se transporte à E. $\square$

Chapitre 4

Points CM

4.1 Définition

Soit $X_0(N)_{/\mathbb{Q}}$ la courbe modulaire compactifiée classifiant les N-isogénies cycliques de courbes elliptiques. On a donc :

$$X_0(N)(\mathbb{C}) = \mathrm{Cusp}(X_0(N)) \coprod \{E_1 \to E_2\}/\sim,$$

où $E_1 \to E_2$ est une isogénie cyclique de degré N entre deux courbes elliptiques définies sur $\mathbb{C}$, et $(E_1 \to E_2) \sim (E_1' \to E_2')$ si, et seulement si, il existe un diagramme commutatif d'isogénies :

$$\begin{array}{ccc} E_1 & \xrightarrow{\simeq} & E_1' \\ \downarrow & & \downarrow \\ E_2 & \xrightarrow{\simeq} & E_2' \end{array}$$

On dit que $x = [E_1 \to E_2] \in X_0(N)(\mathbb{C})$ est un *point CM* si E_1 (et donc aussi E_2) a multiplication complexe par K. Les conducteurs de E_1 et E_2 ne dépendent évidemment pas du choix du représentant $E_1 \to E_2$ de x.

4.2 Corps de définition

Proposition 4.2.1 *Soit $x = [f : E_1 \to E_2] \in X_0(N)(\mathbb{C})$ un point CM. Soit c_i le conducteur de E_i $(i = 1, 2)$ et $c = \mathrm{ppcm}(c_1, c_2)$. Soit S un ensemble fini de nombres premiers tel que : si $(d_K = -3$ ou $-4)$* et *$(c$ est une puissance de $p)$, alors $p \notin S$. Alors il existe deux courbes elliptiques $E'_{1/K[c]}$ et $E'_{2/K[c]}$ ayant bonne réduction au-dessus de S, et une isogénie cyclique de degré N $f' : E'_{1/K[c]} \to E'_{2/K[c]}$ telles qu'il existe un diagramme commutatif d'isogénies sur $\mathbb{C}$:*

$$\begin{array}{ccc} E_1 & \xrightarrow{\simeq} & E_1' \\ f\downarrow & & \downarrow f' \\ E_2 & \xrightarrow{\simeq} & E_2' \end{array}$$

En particulier, $x = [f' : E'_1 \to E'_2] \in X_0(N)(K[c])$.

Preuve: Notre hypothèse sur S implique, par un théorème de Serre-Tate [33, p. 507], que l'on peut trouver une courbe elliptique $E_{/K[c]}$, ayant bonne réduction sur S et multiplication complexe par O_c.

Supposons d'abord que $O_c^* = \{\pm 1\}$. D'après la théorie analytique des courbes elliptiques, E est isogène à E_1, de sorte que l'on peut trouver une isogénie $g : E \to E_1$ définie sur $\mathbb{C}$. Soient $H_1 = \ker(g)$ et $H_2 = \ker(f \circ g)$, de sorte que l'on a un diagramme commutatif :

$$\begin{array}{ccc} E/H_1 & \xrightarrow{\simeq} & E_1 \\ f' \downarrow & & \downarrow f \\ E/H_2 & \xrightarrow{\simeq} & E_2 \end{array}$$

où $f' : E/H_1 \to E/H_2$ est induite par l'inclusion $H_1 \subset H_2$. Soient T_1 et T_2 les deux réseaux de $\hat{V}(E)$ correspondant à H_1 et H_2. Il résulte du lemme 3.2.1 que $c(T_1) = c_1$ et $c(T_2) = c_2$, puis il résulte de la proposition 3.4.1 que H_1 est défini sur $K[c]K[c_1] = K[c]$, et H_2 sur $K[c]K[c_2] = K[c]$. L'isogénie $f' : E/H_1 \to E/H_2$ est donc définie sur $K[c]$, et les courbes elliptiques $E'_{1/K[c]} = E/H_1$ et $E'_{2/K[c]} = E/H_2$ ont évidemment bonne réduction sur S, puisqu'elles sont $K[c]$-isogènes à $E_{/K[c]}$.

Si $O_c^* \neq \{\pm 1\}$, alors $d_K = -3$ ou -4, et $c = c_1 = c_2 = 1$. Dans ce cas, le groupe de Picard $\mathrm{Pic}(O_c)$ est trivial, et d'après la théorie analytique des courbes elliptiques, E, E_1 et E_2 sont isomorphes sur $\mathbb{C}$. Choisissons des isomorphismes $E_{/\mathbb{C}} \to (E_{1/2})_{/\mathbb{C}}$, et soit $f' : E \to E$ l'isogénie déduite de f via ces deux isomorphismes. On a donc : $x = [f' : E \to E]$, et $f' \in \mathrm{End}_{\overline{K}}(E) = \mathrm{End}_{K[1]}(E)$. $\square$

4.3 Action de Galois sur les points CM

Soit $x = [f : E_1 \to E_2] \in X_0(N)(\mathbb{C})$ un point CM, c_1 et c_2 les conducteurs de E_1 et E_2, de sorte que x est rationnel sur $K[c]$, où $c = \mathrm{ppcm}(c_1, c_2)$, d'après la proposition précédente. On veut ici décrire l'action de $\mathrm{Gal}(K[c]/K)$ sur x.

Rappelons pour cela que la théorie du corps de classe nous donne un isomorphisme :

$$\left(\frac{K[c]/K}{\star}\right) : \mathrm{Pic}(O_c) \xleftarrow{\sim} \widehat{K}^*/K^*.\widehat{O}_c \xrightarrow{\sim} \mathrm{Gal}(K[c]/K).$$

Proposition 4.3.1 *Soit* $\sigma \in \mathrm{Gal}(K[c]/K)$*, et* Q *un idéal propre pour* O_c *tel que* $\sigma = \left(\frac{K[c]/K}{Q}\right)$*. Alors :*

$$\sigma.x = [f^Q : E_1^Q \to E_2^Q] \in X_0(N)(K[c])$$

Remarque: Compte tenu de notre convention générale pour l'identification $\mathrm{End}^0_{\mathbb{C}}(E_{1/2}) = K$, l'isogénie f est K-linéaire, c'est-à-dire : f commute à l'action de $O_c = O_{c_1} \cap O_{c_2}$ sur E_1 et E_2. Ou encore : f est un morphisme de schémas en O_c-modules, de sorte que $f^Q : E_1^Q \to E_2^Q$ est bien défini. C'est une isogénie de courbes elliptiques sur $\mathbb{C}$, de noyau

$$\begin{aligned} \ker(f^Q)(\mathbb{C}) &= \ker(f)^Q(\mathbb{C}) \\ &= \mathrm{Hom}_O(Q, \ker(f)(\mathbb{C}) \\ &= \mathrm{Hom}_{O/NO}\left(Q/NQ, \ker(f)(\mathbb{C})\right). \end{aligned}$$

Comme $Q/NQ \simeq O/NO$, puisque Q est O_c-propre, f^Q est en effet une N-isogénie cyclique.
Soit $d \geq 1$ un entier tel que $c \mid d$, donc $K[c] \subset K[d]$. Si Q est un idéal propre pour O_d et $\sigma = \left(\frac{K[d]/K}{Q}\right) \in \mathrm{Gal}(K[d]/K)$, on a de même

$$\sigma.x = [f^Q : E_1^Q \to E_2^Q] \in X_0(N)(K[c]),$$

oùl'on doit maintenant utiliser l'action de $O_d \subset O_c$ pour définir les transformés. Cela résulte tout simplement de ce que, pour tout O_c-module M,

$$\begin{aligned} \mathrm{Hom}_{O_d}(Q, M) &= \mathrm{Hom}_{O_c}(O_c \otimes_{O_d} Q, M) \\ &= \mathrm{Hom}_{O_c}(O_c Q, M), \end{aligned}$$

la deuxième égalité provenant de ce que Q est O_d-plat.

Preuve: (d'après [30]) Par la proposition 4.2.1, on peut supposer que E_1, E_2 et f sont définis sur $K[c]$. Dans ce cas, on a évidemment $\sigma.x = [f^\sigma : E_1^\sigma \to E_2^\sigma]$.

Soit $X_0(N)_{/\mathbb{Z}[1/N]}$ le modèle propre et lisse de $X_0(N)_{/\mathbb{Q}}$. Soit v une place finie de $K[c]$, d'anneau de valuation complété A_v et de corps résiduel k de caractéristique p, et qui soit telle que :

1. $p \nmid N d_K c$ et $E_{1/K[c]}$ a bonne réduction au-dessus de p.
2. L'application de réduction $X_0(N)(K[c]) \to X_0(N)(k)$ induit une injection sur l'ensemble *fini* des points $z \in X_0(N)(K[c])$ qui peuvent être représentés par une isogénie sur $\mathbb{C}$ de la forme $E_a \to E_b$ avec $\mathrm{End}_{\mathbb{C}}(E_a) = O_{c_1}$.
3. Si P est l'idéal premier de O_K sous v, alors $\sigma = \mathrm{Frob}_P(K[c]/K)$, et P est de degré 1 (p est décomposé dans K).

Il existe une infinité de telles places : les deux premières conditions n'excluent qu'un nombre fini de places, tandis que la dernière condition est vérifiée par une infinité de places.

Posons $P_c = P \cap O_c \subset_p O_c$, de sorte que P_c est un idéal propre pour O_c, et $\sigma = \left(\frac{K[c]/K}{Q}\right) = \left(\frac{K[c]/K}{P_c}\right)$, donc $[P_c] = [Q]$ dans $\mathrm{Pic}(O_c)$. A fortiori, les foncteurs $\mathrm{Hom}_{O_c}(P_c, \star)$ et $\mathrm{Hom}_{O_c}(Q, \star)$ sont isomorphes, donc

$$[f^Q : E_1^Q \to E_2^Q] = [f^{P_c} : E_1^{P_c} \to E_2^{P_c}] \in X_0(N)([K[c]).$$

On peut donc supposer que $Q = P_c$.

Compte tenu de la condition (1), E_1, E_2, E_1^σ, E_2^σ, E_1^Q et E_2^Q ont bonne réduction en v. Notant $\widetilde{A}_{/k}$ la fibre spéciale du modèle de Néron d'une variété abélienne $A_{/K[c]}$, et $\widetilde{A}_{/k}^{(p)}$ son "Frobenius twist" (absolu), on a

$$\left(E_1^Q \to E_2^Q\right)^{\sim} = \left(\widetilde{E}_1^Q \to \widetilde{E}_2^Q\right) \quad \text{et} \quad (E_1^\sigma \to E_2^\sigma)^{\sim} = \left(\widetilde{E}_1^{(p)} \to \widetilde{E}_2^{(p)}\right),$$

la deuxième égalité résultant de la condition (3). D'après la condition (2), on doit donc voir que :

$$\left[\widetilde{f}^{(p)} : \widetilde{E}_1^{(p)} \to \widetilde{E}_2^{(p)}\right] = \left[\widetilde{f}^Q : \widetilde{E}_1^Q \to \widetilde{E}_2^Q\right] \in X_0(N)(k).$$

Les deux isogénies concernées s'insèrent dans des diagrammes similaires, à savoir le diagramme classique du Frobenius :

$$\begin{array}{cccc} \widetilde{f} : & \widetilde{E}_1 & \to & \widetilde{E}_2 \\ & \downarrow & & \downarrow \\ \widetilde{f}^{(p)} : & \widetilde{E}_1^{(p)} & \to & \widetilde{E}_2^{(p)} \end{array}$$

et le diagramme induit par l'inclusion $Q = P_c \subset_p O_c$:

$$\begin{array}{cccc} \widetilde{f} : & \widetilde{E}_1 & \to & \widetilde{E}_2 \\ & \downarrow & & \downarrow \\ \widetilde{f}^Q : & \widetilde{E}_1^Q & \to & \widetilde{E}_2^Q \end{array}$$

Dans le premier diagramme, les flèches verticales sont les Frobenius absolus : ce sont des isogénies purement inséparables de rang p. Pour conclure, il faut donc voir que les deux flèches verticales du second diagramme ont un noyau *connexe*, puisqu'on sait déjà que ces isogénies sont de degré p. C'est effectivement le cas, puisque

$$\begin{array}{rcl} \ker(\widetilde{E}_{1/2} \to \widetilde{E}_{1/2}^Q)(\overline{k}) & = & \widetilde{E}_{1/2}^{O_c/Q}(\overline{k}) \\ & = & \mathrm{Hom}_{O_c}\left(O_c/Q, \widetilde{E}_{1/2}(\overline{k})\right) \\ & = & \mathrm{Hom}_{O_c}\left(O_c/P_c, \widetilde{E}_{1/2}[p](\overline{k})\right) \\ & \approx & \mathrm{Hom}_{O_c}(O_c/P_c, O_c/\overline{P_c}) = 0, \end{array}$$

par la proposition 3.3.3, p étant décomposé. $\square$

Chapitre 5

Ensemble de points CM

Soit k un corps, $\ell = \mathrm{car}(k)$, $E_{/k}$ une courbe elliptique, $R = \mathrm{End}_{\overline{k}}(E)$ et $B = \mathrm{End}^0_{\overline{k}}(E)$, de sorte que B est un corps, éventuellement non commutatif. Soit également $N \geq 1$ un entier *premier à* ℓ, et S un ensemble de nombres premiers, *contenant* ℓ si $\ell \neq 0$.

On note $X^{(S)}(E, N)$ l'ensemble des points $[E_1 \to E_2]$ de $X_0(N)(\overline{k})$ tels que : il existe une $\overline{k}$-isogénie $E \to E_1$ de degré *premier* à S. C'est alors une isogénie étale, de même que l'isogénie composée $E \to E_1 \to E_2$. Les points de $X^{(S)}(E, N)$ peuvent donc tous s'écrire : $[E/X_1 \to E/X_2]$, pour $X_1 \subset X_2 \subset E(\overline{k})$, avec X_1 d'ordre premier à S, et $X_2/X_1 \simeq \mathbb{Z}/N\mathbb{Z}$. On se propose de décrire "adéliquement" cet ensemble.

Si S^c est le complémentaire de S dans l'ensemble des nombres premiers, on note aussi $X_{S^c}(E, N) = X^{(S)}(E, N)$.

5.1 Notations

5.1.1 Un schéma en anneau

Pour tout anneau commutatif A, on pose

$$\mathfrak{R}(A) = A \otimes_{\mathbb{Z}} R.$$

En particulier, $B = \mathfrak{R}(\mathbb{Q})$. $\mathfrak{R}$ est un foncteur covariant en anneau (non nécessairement commutatif) sur la catégorie des anneaux commutatifs. Ce foncteur est représenté par l'anneau commutatif des $\mathbb{Z}$-tenseurs symétriques sur le $\mathbb{Z}$-dual de R :

$$S_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Z})).$$

En effet,

$$\begin{aligned} \mathrm{Hom}_{\mathrm{Ann}}(S_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Z})), A) &= \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Z}), A) \\ &\simeq A \otimes_{\mathbb{Z}} R = \mathfrak{R}(A). \end{aligned}$$

Ainsi, $\mathfrak{R}_{/\mathbb{Z}}$ est un *schéma* en anneau, dont le schéma sous-jacent n'est autre que l'espace affine de dimension $\mathrm{rang}_{\mathbb{Z}}(R)$. En particulier, $\mathfrak{R}_{/\mathbb{Z}}$ est lisse.

On pose aussi, pour tout anneau commutatif A,

$$\mathfrak{R}^*(A) = (A \otimes R)^*.$$

$\mathfrak{R}^*$ est un foncteur en groupe, dont on peut encore vérifier qu'il est représentable par un sous-schéma ouvert de $\mathfrak{R}$. Les applications de trace réduite et de norme réduite définissent des morphismes de schémas en groupe

$$\begin{array}{rccc} \mathrm{tr}: & \mathfrak{R} & \to & \mathbb{G}_a \\ \mathrm{nr}: & \mathfrak{R}^* & \to & \mathbb{G}_m. \end{array}$$

On note $\mathfrak{R}^1$ le noyau de nr, de sorte que

$$\mathfrak{R}^1(A) = \{x \in (A \otimes R)^* \mid \mathrm{nr}(x) = 1\}$$

pour tout anneau commutatif A.

Si S est un ensemble de nombres premiers, on pose :

$$\begin{array}{rcl} \widehat{\mathbb{Z}}^{(S)} & = & \prod_{q \notin S} \mathbb{Z}_q \\ \mathbb{Z}_S & = & \prod_{q \in S} \mathbb{Z}_q \\ \widehat{\mathbb{Q}}^{(S)} & = & \widehat{\mathbb{Z}}^{(S)} \otimes \mathbb{Q} \\ \mathbb{Q}_S & = & \mathbb{Z}_S \otimes \mathbb{Q} \end{array}$$

On réservera en général la notation en indice au cas où S est fini.

Enfin, on pose

$$\begin{array}{rcl} R(S) & = & \mathfrak{R}(\mathbb{Q}) \cap \mathfrak{R}(\widehat{\mathbb{Z}}_S) \subset \mathfrak{R}(\widehat{\mathbb{Q}}_S) \\ R^*(S) & = & \mathfrak{R}^*(\mathbb{Q}) \cap \mathfrak{R}^*(\widehat{\mathbb{Z}}_S) \subset \mathfrak{R}^*(\widehat{\mathbb{Q}}_S) \\ R^1(S) & = & \mathfrak{R}^1(\mathbb{Q}) \cap \mathfrak{R}^1(\widehat{\mathbb{Z}}_S) \subset \mathfrak{R}^1(\widehat{\mathbb{Q}}_S), \end{array}$$

de sorte que

$$\begin{array}{rcl} R(S) & = & \{x \in B \mid \forall q \in S \; x \in R_q\} \\ R^*(S) & = & \{x \in B^* \mid \forall q \in S \; x \in R_q^*\} \\ R^1(S) & = & \{x \in B^1 \mid \forall q \in S \; x \in R_q^*\}. \end{array}$$

5.1.2 Variantes de modules de Tate

Par analogie, on définit alors les modules de Tate “modifiés” suivants :

$$\begin{aligned}
\hat{T}^{(S)}(E) &= \prod_{q \notin S} T_q(E) \\
T_S(E) &= \prod_{q \in S} T_q(E) \\
\hat{V}^{(S)}(E) &= \hat{T}^{(S)}(E) \otimes \mathbb{Q} \\
V_S(E) &= T_S(E) \otimes \mathbb{Q}.
\end{aligned}$$

Par construction, chacun de ces groupes est un *module* (à gauche) sur l'anneau des points de $\mathfrak{R}$ à valeur dans l'anneau correspondant : $\hat{T}^{(S)}(E)$ est un $\mathfrak{R}(\widehat{\mathbb{Z}}^{(S)})$-module, $\hat{V}^{(S)}(E)$ est un $\mathfrak{R}(\widehat{\mathbb{Q}}^{(S)})$-module, etc...

5.1.3 Réseaux et sous-groupes

Un ***réseau*** de $\hat{V}^{(S)}(E)$ est un sous-$\widehat{\mathbb{Z}}$-module T de $\hat{V}^{(S)}(E)$ tel qu'il existe un entier n pour lequel nT est inclus dans $\hat{T}^{(S)}(E)$ avec un indice fini. Bien évidemment, on peut alors prendre n premier à S. Un réseau T de $\hat{V}^{(S)}(E)$ se décompose donc en

$$T = \prod_{q \notin S} T_q.$$

Si T est un réseau de $\hat{V}(E)$, on note $T^{(S)} = T \cap \hat{V}^{(S)}(E)$: c'est alors un réseau de $\hat{V}^{(S)}(E)$. Inversement, si T est un réseau de $\hat{V}^{(S)}(E)$, on note T^e le réseau de $\hat{V}(E)$ tel que : $(T^e)_q = T_q$ si $q \notin S$, et $(T^e)_q = T_q(E)$ si $q \in S$. On dit d'un réseau T de $\hat{V}(E)$ qu'il est ***premier à S*** si $T_q = T_q(E)$ pour tout $q \in S$, autrement dit, si $(T^{(S)})^e = T$. L'application :

$$\begin{aligned}
\{\text{réseaux de } \hat{V}^{(S)}(E)\} &\rightarrow \{\text{réseaux de } \hat{V}(E)\} \\
T &\mapsto T^e
\end{aligned}$$

est une bijection sur l'ensemble des réseaux de $\hat{T}(E)$ premiers à S.

Si T est un réseau de $\hat{V}^{(S)}(E)$ contenant $\hat{T}^{(S)}(E)$, le réseau T^e de $\hat{V}(E)$ contient $\hat{T}(E)$. Si X est le sous-groupe de $E(\overline{k})_{\text{tors}} \simeq \hat{V}(E)/\hat{T}(E)$ correspondant à $T^e/\hat{T}(E)$, on dit que X est ***le sous-groupe associé*** à T. L'isogénie étale $E \to E/X$ est définie sur la sous-extension $k(X) = k(T)$ de $\overline{k}/k$ correspondant au sous-groupe ouvert de $\mathrm{Gal}(\overline{k}/k)$:

$$\mathrm{Fix}(T) = \{\sigma \in \mathrm{Gal}(\overline{k}/k) \mid \sigma T = T\} = \{\sigma \in \mathrm{Gal}(\overline{k}/k) \mid \sigma X = X\} = \mathrm{Fix}(X).$$

5.2 Description de $X^{(S)}(E,N)$

Une *N-inclusion de réseaux* de $\hat{V}(E)$ est un couple (T_1, T_2) de réseaux de $\hat{V}(E)$ tels que $T_1 \subset T_2$ et $T_2/T_1 \simeq \mathbb{Z}/N\mathbb{Z}$; on résume cela dans la notation :

$$T_1 \subset_N T_2.$$

Si $\hat{T}(E) \subset T_1$, on dit des deux sous-groupes $X_1 \subset X_2$ correspondant à T_1 et T_2 qu'ils sont *associés* à la N-inclusion $T_1 \subset_N T_2$. L'isogénie $E/X_1 \to E/X_2$ est définie sur la sous-extension $k(T_1, T_2) = k(X_1, X_2)$ de $\overline{k}/k$ fixée par

$$\mathrm{Fix}(T_1) \cap \mathrm{Fix}(T_2) = \{\sigma \in \mathrm{Gal}(\overline{k}/k) \mid \sigma T_1 = T_1 \text{ et } \sigma T_2 = T_2\}.$$

Les $\overline{k}$-points de son noyau forment un $\mathrm{Gal}(\overline{k}/k(X_1, X_2))$-module isomorphe à $X_2/X_1 \simeq T_2/T_1 \simeq T_2/T_1$, et la suite

$$E(\overline{k})_{\mathrm{tors}} \to (E/X_1)(\overline{k})_{\mathrm{tors}} \to (E/X_2)(\overline{k})_{\mathrm{tors}}$$

s'identifie à la suite

$$\hat{V}(E)/\hat{T}(E) \to \hat{V}(E)/T_1 \to \hat{V}(E)/T_2.$$

Considérons l'ensemble des N-inclusions de réseaux $(T_1 \subset_N T_2)$ telles que : T_1 est premier à S, c'est-à-dire $(T_1)_q = T_q(E)$ pour tout $q \in S$, ou encore, $(T_1^{(S)})^e = T_1$. Le groupe $R^*(S) = \{x \in B^* \mid \forall q \in S \; x \in R_q^*\}$ agit à gauche sur cet ensemble par multiplication à gauche : pour $\hat{\lambda} \in \mathbb{R}^*(S)$,

$$\hat{\lambda}.(T_1 \subset_N T_2) = (\hat{\lambda} T_1 \subset_N \hat{\lambda} T_2).$$

Soit $Y^{(S)}(E,N)$ l'ensemble quotient :

$$Y^{(S)}(E,N) = R^*(S) \setminus \{T_1 \subset_N T_2 \text{ réseaux de } \hat{V}(E),\ T_1 \text{ premier à } S\}.$$

Soit $T_1 \subset_N T_2$ une N-inclusion de réseaux de $\hat{V}(E)$, avec T_1 premier à S. Il existe un entier $n \geq 1$ premier à S tel que $\hat{T}(E) \subset n^{-1}T_1 \subset_N n^{-1}T_2$. Soient $X_1 \subset_N X_2$ les sous-groupes finis associés de $E(\overline{k})$, et notons (abusivement) :

$$[E/T_1 \to E/T_2] \in X_0(N)(\overline{k}).$$

le point de $X_0(N)(\overline{k})$ correspondant à la N-isogénie cyclique $E/X_1 \to E/X_2$. Il est clair que c'est un point de $X^{(S)}(E,N)$, et tous les points de $X^{(S)}(E,N)$ peuvent être construits de la sorte. Plus précisément :

Proposition 5.2.1 *La construction*

$$(T_1 \subset_N T_2) \rightsquigarrow [E/T_1 \to E/T_2] \in X_0(N)(\overline{k})$$

induit une bijection

$$H : Y^{(S)}(E,N) \xrightarrow{\simeq} X^{(S)}(E,N) \subset X_0(N)(\overline{k}).$$

Preuve: 1) Montrons d'abord que H est bien définie. Soient donc $T_1 \subset_N T_2$ et $T_1' \subset_N T_2'$ deux N-inclusions de réseaux de $\hat{V}(E)$, avec T_1 et T_2 premiers à S, et $\lambda \in R^*(S)$ tels que :

$$(T_1' \subset_N T_2') = \lambda(T_1 \subset_N T_2).$$

Soient également n et n' deux entiers positifs premiers à S tels que $\hat{T}(E) \subset n^{-1}T_1$ et $\hat{T}(E) \subset n'^{-1}T_1'$. On a alors

$$n'^{-1}(T_1' \subset_N T_2') = (n'^{-1}\lambda n)n^{-1}(T_1 \subset_N T_2),$$

et $n^{-1}\lambda n' \in R^*(S)$. Remplaçant $(T_1 \subset_N T_2)$ par $n^{-1}(T_1 \subset_N T_2)$, $(T_1' \subset_N T_2')$ par $n'^{-1}(T_1' \subset_N T_2')$ et λ par $n^{-1}\lambda n'$, on peut donc supposer $n = n' = 1$, c'est-à-dire : $\hat{T}(E) \subset T_1 \subset_N T_2$ et $\hat{T}(E) \subset T_1' \subset_N T_2'$.

Soient X_1, X_2, X_1' et X_2' les sous-groupes correspondants de $E(\overline{k})_{\text{tors}}$. On veut donc montrer que

$$[f : E/X_1 \to E/X_2] = [f' : E/X_1' \to E/X_2'] \in X_0(N)(\overline{k}).$$

Soit $p_i : E \to E/X_i$, et $p_i' : E \to E/X_i'$ les projections. Comme $\lambda \in R^*(S)$, il existe un entier $m \geq 1$ premier à S tel que $m\lambda \in R$, et alors $m\lambda \in R^*(S) \cap R$. Soit $\varphi : E \to E$ l'isogénie correspondant à $m\lambda$, de sorte que $\varphi : E \to E$ est une isogénie de degré premier à S, et en particulier étale. Soit K_i le noyau de l'isogénie étale

$$g_i : E \xrightarrow{\varphi} E \xrightarrow{p_i'} (E/X_i'),$$

de sorte que l'on a un diagramme commutatif

$$\begin{array}{ccc} E/K_1 & \xrightarrow{\simeq} & E/X_1' \\ f'' \downarrow & & \downarrow f' \\ E/K_2 & \xrightarrow{\simeq} & E/X_2' \end{array}$$

où f' et f'' sont les isogénies naturelles. Par ailleurs,

$$g_i : E(\overline{k})_{\text{tors}} \xrightarrow{\varphi} E(\overline{k})_{\text{tors}} \xrightarrow{p_i'} (E/X_i')(\overline{k})_{\text{tors}}$$

s'identifie à

$$\hat{V}(E)/\hat{T}(E) \xrightarrow{\times m\lambda} \hat{V}(E)/\hat{T}(E) \longrightarrow \hat{V}(E)/T_i',$$

de sorte que $K_i(\overline{k})$ s'identifie au sous-groupe

$$(m\lambda)^{-1}T_i'/\hat{T}(E) = m^{-1}T_i/\hat{T}(E) \subset \hat{V}(E)/\hat{T}(E).$$

Il en résulte que K_i est aussi le noyau de

$$E \xrightarrow{\times m} E \to E/X_i,$$

d'où un deuxième diagramme commutatif :

$$\begin{array}{ccc} E/K_1 & \xrightarrow{\simeq} & E/X_1 \\ f'' \downarrow & & \downarrow f \\ E/K_2 & \xrightarrow{\simeq} & E/X_2 \end{array}$$

Finalement, on obtient donc

$$\begin{array}{ccc} E/X_1 & \xrightarrow{\simeq} & E/X_1' \\ f \downarrow & & \downarrow f' \\ E/X_2 & \xrightarrow{\simeq} & E/X_2' \end{array}$$

et :

$$[f : E/X_1 \to E/X_2] = [f' : E/X_1' \to E/X_2'] \in X_0(N)(\overline{k}).$$

H est donc bien définie.

2) L'application H étant évidemment surjective, montrons qu'elle est également injective : supposons que $H([T_1 \subset T_2]) = H([T_1' \subset T_2'])$, de sorte qu'il existe un diagramme commutatif de $\overline{k}$-isogénies :

$$\begin{array}{ccc} E/X_1 & \xrightarrow{g_1} & E/X_1' \\ f \downarrow & & \downarrow f' \\ E/X_2 & \xrightarrow{g_2} & E/X_2' \end{array}$$

où g_1 et g_2 sont des isomorphismes, et $X_1 \subset_N X_2$, $X_1' \subset_N X_2'$ sont les sous-groupes de $E(\overline{k})$ correspondant à $\hat{T}^{(S)}(E) \subset n^{-1}T_1 \subset_N n^{-1}T_2$ et $\hat{T}^{(S)}(E) \subset n'^{-1}T_1' \subset_N n'^{-1}T_2'$, pour n et n' des entiers convenables premiers à S. On veut montrer que $[T_1 \subset_N T_2] = [T_1' \subset_N T_2']$ dans $Y^{(S)}(E,N)$, et l'on peut donc déjà supposer que $n = n' = 1$. Soit $d_i = \#X_i$ et $d_i' = \#X_i'$ $(i = 1,2)$, de sorte que d_1 et d_1' sont premiers à S.

Soient $p_i : E \to E/X_i$, $p_i' : E \to E/X_i'$ les projections, et définissons l'isogénie $\varphi_i : E \to E$ par

$$\varphi_i : E \xrightarrow{p_i} E/X_i \xrightarrow{g_i} E/X_i' \xrightarrow{(p_i')^{\mathrm{dual}}} E.$$

C'est une isogénie étale de degré $d_i d_i'$. De plus,

$$\begin{array}{rcl} \varphi_2 & = & (p_2')^{\mathrm{dual}} \circ g_2 \circ p_2 \\ & = & (p_1')^{\mathrm{dual}} \circ (f')^{\mathrm{dual}} \circ g_2 \circ f \circ p_1 \\ & = & (p_1')^{\mathrm{dual}} \circ (f')^{\mathrm{dual}} \circ f' \circ g_1 \circ p_1 \\ & = & N.(p_1')^{\mathrm{dual}} \circ g_1 \circ p_1 \\ & = & N\varphi_1. \end{array}$$

D'autre part, on a vu (lemme 3.2.1) que :

$$\begin{array}{rcl} d_i T_i & = & \hat{T}(p_i^{\mathrm{dual}}) \left(\hat{T}(E/X_i)\right) \\ d_i' T_i' & = & \hat{T}(p_i'^{\mathrm{dual}}) \left(\hat{T}(E/X_i')\right), \end{array}$$

de sorte que si $\lambda_i \in R$ correspond à φ_i, on calcule :

$$\begin{aligned}
\lambda_i d_i T_i &= \hat{T}(\varphi_i) \circ \hat{T}(p_i^{\mathrm{dual}}) \left(\hat{T}(E/X_i)\right) \\
&= \hat{T}(p_i')^{\mathrm{dual}} \circ \hat{T}(g_i) \circ \hat{T}(p_i) \circ \hat{T}(p_i^{\mathrm{dual}}) \left(\hat{T}(E/X_i)\right) \\
&= d_i \hat{T}(p_i')^{\mathrm{dual}} \circ \hat{T}(g_i) \left(\hat{T}(E/X_i)\right) \\
&= d_i \hat{T}(p_i')^{\mathrm{dual}} \left(\hat{T}(E/X_i')\right) \\
&= d_i d_i' T_i'
\end{aligned}$$

donc $\lambda_i T_i = d_i' T_i'$. Mais $\lambda_2 = N\lambda_1$ et $d_2' = N d_1'$, donc $\lambda_1(T_1 \subset_N T_2) = (T_1' \subset_N T_2)$. Il ne reste plus qu'à voir que $\lambda_1 \in R^*(S)$: cela résulte de ce que $\deg(\lambda_1) = d_1 d_1'$ est premier à S. □

5.3 Les points CM en caractéristique 0

5.3.1 Définition

Soit F un corps de nombre, $E_{/F}$ une courbe elliptique à multiplication complexe par O_c sur $F \supset K$. Appliquant la théorie précédente avec $S = \emptyset$, on a $R = O_c$, $B = K$, $\mathfrak{R}(\widehat{\mathbb{Z}}) = \widehat{O}_c$, $\mathfrak{R}(\widehat{\mathbb{Q}}) = \widehat{K}$, $R^*(\emptyset) = K^*$, etc... En particulier, on obtient une bijection :

$$\begin{array}{rrcl}
H: \quad Y(E,N) = K^* \setminus \{T_1 \subset_N T_2 \subset \hat{V}(E)\} & \xrightarrow{\simeq} & X(E,N) \subset X_0(N)(\overline{F}) \\
{[T_1 \subset_N T_2]} & \longmapsto & [E/T_1 \to E/T_2]
\end{array}$$

Dans ce cas, $X(E,N)$ est l'ensemble de *tous* les points CM. Cela résulte de ce que toute courbe elliptique à multiplication complexe est $\mathbb{C}$-isogène à E. Par ailleurs, si T_1 est de conducteur c_1, et T_2 de conducteur c_2, alors E/T_1 et E/T_2 sont des courbes elliptiques à multiplication complexe par O_{c_1} et O_{c_2} respectivement, d'après le lemme 3.2.1, et $[E/T_1 \to E/T_2]$ est donc rationnel sur $K[\mathrm{ppcm}(c_1, c_2)]$.

5.3.2 Action de Galois

Rappelons que l'application de réciprocité d'Artin est un morphisme *surjectif* (section 1.8) :

$$[K[\infty]/K, \star] : \widehat{K}^* \to \mathrm{Gal}(K[\infty]/K).$$

Par ailleurs, $\hat{V}(E)$ est un $\widehat{K}$-module, et $\widehat{K}^*$ agit sur l'ensemble des N-inclusions de réseaux de $\hat{V}(E)$ par ($\hat{\lambda} \in \widehat{K}^*$) :

$$\hat{\lambda}(T_1 \subset_N T_2) = (\hat{\lambda} T_1 \subset_N \hat{\lambda} T_2).$$

Cette action est évidemment compatible avec celle de K^*, et l'on obtient ainsi une action à gauche de $\widehat{K}^*$ sur $Y(E,N)$.

Proposition 5.3.1 *L'application $H : Y(E,N) \to X(N)(K[\infty])$ est anti-équivariante pour le morphisme $[K[\infty]/K, \star]$, c'est-à-dire : si $\hat{\lambda} \in \widehat{K}^*$ et $\sigma = [K[\infty]/K, \hat{\lambda}]$, alors pour tout $x \in Y(E,N)$, $H(\hat{\lambda}.x) = \sigma^{-1} H(x)$*

Preuve: Ecrivons $x = [T_1 \subset_N T_2]$, avec $\hat{T}(E) \subset T_1$. Soient X_1 et X_2 les sous-groupes de $E(F^{\mathrm{ab}})$ correspondant à T_1 et T_2, et $d = \mathrm{ppcm}(c(T_1), c(T_2), c)$, de sorte que O_d agit sur E, E/X_1 et E/X_2. Par la proposition 4.2.1,

$$H(x) = [E/X_1 \to E/X_2] \in X_0(N)(K[d]).$$

Si $Q = \hat{\lambda} O_d$, Q est un idéal propre pour O_d et

$$\left(\frac{K[c]/K}{Q}\right) = \sigma \mid_{K[d]} \in \mathrm{Gal}(K[d]/K).$$

de sorte que, d'après la proposition 4.3.1,

$$\sigma H(x) = [(E/X_1)^Q \to (E/X_2)^Q] \in X_0(N)(K[d]).$$

Soient $p_i : E \to E/X_i$ les projections, et $n \geq 1$ un entier tel que $nQ \subset O_d$. On a alors un diagramme commutatif :

$$\begin{array}{ccc} E/X_1 & \to & E/X_2 \\ q_1 \downarrow & & \downarrow q_2 \\ (E/X_1)^{nQ} & \to & (E/X_2)^{nQ} \end{array}$$

D'autre part, les identifications O_d-linéaires

$$\begin{array}{ccccc} E(F^{\mathrm{ab}})_{\mathrm{tors}} & \to & (E/X_i)(F^{\mathrm{ab}})_{\mathrm{tors}} & \to & (E/X_i)^{nQ}(F^{\mathrm{ab}})_{\mathrm{tors}} \\ \downarrow & & \downarrow & & \downarrow \\ \hat{V}(E)/\hat{T}(E) & \to & \hat{V}(E)/T_i & \to & \mathrm{Hom}_{O_d}(nQ, \hat{V}(E)/T_i) \end{array}$$

montrent que le noyau de $q_i p_i$ s'identifie à l'ensemble des éléments $x \in \hat{V}(E)/\hat{T}(E)$ tels que $nQx \subset T_i$, c'est-à-dire, à $(nQ)^{-1}T_i/T_i$. Or $(nQ)^{-1}T_i = n^{-1}\hat{\lambda}^{-1}T_i$, de sorte que : $\sigma H(x) = H\left([\hat{\lambda}^{-1}T_1 \subset \hat{\lambda}^{-1}T_2]\right) = H(\hat{\lambda}^{-1}x)$. □

5.4 Réduction

Soit toujours F un corps de nombre contenant K, et $E_{/F}$ une courbe elliptique à multiplication complexe par O_c.

Soit $X_0(N)_{/\mathbb{Z}[1/N]}$ le modèle propre et lisse de $X_0(N)_{/\mathbb{Q}}$ (cf. [10]), et v une place non-archimédienne de $K[\infty]$ sur un nombre premier $\ell \nmid N$. Soit $A_v \subset K[\infty]$ son anneau de valuation, de sorte que $\mathrm{Frac}(A_v) = K[\infty]$, et $k(v)$ le corps résiduel de A_v. Le schéma $X_0(N)_{/\mathbb{Z}[1/N]}$ étant propre, l'application de "générisation" est bijective ([EGA, II 7.3.8]) :

$$X_0(N)(A_v) \xrightarrow{\simeq} X_0(N)(K[\infty]).$$

On obtient donc une application bien définie

$$\mathrm{red}_v : X_0(N)(K[\infty]) \to X_0(N)(k(v)),$$

et on s'intéresse au morphisme composé

$$Y^{(\ell)}(E,N) \xrightarrow{\simeq} X^{(\ell)}(E,N) \subset X_0(N)(K[\infty]) \xrightarrow{\mathrm{red}_v} X_0(N)(k(v)).$$

5.4.1 Les hypothèses et notations

On fait les hypothèses suivantes :
- $F \subset K[\infty]$ et
- $E_{/F}$ a bonne réduction en $v_0 = v\,|_F$.

Soient A_{v_0} l'anneau de valuation de F en v_0, $k(v_0)$ son corps résiduel, $\mathcal{E}_{/A_{v_0}}$ le modèle de Néron de $E_{/F}$, et $\widetilde{\mathcal{E}}_{/k(v_0)}$ sa fibre spéciale. Soient également v^{ab} une place de $F^{\mathrm{ab}} \supset K[\infty]$ au-dessus de v, $F_v^{\mathrm{ab/nr}} \subset \overline{F}$ l'extension maximale abélienne non-ramifiée en v_0 de F, et $v^{\mathrm{ab/nr}} = \overline{v}\,|_{F_v^{\mathrm{ab/nr}}}$. Les inclusions de corps sont donc

$$F \subset K[\infty] \subset F^{\mathrm{ab}} \quad \text{et} \quad F \subset F^{\mathrm{ab/nr}} \subset F^{\mathrm{ab}};$$

elles induisent des inclusions sur les anneaux locaux

$$A_{v_0} \subset A_v \subset A_v^{\mathrm{ab}} \quad \text{et} \quad A_{v_0} \subset A_v^{\mathrm{ab/nr}} \subset A_v^{\mathrm{ab}},$$

et sur les corps résiduels

$$k(v_0) \subset k(v) \subset k(v^{\mathrm{ab}}) \quad \text{et} \quad k(v_0) \subset k(v^{\mathrm{ab/nr}}) = k(v^{\mathrm{ab}}).$$

De plus, $k(v^{\mathrm{ab}})$ est une clôture algébrique de $k(v_0)$.

On a vu en (3.3.5) :

$$E[n](F_v^{\mathrm{ab/nr}}) \xleftarrow{\simeq} \mathcal{E}[n](A_v^{\mathrm{ab/nr}}) \xrightarrow{\simeq} \widetilde{\mathcal{E}}[n](k(v^{\mathrm{ab}}))$$

A fortiori, la réduction en la place v^{ab} de F^{ab} induit un isomorphisme :

$$\begin{array}{ccc} \hat{T}^{(\ell)}(E) & \xrightarrow{\simeq} & \hat{T}^{(\ell)}(\widetilde{\mathcal{E}}) \\ t & \longmapsto & \widetilde{t} \end{array}$$

et aussi :

$$\hat{V}^{(\ell)}(E) \xrightarrow{\simeq} \hat{V}^{(\ell)}(\widetilde{\mathcal{E}}).$$

Soient $R = \mathrm{End}_{k(v^{\mathrm{ab}})}(\widetilde{\mathcal{E}})$, $B = \mathrm{End}^0_{k(v^{\mathrm{ab}})}(\widetilde{\mathcal{E}})$, $B^{(\ell)} = \{x \in B^* \mid x \in R_\ell^*\}$, et $K^{(\ell)} = \{x \in K^* \mid x \in (O_c)_\ell^*\}$. La réduction en v_0 des éléments de $\mathrm{End}_F(E)$ induit un plongement $i : K^{(\ell)} \hookrightarrow B^{(\ell)}$, compatible avec l'isomorphisme défini ci-dessus, c'est-à-dire tel que : si $t \in \hat{V}^{(\ell)}(E)$ et $\lambda \in K^{(\ell)}$, alors $(\lambda.t)\tilde{} = i(\lambda).\widetilde{t}$. En particulier, on en déduit une *surjection* :

$$\begin{array}{rccc} \mathrm{red}_v : & Y^{(\ell)}(E,N) & \to & Y^{(\ell)}(\widetilde{\mathcal{E}},N) \\ & [T_1 \subset_N T_2] & \mapsto & [\widetilde{T_1} \subset_N \widetilde{T_2}] \end{array}$$

5.4.2 Le résultat

Proposition 5.4.1 *Le diagramme suivant est commutatif :*

$$\begin{array}{cccc}
\mathrm{red}_v : & Y^{(\ell)}(E,N) & \to & Y^{(\ell)}(\widetilde{\mathcal{E}},N) \\
& \downarrow & & \downarrow \\
\mathrm{red}_v : & X_0(N)(K[\infty]) & \to & X_0(N)(k(v))
\end{array}$$

Preuve: Une tautologie. □

Corollaire 5.4.2 *Si ℓ est* décomposé *dans K, et $\ell \nmid c$, alors le morphisme de réduction* $\mathrm{red}_v : X_0(N)(K[\infty]) \to X_0(N)(k(v))$ *induit un isomorphisme*

$$X^{(\ell)}(E,N) \xrightarrow{\simeq} X^{(\ell)}(\widetilde{\mathcal{E}},N)$$

Preuve: On a vu en (3.3.3) que sous les hypothèses du corollaire, et avec les notations du paragraphe précédent, $B^{(\ell)} = K^{(\ell)}$. L'application $\mathrm{red}_v : Y^{(\ell)}(E,N) \to Y^{(\ell)}(\widetilde{\mathcal{E}},N)$ est donc évidemment bijective. □

Le cas où ℓ est inerte ou ramifié dans K est évidemment considérablement différent.

5.5 Le cas supersingulier

Supposons maintenant que k est un corps fini de caractéristique $\ell \nmid N$, et $E_{/k}$ une courbe elliptique supersingulière. On a donc : $R = \mathrm{End}_{\overline{k}}(E)$ est un ordre maximal dans $B = \mathrm{End}^0_{\overline{k}}(E)$, et B est un corps de quaternions, ramifié exactement en ℓ et ∞. E n'ayant pas de ℓ-torsion, la ℓ-composante du module de Tate est triviale : $\hat{V}(E) = \hat{V}^{(\ell)}(E)$.

5.5.1 Le site supersingulier $X_0^{\mathrm{ss}}(N)(k)$

Montrons d'abord :

Lemme 5.5.1 *Pour toute courbe elliptique supersingulière $E'_{/\overline{k}}$, il existe une isogénie* étale $E \to E'$ *définie sur $\overline{k}$.*

Preuve: Il est bien connu que toutes les courbes elliptiques supersingulières sont isogènes sur $\overline{k}$, et l'on peut donc choisir une isogénie $f : E \to E'$ définie sur $\overline{k}$. Soit ℓ^i le rang de la partie connexe de son noyau : $\ell^i = \mathrm{rang}(\ker(f)^0)$. D'après [39, p. 80], il existe un élément $x \in B^*$ de norme réduite ℓ^i. Multipliant cet élément par un entier premier à ℓ convenable, on obtient un élément y de R de norme réduite $n\ell^i$, avec n premier à ℓ. En particulier, le rang de la partie connexe de l'isogénie $fy : E \to E'$ est maintenant ℓ^{2i} : $\mathrm{rang}(\ker(fy)^0) = \ell^{2i}$. Or $E_{/\overline{k}}$ étant supersingulière, pour tout $j \geq 0$, il existe un unique sous-schéma en groupe de rang ℓ^j, à savoir le noyau du Frobenius $F^j : E \to E^{(\ell^j)}$. En particulier,

$$\ker(fy)^0 = \ker(\ell^i),$$

donc fy se factorise par $\ell^i : E \to E$, c'est-à-dire qu'il existe une isogénie $g : E \to E'$ telle que $fy = g\ell^i$. Comparant les degrés respectifs des deux termes, on voit que g est de degré premier à ℓ, donc une isogénie étale. $\square$

Il en résulte que $X^{(\ell)}(E,N) \subset X_0(N)(k)$ est précisément l'ensemble $X_0^{\mathrm{ss}}(N,k)$ des points supersinguliers de $X_0(N)(k)$:

$$X^{(\ell)}(E,N) = X_0^{\mathrm{ss}}(N)(k).$$

Calculons d'autre part $Y^{(\ell)}(E,N)$. $\mathfrak{R}^*(\widehat{\mathbb{Q}}^{(\ell)})$ agit à gauche sur les N-inclusions de réseaux de $\hat{V}(E) = \hat{V}^{(\ell)}(E)$ par

$$\hat{\lambda}(T_1 \subset_N T_2) = (\hat{\lambda}T_1 \subset_N \hat{\lambda}T_2)$$

et l'on a :

Proposition 5.5.2 $\mathfrak{R}^*(\widehat{\mathbb{Q}}^{(\ell)})$ *agit transitivement sur les N-inclusions de réseaux de $\hat{V}(E)$.*

Preuve: Soient $(T_1 \subset_N T_2)$ et $(T_1' \subset_N T_2')$ deux N-inclusions. On veut montrer qu'il existe $\hat{b} = (b_q)_q \in \mathfrak{R}^*(\widehat{\mathbb{Q}}^{(\ell)})$ tel que $(T_1' \subset_N T_2') = \hat{b}(T_1 \subset_N T_2)$. Pour presque tout premier $q \neq \ell$, $(T_1)_q = (T_2)_q = (T_1')_q = (T_2')_q = T_q(E)$, et on pose alors $b_q = 1$. Il ne reste plus qu'à trouver, pour les autres premiers $q \neq \ell$, un élément $b_q \in B_q^*$ tel que $(T_1' \subset_N T_2')_q = b_q(T_1 \subset_N T_2)_q$. Notons que si $q^i \parallel N$, $(T_1)_q \subset_{q^i} (T_2)_q$ et $(T_1')_q \subset_{q^i} (T_2')_q$. Comme $B_q \simeq M_2(\mathbb{Q}_p)$, le résultat découle de la théorie des diviseurs élémentaires. $\square$

Fixons une N-inclusion $T_0 \subset_N T_0'$ de réseaux de $\hat{V}(E)$. Son stabilisateur pour l'action de $\mathfrak{R}^*(\widehat{\mathbb{Q}}^{(\ell)})$ est

$$\{\hat{x} \in \mathfrak{R}^*(\widehat{\mathbb{Q}}^{(\ell)}) \mid \hat{x}T_0 = T_0 \text{ et } \hat{x}T_0' = T_0'\}.$$

Pour tout réseau T de $\hat{V}(E)$, posons

$$O(T) = \{x \in B \mid xT \subset T \text{ et } x \in R_\ell\}.$$

$O(T)$ est un ordre maximal dans B, et $R_0 = O(T_0) \cap O(T_0')$ est donc un *ordre d'Eichler* dans B. Définissant alors pour tout anneau commutatif A, comme dans la section 5.1.1, $\mathfrak{R}_0(A) = A \otimes_{\mathbb{Z}} R_0$, le stabilisateur de la N-inclusions $T_0 \subset_N T_0'$ peut également s'écrire

$$\mathrm{Stab}(T_0 \subset_N T_0') = \mathfrak{R}_0^*(\widehat{\mathbb{Z}}^{(\ell)}) = \prod_{q \neq \ell} (R_0)_q^*.$$

La proposition précédente fournit alors une bijection :

$$\begin{array}{ccc} \mathfrak{R}^*(\widehat{\mathbb{Q}}^{(\ell)})/\mathfrak{R}_0^*(\widehat{\mathbb{Z}}^{(\ell)}) & \xrightarrow{\simeq} & \{N - \text{inclusions de réseaux de } \hat{V}(E)\} \\ [\hat{b}] & \longmapsto & (\hat{b}T_0 \subset_N \hat{b}T_0') \end{array}$$

D'où une bijection :

$$\begin{array}{ccc} R^*(\ell) \setminus \mathfrak{R}^*(\widehat{\mathbb{Q}}^{(\ell)})/\mathfrak{R}_0^*(\widehat{\mathbb{Z}}^{(\ell)}) & \xrightarrow{\simeq} & Y^{(\ell)}(E,N) \\ [\hat{b}] & \longmapsto & [\hat{b}T_0 \subset_N \hat{b}T_0'] \end{array}$$

où l'on rappelle que

$$R^*(\ell) = \{x \in B^* \mid x \in R_\ell^*\} = \{x \in B^* \mid \mathrm{nr}(x) \text{ est premier à } \ell\}.$$

5.5.2 Approximation forte

Soit maintenant $p \neq \ell$ un nombre premier.

Lemme 5.5.3 *Le plongement* $\mathbb{Q}_p \hookrightarrow \widehat{\mathbb{Q}}^{(\ell)}$ *induit une surjection*

$$\mathfrak{R}^1(\mathbb{Q}_p) \twoheadrightarrow R^*(\ell) \setminus \mathfrak{R}^*(\widehat{\mathbb{Q}}^{(\ell)})/\mathfrak{R}_0^*(\widehat{\mathbb{Z}}^{(\ell)}).$$

Preuve: Soit $\hat{b} \in \mathfrak{R}^*(\widehat{\mathbb{Q}}^{(\ell)})$. La norme réduite de $\hat{b}$ est un élément de $\widehat{\mathbb{Q}}^{(\ell)}$. Il existe donc un nombre rationnel positif $q \in \mathbb{Q}^*$ premier à ℓ tel que $\mathrm{nr}(\hat{b}) = q\hat{n}$, où $\hat{n} \in \widehat{\mathbb{Z}}^{(\ell)*}$. Par [39, p. 80], on peut trouver un élément $b_0 \in B^*$ tel que $\mathrm{nr}(b_0) = q^{-1}$, et b_0 appartient alors à $R^*(\ell)$. D'autre part, pour tout nombre premier $q \neq \ell$, $(R_0)_q$ est un ordre d'Eichler dans l'algèbre B_q, donc isomorphe à une algèbre de la forme :

$$\begin{pmatrix} \mathbb{Z}_q & \mathbb{Z}_q \\ q^i\mathbb{Z}_q & \mathbb{Z}_q \end{pmatrix}$$

En particulier, la norme réduite de $(R_0)_q^*$ est égale à $\mathbb{Z}_q^*$, et l'on peut trouver un élément $\hat{r}_0 \in \mathfrak{R}_0^*(\widehat{\mathbb{Z}}^{(\ell)})$ tel que $\mathrm{nr}(\hat{r}_0) = \hat{n}^{-1}$. On a alors $\mathrm{nr}(b_0\hat{b}\hat{r}_0) = 1$, c'est-à-dire $b_0\hat{b}\hat{r}_0 \in \mathfrak{R}^1(\widehat{\mathbb{Q}}^{(\ell)})$.

Or, d'après le théorème d'approximation forte ([39, p. 81]), $\mathfrak{R}^1(\mathbb{Q})\mathfrak{R}^1(\mathbb{Q}_p)$ est dense dans $\mathfrak{R}^1(\widehat{\mathbb{Q}}^{(\ell)})$. $\mathfrak{R}_0^1(\widehat{\mathbb{Z}}^{(\ell)})$ étant *ouvert* dans $\mathfrak{R}^1(\widehat{\mathbb{Q}}^{(\ell)})$, on en déduit :

$$\mathfrak{R}^1(\mathbb{Q})\mathfrak{R}^1(\mathbb{Q}_p)\mathfrak{R}_0^1(\widehat{\mathbb{Z}}^{(\ell)}) = \mathfrak{R}^1(\widehat{\mathbb{Q}}^{(\ell)}).$$

Il existe donc $b^1 \in \mathfrak{R}^1(\mathbb{Q}) \subset R^*(\ell)$, $b_p^1 \in \mathfrak{R}^1(\mathbb{Q}_p)$, et $\hat{r}_0^1 \in \mathfrak{R}_0^1(\widehat{\mathbb{Z}}^{(\ell)})$ tel que : $b_0\hat{b}\hat{r}_0 = b^1b_p^1\hat{r}_0^1$. A fortiori, $[\hat{b}] = [b_p^1]$ dans $R^*(\ell) \setminus \mathfrak{R}^*(\widehat{\mathbb{Q}}^{(\ell)})/\mathfrak{R}_0^*(\widehat{\mathbb{Z}}^{(\ell)})$. □

5.5.3 Conclusion

Prenons pour $T_0 \subset_N T_0'$ une N-inclusion de réseaux de $\hat{V}(E)$, avec $T_0 = \hat{T}(E)$, et renommons $T_0' = T_N$. On a alors : $(R_0)_q = R_q$ pour tout $q \nmid N$.

Soit b_p et b_p' deux éléments de $\mathfrak{R}^*(\mathbb{Q}_p) = B_p^*$ ayant la même image dans $R^*(\ell) \setminus \mathfrak{R}^*(\widehat{\mathbb{Q}}^{(\ell)})/\mathfrak{R}_0^*(\widehat{\mathbb{Z}}^{(\ell)})$. Il existe donc $b \in R^*(\ell)$ et $\hat{r} = (\hat{r}_q)_{q\neq\ell} \in \mathfrak{R}_0^*(\widehat{\mathbb{Z}}^{(\ell)})$ tel que $b_p' = bb_p\hat{r}$ dans $\mathfrak{R}^*(\widehat{\mathbb{Q}}^{(\ell)})$. A une place $q \neq \ell, p$, on a donc $b\hat{r}_q = 1$, d'où $b \in (R_0)_q^*$. A la place $q = \ell$, on sait déjà que $b \in R^*(\ell)$, donc $b \in R_\ell^* = (R_0)_\ell^*$. Finalement, $b \in \mathfrak{R}_0^*(\mathbb{Z}[1/p])$, et $b_p' \in \mathfrak{R}_0^*(\mathbb{Z}[1/p])b_p\mathfrak{R}_0^*(\mathbb{Z}_p)$ dans $B_p^* = \mathfrak{R}_0(\mathbb{Q}_p)$.

Inversement, si $b_p' \in \mathfrak{R}_0^*(\mathbb{Z}[1/p])b_p\mathfrak{R}_0^*(\mathbb{Z}_p)$, soit $b_p' = bb_pr_p$, posons $\hat{r}_q = \hat{r}_p$ si $q = p$, et $\hat{r}_q = b^{-1} \in \mathfrak{R}_0^*(\mathbb{Z}_q)$ si $q \neq p, l$. Alors $\hat{r} = (r_q)_{q\neq l} \in \mathfrak{R}^*(\widehat{\mathbb{Z}}^{(\ell)})$, $b \in R^*(\ell)$, et $b_p' = bb_p\hat{r}$. Ainsi :

Proposition 5.5.4 *On a une bijection*

$$\mathfrak{R}_0^*(\mathbb{Z}[1/p]) \setminus \mathfrak{R}_0^*(\mathbb{Q}_p)/\mathfrak{R}_0^*(\mathbb{Z}_p) \to R^*(\ell) \setminus \mathfrak{R}^*(\widehat{\mathbb{Q}}^{(\ell)})/\mathfrak{R}_0^*(\widehat{\mathbb{Z}}^{(\ell)}).$$

Il en résulte surtout que :

Proposition 5.5.5 *L'application qui, à un élément $b_p \in B_p^*$ associe, d'abord la N-inclusion $b_pT \subset b_pT_N$, puis le point correspondant $[E/b_pT \to E/b_pT_N]$ de $X_0^{ss}(N)(k)$, induit une bijection*

$$\mathfrak{R}_0^*(\mathbb{Z}[1/p]) \setminus B_p^*/(R_0)_p^* \to X_0^{ss}(N)(k).$$

Notons encore que ce résultat implique :

Corollaire 5.5.6 *Pour tout ensemble S de nombres premiers, contenant ℓ, mais ne contenant pas p, les injections naturelles qui suivent sont des bijections :*

$$X_p(E,N) \hookrightarrow X^{(S)}(E,N) \hookrightarrow X^{(\ell)}(E,N) \hookrightarrow X_0^{ss}(N).$$

Chapitre 6

Surjectivité de la réduction

6.1 Notations et Résultat

Soit $E_{/\mathbb{C}}$ une courbe elliptique à multiplication complexe par K, $N \geq 1$ un entier, et p un nombre premier. On écrit $N = p^i N'$, avec $N' \geq 1$ premier à p. Soit $C_{N'}$ un sous-groupe cyclique d'ordre N' de $E(\mathbb{C})$.

Pour toute isogénie $f : E \to E'$ dont le degré est une puissance de p, $f(C_{N'})$ est un sous-groupe cyclique d'ordre N' de $E'(\mathbb{C})$. Si C'_{p^i} est un sous-groupe cyclique d'ordre p^i de $E'(\mathbb{C})$, l'isogénie $E' \to E'/\left(f(C_{N'}) \oplus C'_{p^i}\right)$ est cyclique de degré N, et définit donc un point de $X_0(N)(\mathbb{C})$. Soit $\mathcal{L} \subset X_0(N)(\mathbb{C})$ l'ensemble des points ainsi obtenus.

Lemme 6.1.1 *Soit c_0 le plus grand diviseur premier à p de* $\mathrm{ppcm}(c(E), c(E/C_{N'}))$. *Alors*

$$\mathcal{L} \subset X_0(N)(K[c_0 p^\infty]).$$

Preuve: Les conducteurs possibles pour les ordres des courbes elliptiques E' ne diffèrent de $c(E)$ que d'une puissance de p, d'après la proposition 2.2.1. Ceux des courbes elliptiques $E'/f(C_{N'}) \oplus C'_{p^i}$ ne diffèrent également de $c(E/C_{N'})$ que d'une puissance de p. Le lemme résulte donc de 4.2.1. □

Soit $\mathfrak{S}$ un ensemble fini de places finies de $K[c_0 p^\infty]$, dont les caractéristiques résiduelles sont *inertes* dans K, et ne divisent pas pN. Pour $v \in \mathfrak{S}$, on note $k(v)$ le corps résiduel de v, et

$$\mathrm{red}_v : X_0(N)(K[c_0 p^\infty]) \to X_0(N)(k(v))$$

l'application de réduction en v.

Rappelons que l'on a par ailleurs défini un sous-groupe dénombrable (et dense) de $\mathrm{Gal}(K[c_0 p^\infty]/K)$ (section 2.7) :

$$\mathrm{Gal}(K[c_0 p^\infty]/K)^{\mathrm{rat}} = [K[c_0 p^\infty]/K, \widehat{K}^{(p)*}]$$

où $\widehat{K}^{(p)*} = \left(K \otimes \widehat{\mathbb{Z}}^{(p)}\right)$.

Le but de cette section est de démontrer le résultat suivant :

Théorème 6.1.2 *Si* $\forall v \neq v' \in \mathfrak{S}$, $\mathrm{Gal}(K[c_0 p^\infty]/K)^{\mathrm{rat}} v \neq \mathrm{Gal}(K[c_0 p^\infty]/K)^{\mathrm{rat}} v'$, *alors :*

$$\begin{array}{cccc} \mathrm{RED}: & \mathcal{L} & \to & \prod_{v \in \mathfrak{S}} (X_0^{\mathrm{ss}}(N)(k(v)) \\ & x & \mapsto & (\mathrm{red}_v(x))_{v \in \mathfrak{S}}. \end{array}$$

est surjective.

6.2 Traduction topologique du théorème

6.2.1 Une variante

Soit S l'ensemble des caractéristiques résiduelles de $\mathfrak{S}$, et, pour tout $\ell \in S$, soit $\mathfrak{S}_\ell \subset \mathfrak{S}$ l'ensemble des places dont la caractéristique résiduelle est ℓ. ℓ étant inerte dans K, toutes les places de $\mathfrak{S}_\ell$ sont situées sur un même idéal premier $L = O_K \ell$ de O_K, et sont en particulier conjuguées sous l'action de $\mathrm{Gal}(K[c_0 p^\infty]/K)$.

Fixons dans chaque $\mathfrak{S}_\ell$ une place distinguée v_ℓ. Puis, pour tout $v \in \mathfrak{S}_\ell$, choisissons un élément $\sigma_v \in \mathrm{Gal}(K[c_0 p^\infty]/K)$ tel que $v = v_\ell \circ \sigma_v$. L'hypothèse sur $\mathfrak{R}$ du théorème garantit alors que $\sigma_v \sigma_{v'}^{-1} \notin \mathrm{Gal}(K[c_0 p^\infty]/K)^{\mathrm{rat}}$. D'autre part, σ_v induit un isomorphisme entre le corps résiduel de v et le corps résiduel de v_ℓ, d'où un diagramme commutatif :

$$\begin{array}{cccc} \mathrm{red}_v : & X_0(N)(K[c_0 p^\infty]) & \to & X_0(N)(k(v)) \\ & \sigma \downarrow & & \sigma \downarrow \\ \mathrm{red}_{v_\ell} : & X_0(N)(K[c_0 p^\infty]) & \to & X_0(N)(k(v_\ell)). \end{array}$$

Les flèches verticales sont des bijections. Pour alléger les déjà très lourdes notations de la preuve, nous allons en fait nous borner à démontrer l'énoncé suivant :

Théorème 6.2.1 *Soit S un ensemble fini de nombres premiers $\ell \nmid pN$* inertes *ou* ramifiés *dans K. Pour tout $\ell \in S$, soit v_ℓ une place de $K[c_0 p^\infty]$ sur ℓ, $k(\ell)$ son corps résiduel, et*

$$\mathrm{red}_\ell : X_0(N)(K[c_0 p^\infty]) \to X_0^{ss}(N)(k(\ell))$$

l'application de réduction en v_ℓ. Soit également $\mathcal{R}$ un ensemble fini d'éléments de $\mathrm{Gal}(K[c_0 p^\infty]/K)$*, tel que :*

$$\forall (\sigma \neq \sigma') \in \mathcal{R}^2 : \qquad \sigma^{-1} \sigma' \notin \mathrm{Gal}(K[c_0 p^\infty]/K)^{\mathrm{rat}}.$$

Alors l'application suivante est surjective :

$$\begin{array}{cccc} \mathrm{RED}: & \mathcal{L} & \to & \prod_{\ell \in S} (X_0^{\mathrm{ss}}(N)(k(\ell))^{\mathcal{R}} \\ & x & \mapsto & (\mathrm{red}_\ell(\sigma.x))_{(\sigma,\ell) \in \mathcal{R} \times S}. \end{array}$$

Notons que l'on a rajouté les places ramifiées. Le lecteur se convaincra aisément de la validité du théorème 6.1.2.

On fixe les notations S et $\mathcal{R}$ dans toute la suite de cette section.

6.2.2 Normalisation de E et $C_{N'}$

Soit $c = \mathrm{ppcm}(c(E), c(E/C_{N'}))$.

Par la proposition 4.2.1, on peut trouver deux courbes elliptiques $E_{1/K[c]}$ et $E_{2/K[c]}$, ayant bonne réduction au-dessus de S, et un diagramme commutatif d'isogénies sur $\mathbb{C}$:

$$\begin{array}{ccc} E & \overset{\simeq}{\longrightarrow} & E_1 \\ \downarrow & & \downarrow \\ E/C_{N'} & \overset{\simeq}{\longrightarrow} & E_2 \end{array}$$

... sous réserve que, si $d_K = -3$ ou -4 et $c = q^n$, alors $q \notin S$. Mais il résulte de la définition de $\mathcal{L}$ que l'on peut changer E et $C_{N'}$ (sans changer l'ensemble $\mathcal{L} \subset X_0(N)(\mathbb{C})$), en E' et $f(C_{N'})$, où $f : E \to E'$ est une isogénie dont le degré est une puissance de p. Un choix convenable de f permet alors de garantir que *p divise c*, et comme $p \notin S$, la proposition 4.2.1 s'applique.

En fait, on choisit directement de remplacer E et $C_{N'}$ par E' et $f(C_{N'})$, où $f : E \to E'$ est une isogénie de degré une puissance de p, telle que *p^2 divise le conducteur $c(E')$* de E'. On fait ce choix pour éviter tous les cas particuliers : $O_c^* \neq \{\pm 1\}$, il y a des idéaux Q de O_c qui sont ramifiés et principaux, etc...

On suppose donc que E *a multiplication complexe par O_c, avec $p^2 \mid c$; que E est définie sur $F = K[c] \subset K[c_0 p^\infty]$, et $E_{/F}$ a bonne réduction au-dessus de S.*

6.2.3 Situation galoisienne résiduelle

Pour tout $\ell \in S$, *choisissons* une place v_ℓ^{ab} de $F^{\mathrm{ab}} \supset K[c_0 p^\infty]$ au-dessus de la place v_ℓ de $K[c_0 p^\infty]$, et notons v_ℓ^0 la place de F sous v_ℓ. Soient

$$O_K/\ell O_K \subset k(v_\ell^0) \subset k(\ell) \subset k(v_\ell^{\mathrm{ab}})$$

les corps résiduels respectifs de v_ℓ^0, v_ℓ et v_ℓ^{ab}. On a alors :

Lemme 6.2.2

1. *Si ℓ est inerte dans K,*

$$O_K/\ell O_K = k(v_\ell^0) = k(\ell) \simeq \mathbb{F}_{\ell^2}$$

et $k(v_\ell^{ab})$ en est une clôture algébrique.

2. *Si ℓ est ramifié dans K, $\ell O_K = L^2$,*

$$\mathbb{F}_\ell \simeq O_K/L \subset k(v_\ell^0) = k(\ell) \simeq \mathbb{F}_{\ell^2}$$

et $k(v_\ell^{ab})$ en est une clôture algébrique.

Preuve: La sous-extension maximale non ramifiée en ℓO_K de $K[\infty]/K$ est la réunion des ring class field de conducteur n premier à ℓ, c'est-à-dire

$$K[\infty]_\ell^{\mathrm{nr}} = \bigcup_{\ell \nmid n} K[n].$$

Il est bien connu que $k(v_\ell^{\mathrm{ab}})$ est une clôture algébrique de $k(v_\ell^0)$.

1) Si ℓ est inerte dans K, dans chaque groupe $\mathrm{Gal}(K[n]/K)$, n premier à ℓ, le Frobénius de ℓO_K est

$$\left(\frac{K[n]/K}{\ell O_n}\right) = 1 \in \mathrm{Gal}(K[n]/K),$$

et ℓO_K est donc totalement décomposé dans $K[\infty]_\ell^{\mathrm{nr}}$. Ainsi :

$$O_K/\ell O_K = k(v_\ell^{\mathrm{ab}} \mid_{K[\infty]_\ell^{\mathrm{nr}}}).$$

Mais v est ensuite *totalement ramifié* dans $K[\infty]/K[\infty]_\ell^{nr}$, de sorte qu'également :

$$k(v_\ell^{\mathrm{ab}} \mid_{K[\infty]_\ell^{\mathrm{nr}}}) = k(v_\ell^{\mathrm{ab}} \mid_{K[\infty]}).$$

A fortiori, $O_K/\ell O_K = k(v_\ell^0) = k(\ell)$.

2) Si ℓ est ramifié dans K, $\ell O_K = L^2$, le *carré* du frobénius σ de L dans $\mathrm{Gal}(K[n]/K)$ (n premier à ℓ) est de même trivial :

$$\sigma^2 = \left(\frac{K[n]/K}{O_n \cap L}\right)^2 = \left(\frac{K[n]/K}{\ell O_n}\right) = 1 \in \mathrm{Gal}(K[n]/K)$$

De plus $\sigma = 1$ si et seulement si $O_n \cap L$ est un idéal O_n-principal, et cela ne peut se produire, d'après le lemme 1.3.4, que lorsque $n = 1$ ou 2. On conclut à partir de là comme dans le cas inerte que :

$$\mathbb{F}_\ell \simeq O_K/L \subset k(v_\ell^{\mathrm{ab}} \mid_{K[\infty]_\ell^{\mathrm{nr}}}) = k(v_\ell^{\mathrm{ab}} \mid_{K[\infty]}) \simeq \mathbb{F}_{\ell^2}$$

Comme $p^2 \mid c$ est premier à ℓ, le lemme 1.3.4 implique que $k(v_\ell^0)$ contient $\mathbb{F}_{\ell^2}$. □

On choisit comme clôture algébrique de $k(\ell)$:

$$\overline{k(\ell)} = k(v_\ell^{\mathrm{ab}}).$$

6.2.4 Choix d'idèles représentant les éléments de $\mathcal{R}$

Pour tout $\sigma \in \mathcal{R}$, soit $\hat{\lambda}_\sigma \in \widehat{K}^*$ un idéle fini tel que

$$[K[c_0 p^\infty]/K, \hat{\lambda}_\sigma] = \sigma \in \mathrm{Gal}(K[c_0 p^\infty]/K).$$

Lemme 6.2.3 *On peut choisir $\hat{\lambda}_\sigma$ de sorte que pour tout $\ell \in S$, $(\hat{\lambda}_\sigma)_\ell \in (O_{c_0})_\ell^*$.*

Preuve: Partant d'un choix arbitraire de $\hat{\lambda}_\sigma$, considérons le O_{c_0}-idéal propre $\hat{\lambda}_\sigma.O_{c_0}$. D'après la proposition1.7.1, il existe un élément $\lambda \in K^*$ tel que $\lambda\hat{\lambda}_\sigma.O_{c_0}$ soit un idéal *premier* à S. On a alors $(\lambda\hat{\lambda}_\sigma.O_{c_0})_\ell = (O_{c_0})_\ell$ pour tout $\ell \in S$, donc $(\lambda\hat{\lambda}_\sigma)_\ell \in (O_{c_0})_\ell^*$. On peut alors remplacer $\hat{\lambda}_\sigma$ par $\lambda\hat{\lambda}_\sigma$, car $[K[c_0 p^\infty]/K, \star]$ est trivial sur K^*. □

On fait ce choix, et on suppose donc que :

$$\forall \sigma \in \mathcal{R}, \forall \ell \in S : \quad (\hat{\lambda}_\sigma)_\ell \in (O_{c_0})_\ell^*. \tag{6.1}$$

On étend alors σ à K^{ab} en posant : $\sigma = [K^{\mathrm{ab}}/K, \hat{\lambda}_\sigma]$.

6.2.5 Description de $\mathcal{L}$

Avec les notations de la section 5.2,

$$\mathcal{L} \subset X_p(E,N) \subset X^{(S)}(E,N) \subset X_0(N)(\overline{F}).$$

Rappelons que l'on a défini une bijection (5.3.1) :

$$\begin{array}{rrcl} H: & K^* \setminus \{T_1 \subset_N T_2 \subset \hat{V}(E)\} & \xrightarrow{\simeq} & X(E,N) \subset X_0(N)(\overline{F}) \\ & [T_1 \subset_N T_2] & \longmapsto & [E/T_1 \to E/T_2] \end{array}$$

Au demeurant, nous allons travailler uniquement *en dehors* de S, ce qui est loisible dans la mesure où les éléments $\ell \in S$ sont premiers à pN. Si $T_1 \subset_N T_2$ est une N-inclusion de réseau de $\hat{V}^{(S)}(E)$, nous noterons donc :

$$[E/T_1 \to E/T_2] = [E/T_1^e \to E/T_2^e],$$

où l'on rappelle que pour un réseau T de $\hat{V}^{(S)}(E)$, T^e est l'unique réseau de $\hat{V}(E)$ coincidant avec $\hat{T}(E)$ en S, et avec T en dehors de S.

Soit $T_1 = \hat{T}^{(S)}(E)$ le module de Tate de E, et $T_1 \subset_{N'} T'$ le réseau de $\hat{V}^{(S)}(E)$ correspondant au sous-groupe $C_{N'}$ de $E(F^{\mathrm{ab}})[N']$ via l'isomorphisme :

$$\hat{V}^{(S)}(E)/\hat{T}^{(S)}(E) \xrightarrow{\simeq} E(F^{\mathrm{ab}})_{\mathrm{non}-S-\mathrm{torsion}}$$

On *choisit* également une structure de niveau p^i, c'est-à-dire un réseau T_2 de $\hat{V}^{(S)}(E)$ tel que $T' \subset_{p^i} T_2$, de sorte que $T_1 \subset_N T_2$.

Cela étant, on dira d'une N-inclusion $T_1' \subset_N T_2'$ de réseaux de $\hat{V}(E)$ (ou de $\hat{V}^{(S)}(E)$) qu'elle est *normale* si :

$$\forall q \neq p: \quad (T_1')_q = (T_1)_q \text{ et } (T_2')_q = (T_2)_q. \tag{6.2}$$

Le mot "normal" abrège l'expression véritablement correcte, qui serait : ... sous forme normale en p relativement à $T_1 \subset_N T_2$.

Pour se donner une inclusion normale, il suffit donc de se donner une p^i-inclusion $(T_1')_p \subset_{p^i} (T_2')_p$ de réseaux de $V_p(E)$. Par définition, on a finalement :

$$\mathcal{L} = \Big\{[E/T_1' \to E/T_2'] \mid T_1' \subset_N T_2' \subset \hat{V}^{(S)}(E) \text{ normale}\Big\} \subset X_0(N)(K[c_0p^\infty]).$$

6.2.6 Paramétrisation de $\mathcal{L}$

Choisissons une base du $\mathbb{Z}_p$-module libre de rang deux $T_p(E)$, c'est-à-dire un isomorphisme

$$\xi : \mathbb{Z}_p^2 \xrightarrow{\simeq} T_p(E). \tag{6.3}$$

On note également

$$\xi : \mathbb{Q}_p^2 \xrightarrow{\simeq} V_p(E)$$

l'isomorphisme obtenu par tensorisation de (6.3) avec $\mathbb{Q}_p$. L'action de K_p sur $V_p(E)$ induit alors un plongement

$$\iota : K_p \hookrightarrow M_2(\mathbb{Q}_p)$$

caractérisé par : si $v \in \mathbb{Q}_p^2$ et $\lambda \in K_p$,

$$\lambda\xi(v) = \xi(\iota(\lambda) \cdot v).$$

Il est bien connu que $GL_2(\mathbb{Q}_p)$ agit *transitivement* (par multiplication à gauche) sur l'ensemble des inclusions de $\mathbb{Z}_p$-réseaux complets $N_1 \subset_{p^i} N_2 \subset \mathbb{Q}_p^2$. Ceci nous permet de paramétrer les N-inclusions normales de $\hat{V}^{(S)}(E)$ de la manière suivante : à un élément $g \in GL_2(\mathbb{Q}_p)$, on associe l'unique N-inclusion normale de $\hat{V}^{(S)}(E)$ dont la p-composante est

$$\xi\left(g \cdot \xi^{-1}\left((T_1)_p \subset_{p^i} (T_2)_p\right)\right)$$

On note symboliquement $gT_1 \subset_N gT_2$ cette inclusion.

On obtient ainsi une application *surjective* :

$$\begin{array}{cccc} \mathcal{H}: & GL_2(\mathbb{Q}_p) & \twoheadrightarrow & \mathcal{L} \subset X_0(N)(K[c_0p^\infty]) \\ & g & \mapsto & [E/gT_1 \to gT_2]. \end{array}$$

6.2.7 Action de Galois

D'après la proposition 5.3.1, pour tout $\sigma \in \mathcal{R}$, on a

$$\sigma\mathcal{H}(g) = [E/\hat{\lambda}_\sigma^{-1}(gT_1)^e \to E/\hat{\lambda}_\sigma^{-1}(gT_2)^e].$$

Notons que si $\ell \in S$, $(gT_1)_\ell = (gT_2)_\ell = T_\ell(E)$, car $gT_1 \subset_N gT_2$ est normale, et $\ell \nmid pN$. Mais on a choisi $\hat{\lambda}_\sigma$ de sorte que $\hat{\lambda}_{\sigma,\ell} \in (O_{c_0})_\ell^* = (O_c)_\ell^*$ (cf 6.1), donc

$$\left(\hat{\lambda}_\sigma^{-1}(gT_i)^e\right)_\ell = \hat{\lambda}_{\sigma,\ell}^{-1} T_\ell(E) = T_\ell(E),$$

et

$$\hat{\lambda}_\sigma^{-1}\left(gT_1 \subset gT_2\right)^e = \left(\hat{\lambda}_\sigma^{-1}\left(gT_1 \subset gT_2\right)\right)^e.$$

Ainsi, avec nos conventions d'écriture :

$$\sigma\mathcal{H}(g) = [E/\hat{\lambda}_\sigma^{-1}gT_1 \to E/\hat{\lambda}_\sigma^{-1}gT_2]$$

Notons cependant que $\hat{\lambda}_\sigma^{-1}\left(gT_1 \subset gT_2\right)$ n'est pas nécessairement sous forme normale.

6.2.8 Réduction

Pour $\ell \in S$, soient :
- $\widetilde{E}_{/k(\ell)}$ la réduction de E en la place v_ℓ^0 de F,
- $R(\ell) = \mathrm{End}_{k(\ell)}(\widetilde{E})$ son anneau d'endomophisme,
- $B(\ell) = \mathrm{End}^0_{k(\ell)}(\widetilde{E}) = R(\ell) \otimes \mathbb{Q}$,
- $T_q(\widetilde{E})$, $\hat{T}(\widetilde{E})$ ses modules de Tate,
- $V_q(\widetilde{E}) = T_q(\widetilde{E}) \otimes \mathbb{Q}$ et $\hat{V}(\widetilde{E}) = \hat{T}(\widetilde{E}) \otimes \mathbb{Q}$.

$E_{/F}$ ayant bonne réduction en ℓ, et multiplication complexe par O_c, avec $p \mid c$ premier à ℓ, il résulte de la proposition 3.3.4 que $R(\ell) = \mathrm{End}_{\overline{k(\ell)}}(\widetilde{E})$ est un ordre maximal dans le corps de quaternions $B(\ell) = \mathrm{End}_{\overline{k(\ell)}}(\widetilde{E})$, ramifié exactement en ℓ et ∞.

Il résulte d'autre part de la proposition 3.3.5 que, comme dans la section 5.4, la réduction en la place v_ℓ^{ab} de F^{ab} induit un isomorphisme :

$$\begin{array}{ccc} \hat{T}^{(\ell)}(E) & \xrightarrow{\simeq} & \hat{T}^{(\ell)}(\widetilde{E}) \\ t & \longmapsto & \widetilde{t} \end{array}$$

A fortiori, on obtient des isomorphismes :

$$\begin{array}{ccc} \hat{T}^{(S)}(E) & \xrightarrow{\simeq} & \hat{T}^{(S)}(\widetilde{E}) \\ \hat{V}^{(S)}(E) & \xrightarrow{\simeq} & \hat{V}^{(S)}(\widetilde{E}) \end{array}$$

Si $T_1' \subset_N T_2'$ est une N-inclusion de réseaux de $\hat{V}^{(S)}(E)$, on note $\widetilde{T}_1' \subset_N \widetilde{T}_2'$ son image dans $\hat{V}^{(S)}(\widetilde{E})$. La proposition 5.4.1 permet alors d'écrire :

$$\mathrm{red}_{v_\ell^{\mathrm{ab}}}([E/T_1' \to E/T_2']) = [\widetilde{E}/\widetilde{T}_1' \to \widetilde{E}/\widetilde{T}_2'] \in X_0(N)(\overline{k(\ell)}).$$

En particulier, si $\sigma \in \mathcal{R}$ et $g \in GL_2(\mathbb{Q}_p)$, on obtient :

$$\mathrm{red}_\ell(\sigma.\mathcal{H}(g)) = [\widetilde{E}/(\hat{\lambda}_\sigma^{-1} g T_1)^{\sim} \to \widetilde{E}/(\hat{\lambda}_\sigma^{-1} g T_2)^{\sim}] \in X_0(N)(k(\ell)).$$

Autrement dit, le point $\mathrm{red}_\ell(\sigma.\mathcal{H}(g))$ correspond à l'inclusion de réseaux :

$$\left(\hat{\lambda}_\sigma^{-1} g T_1 \subset_N \hat{\lambda}_\sigma^{-1} g T_2\right)^{\sim} = \hat{\lambda}_\sigma^{-1}\left((gT_1)^{\sim} \subset_N (gT_2)^{\sim}\right) \subset \hat{V}^{(S)}(\widetilde{E}).$$

6.2.9 Description de $X_0^{\mathrm{ss}}(N)(k(\ell))$

Nous allons utiliser l'inclusion $\hat{T}^{(S)}(\widetilde{E}) = \widetilde{T_1} \subset_N \widetilde{T_2}$ de réseaux de $\hat{V}^{(S)}(\widetilde{E})$ pour normaliser la bijection de la proposition 5.5.5. Soit donc $R^0(\ell) \subset R(\ell)$ l'ordre d'Eichler associé à $\widetilde{T_1} \subset_N \widetilde{T_2}$. Il est caratérisé par les conditions locales suivantes :

$$\forall q : \quad \left(R^0(\ell)\right)_q = \begin{cases} R(\ell)_q & \text{si } q \in S \\ \left\{x \in B(\ell)_q \mid x(\widetilde{T}_1)_q \subset (\widetilde{T}_1)_q \text{ et } x(\widetilde{T}_2)_q \subset (\widetilde{T}_2)_q\right\} & \text{si } q \notin S \end{cases}$$

En particulier,

$$\left(R^0(\ell)\right)_q = R(\ell)_q \quad \text{si } q \nmid pN,$$

et $\left(R^0(\ell)\right)_p$ est un ordre d'Eichler de niveau p^i dans $B(\ell)_p$.

Posons $\mathfrak{R}^0_\ell(A) = A \otimes_{\mathbb{Z}} R^0(\ell)$ pour tout anneau commutatif A. La bijection de la proposition 5.5.5 s'écrit alors :

$$\begin{array}{rcl} \mathfrak{R}^{0*}_\ell(\mathbb{Z}[1/p]) \setminus \mathfrak{R}^{0*}_\ell(\mathbb{Q}_p)/\mathfrak{R}^{0*}_\ell(\mathbb{Z}_p) & \xrightarrow{\simeq} & X_0^{\mathrm{ss}}(N)(k(\ell)) \\ [b_p] & \longmapsto & [\widetilde{E}/b_p\widetilde{T_1} \to \widetilde{E}/b_p\widetilde{T_2}] \end{array}$$

Ou encore :

$$\mathfrak{R}^{0*}_\ell(\mathbb{Z}[1/p]) \setminus B(\ell)^*_p/\left(R^0(\ell)\right)^*_p \xrightarrow{\simeq} X_0^{\mathrm{ss}}(N)(k(\ell)).$$

6.2.10 Retour à $GL_2(\mathbb{Q}_p)$

Nous voulons réécrire cette bijection en utilisant les isomorphismes

$$\xi : \mathbb{Q}_p^2 \xrightarrow{\simeq} V_p(E),$$

et

$$\begin{array}{rcl} V_p(E) & \xrightarrow{\simeq} & V_p(\widetilde{E}) \\ t & \longmapsto & \widetilde{t} \end{array}$$

Ils induisent en effet un isomorphisme

$$\rho_\ell : B(\ell)_p \to M_2(\mathbb{Q}_p),$$

caractérisé par : pour $b \in B(\ell)_p$ et $x \in \mathbb{Q}_{p^2}$,

$$b \cdot \widetilde{\xi(x)} = (\rho_\ell(b)x)\widetilde{\ }.$$

Notons que $\rho_\ell(R(\ell))$ est un ordre maximal de $M_2(\mathbb{Q}_p)$, et stabilise $\mathbb{Z}_p^2$, donc $\rho_\ell(R(\ell)) = M_2(\mathbb{Z}_p)$. D'autre part, avec ces définitions, il est clair que la p-composante des réseaux $(gT_i)\widetilde{\ }$ $(i = 1, 2)$ de $\hat{V}(\widetilde{E})$ n'est autre que :

$$(gT_i)\widetilde{\ }_p = \rho_\ell^{-1}(g) \cdot \widetilde{T}_i.$$

Enfin, ρ_ℓ est compatible avec les plongements $K_p \hookrightarrow B(\ell)_p$ et $\iota : K_p \hookrightarrow M_2(\mathbb{Q}_p)$: si $\lambda \in K_p$,

$$\rho_\ell(\lambda) = \iota(\lambda). \tag{6.4}$$

On pose alors :

$$\begin{array}{rcl} \Gamma(\ell) & = & \rho_\ell\left(\mathfrak{R}^{0*}_\ell(\mathbb{Z}[1/p])\right) \subset GL_2(\mathbb{Q}_p) \\ M(\ell) & = & \rho_\ell\left(\left(R^0(\ell)\right)_p\right) \end{array}$$

de sorte que $M(\ell)$ est un ordre d'Eichler de niveau p^i dans $M_2(\mathbb{Z}_p)$, et $\Gamma(\ell)$ un sous-groupe de $GL_2(\mathbb{Q}_p)$. La bijection de la section précédente devient (pour $b_p \in B(\ell)_p^*$) :

$$\begin{array}{rrcl} \theta_\ell : & \Gamma(\ell) \backslash GL_2(\mathbb{Q}_p)/M(\ell)^* & \xrightarrow{\simeq} & X_0^{\mathrm{ss}}(N)(k(\ell)) \\ & [\rho_\ell(b_p)] & \longmapsto & [\widetilde{E}/b_p\widetilde{T}_1 \to \widetilde{E}/b_p\widetilde{T}_2] \end{array}$$

6.2.11 Réduction et action de Galois

Nous voulons maintenant réécrire le point $\mathrm{red}_\ell\,(\sigma\mathcal{H}(g) \in X_0^{\mathrm{ss}}(N)(k(\ell))$ en utilisant cette nouvelle bijection. Rappelons que l'on a déjà calculé :

$$\mathrm{red}_\ell(\sigma.\mathcal{H}(g)) = \left[\widetilde{E}/\left(\hat{\lambda}_\sigma^{-1}(gT_1)\widetilde{\ }\right) \to \widetilde{E}/\left(\hat{\lambda}_\sigma^{-1}(gT_2)\widetilde{\ }\right)\right] \in X_0(N)\,(k(\ell))\,.$$

Le problème est que l'inclusion $\hat{\lambda}_\sigma^{-1}\,(gT_1 \subset_N gT_2)\widetilde{\ }$ de réseaux de $\hat{V}^{(S)}(\widetilde{E})$ n'est pas sous forme normale. On veut donc la ramener sous forme normale : le fait que ce soit possible est précisément le contenu du corollaire 5.5.6.

Mais travaillons soigneusement : d'après ce corollaire, joint à la proposition 5.2.1, il existe un élément $b_{\ell,\sigma} \in B(\ell)^*$, entier relativement à $R(\ell)$ en toutes les places de S, et tel que l'inclusion

$$b_{\ell,\sigma}\hat{\lambda}_\sigma^{-1}\left(\widetilde{T_1} \subset_N \widetilde{T_2}\right)$$

soit sous forme normale. La condition

$$\forall \ell' \in S : \quad b_{\ell,\sigma} \in (R(\ell))_{\ell'}^*\,,$$

signifie que, pour toute inclusion $U_1 \subset_N U_2$ de réseaux de $\hat{V}^{(S)}(\widetilde{E})$, les inclusions $U_1 \subset_N U_2$ et $b_{\ell,\sigma}\,(U_1 \subset_N U_2)$ définissent le même point de $X_0^{\mathrm{ss}}(N)(k(\ell))$ (cf. 5.2.1).

Pour *tout* élément $g \in GL_2(\mathbb{Q}_p)$, l'inclusion

$$b_{\ell,\sigma}\hat{\lambda}_\sigma^{-1}\,(gT_1 \subset_N gT_2)\widetilde{\ }$$

est alors tout d'abord sous forme normale. En particulier, on peut calculer cette inclusion en n'utilisant que la p-composante de l'idèle $b_{\sigma,\ell}\hat{\lambda}_\sigma^{-1}$:

$$\begin{aligned} b_{\ell,\sigma}\hat{\lambda}_\sigma^{-1}\left(g\widetilde{T_1} \subset_N g\widetilde{T_2}\right) &= b_{\ell,\sigma}(\hat{\lambda}_{\sigma,p}^{-1})\left(g\widetilde{T_1} \subset_N g\widetilde{T_2}\right) \\ &= b_{\ell,\sigma}(\hat{\lambda}_{\sigma,p}^{-1})\rho_\ell^{-1}(g)\left(\widetilde{T_1} \subset_N \widetilde{T_2}\right) \end{aligned}$$

où l'on considère $b_{\sigma,\ell}$ comme un élément de $B(\ell)_p^* \supset B(\ell)^*$. D'autre part, cette inclusion maintenant normale définit le *même* point que $\hat{\lambda}_\sigma^{-1}\left(g\widetilde{T_1} \subset_N g\widetilde{T_2}\right)$, c'est à dire

$$\mathrm{red}_\ell\,(\sigma\mathcal{H}(g)) = [\widetilde{E}/b_{\ell,\sigma}(\hat{\lambda}_{\sigma,p}^{-1})\rho_\ell^{-1}(g)\widetilde{T}_1 \to \widetilde{E}/b_{\ell,\sigma}(\hat{\lambda}_{\sigma,p}^{-1})\rho_\ell^{-1}(g)\widetilde{T}_2] \in X_0(N)(k(\ell)).$$

Il ne nous reste plus qu'à exprimer ceci grâce à θ_ℓ. Comme

$$\rho_\ell\left(b_{\ell,\sigma}(\hat{\lambda}_{\sigma,p}^{-1})\rho_\ell^{-1}(g)\right) = \rho_\ell(b_{\ell,\sigma})\iota(\hat{\lambda}_{\sigma,p}^{-1})g,$$

on a donc :

$$\theta_\ell\left(\rho_\ell(b_{\ell,\sigma})\iota(\hat{\lambda}_{\sigma,p}^{-1})g\right) = \mathrm{red}_\ell\left(\sigma\mathcal{H}(g)\right)$$

6.2.12 Un diagramme commutatif

Posons

$$\alpha_{\ell,\sigma} = \rho_\ell(b_{\ell,\sigma})\iota(\hat{\lambda}_{\sigma,p}^{-1}) \in GL_2(\mathbb{Q}_p),$$

de sorte que

$$\forall g \in GL_2(\mathbb{Q}_p): \quad \theta_\ell\left(\alpha_{\ell,\sigma}g\right) = \mathrm{red}_\ell\left(\sigma\mathcal{H}(g)\right).$$

D'autre part, pour tous éléments $x, x' \in GL_2(\mathbb{Q}_p)$,

$$\Gamma(\ell)\alpha_{\ell,\sigma}xM(\ell)^* = \Gamma(\ell)\alpha_{\ell,\sigma}x'M(\ell)^* \quad \Longleftrightarrow \quad \Gamma_{\ell,\sigma}xM(\ell)^* = \Gamma_{\ell,\sigma}x'M(\ell)^*,$$

où

$$\Gamma_{\ell,\sigma} = \alpha_{\ell,\sigma}^{-1}\Gamma(\ell)\alpha_{\ell,\sigma}.$$

Autrement dit, la multiplication à gauche par $\alpha_{\ell,\sigma}$ dans $GL_2(\mathbb{Q}_p)$ induit une bijection :

$$\Gamma_{\ell,\sigma} \setminus GL_2(\mathbb{Q}_p)/M(\ell)^* \xrightarrow{\simeq} \Gamma(\ell) \setminus GL_2(\mathbb{Q}_p)/M(\ell)^*.$$

Composant celle-ci avec θ_ℓ, on obtient une bijection :

$$\theta_{\ell,\sigma}:\ \Gamma_{\ell,\sigma} \setminus GL_2(\mathbb{Q}_p)/M(\ell)^* \xrightarrow{\simeq} X_0^{\mathrm{ss}}(N)(k(\ell)).$$

telle que $\theta_{\ell,\sigma}(g) = \mathrm{red}_\ell\left(\sigma.\mathcal{H}(g)\right)$ pour tout $g \in GL_2(\mathbb{Q}_p)$.

Soit enfin θ le produit des bijections $\theta_{\ell,\sigma}$:

$$\theta: \prod_{\ell,\sigma\in S\times\mathcal{R}} \Gamma_{\ell,\sigma} \setminus GL_2(\mathbb{Q}_p)/M(\ell)^* \longrightarrow \prod_{\ell\in S}\left(X_0^{\mathrm{ss}}(N)(k(\ell))\right)^{\mathcal{R}},$$

et Δ la "diagonale" :

$$\Delta: GL_2(\mathbb{Q}_p) \longrightarrow \prod_{\ell,\sigma\in S\times\mathcal{R}} \Gamma_{\ell,\sigma} \setminus GL_2(\mathbb{Q}_p)/M(\ell)^*. \tag{6.5}$$

Alors, pour tout $g \in GL_2(\mathbb{Q}_p)$:

$$\mathrm{RED}(\mathcal{H}(g)) = \theta(\Delta(g))$$

Il en résulte que la surjectivité de RED (théorème 6.2.1) est équivalente à la surjectivité de Δ.

6.2.13 De GL_2 à PSL_2

Examinons plus en détail ce qu'est $\Gamma_{\ell,\sigma}$. A savoir :

$$\begin{aligned}\Gamma_{\ell,\sigma} &= \alpha_{\ell,\sigma}^{-1}\Gamma(\ell)\alpha_{\ell,\sigma}\\ \Gamma(\ell) &= \rho_\ell\left(\mathfrak{R}_\ell^{0*}(\mathbb{Z}[1/p])\right)\\ \mathfrak{R}_\ell^{0*}(\mathbb{Z}[1/p]) &= \left(R^0(\ell)[1/p]\right)^*\end{aligned}$$

et $R^0(\ell)$ est un ($\mathbb{Z}$-)ordre d'Eichler de niveau N dans le corps de quaternion $B(\ell)$.

Lemme 6.2.4 $\pm p^{\mathbb{Z}} \subset \Gamma_{\ell,\sigma}$ *et* $\det(\Gamma_{\ell,\sigma}) = p^{\mathbb{Z}}$ *pour tout* $\ell \in S$, $\sigma \in \mathcal{R}$.

Preuve: Il suffit de voir que $\pm p^{\mathbb{Z}} \subset \left(R^0(\ell)[1/p]\right)^*$(c'est évident), et que

$$\mathrm{nr}\left(R^0(\ell)[1/p]\right)^* = p^{\mathbb{Z}},$$

ce qui résulte de [39, p. 90]. □

D'un autre côté, $M(\ell) \subset M_2(\mathbb{Z}_p)$ est un ($\mathbb{Z}_p-$)ordre d'Eichler de niveau p^i dans $M_2(\mathbb{Q}_p)$, et en particulier,

$$\mathbb{Z}_p^* \subset M(\ell)^* \quad \text{et} \quad \det(M(\ell)^*) = \mathbb{Z}_p^*.$$

Il en résulte déjà que

$$\Gamma_{\ell,\sigma} \setminus GL_2(\mathbb{Q}_p)/M(\ell)^* = \Gamma_{\ell,\sigma} \setminus GL_2(\mathbb{Q}_p)/\mathbb{Q}_p^* M(\ell)^*.$$

De plus, si $g \in GL_2(\mathbb{Q}_p)$, il existe d'abord un élément $\gamma \in \Gamma_{\ell\,\sigma}$ tel que $\det(\gamma g) \in \mathbb{Z}_p^*$, puis un élément $m \in M(\ell)^*$ tel que $\det(\gamma g m) = 1$. En d'autres termes :

$$PSL_2(\mathbb{Q}_p) \to \Gamma_{\ell,\sigma} \setminus GL_2(\mathbb{Q}_p)/\mathbb{Q}_p^* M(\ell)^*$$

est *surjective.*

Soient g_1 et g_2 deux éléments de $SL_2(\mathbb{Q}_p)$ tels que $\Gamma_{\ell,\sigma} g_1 M(\ell)^* = \Gamma_{\ell,\sigma} g_2 M(\ell)^*$. Soient $\gamma \in \Gamma_{\ell,\sigma}$ et $m \in M(\ell)^*$ tels que $g_2 = \gamma g_1 m$; alors $\det(\gamma)\det(m) = 1$ donc $\det(m) \in p^{\mathbb{Z}} \cap \mathbb{Z}_p^* = 1$, et également $\det(\gamma) = 1$.

Ainsi, notant :

$$\begin{aligned}\Gamma_{\ell,\sigma}^1 &= \left(\Gamma_{\ell,\sigma} \cap SL_2(\mathbb{Q}_p)\right)/\{\pm 1\},\\ M(\ell)^1 &= \left(M(\ell) \cap SL_2(\mathbb{Q}_p)\right)/\{\pm 1\},\end{aligned}$$

(de sorte que $\Gamma_{\ell,\sigma}^1$ et $M(\ell)^1$ sont des sous-groupes de $PSL_2(\mathbb{Q}_p)$), on obtient :

$$\Gamma_{\ell,\sigma}^1 \setminus PSL_2(\mathbb{Q}_p)/M(\ell)^1 \xrightarrow{\simeq} \Gamma_{\ell,\sigma} \setminus GL_2(\mathbb{Q}_p)/\mathbb{Q}_p^* M(\ell)^*.$$

Par conséquent, la surjectivité de l'application Δ de (6.5) (et donc aussi celle de RED) est impliquée par la surjectivité de l'application "diagonale" :

$$\Delta : PSL_2(\mathbb{Q}_p) \to \prod_{\ell,\sigma \in S \times \mathcal{R}} \Gamma_{\ell,\sigma}^1 \setminus PSL_2(\mathbb{Q}_p)/M(\ell)^1. \tag{6.6}$$

6.2.14 Un peu de topologie

Posons $G = PSL_2(\mathbb{Q}_p)$. C'est un groupe de Lie p-adique, et c'est un groupe simple ([12, XIII 8]). $M(\ell)^1$ en est un sous-groupe ouvert et compact, et $\Gamma^1_{\ell,\sigma}$ un sous-groupe discret et cocompact ([39, IV Theo 1.1]).

Posons :

$$\begin{aligned}\Gamma^1 &= \prod_{\ell,\sigma\in S\times\mathcal{R}} \Gamma^1_{\ell,\sigma}\\ M^1 &= \prod_{\ell\in S} M(\ell)^{\mathcal{R}}\end{aligned}$$

Γ^1 est donc un sous-groupe discret et cocompact de $G^{S\times\mathcal{R}}$, et M^1 un sous-groupe ouvert. Soit $\Delta : G \to G^{S\times\mathcal{R}}$ la diagonale. Alors :

Proposition 6.2.5 *Si $\Gamma^1\Delta(G)$ est dense dans $G^{S\times\mathcal{R}}$, l'application diagonale*

$$\overline{\Delta} : G \to \Gamma^1 \setminus G^{S\times\mathcal{R}}/M^1$$

est surjective.

Preuve: Soit $x = [g] \in \Gamma^1 \setminus G^{S\times\mathcal{R}}/M^1$, avec $g \in G^{S\times\mathcal{R}}$. Comme M^1 est ouvert et non vide, et $\Gamma^1\Delta(G)$ est dense dans $G^{S\times\mathcal{R}}$, l'intersection $\Gamma^1\Delta(G) \cap gM_1$ est non vide. Si

$$gm = \gamma\Delta(g') \quad m \in M_1, g' \in G$$

est un élément de cette intersection, alors $g = \gamma\Delta(g')m^{-1} \in \Gamma^1\Delta(g')M^1$, donc $\overline{\Delta}(g') = x$. □

6.3 Un lemme sur les groupes simples non commutatifs

Si G est un groupe et S un ensemble fini, on note $G^S = \prod_{s\in S} G$ et, pour $s \in S$, $p_s : G^S \to G$ la projection sur le s^{e} facteur. Si $S' \subset S$, on identifie $G^{S'}$ avec le sous-groupe correspondant de G^S :

$$G^{S'} = \left\{x \in G^S \mid p_{s'}(x) = 1\,\forall s' \in S \setminus S'\right\}.$$

On note alors $\Delta^{S'} : G \to G^{S'} \subset G^S$ la diagonale de $G^{S'}$ dans G^S. Pour $S' = S$, on écrit aussi $\Delta = \Delta^S$.

Définition *On dit qu'un sous-groupe H de G^S est un* produit de diagonales *s'il existe un ensemble fini I, et des sous-ensembles* disjoints $(S_i)_{i\in I}$ *de S tels que :*

$$H = \prod_{i\in I} \Delta^{S_i}(G) \subset G^S$$

Notons que le produit défini ci-dessus est commutatif. Il est clair que tout produit de diagonales est normalisé par $\Delta(G)$. Inversement, on a le résultat suivant (qui précise [38, Lemma 5.10]) :

Proposition 6.3.1 *Les conditions suivantes sont équivalentes :*

1. *G est* simple *et* non commutatif.
2. *Tout sous-groupe $H \subset G^S$ normalisé par $\Delta(G)$ est un produit de diagonales.*

Preuve: 1) $\Rightarrow$ 2) On raisonne par récurrence sur $n = \#S$. Le cas $n = 1$ étant trivial, on suppose donc que $n > 1$, et que le résultat est vrai pour tout ensemble S' de cardinal $\#S' < n$.

Pour $S' \subset S$, notons

$$H^{S'} = H \cap G^{S'}.$$

C'est un sous-groupe de G^S normalisé par $\Delta(G)$, et un sous-groupe de $G^{S'}$ normalisé par $\Delta^{S'}(G)$. Si $S' \neq S$, l'hypothèse de récurrence implique alors que $H^{S'}$ est un produit de diagonales dans $G^{S'}$, donc aussi dans G^S. Notons d'autre part que pour tout $s \in S$, $p_s(H^{S'})$ est un sous-groupe de G normalisé par $p_s(\Delta^S(G)) = G$, donc égal à 1 ou G puisque G est simple.

S'il existe $s \in S$ tel que $p_s(H) = 1$, alors $H = H^{S\setminus\{s\}}$ est un produit de diagonales. On peut donc supposer :

$$\forall s \in S : \quad p_s(H) = G. \tag{6.7}$$

Soit alors S_0 un sous-ensemble *minimal* de S tel que $H^{S_0} \neq 1$.

Supposons d'abord que $S_0 \neq S$, choisissons un élément $s_0 \in S_0$, et posons $S_1 = S \setminus \{s_0\}$. L'hypothèse de récurrence garantit alors que H^{S_1} et H^{S_0} sont des produits de diagonales, et la minimalité de S_0 implique que $H^{S_0} = \Delta^{S_0}(G)$. Soit $S_2 \subset S_1$ le support d'une diagonale de H^{S_1} :

$$\Delta^{S_2}(G) \subset H^{S_1} \subset H.$$

G étant non commutatif, il existe $g, g' \in G^2$ tel que $gg' \neq g'g$; posons

$$x = \Delta^{S_0}(g)\Delta^{S_2}(g')\Delta^{S_0}(g^{-1})\Delta^{S_2}(g'^{-1}) \in H,$$

de sorte que :

$$p_s(x) = \left\{ \begin{array}{lcl} gg'(g'g)^{-1} & \neq & 1 \\ gg^{-1} & = & 1 \\ g'g'^{-1} & = & 1 \\ 1 & = & 1 \end{array} \right. \text{si} \left\{ \begin{array}{l} s \in S_0 \cap S_2 \\ s \in S_0 \setminus S_2 \\ s \in S_2 \setminus S_1 \\ s \in S \setminus (S_0 \cup S_2) \end{array} \right.$$

Donc $x \in H^{S_0 \cap S_2}$, et $x \neq 1$ si $S_0 \cap S_2 \neq \emptyset$. Comme $S_0 \cap S_2 \subsetneq S_0$, la minimalité de S_0 implique ainsi que $S_0 \cap S_2 = \emptyset$.

Il en résulte que pour tout $x \in H$ et tout $s \in S_0$, posant $g = p_{s_0}(x)$, on a

$$p_s\left(\Delta^{S_0}\left(g^{-1}\right)x\right) = 1,$$

donc

$$x = \Delta^{S_0}(g) \times \Delta^{S_0}\left(g^{-1}\right) x \text{ avec } \Delta^{S_0}\left(g^{-1}\right) x \in H^{S_0^c}$$

où S_0^c est le complémentaire de S_0 dans S. En d'autres termes,

$$H = H^{S_0} H^{S_0^c}$$

et l'hypothèse de récurrence implique que H est un produit de diagonales.

Supposons ensuite que $S_0 = S$, ce qui signifie

$$\forall S' \subsetneq S : \quad H^{S'} = 1. \tag{6.8}$$

En particulier, pour tout $s \in S$, $p_s |_H \colon H \to G$ est surjective par (6.7) et injective par (6.8), donc bijective. Fixons $s_0 \in S$, et soit $f = (p_{s_0}) |_H^{-1} \colon G \to H$, de sorte que $f(G) = H$. Pour tout $s \in S$, soit

$$\delta_s = p_s \circ f : G \to H \to G.$$

C'est un isomorphisme de groupe.

Soient g et g' deux éléments de G, et $h' = f(g') \in H$. H étant normalisé par la diagonale $\Delta(G)$,

$$\Delta(g^{-1}) h' \Delta(g) \in H.$$

Mais

$$p_{s_0}\left(\Delta(g^{-1}) h' \Delta(g)\right) = g^{-1} g' g,$$

donc

$$f(g^{-1} g' g) = \Delta(g^{-1}) f(g') \Delta(g),$$

Il en résulte que pour tout $s \in S$,

$$\begin{aligned}
\delta_s(g)^{-1} \delta_s(g') \delta_s(g) &= \delta_s(g^{-1} g' g) \\
&= p_s \circ f(g^{-1} g' g) \\
&= p_s\left(\Delta(g^{-1}) f(g') \Delta(g)\right) \\
&= g^{-1} \delta_s(g') g,
\end{aligned}$$

Donc

$$\left(g \delta_s(g)^{-1}\right) \delta_s(g') = \delta_s(g') \left(g \delta_s(g)^{-1}\right).$$

En particulier, comme δ_s est surjective, $g\delta_s(g)^{-1}$ est dans le centre de G. G étant simple et non commutatif, on a donc $g = \delta_s(g)$ pour tout $s \in S$, c'est-à-dire $f = \Delta$, donc $H = \Delta(G)$.

2) $\Rightarrow$ 1) Tout sous-groupe normal H de G est un produit de diagonales, donc égal à 1 ou G : G est donc simple. Si G était commutatif, on aurait donc $G \simeq \mathbb{F}_q$ comme groupe, avec $q = \#G$ premier. Mais si $q \neq 2$, le sous-groupe H de $\mathbb{F}_q^2$ engendré par $(1, 2)$ n'est pas un produit de diagonales ; si $q = 2$, le sous-groupe H de $\mathbb{F}_q^3$ engendré par $(1, 1, 0)$ et $(0, 1, 1)$ n'est pas un produit de diagonales. Donc H n'est pas commutatif. $\square$

6.4 Une application d'un théorème de M. Ratner

6.4.1 Le théorème de Ratner

Soit G un groupe de Lie p-adique localement compact. On dit d'un sous-groupe *discret* $\Gamma \subset G$ que c'est un *réseau* de G s'il existe une mesure finie sur $\Gamma \setminus G$ qui est invariante par translation à droite. Un sous-ensemble $A \subset \Gamma \setminus G$ est *homogène* s'il existe $[x] \in \Gamma \setminus G$, et un sous-groupe fermé $H \subset G$, tels que : $xHx^{-1} \cap \Gamma$ est un réseau dans xHx^{-1}, et $A = [x]H$.

Si $\varphi : (\mathbb{Q}_p, +) \to G$ est un homomorphisme de groupe de Lie tel que $\frac{d\varphi(t)}{dt}(0) \neq 0$, on dit de l'ensemble $\{\varphi(t) \mid t \in \mathbb{Q}_p^*\}$ que c'est un *sous-groupe à un paramètre* de G. Un élément $g \in G$ est dit *Ad-unipotent* si le morphisme induit sur les algèbres de Lie

$$\mathrm{Ag}_g : \mathrm{Lie}(G) \to \mathrm{Lie}(G)$$

est un automorphisme *unipotent* de $\mathrm{Lie}(G)$, c'est-à-dire, si $1 - \mathrm{Ad}_g$ est un endomorphisme *nilpotent*. Un sous-groupe à un paramètre est dit *Ad-unipotent* si ses éléments le sont.

G est dit *Ad-régulier* si le noyau de la représentation adjointe $\mathrm{Ad}_\star : G \to \mathrm{Aut}(\mathrm{Lie}(G))$ est égal au centre de G : $\ker(\mathrm{Ad}_\star) = Z(G)$. G est *régulier* si de plus l'ordre de ses sous-groupes finis est borné.

Le théorème de M. Ratner dont nous aurons besoin est :

Théorème *[25, Theorem 2] Supposons G régulier. Soit U un sous-groupe de G engendré par des sous-groupes à un paramètre Ad-unipotents de G. Soit Γ un réseau de G. Alors pour tout élément $[x] \in \Gamma \setminus G$, l'adhérence de xU dans $\Gamma \setminus G$ est homogène.*

Plus précisément, nous aurons besoin du corollaire suivant :

Corollaire 6.4.1 *L'adhérence de ΓU dans G est égal à ΓH, pour un sous-groupe fermé H de G contenant U.*

Preuve: Soit $q : G \to \Gamma \setminus G$ la projection. D'après le théorème, $\overline{[1]U}$ est homogène, c'est-à-dire qu'il existe un sous-groupe fermé H' de G tel que $H' \cap \Gamma$ soit un réseau de H' et $\overline{[1]U} = [1]H'$. On a alors

$$\overline{\Gamma U} = q^{-1}(\overline{[1]U}) = q^{-1}([1]H') = \Gamma H'.$$

Soit H l'adhérence du sous-groupe H'' de G engendré par U et H', de sorte que H est un sous-groupe fermé de G contenant U. ΓU étant stable par multiplication à droite par les éléments de U, il en est de même de son adhérence $X = \overline{\Gamma U} = \Gamma H'$, qui est donc stable par multiplication à droite par les éléments de H''. X étant de surcroît fermé, est stable par multiplication à droite par les éléments de $H = \overline{H''}$. Donc

$$X = XH = \Gamma H' H = \Gamma H.$$

□

6.4.2 Vérification des hypothèses

Soient G et PG les groupes de Lie p-adiques :

$$G = SL_2(\mathbb{Q}_p), \quad PG = PSL_2(\mathbb{Q}_p)$$

La projection

$$q : G \to G/\{\pm 1\} = PG$$

est une submersion [31, IV §5 Theo 1], et l'algèbre de Lie de son noyau $\{\pm 1\}$ est triviale, égale au noyau du morphisme $\mathrm{Lie}(q)$ induit par q sur les algèbres de Lie (d'après [31, V §2.4]), donc $\mathrm{Lie}(q)$ est un isomorphisme, et q est étale.

Soit d'autre part $\mathfrak{G}_{/\mathbb{Q}_p}$ le schéma en groupe

$$\mathfrak{G} = SL_{2/\mathbb{Q}_p}.$$

Il est clair que l'algèbre de Lie du *groupe de Lie p-adique* $SL_2(\mathbb{Q}_p)$ (définie dans [31, V §1]), est égale à l'algèbre de Lie du *schéma en groupe* $\mathfrak{G}_{/\mathbb{Q}_p}$, noyau de $\mathfrak{G}(\mathbb{Q}_p[\varepsilon]/\varepsilon^2]) \to \mathfrak{G}(\mathbb{Q}_p)$. Finalement,

$$\begin{aligned}
\mathrm{Lie}(PG) &= \left\{ \begin{pmatrix} 1 + x\varepsilon & y\varepsilon \\ z\varepsilon & 1 + t\varepsilon \end{pmatrix} \mid x, y, z, t \in \mathbb{Q}_p, \quad \det = 1 \right\} \\
&= \left\{ \begin{pmatrix} 1 + x\varepsilon & y\varepsilon \\ z\varepsilon & 1 - x\varepsilon \end{pmatrix} \mid x, y, z \in \mathbb{Q}_p \right\} \\
&\simeq Sl_2(\mathbb{Q}_p).
\end{aligned}$$

Proposition 6.4.2 *Soit $n \geq 1$ un entier, et $\Delta : PG \to PG^n$ la diagonale de PG^n. Alors :*

1. *PG^n est Ad-régulier.*
2. *PG^n est régulier.*
3. *$\Delta(PG)$ est engendré par des sous-groupes à un paramètre Ad-unipotents de G^n.*
4. *Tout sous-groupe discret et cocompact de PG^n est un réseau.*

Preuve: 1) Comme $\ker(\mathrm{Ad}_{PG^n}) = \ker\left((\mathrm{Ad}_{PG})^n\right) = \left(\ker(\mathrm{Ad}_{PG})\right)^n$ et $Z(PG^n) = Z(PG)^n$,

$$PG^n \,\mathrm{est\,Ad-régulier} \iff PG \,\mathrm{est\,Ad-régulier}.$$

Mais $\mathrm{Ad}_G = \mathrm{Ad}_{PG} \circ q$, et

$$q^{-1}\left(Z(PG)\right) = q^{-1}(1) = Z\left(G\right) = \{\pm 1\},$$

donc

$$PG \,\mathrm{est\,Ad-régulier} \iff G \,\mathrm{est\,Ad-régulier}.$$

Il reste donc à voir que G est Ad-régulier. Soit $g \in G$ tel que l'automorphisme intérieur de G défini par g induise l'identité sur $\mathrm{Lie}(G)$. L'automorphisme intérieur du schéma en groupe $\mathfrak{G}_{/\mathbb{Q}_p}$ défini par $g \in \mathfrak{G}(\mathbb{Q}_p)$ induit alors l'identité sur $\mathrm{Lie}\,(\mathfrak{G}(\mathbb{Q}_p))$. D'après [DG, II §6.2.1], cet automorphisme est donc lui-même égal à l'identité, donc $g \in Z(G) = \{\pm 1\}$ et G est Ad-régulier.

2) D'après [31, IV §9 Theo 5] (voir aussi [31, p. 125]), le cardinal d'un sous-groupe fini de $GL_2(\mathbb{Q}_p)$ est inférieur à $(p-1)^2 p(p+1)$ si p est impair, et inférieur à 96 si $p = 2$. Il en résulte aisément que le cardinal d'un sous-groupe fini de PG^n est inférieur à

$$\begin{cases} \left((p-1)^2 p(p+1)\right)^n & \text{si}\, p \neq 2 \\ 96^n & \text{si}\, p = 2 \end{cases}$$

donc PG^n est régulier.

3) D'après [12, XIII 8.1], G est engendré par les matrices de la forme

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \text{ pour } b, c \in \mathbb{Q}_p .$$

Donc $\Delta(PG)$ est engendré par les sous-groupes à un paramètre

$$\left\{\Delta\left(q\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\right), b \in \mathbb{Q}_p\right\} \text{ et } \left\{\Delta\left(q\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}\right), c \in \mathbb{Q}_p\right\}.$$

Pour conclure, il nous faut donc voir que si (par exemple) $g = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, alors

$$\mathrm{Ad}_{\Delta(q(g))} - \mathrm{Id} : \mathrm{Lie}(PG^n) \to \mathrm{Lie}(PG^n)$$

est un endomorphisme nilpotent. Mais, via l'isomorphisme

$$\mathrm{Lie}(G)^n \xrightarrow{\simeq} \mathrm{Lie}(PG^n),$$

$\mathrm{Ad}_{\Delta(q(g))} - \mathrm{Id}$ devient $(\mathrm{Ad}_g - \mathrm{Id})^n$, et il suffit donc de voir que

$$\mathrm{Ad}_g - \mathrm{Id} : \mathrm{Lie}(G) \to \mathrm{Lie}(G)$$

est nilpotent.

Si $M = \begin{pmatrix} x & y \\ z & -x \end{pmatrix} \in Sl_2(\mathbb{Q}_p) \simeq \mathrm{Lie}(G)$,

$$\begin{aligned} g^{-1}(1+\varepsilon M)g &= \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1+x\varepsilon & y\varepsilon \\ z\varepsilon & 1-x\varepsilon \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1+(x-bz)\varepsilon & (2bx+y-b^2z)\varepsilon \\ z\varepsilon & 1+(bz-x)\varepsilon \end{pmatrix} \end{aligned}$$

donc

$$\begin{aligned} (\mathrm{Ad}_g - \mathrm{Id})(M) &= \begin{pmatrix} -bz & (2bx-b^2z) \\ 0 & bz \end{pmatrix} \\ (\mathrm{Ad}_g - \mathrm{Id})^2(M) &= \begin{pmatrix} 0 & -2b^2z \\ 0 & 0 \end{pmatrix} \\ (\mathrm{Ad}_g - \mathrm{Id})^3(M) &= 0 \end{aligned}$$

et $(\mathrm{Ad}_g - \mathrm{Id})^3 = 0$.

4) [32, p. 115]. □

6.4.3 Un corollaire du théorème de Ratner

Proposition 6.4.3 *Soient $G = PSL_2(\mathbb{Q}_p)$, $X \neq \emptyset$ un ensemble fini et, pour $x \in X$, Γ_x un sous-groupe discret et cocompact de G. Posons $\Gamma = \prod_{x \in X} \Gamma_x \subset G^X$, et soit $\Delta : G \to G^X$ la diagonale. Si $\forall (x_1 \neq x_2) \in X^2$, Γ_{x_1} et Γ_{x_2}* ne sont pas commensurables*, alors $\Gamma\Delta(G)$ est dense dans G^X.*

Preuve: On raisonne par récurrence sur $n = \#X$. Si $n = 1$, il n'y a rien à prouver, puisque $\Delta(G) = G$. On suppose donc $n > 1$.

D'après 6.4.2, on peut appliquer le théorème de Ratner aux sous-groupes Γ et $U = \Delta(G)$ de G^n. Son corollaire 6.4.1 affirme qu'il existe un sous-groupe fermé $H \subset G^X$ contenant $\Delta(G)$, et tel que $\overline{\Gamma\Delta(G)} = \Gamma H$. G étant simple et non commutatif, et $\Delta(G)$ normalisant H, la proposition 6.3.1 affirme alors que H est un "produit de diagonales". Comme $\Delta(G) \subset H$, cela signifie qu'il existe une *partition* $(X_i)_{i\in I}$ de X telle que, avec les notations de cet proposition, $H = \prod_{i \in I} \Delta^{X_i}(G)$.

Supposons que $\#I = 1$, c'est-à-dire que $H = \Delta(G)$ et $\Gamma\Delta(G)$ est déjà fermé dans G^X. Il en résulte alors que $\Gamma \setminus \Gamma\Delta(G)$ est un sous-ensemble fermé de $\Gamma \setminus G^X = \prod_{x\in X} \Gamma_x \setminus G$, donc compact puisque chaque $\Gamma_x \subset G$ est cocompact. Or,

$$\left(\bigcap_{x\in X} \Gamma_x\right) \setminus G \xrightarrow{\simeq} \Gamma \cap \Delta(G) \setminus \Delta(G) \xrightarrow{\simeq} \Gamma \setminus \Gamma\Delta(G),$$

donc $\bigcap_{x\in X} \Gamma_x$ est (discret et) *cocompact* dans G. Choisissant $x_0 \in X$, l'ensemble $\left(\bigcap_{x\in X} \Gamma_x\right) \backslash \Gamma_{x_0}$ serait alors à la fois discret et compact, donc fini, ce qui contredit la non commensurabilité des Γ_x (puisque $n > 1$).

Ainsi, $\#I \neq 1$, et pour tout $i \in I$, $\#X_i < n$. Par l'hypothèse de récurrence, $\Gamma^{X_i}\Delta^{X_i}(G)$ est dense dans G^{X_i} ; comme

$$\Gamma^{X_i}\Delta^{X_i}(G) \subset \Gamma H = \overline{\Gamma\Delta(G)},$$

on a donc $G^{X_i} \subset \overline{\Gamma\Delta(G)}$ pour tout $i \in I$, d'où $G^X = \overline{\Gamma\Delta(G)}$. □

Remarque: Si l'on supprime l'hypothèse de non commensurabilité des réseaux Γ_x, notre preuve montre que l'adhérence de $\Gamma\Delta(G)$ dans G^X est un produit de diagonales, dont les supports forment une partition de X. De plus, la relation d'équivalence sur X définie par cette partition est précisément :

$$x \sim x' \Leftrightarrow \Gamma_x \text{ et } \Gamma_{x'} \text{ sont commensurables.}$$

6.5 Commensurateurs et rationalité

D'après les sections 6.2.12 et 6.2.13, les propositions 6.2.5 et 6.4.3 impliquent que, pour prouver le théorème 6.2.1, il ne nous reste plus qu'à voir que les sous-groupes $(\Gamma^1_{\ell,\sigma})_{\ell,\sigma\in S\times\mathcal{R}}$ de $PSL_2(\mathbb{Q}_p)$ sont deux à deux non commensurables.

Comme $\Gamma^1_{\ell,\sigma} = (\Gamma_{\ell,\sigma} \cap SL_2(\mathbb{Q}_p))/\{\pm 1\}$, il revient au même de voir que les sous-groupes $\Gamma_{\ell,\sigma} \cap SL_2(\mathbb{Q}_p)$ de $SL_2(\mathbb{Q}_p)$ sont deux à deux non commensurables. Comme enfin $\pm p^{\mathbb{Z}} \subset \Gamma_{\ell,\sigma}$ et $\det(\Gamma_{\ell,\sigma}) = p^{\mathbb{Z}}$ pour tout $\ell, \sigma \in S \times \mathcal{R}$, il revient au même de voir que les sous-groupes $\Gamma_{\ell,\sigma}$ de $GL_2(\mathbb{Q}_p)$ sont deux à deux non commensurables.

Rappelons que

$$\begin{aligned} \Gamma_{\ell,\sigma} &= \alpha_{\ell,\sigma}^{-1}\Gamma(\ell)\alpha_{\ell,\sigma} \\ \Gamma(\ell) &= \rho_\ell\left(R^0(\ell)[1/p]\right)^* \end{aligned}$$

où $R^0(\ell)$ est un ($\mathbb{Z}$-)ordre d'Eichler de niveau N dans le corps de quaternion $B(\ell)$, $\rho_\ell : B(\ell)_p \to M_2(\mathbb{Q}_p)$ est un isomorphisme, et

$$\alpha_{\ell,\sigma} = \rho_\ell(b_{\ell,\sigma})\iota(\hat{\lambda}_{\sigma,p}^{-1}) \in GL_2(\mathbb{Q}_p)$$

pour un élément $b_{\ell,\sigma} \in B(\ell)^*$ tel que

$$\forall \ell' \in S : \quad b_{\ell,\sigma} \in (R(\ell))^*_{\ell'} = \left(R^0(\ell)\right)^*_{\ell'}.$$

Cela étant, le commensurateur de $\Gamma(\ell)$ dans $GL_2(\mathbb{Q}_p)$ est, d'après [39, IV Coro 1.5] :

$$\mathrm{Com}\left(\Gamma(\ell), GL_2(\mathbb{Q}_p)\right) = \mathbb{Q}_p^*\rho_\ell(B(\ell))^*.$$

Le commensurateur de $\Gamma_{\ell,\sigma}$ est donc :

$$\mathrm{Com}\left(\Gamma_{\ell,\sigma}, GL_2(\mathbb{Q}_p)\right) = \mathbb{Q}_p^*\rho_{\ell,\sigma}(B(\ell))^*$$

où $\rho_{\ell,\sigma}(x) = \alpha_{\ell,\sigma}^{-1}\rho_\ell(x)\alpha_{\ell,\sigma}$.

6.5.1 Le cas $\ell \neq \ell'$

Considérons d'abord le cas d'un couple $(\ell,\sigma), (\ell',\sigma') \in (S \times \mathcal{R})^2$ avec $\ell \neq \ell'$. Alors $\Gamma_{\ell,\sigma}$ et $\Gamma_{\ell',\sigma'}$ sont non commensurables, car ils n'ont pas le même commensurateur : il suffit d'appliquer le lemme suivant aux isomorphismes

$$\rho_{\ell,\sigma} : B(\ell)_p \to GL_2(\mathbb{Q}_p) \quad \text{et} \quad \rho_{\ell',\sigma'} : B(\ell')_p \to GL_2(\mathbb{Q}_p).$$

Lemme 6.5.1 *Soient B et B' deux algèbres de quaternions* non isomorphes*, et non ramifiées en p ; choisissons des isomorphismes de $B_p \approx M_2(\mathbb{Q}_p)$ et $B'_p \approx M_2(\mathbb{Q}_p)$, aux moyens desquels on identifie B et B' à des sous-anneaux de $M_2(\mathbb{Q}_p)$. Alors :*

$$\mathbb{Q}_p^* B^* \neq \mathbb{Q}_p^* B'^* \quad \text{dans} \quad GL_2(\mathbb{Q}_p)$$

Preuve: Supposons que $\mathbb{Q}_p^* B^* = \mathbb{Q}_p^* B'^*$. En particulier, on en déduit une inclusion $B \subset \mathbb{Q}_p B'$, qui permet d'écrire tout élément b de B comme un produit $b = \lambda b'$, avec$\lambda \in \mathbb{Q}_p$ and $b \in B'$. On a alors $\mathrm{tr}(b) = \lambda \mathrm{tr}(b')$. Si la trace réduite de b est non nulle, on a donc $\mathrm{tr}(b') \neq 0$, et $\lambda = \mathrm{tr}(b)/\mathrm{tr}(b') \in \mathbb{Q}^*$, donc $b = \lambda b' \in B'$. Si la trace de b est nulle, $\mathrm{tr}(b-1) = 1 \neq 0$, et $b - 1 \in B$, donc par le cas précédent, $b - 1 \in B'$, d'ou $b \in B'$. Finalement, $B \subset B'$. Par symétrie, $B = B'$: les deux sous-anneaux B et B' de $M_2(\mathbb{Q}_p)$ étant *égaux*, sont à fortiori isomorphes, une contradiction. □

6.5.2 Le cas $\ell = \ell'$

Supposons ensuite que $\ell = \ell'$. Dans ce cas, $\Gamma_{\ell,\sigma}$ et $\Gamma_{\ell,\sigma'}$ sont commensurables si, et seulement si :

$$\alpha_{\ell,\sigma}\alpha_{\ell,\sigma'}^{-1} \in \mathrm{Com}\,(\Gamma(\ell), GL_2(\mathbb{Q}_p)) = \mathbb{Q}_p^* \rho_\ell(B(\ell))^*. \tag{6.9}$$

Comme

$$\alpha_{\ell,\sigma} = \rho_\ell(b_{\ell,\sigma})\iota(\hat{\lambda}_{\sigma,p}^{-1}) \quad \text{et} \quad b_{\ell,\sigma} \in B(\ell)^*,$$

(6.9) est équivalent à :

$$\iota(\hat{\lambda}_{\sigma,p}^{-1})\iota(\hat{\lambda}_{\sigma',p}) \in \mathbb{Q}_p^* \rho_\ell(B(\ell))^*. \tag{6.10}$$

D'après (6.4), on a : $\iota(\hat{\lambda}_{\sigma,p}) = \rho_\ell(\hat{\lambda}_{\sigma,p})$ (via le plongement $K_p \hookrightarrow B(\ell)_p$). Ainsi, (6.10) est équivalent à :

$$\hat{\lambda}_{\sigma,p}^{-1}\hat{\lambda}_{\sigma',p} \in \mathbb{Q}_p^* B(\ell)^*. \tag{6.11}$$

Mais, si $\hat{\lambda}_{\sigma,p}^{-1}\hat{\lambda}_{\sigma',p} = xy$, avec $x \in \mathbb{Q}_p^*$ et $y \in B(\ell)^*$, alors y commute aux éléments de $K \subset B(\ell)$, donc $y \in K^*$. Ainsi, (6.11) est équivalent à :

$$\hat{\lambda}_{\sigma,p}^{-1}\hat{\lambda}_{\sigma',p} \in \mathbb{Q}_p^* K^*. \tag{6.12}$$

Or

$$\left[K[c_0 p^\infty]/K\ ,\ \widehat{\mathbb{Q}}^* K^*\right] = 1 \in \mathrm{Gal}(K[c_0 p^\infty]/K),$$

de sorte que (6.12) implique :

$$\sigma^{-1}\sigma' \in \left[K[c_0 p^\infty]/K\ ,\ \widehat{K}^{(p)}\right] = \mathrm{Gal}(K[c_0 p^\infty]/K)^{\mathrm{rat}}.$$

Compte tenu de notre hypothèse sur $\mathcal{R}$, on a donc finalement : $\Gamma_{\ell,\sigma}$ et $\Gamma_{\ell,\sigma'}$ sont commensurables si et seulement si $\sigma = \sigma'$.

Ce qui achève de prouver le théorème 6.2.1.

Troisième partie

La conjecture de Mazur

Chapitre 7

Un théorème d'Ihara

Soit $\ell \nmid 6N$ un nombre premier, et $k = \mathbb{F}_{l^2}$. Soit $X_0(N)_{/\mathbb{Z}[1/N]}$ le modèle propre et lisse de $X_0(N)_{/\mathbb{Q}}$ (cf. [10]). $J_0(N) = \mathrm{Pic}^0(X_0(N)_{/\mathbb{Z}[1/N]}$ est alors un schéma abélien [3, 9.4 Prop 4]. Le plongement classique de $X_0(N)$ dans sa Jacobienne, qui envoie la pointe $\infty \in X_0(N)(\mathbb{Q})$ sur $0 \in J_0(N)(\mathbb{Q})$, s'étend par la propriété universelle du modèle de Néron (par exemple), en un morphisme $X_0(N) \to J_0(N)$, que l'on note symboliquement $x \mapsto (x - \infty)$.

Soit $J_0^{\mathrm{ss}}(N)(k)$ le sous-groupe de $J_0(N)(k)$ engendré par les diviseurs de la forme

$$(x - y) = (x - \infty) - (y - \infty) \in J_0(N)(k),$$

pour $x, y \in X_0^{\mathrm{ss}}(N)(k)$.

Proposition *L'indice de* $J_0^{\mathrm{ss}}(N)(k)$ *dans* $J_0(N)(k)$ *est égal à l'ordre du sous-groupe de Shimura* Sh_N *de* $J_0(N)(\mathbb{C})$. *En particulier, cet indice divise* $\varphi(N) = \#(\mathbb{Z}/N\mathbb{Z})^*$.

Ce résultat semble bien connu, et découle d'un théorème d'Ihara [9].

7.1 Le théorème d'Ihara

Pour énoncer ce théorème, nous allons tout d'abord rappeler les grandes lignes de la construction, par Ihara, d'un modèle propre et lisse sur $\mathbb{Z}_{\ell^2}$ de la courbe modulaire associée au sous-groupe de congruence principal :

$$\Gamma(N) = \left\{ x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid x \equiv 1 \bmod N \right\}$$

7.1.1 Le niveau fini

Pour un entier $n \geq 1$ *premier* à ℓ, soit $X(n)_{/\mathbb{Z}_\ell}$ l'espace de module compactifié "classifiant" les paires $(E_{/S/\mathbb{Z}_\ell}, \varphi)$, où E est une courbe elliptique sur le $\mathbb{Z}_\ell$-schéma S, et φ est un isomorphisme $(\frac{1}{n}\mathbb{Z}/\mathbb{Z})_S \to E[n]_{/S}$. L'accouplement de Weil induit un morphisme $X(n) \to \mu_n^*$, où $\mu_{n/\mathbb{Z}_\ell}^*$ est le schéma des racines primitives n^{e} de l'unité, c'est-à-dire :

$$\mu_n^* = \mathrm{Spec}\,(\mathbb{Z}_\ell[X]/\Phi_n)$$

où Φ_n est le n^{e} polynome cyclotomique. Le groupe $GL_2(\mathbb{Z}/n\mathbb{Z})$ agit sur les $\mathbb{Z}_\ell$-schémas $X(n)$ et μ_n^* (via le déterminant), et $X(n) \to \mu_n^*$ est équivariant pour ces actions.

Soit $H \subset GL_2(\mathbb{Z}/n\mathbb{Z})$ un sous-groupe. On peut alors former le morphisme de $\mathbb{Z}_\ell$-schémas :

$$(X(n) \to \mu_n^*)\,/H = (X(n)/H \to \mu_n^*/\det(H))\,.$$

Avec $H = B^1 = \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$ ou $H = B = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$, on obtient ainsi respectivement (cf. [10, Chap 9]) :

$$X_1(N) \to \mathrm{Spec}(\mathbb{Z}_\ell) \quad \text{et} \quad X_0(N) \to \mathrm{Spec}(\mathbb{Z}_\ell).$$

7.1.2 Le schéma $\mu_{n/\mathbb{Z}_\ell}^*$

Posons $A = \mathbb{Z}_\ell[X]/\Phi_n$, de sorte que $\mu_n^* = \mathrm{Spec}(A)$. μ_n^* étant fini et étale sur l'anneau local hensélien $\mathbb{Z}_\ell$, A se décompose en un produit fini d'anneaux locaux henséliens, finis et étales sur $\mathbb{Z}_\ell$ (cf. [35], ou [17, I.4] ou [EGA, IV 18.5]) :

$$A = \prod_i A_i.$$

Cette décomposition correspond à la décomposition en composantes connexes :

$$\mu_n^* = \coprod_i (\mu_n^*)_i$$

où pour tout i, $(\mu_n^*)_i = \mathrm{Spec}(A_i)$ est un schéma étale, connexe, plat et fini sur $\mathbb{Z}_\ell$.

Le groupe fondamental algébrique du schéma $\mathrm{Spec}(\mathbb{Z}_\ell)$ n'est autre que le groupe de Galois de l'extension abélienne maximale non-ramifiée $\mathbb{Q}_{\ell^\infty}$ de $\mathbb{Q}_\ell$, et l'anneau des entiers $\mathbb{Z}_{\ell^\infty}$ de $\mathbb{Q}_{\ell^\infty}$ est un hénsélisé strict de $\mathbb{Z}_\ell$ ([17, I.5] ou [3, I.2.4 Prop 11] ou [EGA, IV 18.10.16]). D'après le théorème fondamental de classification des schémas finis et étales sur une base connexe ([20] ou [16]), la donnée du schéma μ_n^* est équivalente à la donnée du $\mathrm{Gal}(\mathbb{Q}_{\ell^\infty}/\mathbb{Q}_\ell)$-ensemble fini et discret

$$\mu_n^*(\mathbb{Q}_{\ell^\infty}) = \mu_n^*(\mathbb{Z}_{\ell^\infty}) = \mu_n^*(\overline{k}).$$

En particulier, les composantes connexes (ou irréductibles) $(\mu_n^*)_i$ de μ_n^* sont en bijection avec les orbites de l'action de Galois sur cet ensemble. Le Frobénius de $\mathrm{Gal}(\mathbb{Q}_{\ell^\infty}/\mathbb{Q}_\ell)$ est un générateur topologique de $\mathrm{Gal}(\mathbb{Q}_{\ell^\infty}/\mathbb{Q}_\ell)$, et agit sur $\mu_n^*(\mathbb{Z}_{\ell^\infty})$ par élévation à la puissance ℓ. Ainsi, l'action de $(\mathbb{Z}/n\mathbb{Z})^*$ sur le $\mathbb{Z}_\ell$-schéma μ_n^* induit une action *transitive* sur l'ensemble des composantes connexes, et le stabilisateur de chacune d'entre elles est égal au sous-groupe engendré par $\ell \in (\mathbb{Z}/n\mathbb{Z})^*$.

Toute racine $\zeta_n \in \mu_n^*(\mathbb{Z}_{l^\infty})$ détermine un morphisme

$$\mathrm{Spec}(\mathbb{Z}_\ell[\zeta_n]) \to \mu_n^*$$

qui est un isomorphisme sur l'une des composantes connexes de μ_n^*. On définit alors le $\mathrm{Spec}(\mathbb{Z}_\ell[\zeta_n])$-schéma $X(N)^{(\zeta_n)}$ par le diagramme cartésien :

$$\begin{array}{ccc} X(n)^{(\zeta_n)} & \to & X(n) \\ \downarrow & & \downarrow \\ \mathrm{Spec}(\mathbb{Z}_\ell[\zeta_n]) & \to & \mu_n^* \end{array}$$

Par construction, le groupe

$$G_1(n) = \left\{x \in GL_2(\mathbb{Z}/n\mathbb{Z}) \mid \det(x) \in (\ell \bmod n)^{\mathbb{Z}} \subset (\mathbb{Z}/n\mathbb{Z})^*\right\}$$

agit sur $X(n)^{(\zeta_n)}$ et $\mathrm{Spec}(\mathbb{Z}_\ell[\zeta_n])$ (via le déterminant), et le morphisme

$$X(n)^{(\zeta_n)} \to \mathrm{Spec}(\mathbb{Z}_\ell[\zeta_n])$$

est équivariant pour ces actions.

Si H est un sous-groupe de $GL_2(\mathbb{Z}/n\mathbb{Z})$ tel que $\det(H) = (\mathbb{Z}/n\mathbb{Z})^*$, on a donc

$$\begin{aligned} (X(n) \to \mu_n^*)/H &= \left(X(n)^{(\zeta_n)} \to \mathrm{Spec}\,(\mathbb{Z}_\ell[\zeta_n])\right)/H_1(n) \\ &= \left(X(n)^{(\zeta_n)}/H_1(n) \to \mathrm{Spec}\,(\mathbb{Z}_\ell[\zeta_n])/\det(H_1(n))\right) \\ &= X(n)^{(\zeta_n)}/H_1(n) \to \mathrm{Spec}(\mathbb{Z}_\ell), \end{aligned}$$

où

$$H_1(n) = H \cap G_1(n).$$

7.1.3 Changement de base

Soit r l'ordre de ℓ dans $(\mathbb{Z}/n\mathbb{Z})^*$. Si $r' \mid r$, notons

$$G_{r'}(n) = \left\{x \in GL_2(\mathbb{Z}/n\mathbb{Z}) \mid \det(x) \in (\ell \bmod n)^{r'\mathbb{Z}} \subset (\mathbb{Z}/n\mathbb{Z})^*\right\}$$

de sorte que $G_{r'}(n)$ est un sous-groupe d'indice r' de $G_1(n)$; comme

$$\det(G_{r'}(n)) = (\ell \bmod n)^{r'\mathbb{Z}},$$

on a donc

$$\mathrm{Spec}\,(\mathbb{Z}_\ell[\zeta_n])/\det(G_{r'}(n)) = \mathrm{Spec}(\mathbb{Z}_{\ell^{r'}}).$$

Si H est un sous-groupe de $GL_2(\mathbb{Z}/n\mathbb{Z})$ tel que $\det(H) = (\mathbb{Z}/n\mathbb{Z})^*$, posant

$$H_{r'}(n) = H \cap G_{r'}(n),$$

on a donc :

$$\left(X(n)^{(\zeta_n)} \to \mathrm{Spec}\,(\mathbb{Z}_\ell[\zeta_n])\right)/H_{r'}(n) = \left(X(n)^{(\zeta_n)}/H_{r'}(n) \to \mathrm{Spec}(\mathbb{Z}_{\ell^{r'}})\right).$$

On en déduit un morphisme

$$f : X(n)^{(\zeta_n)}/H_{r'}(n) \to \left(X(n)^{(\zeta_n)}/H_1(n)\right) \times_{\mathrm{Spec}(\mathbb{Z}_\ell)} \mathrm{Spec}(\mathbb{Z}_{\ell^{r'}}).$$

Ce morphisme est fini, et plat car

$$\left(X(n)^{(\zeta_n)}/H_1(n)\right) \times_{\mathrm{Spec}(\mathbb{Z}_\ell)} \mathrm{Spec}(\mathbb{Z}_{\ell^{r'}}) \to \left(X(n)^{(\zeta_n)}/H_1(n)\right)$$

est étale, et

$$\left(X(n)^{(\zeta_n)}/H_{r'}(n)\right) \to \left(X(n)^{(\zeta_n)}/H_1(n)\right)$$

est plat (cf. [EGA, IV 18.4.10]). Comparant les degrés, on voit donc que f est un isomorphisme.

En particulier, avec $H = B^1 = \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$ ou $H = B = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$, on obtient respectivement :

$$\begin{aligned}(X_1(N) \times_{\mathbb{Z}_\ell} \mathrm{Spec}(\mathbb{Z}_{\ell^{r'}}) \to \mathrm{Spec}(\mathbb{Z}_{\ell^{r'}})) &= \left(X(n)^{(\zeta_n)}/B^1_{r'}(n) \to \mathrm{Spec}(\mathbb{Z}_{\ell^{r'}})\right)\\ (X_0(N) \times_{\mathbb{Z}_\ell} \mathrm{Spec}(\mathbb{Z}_{\ell^{r'}}) \to \mathrm{Spec}(\mathbb{Z}_{\ell^{r'}})) &= \left(X(n)^{(\zeta_n)}/B_{r'}(n) \to \mathrm{Spec}(\mathbb{Z}_{\ell^{r'}})\right).\end{aligned}$$

7.1.4 Limite projective

Considérons maintenant le système projectif de morphismes de $\mathbb{Z}_\ell$-schémas

$$(X(n) \to \mu_n^*)_{\gcd(n,l)=1}.$$

Soit $X \to \mu^*$ sa limite projective. Les morphismes de transition étant affines, X et μ^* sont des schémas sur $\mathbb{Z}_\ell$, au demeurant non noethériens. Si $(\zeta_n)_{\gcd(n,l)=1}$ est un système compatible de racines primitives n^{e} de l'unité, les constructions ci-dessus passent à la limite : les diagrammes cartésiens :

$$\begin{array}{ccc} X(n)^{(\zeta_n)} & \to & X(n) \\ \downarrow & & \downarrow \\ \mathrm{Spec}(\mathbb{Z}_\ell[\zeta_n]) & \to & \mu_n^* \end{array}$$

induisent alors un diagramme cartésien :

$$\begin{array}{ccc} X^{(\zeta)} & \to & X \\ \downarrow & & \downarrow \\ \mathrm{Spec}(\mathbb{Z}_{\ell^\infty}) & \to & \mu^* \end{array}$$

Le groupe $\hat{G} = GL_2(\widehat{\mathbb{Z}}^{(\ell)})$ agit sur X et μ^*, et le morphisme $X \to \mu^*$ est équivariant pour ces actions. Le sous-groupe

$$\hat{G}_1 = \left\{ x \in GL_2(\widehat{\mathbb{Z}}^{(\ell)}) \mid \det(x) \in \ell^{\widehat{\mathbb{Z}}} \subset \widehat{\mathbb{Z}}^{(\ell)*} \right\}$$

agit donc sur $X^{(\zeta)}$ et $\mathrm{Spec}(\mathbb{Z}_{\ell^\infty})$, et le morphisme $X^{(\zeta)} \to \mathrm{Spec}(\mathbb{Z}_{\ell^\infty})$ est $\hat{G}_1$-équivariant.

7.1.5 Quotients de $X^{(\zeta)}$.

Si enfin H est un sous-groupe de $GL_2(\mathbb{Z}/N\mathbb{Z})$ tel que $\det(H) = (\mathbb{Z}/N\mathbb{Z})^*$, posant

$$\hat{H}(N) = \{x \in G \mid x \bmod N \in H\}$$

on a donc :

$$\begin{aligned} (X(N)/H \to \mathrm{Spec}(\mathbb{Z}_\ell)) &= (X \to \mu^*)\,/\hat{H}(N) \\ &= \left(X^{(\zeta)} \to \mathrm{Spec}(\mathbb{Z}_{\ell^\infty})\right)/\hat{H}_1(N) \end{aligned}$$

où $\hat{H}_1(N) = \hat{H}(N) \cap \hat{G}_1$.

Plus généralement, posant

$$\hat{G}_r = \left\{ x \in GL_2(\widehat{\mathbb{Z}}^{(\ell)}) \mid \det(x) \in \ell^{r\widehat{\mathbb{Z}}} \subset \widehat{\mathbb{Z}}^{(\ell)*} \right\}$$

pour $r \geq 1$, et

$$\hat{G}_\infty = SL_2(\widehat{\mathbb{Z}}^{(\ell)}),$$

on obtient :

$$(X(N)/H \to \mathrm{Spec}(\mathbb{Z}_\ell)) \times_{\mathbb{Z}_\ell} \mathbb{Z}_{\ell^r} = \left(X^{(\zeta)} \to \mathrm{Spec}(\mathbb{Z}_{\ell^\infty})\right)/\hat{H}_r(N),$$

où $\hat{H}_r(N) = \hat{H}(N) \cap \hat{G}_r$.

Notons que si $\begin{pmatrix} \ell & 0 \\ 0 & \ell \end{pmatrix} \in H$, on a

$$\hat{H}_2(N) = \begin{pmatrix} \ell & 0 \\ 0 & \ell \end{pmatrix}^{\widehat{\mathbb{Z}}} \times \hat{H}_\infty(N).$$

dans $\hat{G}_2$.

7.1.6 Le modèle d'Ihara

Si n est un entier premier à ℓ et divisible par N, posons

$$G_n(N) = \{x \in SL_2(\mathbb{Z}/n\mathbb{Z}) \mid x \equiv 1 \bmod N\}.$$

On a alors :

$$\left(X(n)^{(\zeta_n)} \to \operatorname{Spec}(\mathbb{Z}_\ell[\zeta_n])\right)/G_n(N) =$$

$$= \left(X(n)^{(\zeta_n)}/G_n(N) \to \operatorname{Spec}(\mathbb{Z}_\ell[\zeta_n])\right)$$

$$= \left(X(N)^{(\zeta_N)} \times_{\operatorname{Spec}(\mathbb{Z}_\ell[\zeta_N])} \operatorname{Spec}(\mathbb{Z}_\ell[\zeta_n]) \to \operatorname{Spec}(\mathbb{Z}_\ell[\zeta_n])\right)$$

Il en résulte que, si

$$\hat{G}_\infty(N) = \left\{x \in \hat{G}_\infty \mid x \equiv 1 \bmod N\right\}$$

alors

$$\left(X^{(\zeta)} \to \operatorname{Spec}(\mathbb{Z}_{\ell^\infty})\right)/\hat{G}_\infty(N) =$$

$$= \left(X(N)^{(\zeta_N)} \times_{\operatorname{Spec}(\mathbb{Z}_\ell[\zeta_N])} \operatorname{Spec}(\mathbb{Z}_{\ell^\infty}) \to \operatorname{Spec}(\mathbb{Z}_{\ell^\infty})\right)$$

Suivant Ihara, on définit :

$$\hat{I}_2(N) = \left\{x \in GL_2(\widehat{\mathbb{Z}}^{(\ell)}) \mid \exists \hat{a} \in \widehat{\mathbb{Z}} \text{ t.q. } \det(x) = \ell^{2\hat{a}} \text{ et } x \equiv \begin{pmatrix} \ell^{\hat{a}} & 0 \\ 0 & \ell^{\hat{a}} \end{pmatrix} \bmod N\right\},$$

de sorte que

$$\ell^{\widehat{\mathbb{Z}}} \subset \hat{I}_2(N) \subset \hat{G}_2 \quad \text{et} \quad \det(\hat{I}_2(N)) = \ell^{2\widehat{\mathbb{Z}}}.$$

On pose alors :

$$(X_I(N) \to \operatorname{Spec}(\mathbb{Z}_{\ell^2})) = \left(X^{(\zeta)} \to \operatorname{Spec}(\mathbb{Z}_{\ell^\infty})\right)/\hat{I}_2(N).$$

On voit aisément que

$$\hat{I}_2(N) = \begin{pmatrix} \ell & 0 \\ 0 & \ell \end{pmatrix}^{\widehat{\mathbb{Z}}} \times \hat{G}_\infty(N),$$

de sorte que

$$\left(X_I(N) \times_{\mathbb{Z}_{\ell^2}} \mathbb{Z}_{\ell^\infty} \to \operatorname{Spec}(\mathbb{Z}_{\ell^\infty})\right) = \left(X^{(\zeta)} \to \operatorname{Spec}(\mathbb{Z}_{\ell^\infty})\right)/\hat{G}_\infty(N),$$

donc

$$X_I(N) \times_{\mathbb{Z}_{\ell^2}} \mathbb{Z}_{\ell^\infty} = X(N)^{(\zeta_N)} \times_{\mathbb{Z}_\ell[\zeta_N]} \mathbb{Z}_{\ell^\infty}.$$

Comme $X(N) \to \mu_N^*$ est une courbe (relative) propre et lisse à fibre géométriquement connexe par [10, 10.9.2],

$$X(N)^{(\zeta_N)} \to \operatorname{Spec}(\mathbb{Z}_\ell[\zeta_N]) \quad \text{et} \quad X_I(N) \times_{\operatorname{Spec}(\mathbb{Z}_{\ell^2})} \operatorname{Spec}(\mathbb{Z}_{\ell^\infty}) \to \operatorname{Spec}(\mathbb{Z}_{\ell^\infty})$$

le sont également. Par descente étale le long de

$$\operatorname{Spec}(\mathbb{Z}_{\ell^\infty}) \to \operatorname{Spec}(\mathbb{Z}_{\ell^2})$$

(cf. [EGA, IV]), $X_I(N)_{/\mathbb{Z}_{\ell^2}}$ est donc une courbe relative propre et lisse à fibre géométriquement connexe, et un modèle sur $\mathbb{Z}_{\ell^2}$ de $X(N)^{(\zeta_N)}$.

7.1.7 $X_0(N)$ est un quotient de $X_I(N)$

En effet, avec les notations précédentes, si $B = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$, alors

$$\hat{I}_2(N) = \begin{pmatrix} \ell & 0 \\ 0 & \ell \end{pmatrix}^{\hat{\mathbb{Z}}} \times \hat{G}_\infty(N) \subset \hat{B}_2(N) = \begin{pmatrix} \ell & 0 \\ 0 & \ell \end{pmatrix}^{\hat{\mathbb{Z}}} \times \hat{B}_\infty(N).$$

de sorte que $X_0(N) \times_{\mathrm{Spec}(\mathbb{Z}_\ell)} \mathrm{Spec}(\mathbb{Z}_{\ell^2})$ est un quotient de $X_I(N)$. On note

$$\alpha : X_I(N) \to X_0(N)_{\mathbb{Z}_{\ell^2}}$$

ce quotient.

Remarquons également que

$$\begin{aligned} \hat{B}_\infty(N)/\hat{G}_\infty(N) &\simeq \left\{ x \in SL_2(\mathbb{Z}/N\mathbb{Z}) \mid \exists a \text{ t.q. } x \equiv \begin{pmatrix} a & * \\ 0 & a^{-1} \end{pmatrix} \bmod N \right\} \\ &= \Gamma_0(N). \end{aligned}$$

7.1.8 Le théorème d'Ihara

Soit $J_I(N)_{/\mathbb{Z}_{\ell^2}}$ le "Pic^0 relatif" de la courbe $X_I(N)_{/\mathbb{Z}_{\ell^2}}$. D'après [3, 9.4 Prop 4], $J_I(N)_{/\mathbb{Z}_{\ell^2}}$ est un schéma abélien. Posons $S = \mathrm{Spec}(\mathbb{Z}_{l^2})$, $L = \mathbb{Q}_{l^2}$ et $k = \mathbb{F}_{l^2}$. Notant $\widetilde{Y}_{/k}$ la fibre spéciale d'un S-schéma Y, le théorème d'Ihara dont nous aurons besoin est :

Théorème *[9, p. 169] Les points supersinguliers de $\widetilde{X}_I(N)_{/k}$ sont de degré un sur k et engendrent le groupe de Picard de $\widetilde{X}_I(N)$.*

Corollaire 7.1.1 $\mathrm{Pic}^0(\widetilde{X}_I(N)) = J_I(N)(k)$ *est engendré par les diviseurs de la forme $(x - y)$, où x et y sont des points supersinguliers de $\widetilde{X}_I(N)$.*

7.2 Interlude

7.2.1 Schéma de Picard

Pour un schéma X, on note $\mathrm{Pic}(X) = \mathrm{H}^1(X, O_X^*)$ le groupe de Picard absolu de X : c'est le groupe des classes d'isomorphismes de faisceaux inversibles sur X. Si X est un S-schéma, on note

$$P(X_{/S})(T) = \mathrm{Pic}(X \times_S T)$$

pour tout S-schéma T, et

$$T \to \mathrm{Pic}(X_{/S})(T)$$

le faisceau associé au préfaisceau $T \to P_{X_{/S}}(T)$ pour la topologie fppf.

Si le morphisme structural $f : X \to S$ est quasi-compact et quasi-séparé, et si $f_*(O_X) = O_S$ est valable universellement, on a une suite exacte (cf. [3, 8.1]) :

$$0 \to \mathrm{Pic}(T) \to \mathrm{Pic}(X \times_S T) \to \mathrm{Pic}(X_{/S})(T) \to \mathrm{Br}(T) \to \mathrm{Br}(X \times_S T) \to 0. \tag{7.1}$$

Si de plus f admet une section,

$$\mathrm{Pic}(X_{/S})(T) = \mathrm{Pic}(X \times_S T)/\mathrm{Pic}(T).$$

Proposition 7.2.1 *Si S est localement noethérien, et $f : X \to S$ propre, lisse et à fibre géométriquement connexe, alors $f_*(O_X) = O_S$ est valable universellement.*

Preuve: Cela résulte de [EGA, III 7.8.8], compte-tenu de [8, II, Ex. 4.5]. □

7.2.2 Schéma abélien dual

Soit L une extension finie de $\mathbb{Q}_\ell$, R l'anneau des entiers de L, k son corps résiduel, et $S = \mathrm{Spec}(R)$. D'après [19, p. 16] ou [26], tout schéma abélien $A_{/S}$ est projectif. D'après [3, 8.4 Theo 5], le Pic^0 relatif de $A_{/S}$ est donc un schéma abélien projectif, que l'on note $A^{\mathrm{dual}}_{/S}$, et il existe un S-isomorphisme canonique de schémas abéliens $A \to (A^{\mathrm{dual}})^{\mathrm{dual}}$ (cf. par exemple [24]).

D'après [24, III 19.1], si $\phi : A \to B$ est une *isogénie* de S-schémas, alors $\phi^{\mathrm{dual}} : B^{\mathrm{dual}} \to A^{\mathrm{dual}}$ est une isogénie, et son noyau est le dual de Cartier du noyau de ϕ :

$$\ker(\phi^{\mathrm{dual}}) = \ker(\phi)^D.$$

Proposition 7.2.2 *On suppose que l'indice de ramification absolu e de $L/\mathbb{Q}_\ell$ vérifie : $e < \ell - 1$. Soit $\phi : A \to B$ un morphisme de schémas abéliens.*

1. *Si $\phi_L : A_L \to B_L$ a un noyau fini sur L, $\ker(\phi)_{/S}$ est fini et plat, $\phi^{\mathrm{dual}} : B^{\mathrm{dual}} \to A^{\mathrm{dual}}$ est fidèlement plat, et le noyau de ϕ^{dual} est une extension (fpqc) du dual de Cartier de $\ker(\phi)$ par un schéma abélien, modèle de Néron de la composante connexe du noyau de ϕ_L^{dual}. De plus,*

$$B^{\mathrm{dual}}(k)/\phi^{\mathrm{dual}}(A^{\mathrm{dual}}(k)) \simeq \mathrm{H}^1(k, \ker(\phi)^D).$$

2. *Si $\phi_L : A_L \to B_L$ est surjective, ϕ est fidèlement plat, $\ker(\phi^{\mathrm{dual}})_{/S}$ est fini et plat, et $\ker(\phi)$ est une extension (fpqc) du dual de Cartier de $\ker(\phi^{\mathrm{dual}})_{/S}$ par un schéma abélien, modèle de Néron de la composante connexe du noyau de ϕ_L. De plus,*

$$B(k)/\phi(A(k)) \simeq \mathrm{H}^1(k, \ker(\phi^{\mathrm{dual}})^D).$$

Preuve: 1) Soit $I_L = \phi(A_L)$ l'image de $\phi_L : A_L \to B_L$, et $Q_L = B_L/I_L$ le conoyau, de sorte que I_L et Q_L sont des variétés abéliennes (connexes) ayant bonne réduction sur S d'après [33], et $A_L \to I_L$ est une isogénie. Soient $I_{/S}$ et $Q_{/S}$ les modèles de Nérons de I_L et Q_L. D'après [3, 7.5 Theo 4], la suite

$$0 \to I \to B \to Q \to 0 \tag{7.2}$$

est exacte, et d'après [3, 7.3 Prop 6], le morphisme $A \to I$ est une isogénie. En particulier, le noyau de $\phi : A \to B$ est égal au noyau de l'isogénie $A \to I$, et est donc fini et plat.

Travaillant dans la catégorie des faisceaux (fpqc) en groupes commutatifs, appliquons le foncteur $\underline{\mathrm{Hom}}_S(\star, \mathbb{G}_m)$ à (7.2). On obtient :

$$\cdots \to \underline{\mathrm{Hom}}_S(I, \mathbb{G}_m) \to \underline{\mathrm{Ext}}^1_S(Q, \mathbb{G}_m) \to \underline{\mathrm{Ext}}^1_S(B, \mathbb{G}_m) \to \\ \to \underline{\mathrm{Ext}}^1_S(I, \mathbb{G}_m) \to \underline{\mathrm{Ext}}^2_S(Q, \mathbb{G}_m) \to \cdots$$

Mais $\underline{\mathrm{Hom}}_S(I, \mathbb{G}_m) = 0$ car I est un schéma abélien, et $\underline{\mathrm{Ext}}^1_S(X, \mathbb{G}_m) = X^{\mathrm{dual}}$ pour tout S-schéma abélien projectif ([24, III 18]). Comparant les dimensions relatives, on voit que le morphisme $B^{\mathrm{dual}} \to I^{\mathrm{dual}}$ est surjectif par fibre, donc fidèlement plat, et finalement, on obtient une suite exacte :

$$0 \to Q^{\mathrm{dual}} \to B^{\mathrm{dual}} \to I^{\mathrm{dual}} \to 0. \tag{7.3}$$

D'autre part, appliquant le même foncteur à la suite exacte

$$0 \to \ker(\phi) \to A \to I \to 0,$$

on obtient cette fois-ci :

$$0 \to \underline{\mathrm{Hom}}_S(\ker(\phi), \mathbb{G}_m) \to \underline{\mathrm{Ext}}^1_S(I, \mathbb{G}_m) \to \underline{\mathrm{Ext}}^1_S(A, \mathbb{G}_m) \to \underline{\mathrm{Ext}}^1_S(\ker(\phi), \mathbb{G}_m),$$

soit :

$$0 \to \ker(\phi)^D \to I^{\mathrm{dual}} \to A^{\mathrm{dual}} \to 0 \tag{7.4}$$

par le même raisonnement. En particulier, $\phi^{\mathrm{dual}} : B^{\mathrm{dual}} \to I^{\mathrm{dual}} \to A^{\mathrm{dual}}$ est fidèlement plat, et on a une suite exacte (fpqc) :

$$0 \to Q^{\mathrm{dual}} \to \ker(\phi^{\mathrm{dual}}) \to \ker(\phi)^D \to 0.$$

Il est clair que le schéma abélien Q^{dual} est le modèle de Néron de la composante connexe du noyau de ϕ^{dual}.

Appliquons maintenant le foncteur $\Gamma(k, \star)$ aux suites (7.3) et (7.4). Dans le premier cas, on obtient :

$$\cdots \to B^{\mathrm{dual}}(k) \to I^{\mathrm{dual}}(k) \to \mathrm{H}^1(k, Q^{\mathrm{dual}}) = 0,$$

car $\mathrm{H}^1(k, X) = 0$ pour toute variété abélienne $X_{/k}$, le corps k étant fini. Dans le second cas, on obtient :

$$\cdots \to I^{\mathrm{dual}}(k) \to A^{\mathrm{dual}}(k) \to \mathrm{H}^1(k, \ker(\phi)^D) \to \mathrm{H}^1(k, I^{\mathrm{dual}}) = 0,$$

donc finalement,

$$A^{\mathrm{dual}}(k)/\phi(B^{\mathrm{dual}}(k)) \simeq \mathrm{H}^1(k, \ker(\phi)^D).$$

2) Si K_L est la composante connexe du noyau de ϕ_L, $A_L/K_L \to B_L$ est une isogénie, donc $B_L^{\mathrm{dual}} \to (A_L/K_L)^{\mathrm{dual}}$ aussi. Mais le même raisonnement que plus haut (en travaillant seulement sur L) montre d'autre part que

$$(A_L/K_L)^{\mathrm{dual}} \to A_L$$

est une immersion fermée, donc le noyau de $B_L^{\mathrm{dual}} \to A_L^{\mathrm{dual}}$ est fini. Par dualité, 2) résulte donc de 1). □

On utilise la topologie fpqc pour faire comme dans [24]. On peut aussi bien utiliser la topologie fppf : tous les morphismes considérés sont de présentation finie.

7.2.3 Jacobiennes

Soit $X_{/S}$ une courbe propre et lisse à fibres géométriquement connexes. D'après [3, 9.4 Prop 4], le Pic^0 relatif de $X_{/S}$ est un schéma abélien, donc égal au modèle de Néron de sa fibre générique, qui n'est autre que la jacobienne de $X_{/L}$. Il est bien connu que $J(X)_{/L}$ est canoniquement auto-duale : il existe un isomorphisme canonique de L-variétés abéliennes $J(X_{/L}) \to J(X_{/L})^{\mathrm{dual}}$. Mais $J(X_{/L})^{\mathrm{dual}} = \left(J(X)^{\mathrm{dual}}\right)_{/L}$, donc il existe un isomorphisme canonique de S-schémas abéliens $J(X) \to J(X)^{\mathrm{dual}}$, par unicité des modèles de Néron. Il est clair que la restriction à chaque fibre de cet isomorphisme, est l'isomorphisme classique d'autodualité d'une Jacobienne d'une courbe lisse.

Soit $\alpha : X \to Y$ un S-morphisme de courbes propres et lisses à fibres géométriquement connexes. Par fonctorialité de Picard, on obtient un S-morphisme $\alpha^* : J(Y) \to J(X)$, puis un S-morphisme $\alpha_* = \alpha^{**} : J(X) \to J(Y)$, dont on dit qu'il est induit par α par fonctorialité d'Albanese.

Proposition 7.2.3 *On suppose que l'indice de ramification absolu e de $L/\mathbb{Q}_\ell$ vérifie : $e < \ell - 1$. Si $Y = X/G$ pour un groupe fini (constant) G agissant sur $X_{/S}$, et $Y(L) \neq \emptyset$, alors il existe un quotient abélien G' de G tel que*

$$\ker\left(\mathrm{Pic}^0(Y_{/S}) \to \mathrm{Pic}^0(X_{/S})\right) = (G')^D.$$

Preuve: Soit $C_{/S} = \ker\left(\mathrm{Pic}^0(Y) \to \mathrm{Pic}^0(X)\right)$. D'après la proposition (7.2.2), si $C_{/L}$ est fini, alors $C_{/S}$ est fini et plat. D'après [27], il existe alors un unique prolongement fini et plat de $C_{/L}$. Si $C_{/L} \simeq (G')^D_{/L}$, on a donc $C_{/S} \simeq (G')^D_{/S}$: on est ainsi directement ramené à la proposition suivante : □

Proposition 7.2.4 *Soit L un corps, $X_{/L}$ une courbe lisse, propre et connexe, munie d'une action d'un groupe fini (constant) G. Si $Y = X/G$ a un point L-rationnel, il existe un quotient abélien G' de G tel que :*

$$\ker\left(\mathrm{Pic}^0(Y_{/S}) \to \mathrm{Pic}^0(X_{/S})\right) = (G')^D.$$

Preuve: Soient $f : X \to L$ et $g : Y \to L$ les morphismes structuraux. On pose :

$$C_{/L} = \ker\left(\mathrm{Pic}(Y_{/L}) \to \mathrm{Pic}(X_{/L})\right).$$

Soit T un L-schéma, et $x \in C(T)$. Par hypothèse, Y admet une L-section, donc par la proposition 7.2.1,

$$\mathrm{Pic}(Y_{/L})(T) = \mathrm{Pic}(Y \times_L T)/\mathrm{Pic}(T).$$

Soit $\mathcal{L}$ un faisceau inversible sur $Y \times_L T$ correspondant à x. Comme le faisceau inversible $\alpha^*(\mathcal{L})$ de $X \times_L T$ devient trivial dans $\mathrm{Pic}(X_{/L})(T)$, il résulte de (7.1) que $\alpha^*(\mathcal{L}) \approx f^*(\mathcal{L}_0)$, pour un faisceau inversible $\mathcal{L}_0$ sur T. Remplaçant $\mathcal{L}$ par $\mathcal{L} \otimes g^*(\mathcal{L}_0^{-1})$, on obtient : $\alpha^*(\mathcal{L}) \approx O_{X \times_L T}$. Fixant un tel isomorphisme, l'action de G sur $\alpha^*(\mathcal{L})$ induit alors un morphisme $G \to \mathrm{Aut}(O_{X \times_L T}) = \Gamma\left(X \times_L T, O^*_{X \times_L T}\right)$. Comme $f_*(O_{X \times_L T}) = O_T$ d'après la proposition 7.2.1, on en déduit donc un morphisme

$$G \to O_T(T)^* = \mathbb{G}_m(T),$$

qui se factorise nécéssairement en :

$$\theta(x) : G^{\mathrm{ab}} \to \mathbb{G}_m(T).$$

On vérifie aisément que $\theta(x)$ ne dépend, ni du choix de $\mathcal{L}$ dans la classe de x vérifiant $\alpha^*(\mathcal{L}) \approx O_{X \times_L T}$, ni du choix de cet isomorphisme.

On obtient ainsi un morphisme de L-schémas en groupes :

$$\theta : C \to (G^{\mathrm{ab}})^D.$$

Mais θ est injectif : cela résulte par exemple de [3, Theo 4] (descente fpqc des morphismes de faisceaux quasi-cohérents). En particulier, $C(\overline{L})$ est fini, donc son image dans le groupe de Néron-Séveri de Y est triviale, puisque ce groupe est sans torsion (cf. [3, 9.3 Coro 14]). A fortiori, C est aussi le noyau de $\mathrm{Pic}^0(\alpha)$:

$$C_{/L} = \ker\left(\alpha^* : \mathrm{Pic}^0(Y_{/L}) \to \mathrm{Pic}^0(X_{/L})\right)$$

Pour conclure, il ne nous reste donc plus qu'à vérifier que

$$\theta(C(\overline{L})) = (G')^D(\overline{L}) \subset (G^{\mathrm{ab}})^D(\overline{L})$$

pour un quotient G' de G^{ab} : cela résulte de [DG, II §1.2.11 et IV §1.1.7]. $\square$

7.3 Conclusion

On prend maintenant $L = \mathbb{Q}_{\ell^2}$, $R = \mathbb{Z}_{\ell^2}$, $k = \mathbb{F}_{\ell^2}$, et $S = \mathrm{Spec}(R)$. Comme $\ell \neq 2, 3$, $2 < \ell - 1$. Soit $J_I(N)_{/S}$ le Pic^0 relatif de $X_I(N)_{/S}$ et $J_0(N)_{/S}$ celui de $X_0(N)_{/S}$.

D'après la section 7.1, le morphisme

$$\alpha : X_I(N) \to X_0(N)_{\mathbb{Z}_{\ell^2}}$$

est de la forme

$$X_I(N) \to X_I(N)/G.$$

pour le groupe fini (constant) $G = \Gamma_0(N)$. Il résulte donc de la proposition 7.2.3 que le noyau de

$$\mathrm{Pic}^0(\alpha) = \alpha^* : J_0(N) \to J_I(N)$$

est le dual de cartier d'un quotient abélien G' de G :

$$\ker(\alpha^*) = (G')^D_{/S}.$$

D'autre part, $\mathrm{Sh}_N = \ker(\alpha^*)(\overline{L})$ est le sous-groupe de Shimura de $J_0(N)(\overline{L})$; c'est aussi le noyau de $J_0(N)(\overline{L}) \to J_1(N)(\overline{L}) = \mathrm{Pic}^0(X_1(N))(\overline{L})$, et son cardinal divise $\varphi(N)$ (cf. [14]). Le cardinal de G' est donc précisément le cardinal de Sh_N, et divise $\varphi(N)$.

Par ailleurs, la proposition 7.2.2 montre que

$$J_0(N)(k)/\alpha_* \left(J_I(N)(k)\right) \simeq \mathrm{H}^1(k, G') \simeq G'$$

(puisque G' est constant).

Comme $\alpha_{/k}$ envoie l'ensemble des points supersinguliers de $X_I(N)_{/k}$ sur l'ensemble $X_0^{\mathrm{ss}}(N)(k)$ des points supersinguliers de $X_0(N)_{/k}$, le théorème d'Ihara, et plus précisément son corollaire 7.1.1 implique que le sous-groupe $J_0^{\mathrm{ss}}(N)(k)$ de $J_0(N)(k)$ engendré par $(x - y)$, pour tous $x, y \in X_0^{\mathrm{ss}}(N)(k)$, est précisément :

$$J_0^{\mathrm{ss}}(N)(k) = \alpha_* \left(J_I(N)(k)\right).$$

Finalement, on obtient donc

$$J_0(N)(k)/J_0^{\mathrm{ss}}(N)(k) \simeq G',$$

et la propositionest établie.

Chapitre 8

Torsion rationnelle

Soit p un nombre premier, c un entier premier à p. Le but de cette section est d'étudier le sous-groupe :

$$\mathrm{Gal}(K[cp^\infty]/K)^{\mathrm{rat}}_{\mathrm{tors}} \subset \mathrm{Gal}(K[cp^\infty]/K)_{\mathrm{tors}} = \mathrm{Gal}(K[cp^\infty]/H_{p^\infty}).$$

Soit donc $\hat{\lambda} = (\hat{\lambda}_q)_q \in \widehat{K}$ tel que $\hat{\lambda}_p = 1$, et

$$\sigma = [K[cp^\infty]/K, \hat{\lambda}] \in \mathrm{Gal}(K[cp^\infty]/K)_{\mathrm{tors}}.$$

Soit r *l'ordre exact* de σ. On pose, pour tout $n \geq 0$:

$$I_n = O_{cp^n}.\hat{\lambda}.$$

C'est un idéal O_{cp^n}-propre, et pour tout nombre premier q,

$$(I_n)_q = \begin{cases} (I_0)_q & \text{si } q \neq p \\ (O_{cp^n})_q & \text{si } q = p. \end{cases}$$

En particulier, si $n' \geq n$,

$$O_{cp^n} I_{n'} = I_n. \tag{8.1}$$

D'autre part, le noyau de $[K[cp^\infty]/K, \star]$ contient $K^*\widehat{\mathbb{Z}} = K^*\widehat{\mathbb{Q}}^*$. On peut donc changer chaque composante $\hat{\lambda}_q$, $q \neq p$, en $q^{n_q}\hat{\lambda}_q$, sans changer l'élément σ. Un choix judicieux des $n_q \in \mathbb{Z}$ permet de garantir que

$$I_0 \subset_N O_c$$

pour un entier N convenable, premier à p. On a alors, pour tout $n \geq 0$:

$$I_n \subset_N O_{cp^n}.$$

Pour tout nombre premier q, soit $v(q) = v_q(N)$ la q-valuation de N, et définissons l'idéal $I_n(q)$ par :

$$I_n(q)/I_n = q^{v(q)}\left(O_{cp^n}/I_n\right).$$

Fait 8.0.1

1. *$I_n \subset_{N/q^{v(q)}} I_n(q) \subset_{q^{v(q)}} O_{cp^n}$.*
2. *$I_n(q)$ est O_{cp^n}-propre.*
3. *Si $n' \geq n$, $O_{cp^n} I_{n'}(q) = I_n(q)$.*
4. *$I_n = \prod_{q|N} I_n(q) = \bigcap_{q|N} I_n(q)$.*

Preuve: 1) est évident. Pour tout nombre premier q', on a :

$$(I_n(q))_{q'} = \begin{cases} (O_{cp^n})_q & \text{si } q \neq q' \\ (I_n)_q & \text{si } q = q'. \end{cases}$$

Donc : 2) $J_n(q)$ est localement principal donc propre. 3) et 4) se vérifient de même place par place. □

Fait 8.0.2 *Pour tout nombre premier q,*

1. *$r \times v(q)$ est pair.*
2. *$I_n(q)^r = q^{\frac{r \times v(q)}{2}} O_{cp^n}$.*
3. *Si $q \nmid c$, $v(q) = 0$ si q est inerte ou décomposé, et $v(q) = 0$ ou 1 si q est ramifié dans K.*

Preuve: Par hypothèse,

$$\left(\frac{K[cp^n]/K}{I_n}\right)^r = 1 = \left(\frac{K[cp^n]/K}{I_n^r}\right)$$

donc I_n^r est principal, et d'indice N^r dans O_{cp^n}. Soit x_n un générateur : $I_n^r = O_{cp^n} x_n$. Donc $I_0^r = O_c x_n$ pour tout n, et en particulier, $x_n \in O_c$ ne prend qu'un nombre fini de valeurs puisque I_0^r n'a qu'un nombre fini de générateurs. Soit $x \in O_c$ tel que $x_n = x$ pour une infinité de n. D'après (8.1), on a alors : $I_n^r = O_{cp^n} x$ pour tout n.

1) Ecrivant $O_K = [1, \varpi_K]$ (notations de 1.1) et $x = a + bc\varpi_K$ avec $a, b \in \mathbb{Z}$, on a : $x \in [1, cp^n \varpi_K]$ pour tout n, donc $b = 0$ et $x = a \in \mathbb{Z}$. Quitte à changer x en $-x$, on peut donc supposer que $x \in \mathbb{N}^*$, de sorte que I_n^r étant d'indice N^r dans O_{cp^n}, $x = \sqrt{N^r} \in \mathbb{N}$, et pour tout $q \mid N$, $r \times v(q)$ est pair.

2) On a

$$I_n^r \subset_{N/q^{r \times v(q)}} I_n(q)^r \subset_{q^{r \times v(q)}} O_{cp^n} \quad \text{et} \quad I_n^r \subset_{N/q^{r \times v(q)}} q^{\frac{r \times v(q)}{2}} O_{cp^n} \subset_{q^{r \times v(q)}} O_{cp^n}.$$

Donc $I_n(q)^r = q^{\frac{r \times v(q)}{2}} O_{cp^n}$.

3) Bien entendu, $v(q) \neq 0$ si et seulement si $q \mid N$. Soit donc $q \mid N$, $q \nmid c$. L'idéal $J_n(q)$ défini par :

$$J_n(q)/I_n = q\,(O_{cp^n}/I_n)$$

est propre par la proposition 1.7.1, et vérifie :

$$J_n(q) \subset_q O_{cp^n}$$

D'après la proposition 1.3.2, q ne peut pas être inerte dans K. Mais q ne peut pas non plus être décomposé : s'il l'était, $J_n(q) = Q$ serait l'un des deux idéaux premiers de O_{cp^n} sur q. Mais de $I_n(q) \subset_{q^{v(q)}} O_{cp^n}$ et $I_n(q) \subset Q$, on déduirait alors que $I_n(q) = Q^{v(q)}$. Or $I_n(q)^r = q^{\frac{r \times v(q)}{2}} O_{cp^n} = Q^r$, une contradiction, puisque O_{cp^n}/Q^r est cyclique. Donc, si $q \nmid c$ et $q \mid N$, q est ramifié. Soit Q l'unique idéal premier de O_{cp^n} sur q. On a alors : $I_n(q) = Q^{v(q)}$. Si $v(q)$ était supérieur à 2, on aurait donc $I_n(q) \subset Q^2 = qO_{cp^n} \subset O_{cp^n}$, ce qui contredirait le fait que $I_n(q) \subset_N O_{cp^n}$. Donc $v(q) = 1$. $\square$

Corollaire 8.0.3 $\mathrm{Gal}(K[p^\infty]/K)^{\mathrm{rat}}_{\mathrm{tors}}$ *est le sous-groupe de* $\mathrm{Gal}(K[p^\infty]/K)$ *engendré par les Frobenius des nombres premiers* $q \neq p$ *qui sont ramifiés dans* K.

Chapitre 9

La conjecture de Mazur

9.1 Résultat principal

9.1.1 Préliminaires

Soit $N \geq 1$ un entier, et p un nombre premier. On écrit $N = N_0 p^{\mu}$, où N_0 est premier à p.

On souhaite dans cette section considérer des familles infinies de points CM *définis sur* $K[p^{\infty}]$. Compte tenu des résultats de la section sur le graphe des p-isogénies, et notamment la proposition 2.3.2, on voit qu'il nous faut faire l'hypothèse suivante :

– Si q est un facteur premier de N_0, alors soit q est décomposé dans K, soit q est ramifié dans K, mais alors q divise exactement N_0.

Dans ce cas, on peut effectivement construire de telles familles. Plus précisément, choisissons pour tout facteur premier q de N_0 un idéal premier Q de O_K sur q, et soit $\mathcal{N}_0$ l'idéal propre de O_K défini par :

$$\mathcal{N}_0 = \prod_{q|N_0} Q^{v_q(N_0)}.$$

On pose également, pour tout $n \geq 0$,

$$\mathcal{N}_n = \mathcal{N}_0 \cap O_{p^n}.$$

C'est un idéal O_{p^n}-propre de O_K, et $\mathcal{N}_n \subset_{N_0} O_{p^n}$.

Soit $E_{/\mathbb{C}}$ une courbe elliptique *à multiplication complexe par* O_K, et définissons le sous-groupe $C \subset E(\mathbb{C})$ par :

$$C = E(\mathbb{C})[\mathcal{N}_0].$$

C'est un sous-groupe cyclique d'ordre N_0 de $E(\mathbb{C})$, et la courbe elliptique E/C a également multiplication complexe par O_K.

On définit alors l'ensemble

$$\mathcal{L}(E, \mathcal{N}_0) \subset X_0(N)(\mathbb{C})$$

comme dans la section 6.1, c'est-à-dire qu'un point de $\mathcal{L}(E,\mathcal{N}_0)$ correspond à une isogénie cyclique de degré N, $f : E_1 \to E_2$, telle qu'il existe une isogénie $g : E \to E_1$ de degré une puissance de p, vérifiant de plus $g(C) = \ker(f)[N_0]$. Choisissant les identifications de K avec les $\mathrm{End}^0_{\mathbb{C}}(\star)$ des courbes elliptiques comme expliqué dans la section 3.1, le sous-groupe $g(C)$ de $E_1(\mathbb{C})$ peut alors également être décrit comme :

$$g(C) = E_1(\mathbb{C})[\mathcal{N}_n],$$

où $p^n = c(E_1)$ est le conducteur de E_1. La courbe elliptique E_2 est alors de conducteur $c(E_2) = p^{n+\delta}$, où $\delta \in [-\mu \cdots + \mu]$, et

$$x = [f : E_1 \to E_2] \in X_0(N)(K[p^{n+\max(0,\delta)}]$$

d'après la proposition 4.2.1. En particulier, on a bien :

$$\mathcal{L}(E,\mathcal{N}_0) \subset X_0(N)(K[p^\infty]).$$

On peut encore décrire cet ensemble de la manière suivante : pour se donner un point de $\mathcal{L}$, il suffit de se donner une inclusion $C_1 \subset C_2$ de sous-groupes de $E(\mathbb{C})$ telle que : C_1 soit d'ordre une puissance de p, et $C_2/C_1 \simeq \mathbb{Z}/p^\mu\mathbb{Z}$. Le point correspondant de $\mathcal{L}(E,\mathcal{N}_0)$ est alors :

$$x(C_1 \subset_{p^\mu} C_2) = [E/C_1 \to E/\left(C \oplus C_2\right)] \in X_0(N)\left(K[p^\infty]\right).$$

9.1.2 Notations

Nous avons en fait besoin d'une hypothèse plus forte sur N_0, à savoir l'*hypothèse de Heegner* selon laquelle :

– Tout facteur premier q de N_0 est décomposé dans K.

D'un autre côté, notons que p peut diviser N, et être inerte, ramifié ou décomposé dans K. On note

$$\mathcal{L} = \mathcal{L}(E,\mathcal{N}_0) \subset X_0\left(K[p^\infty]\right)$$

l'ensemble de points CM décrit précédemment.

D'autre part, posons :

$$G_0 = \mathrm{Gal}(K[p^\infty]/K)_{\mathrm{tors}}$$

de sorte que $G_0 = \mathrm{Gal}(K[p^\infty]/H_\infty)$ (cf. la définition). Si $\chi : G_0 \to A^*$ est un caractére de G_0 à valeur dans le groupe multiplicatif d'un anneau A, on note

$$e_\chi = \sum_{g\in G_0} \chi^{-1}(g)g \in A[G_0]$$

l'idempotent correspondant.

Soit enfin $\mathbb{A}_{/\mathbb{Q}}$ une variété abélienne *modulaire*, ce par quoi l'on entend qu'il existe un morphisme surjectif de variétés abéliennes $\alpha : J_0(N)_{/\mathbb{Q}} \to \mathbb{A}_{/\mathbb{Q}}$. On note alors $\pi : X_0(N) \to \mathbb{A}$ le composé de α avec le plongement usuel $X_0(N) \to J_0(N)$ qui envoie la pointe ∞ sur 0.

9.1.3 Résultats principaux

Théorème A *Pour tout caractère* $\chi : G_0 \to \mathbb{C}^*$*, l'espace vectoriel* $\mathcal{H}_\chi$ *engendré par*

$$\{e_\chi(\pi(a) \otimes 1) \mid a \in \mathcal{L}\} \subset \mathbb{A}(K[p^\infty]) \otimes \mathbb{C}$$

est de dimension infinie.

Avec $\chi = 1$, on obtient la conjecture de Mazur.

Théorème B *Soit* η_0 *le nombre de composantes connexes de* $\ker(\alpha)$*, et soit* q *un nombre premier ne divisant pas* $\varphi(Nd_K) \times \eta_0$*. Alors pour tout caractère* $\chi : G_0 \to \mathbb{F}_q^*$*, l'espace vectoriel* $\mathcal{H}_\chi$ *engendré par*

$$\{e_\chi(a \otimes 1) \mid a \in \mathcal{L}\} \subset \mathbb{A}(K[p^\infty]) \otimes \mathbb{F}_q$$

est de dimension infinie.

9.1.4 Le théorème B implique le théorème A.

Remarquons tout de suite que :

Lemme 9.1.1 *Le groupe* $\mathbb{A}(K[p^\infty])_{\rm tors}$ *est fini, et le groupe* $\mathbb{A}(K[p^\infty])/\mathbb{A}(K[p^\infty])_{\rm tors}$ *est libre.*

Preuve: [21] Soit v une place de $K[p^\infty]$ au-dessus d'un nombre premier $\ell \nmid N$ inerte dans K. Comme $\mathbb{A}_{/\mathbb{Q}}$ a bonne réduction en ℓ (étant un quotient de $J_0(N)_{/\mathbb{Q}}$), la réduction en v induit une application injective :

$$\mathbb{A}(K[p^\infty])_{\text{torsion}\neq\ell} \to \mathbb{A}(\mathbb{F}_{\ell^2})$$

Utilisant alors une deuxième place v' au-dessus d'un deuxième nombre premier $\ell' \nmid N\ell$, on obtient finalement que $\mathbb{A}(K[p^\infty])_{\rm tors}$ est fini. Soit alors $n_0 \geq 0$ un entier tel que $\mathbb{A}(K[p^\infty])_{\rm tors} = \mathbb{A}(K[p^{n_0}])_{\rm tors}$. Si $n' \geq n \geq n_0$, $\mathbb{A}(K[p^{n'}])/\mathbb{A}(K[p^n])$ est alors un groupe abélien libre (de rang fini), et le lemme en découle aisément. $\square$

Soit alors $\chi : G_0 \to \mathbb{C}^*$ un caractère de G_0, et O_χ l'anneau des entiers de $\mathbb{Q}(\chi(G_0))$. La dimension de $\mathcal{H}_\chi$ sur $\mathbb{C}$ est égal au rang du O_χ-module M_χ engendré dans $\mathbb{A}(K[p^\infty]) \otimes O_\chi$ par $\{e_\chi(a \otimes 1) \mid a \in \mathcal{L}\}$. D'autre part, pour tout idéal premier Q de O_χ tel que $O_\chi/Q \simeq \mathbb{F}_q$ (q un nombre premier), $\chi \bmod Q$ est un caractère de G_0 à valeur dans $\mathbb{F}_q^*$, et l'application

$$M_\chi/QM_\chi \to \mathcal{H}_{\chi \bmod Q}$$

est surjective. Si donc $\mathcal{H}_\chi$ était de dimension finie sur $\mathbb{C}$, M_χ serait de rang fini, donc de *type* fini d'après le lemme, et à fortiori, $\mathcal{H}_{\chi \bmod Q}$ serait de dimension finie sur $\mathbb{F}_q$.

Comme il existe une infinité d'idéaux premiers Q de O_χ de degré un (tel que $O_\chi/Q \simeq \mathbb{F}_q$ pour un nombre premier q), le théorème B implique le théorème A.

9.2 Preuve : la partie géométrique

Pour prouver le théorème B, on fixe un nombre premier q ne divisant pas $\varphi(Nd_K) \times \eta_0$, et un caractère

$$\chi : G_0 \to \mathbb{F}_q^*.$$

9.2.1 Changement de niveau

Soit

$$G_0^{\mathrm{rat}} = \mathrm{Gal}(K[p^\infty]/K)_{\mathrm{tors}}^{\mathrm{rat}} \subset G_0,$$

de sorte que d'après le corollaire 8.0.3, G_0^{rat} est exactement le sous-groupe de G_0 engendré dans $\mathrm{Gal}(K[p^\infty]/K)$ par les Frobénius des idéaux premiers Q qui sont ramifiés dans K et ne divisent pas p :

$$G_0^{\mathrm{rat}} =< \mathrm{Frob}_Q(K[p^\infty]/K) \ \mid \ Q \mid q \mid d_K,\, q \neq p >\subset G_0.$$

Ces Frobénius étant d'ordre deux, G_0^{rat} est un $\mathbb{F}_2$-espace vectoriel, et on peut en choisir une base parmi les Frob_Q :

$$G_0^{\mathrm{rat}} =\ll \mathrm{Frob}_{Q_i} \mid i = 1, \dots, g \gg,$$

où, si $i \in \{1, \dots, g\}$, $Q_i^2 = q_i O_K$ avec $q_i \mid d_K$ et $q_i \neq p$.

Posons alors $M = q_1 \cdots q_g$ (donc M est premier à pN), et pour tout diviseur $d \geq 1$ de M, définissons

$$\tau_d = \prod_{q_i \mid d} \mathrm{Frob}_{Q_i}(K[p^\infty]/K).$$

Par construction, on a donc

$$G_0^{\mathrm{rat}} = \{\tau_d \mid \quad d \mid M\}.$$

Soit $\mathcal{N}_0'$ l'idéal de O_K défini par

$$\mathcal{N}_0' = \mathcal{N}_0 Q_1 \cdots Q_g \subset_{N_0 M} O_K,$$

de sorte que

$$C' = E[\mathcal{N}_0'] = C \oplus E[Q_1 \cdots Q_g]$$

est un sous-groupe cyclique d'ordre $N_0 M$ de E, qui nous permet de définir, comme expliqué dans la section 9.1.1, un ensemble de points CM de niveau $NM = N_0 M p^\mu$:

$$\mathcal{L}' = \mathcal{L}(E, \mathcal{N}_0') \subset X_0(NM)\,(K[p^\infty])\,.$$

Les points de cet ensemble peuvent être paramétrés par les inclusions $C_1 \subset_{p^\mu} C_2$ de sous-groupes finis de $E(\mathbb{C})_{p-\mathrm{tors}}$: à une telle inclusion, on associe le point

$$x'(C_1 \subset_{p^\mu} C_2) = [E/C_1 \to E/\left(C' \oplus C_2\right)] \in \mathcal{L}'.$$

9.2.2 Action "géométrico-galoisienne" de $G_0^{\mathbf{rat}}$

Pour tout $d \mid M$, soit $\beta_d : X_0(NM) \to X_0(N)$ l'application de dégénérescence induite par

$$\beta_d[\mathcal{E} \to \mathcal{E}/\mathcal{C}] = [\mathcal{E}/\mathcal{C}\,[d] \to (\mathcal{E}/\mathcal{C}\,[d])\,/\,(\mathcal{C}\,[Nd]\,/\mathcal{C}\,[d])]$$

(pour $\mathcal{E}$ une courbe elliptique, $\mathcal{C}$ une $\Gamma_0(NM)$-structure).

On voit facilement que pour toute inclusion $C_1 \subset_{p^\mu} C_2 \subset E(\mathbb{C})_{p-\mathrm{tors}}$,

$$\beta_1\left(x'(C_1 \subset_{p^\mu} C_2)\right) = x(C_1 \subset_{p^\mu} C_2).$$

Ainsi, $\beta_1(\mathcal{L}') = \mathcal{L}$. Mais plus généralement,

Lemme 9.2.1 *Pour tout $d \mid M$ et toute inclusion $C_1 \subset_{p^\mu} C_2 \subset E(\mathbb{C})_{p-tors}$,*

$$\beta_d\left(x'(C_1 \subset_{p^\mu} C_2)\right) = \tau_d \cdot x(C_1 \subset_{p^\mu} C_2)$$

Preuve: Posons $a = x(C_1 \subset_{p^\mu} C_2)$ et $a' = x'(C_1 \subset_{p^\mu} C_2)$, de sorte que

$$\begin{array}{rcl} a & = & [E/C_1 \to E/\left(C \oplus C_2\right)] \\ a' & = & [E/C_1 \to E/\left(C \oplus E[Q_1 \cdots Q_g] \oplus C_2\right)]\,. \end{array}$$

Soit p^n le plus grand des conducteurs des quatre courbes elliptiques impliquées, de sorte que

$$\begin{array}{rcl} a & \in & X_0(N)(K[p^n]) \\ a' & \in & X_0(NM)(K[p^n]). \end{array}$$

Pour tout $d \mid M$, posons

$$Q_{d,n} = \prod_{q_i \mid d} Q_{i,n} \quad \text{où} \quad Q_{i,n} = Q_i \cap O_{p^n}\,.$$

de sorte que $Q_{d,n}$ est un O_{p^n}-ideal propre, et $\tau_d = \left(\frac{K[p^n]/K}{Q_{d,n}}\right)$. D'après la proposition 4.3.1, on a donc :

$$\tau_d a = \left[(E/C_1)^{Q_{d,n}} \to \left(E/\left(C \oplus C_2\right)\right)^{Q_{d,n}}\right]$$

Mais l'inclusion d'idéaux O_{p^n}-propres $Q_{d,n} \subset_d O_{p^n}$ induit un diagramme commutatif à lignes exactes :

$$\begin{array}{ccccc} (E/C_1)\,[Q_{d,n}] & \hookrightarrow & (E/C_1) & \twoheadrightarrow & (E/C_1)^{Q_{d,n}} \\ \downarrow & & \downarrow & & \downarrow \\ (E/\left(C \oplus C_2\right))\,[Q_{d,n}] & \hookrightarrow & (E/\left(C \oplus C_2\right)) & \twoheadrightarrow & (E/\left(C \oplus C_2\right))^{Q_{d,n}} \end{array}$$

et il est clair que :

$$\begin{array}{rcl} (E/C_1)\,[Q_{d,n}] & = & (C_1 \oplus E[Q_d])\,/C_1 \\ (E/\left(C \oplus C_2\right))\,[Q_{d,n}] & = & (C \oplus C_2 \oplus E[Q_d])\,/C_1. \end{array}$$

Ainsi,

$$\tau_d a = [(E/(C_1 \oplus E[Q_d])) \to (E/(C \oplus C_2 \oplus E[Q_d]))].$$

D'autre part, pour calculer $\beta_d(a')$, écrivons :

$$D = \left(C \oplus C_2 \oplus E[Q_{M/d}] \oplus E[Q_d]\right)/C_1 \subset (E/C_1)(\mathbb{C}).$$

On a donc :

$$\begin{aligned}\beta_d(a') &= \beta_d\,[(E/C_1) \to (E/C_1)/D] \\ &= [(E/C_1)/D[d] \to (E/C_1)/(D[Nd]/D[d])].\end{aligned}$$

Mais

$$D[d] = (C_1 \oplus E[Q_d])/C_1 \quad \text{et} \quad D[Nd] = (C \oplus C_2 \oplus E[Q_d])/C_1$$

de sorte que

$$\beta_d(a') = [(E/(C_1 \oplus E[Q_d])) \to (E/(C \oplus C_2 \oplus E[Q_d]))] = \tau_d a$$

$\square$

9.2.3 Une nouvelle paramétrisation

La restriction du caractère χ à G_0^{rat} se factorise par $\{\pm 1\} \subset \mathbb{F}_q^*$. On peut donc relever cette restriction en un caractère de G_0^{rat} à valeur dans $\{\pm 1\} \subset \mathbb{Z}$. Soit $\mathrm{Div}(M)$ l'ensemble des diviseurs positifs de M : on a donc $\#\mathrm{Div}(M) = 2^g$. On définit alors :

- $u : X_0(NM) \to X_0(N)^{\mathrm{Div}(M)}$ par $u(x) = (\beta_d(x))_{d|M}$,
- $s_\chi : \mathbb{A}^{\mathrm{Div}(M)} \to \mathbb{A}$ par $s_\chi(x_d)_{d|M} = \sum_{d|M} \chi(\tau_d) x_d$, et
- $\pi_\chi : X_0(NM) \to \mathbb{A}$ par $\pi_\chi = s_\chi \circ (\pi^{\mathrm{Div}(M)}) \circ u$.

Choisissons également un système complet de représentants $\{1\} \in \mathcal{R} \subset G_0$ de G_0/G_0^{rat}. Le lemme 9.2.1 montre que pour tout élément $a \in \mathcal{L}$, il existe un élément $a' \in \mathcal{L}'$ tel que, dans $\mathbb{A}(K[p^\infty]) \otimes \mathbb{F}_p$,

$$\begin{aligned} e_\chi(\pi(a) \otimes 1) &= \sum_{\sigma \in \mathcal{R}} \chi^{-1}(\sigma) \cdot \sigma \cdot (\pi_\chi(a') \otimes 1) \\ &= \sum_{\sigma \in \mathcal{R}} \chi^{-1}(\sigma) \cdot (\pi_\chi(\sigma \cdot a') \otimes 1). \end{aligned} \tag{9.1}$$

Comme $\beta_d(\infty \in X_0(NM)) = (\infty \in X_0(N))$, le morphisme

$$(\beta_d)_* : J_0(NM) \to J_0(N)$$

induit par β_d par fonctorialité d'Albanese, commute avec les plongements usuels des courbes modulaires dans leurs Jacobiennes. Soient :

- $u_* : J_0(NM) \to J_0(N)^{\mathrm{Div}(M)}$ le produit de ces morphismes,

- $s_\chi : J_0(N)^{\mathrm{Div}(M)} \to J_0(N)$ donné par $(x_d)_{d|M} \mapsto \sum_{d|M} \chi(\tau_d)x_d$, et
- $\alpha_\chi = \alpha \circ s_\chi \circ u_* : J_0(NM) \to \mathbb{A}$.

On a donc $\alpha_\chi(x - \infty) = \pi_\chi(x)$ pour tout $x \in X_0(NM)$. D'autre part, le dual de α_χ est un morphisme $\alpha_\chi^{\mathrm{dual}} : \mathbb{A}^{\mathrm{dual}} \to J_0(NM)^{\mathrm{dual}} = J_0(NM)$, composé de :

- $\alpha^{\mathrm{dual}} : \mathbb{A}^{\mathrm{dual}} \to J_0(N)^{\mathrm{dual}} = J_0(N)$, dont le noyau est fini et isomorphe au dual de Cartier du groupe des composantes connexes de $\ker(\alpha)$ (cf. 7.2.2),
- $s_\chi^{\mathrm{dual}} : J_0(N) \to J_0(N)^{\mathrm{Div}(M)}$, le plongement $x \mapsto (\chi(\tau_d)x)_{d|M}$, et
- $u^{\mathrm{dual}} : J_0(N)^{\mathrm{Div}(M)} \to J_0(NM)$, donné par $(x_d)_{d|M} \mapsto \sum_{d|M} \beta_d^*(x)$.

Lemme 9.2.2 $\ker(u^{\mathrm{dual}})$ *est fini, de rang divisant une puissance de* $\varphi(NM)$.

Preuve: Si $g = 0$, $M = 1$ et il n'y a rien à prouver. Sinon, posons $M' = q_1 \ldots q_{g-1}$, et considérons la factorisation suivante de u^{dual} :

$$\left(J_0(NM)^2\right)^{\mathrm{Div}(M')} \overset{v^{\mathrm{Div}(M')}}{\longrightarrow} J_0(NM')^{\mathrm{Div}(M')} \overset{u'^{\mathrm{dual}}}{\longrightarrow} J_0(N)$$

où $v : J_0(NM)^2 \to J_0(NM')$ est la somme des deux applications de dégénérescence $J_0(NM) \to J_0(NM')$, et u'^{dual} est construit exactement comme u^{dual}, mais avec M remplacé par M'. D'après [29, Theo. 4.3] :

$$\ker(v)(\mathbb{C}) = \{(x, y) \in \mathrm{Sh}_{NM} \mid x + y = 0\}$$

où $\mathrm{Sh}_{NM} = \ker\left(J_0(NM) \to J_1(NM)\right)(\mathbb{C})$ est le sous-groupe de Shimura de $J_0(NM)$. Le rang de $\ker(v)$ divise donc $\varphi(NM)$ (cf. [14]), et le lemme en découle par induction. $\square$

Il en résulte que le noyau $\ker(\alpha_\chi^{\mathrm{dual}})$ est fini, de rang divisant une puissance de $\varphi(Nd_K) \times \eta_0$ (puisque $M \mid d_K$).

Les morphismes $\alpha_\chi : J_0(NM) \to \mathbb{A}$ et $\alpha_\chi^{\mathrm{dual}} : \mathbb{A}^{\mathrm{dual}} \to J_0(NM)$, initialement définis sur $\mathbb{Q}$, s'étendent uniquement aux modèles de Néron en des morphismes :

$$\alpha_\chi : J_0(NM)_{/\mathbb{Z}[1/NM]} \to \mathbb{A}_{/\mathbb{Z}[1/NM]}$$

et

$$\alpha_\chi^{\mathrm{dual}} : (\mathbb{A})^{\mathrm{dual}}_{/\mathbb{Z}[1/NM]} \to J_0(NM)_{/\mathbb{Z}[1/NM]}$$

Proposition 9.2.3 *Pour tout nombre premier* $\ell \nmid 6NM$,

$$(\alpha_\chi \otimes 1)\left(J_0^{\mathrm{ss}}(NM)(\mathbb{F}_{\ell^2}) \otimes \mathbb{F}_q\right) = \mathbb{A}(\mathbb{F}_{\ell^2}) \otimes \mathbb{F}_q,$$

où $J_0^{\mathrm{ss}}(NM)(\mathbb{F}_{\ell^2})$ *est le sous-groupe de* $J_0(NM)(\mathbb{F}_{\ell^2})$ *engendré par* $(x - y)$, $x, y \in X_0^{\mathrm{ss}}(NM)(\mathbb{F}_{\ell^2})$.

Preuve: D'après la proposition 7.2.2, l'indice

$$[\mathbb{A}(\mathbb{F}_{\ell^2}) : \alpha_\chi\left(J_0(NM)(\mathbb{F}_{\ell^2})\right)]$$

divise une puissance de $\varphi(Nd_K) \times \eta_0$. En particulier,

$$(\alpha_\chi \otimes 1)\left(J_0(NM)(\mathbb{F}_{\ell^2}) \otimes \mathbb{F}_q\right) = \mathbb{A}(\mathbb{F}_{\ell^2}) \otimes \mathbb{F}_q.$$

D'autre part, la propositionaffirme que

$$[J_0(NM)(\mathbb{F}_{\ell^2}) : J_0^{\mathrm{ss}}(NM)(\mathbb{F}_{\ell^2})] \text{ divise } \varphi(NM),$$

donc à nouveau,

$$J_0^{\mathrm{ss}}(NM)(\mathbb{F}_{l^2}) \otimes \mathbb{F}_q = J_0(NM)(\mathbb{F}_{l^2}) \otimes \mathbb{F}_q .$$

D'où la proposition. □

9.3 Preuve : la partie chaotique

Comme les éléments de $\mathcal{R}$ sont par définition deux à deux non congruents modulo G_0^{rat}, et sont de plus d'ordre fini, ils sont également deux à deux non congruents modulo $\mathrm{Gal}(K[p^\infty]/K)^{\mathrm{rat}}$. On peut ainsi appliquer le théorème 6.2.1 à $\mathcal{R}$, avec l'ensemble $\mathcal{L}'$ de points CM de $X_0(NM)(K[p^\infty])$.

Soit donc S un ensemble fini de nombres premiers inertes dans K, ne divisant pas $6NMp$, et choisissons pour chaque $\ell \in S$ une place v_ℓ de $K[p^\infty]$ sur ℓ, de corps résiduel $k(\ell) \approx \mathbb{F}_{\ell^2}$. Avec les notations du théorème 6.2.1, l'application

$$\begin{array}{rccc} \mathrm{RED} : & \mathcal{L}' & \to & \prod_{l\in S} \left(X_0^{\mathrm{ss}}(NM)(k(\ell))\right)^{\mathcal{R}} \\ & a' & \mapsto & (\mathrm{red}_\ell(\sigma\cdot a'))_{\sigma,\ell\in\mathcal{R}\times S} \end{array}$$

est surjective.

Considérons alors l'application $\mathbb{F}_q$-linéaire :

$$\begin{array}{rccc} \mathrm{R}_S : & \mathbb{A}(K[p^\infty])\otimes\mathbb{F}_q & \to & \bigoplus_{\ell\in S}\mathbb{A}(k(\ell))\otimes\mathbb{F}_q \\ & x\otimes 1 & \mapsto & \bigoplus_{\ell\in S}\mathrm{red}_\ell(x)\otimes 1 \end{array}$$

Pour $\ell \in S$ et $x, y \in X_0^{\mathrm{ss}}(NM)(k(\ell))$, on peut trouver des éléments $a', b' \in \mathcal{L}'$ tels que *toutes* les composantes de $\mathrm{RED}(a')$ coïncident avec celles de $\mathrm{RED}(b')$, *sauf* celle correspondant à $(\ell, 1) \in S \times \mathcal{R}$, où $\mathrm{red}_\ell(a') = x$ et $\mathrm{red}_\ell(b') = y$. Posons $a = \beta_1(a')$ et $b = \beta_1(b')$, de sorte que a et b sont des éléments de $\mathcal{L}$, et, en utilisant (9.1), on a :

$$e_\chi.(\pi(a)\otimes 1) - e_\chi.(\pi(b)\otimes 1) = \sum_{\sigma\in\mathcal{R}} \chi^{-1}(\sigma)\cdot(\pi_\chi(\sigma\cdot a')\otimes 1 - \pi_\chi(\sigma\cdot b')\otimes 1).$$

Par suite, pour tout $\ell' \in S$,

$$\begin{aligned} &(\mathrm{red}_{\ell'}\otimes 1)\left(e_\chi.(\pi(a)\otimes 1) - e_\chi.(\pi(b)\otimes 1)\right) \\ &\qquad = \sum_{\sigma\in\mathcal{R}} \chi^{-1}(\sigma)\cdot\left(\pi_\chi(\mathrm{red}_{\ell'}(\sigma.a')) - \pi_\chi(\mathrm{red}_{\ell'}(\sigma.b'))\right)\otimes 1 \\ &\qquad = \begin{cases} 0 & \text{si } \ell' \neq \ell \\ \pi_\chi(x) - \pi_\chi(y) & \text{si } \ell' \neq \ell \end{cases} \end{aligned}$$

Donc,

$$\begin{aligned}
&\mathrm{R}_S\left(e_\chi.(\pi(a)\otimes 1)\right) - \mathrm{R}_S\left(e_\chi.(\pi(b)\otimes 1)\right)\\
&\qquad = \quad (0,\cdots,0,\pi_\chi(x)-\pi_\chi(y)\otimes 1,0,\cdots,0)\\
&\qquad = \quad (0,\cdots,0,\alpha_\chi(x-y)\otimes 1,0,\cdots,0)
\end{aligned}$$

La proposition 9.2.3 implique alors que R_S est *surjective* sur $\mathcal{H}_\chi$. En particulier,

$$\dim_{\mathbb{F}_q}(\mathcal{H}_\chi) \geq \sum_{\ell\in S} \dim_{\mathbb{F}_q}(\mathbb{A}(k(\ell))\otimes\mathbb{F}_q) \tag{9.2}$$

Pour conclure la preuve du théorème B, il nous reste donc à voir que l'on peut choisir l'ensemble S de telle sorte que le terme de droite dans (9.2) soit arbitrairement grand.

Posons $L = K(\mathbb{A}[q])$. C'est une extension galoisienne de $\mathbb{Q}$, que l'on plonge dans $\mathbb{C}$, pour obtenir une conjugaison complexe $\tau \in \mathrm{Gal}(L/\mathbb{Q})$. Soit S_∞ l'ensemble des nombres premiers $\ell \nmid 6NMq$, non ramifiés dans L, et tels que

$$\mathrm{Frob}_\ell(L/\mathbb{Q}) = [\tau] \in \mathrm{Gal}(L/\mathbb{Q})^{\mathrm{ab}}$$

Par le théorème de densité de Dirichlet, S_∞ est un ensemble *infini*.

Soit S un sous-ensemble fini de S_∞, et choisissons pour tout $\ell \in S$ un idéal premier Q_ℓ de L au-dessus de ℓ tel que $\mathrm{Frob}_{Q_\ell}(L/\mathbb{Q}) = \tau \in \mathrm{Gal}(L/\mathbb{Q})$. Choisissons encore une place v'_ℓ de $K[p^\infty](\mathbb{A}[q])$ sur Q_ℓ, puis prenons pour place v_ℓ de $K[p^\infty]$ sur ℓ la restriction de v'_ℓ à $K[p^\infty]$. Alors, ℓ est inerte dans K, et

$$\dim_{\mathbb{F}_q}(\mathbb{A}(k(\ell))\otimes\mathbb{F}_q) = 2\times\dim(A).$$

D'après (9.2), on a donc $\dim_{\mathbb{F}_q}(\mathcal{H}_\chi) \geq \#S \times 2 \times \dim(A)$. Choisissant S arbitrairement grand, on obtient en effet

$$\dim_{\mathbb{F}_q}(M_\chi) \geq \infty.$$

Quatrième partie

Appendice

Chapitre 10

Généralités

Tous les anneaux considérés sont supposés unitaires, mais pas nécessairement commutatifs. Un O-module est un O-module *à gauche*, sauf mention explicite du contraire. Tous les schémas en groupes sont commutatifs.

10.1 Le formalisme

On utilise une topologie Top sur les schémas, qui soit moins fine que la topologie canonique. Soit S un schéma, $\mathrm{Sch}_{/S}$ la catégorie des S-schémas, et O un anneau. On note ${}_O\mathrm{Pref}_{/S}$ la catégorie des S-préfaisceaux en O-module, ${}_O\mathrm{Fais}_{/S}$ la sous-catégorie pleine de ${}_O\mathrm{Pref}_{/S}$ des S-faisceaux (pour Top) en O-module, et enfin ${}_O\mathrm{Sch}_{/S}$ la sous-catégorie pleine de ${}_O\mathrm{Fais}_{/S}$ des S-schémas en O-module. On note également ${}_O\mathrm{Mod}$ la catégorie des O-module.

Si M est un O-module, et $G \in {}_O\mathrm{Pref}_{/S}$, on définit le préfaisceau en groupe abélien G^M par :

$$\forall T \in \mathrm{Sch}_{/S} : \qquad G^M(T) = \mathrm{Hom}_O(M, G(T)).$$

Cette construction est covariante et exacte à gauche en $G \in {}_O\mathrm{Pref}_{/S}$, contravariante et exacte à droite en $M \in {}_O\mathrm{Mod}$, et commute aux changements de base $S' \to S$.

10.1.1 Premières propriétés

Proposition 10.1.1

1. *Si G est un faisceau, G^M est un faisceau.*
2. *Si G est un schéma, et M un O-module de présentation finie, alors G^M est un schéma.*
3. *Si G est un schéma affine, et O un anneau noethérien à gauche, G^M est un schéma affine.*

Preuve: 1) Soit $(T_i \to T)_i$ un recouvrement de T pour la topologie Top. Si $G \in {}_O\mathrm{Fais}_{/S}$,

$$0 \to G(T) \to \prod_i G(T_i) \rightrightarrows \prod_i G(T_i \times_T T_j)$$

est exacte. Appliquant le foncteur exact à gauche $\mathrm{Hom}_O(M, \star)$, on obtient une suite exacte

$$0 \to G^M(T) \to \prod_i G^M(T_i) \rightrightarrows \prod_i G^M(T_i \times_T T_j).$$

Il en résulte que G^M est un faisceau.

2) Soit $O^m \to O^n \to M \to 0$ une présentation de M. Pour tout S-schéma T, le foncteur $\mathrm{Hom}_O(\star, G(T))$ étant exact à droite, on obtient :

$$0 \to G^M(T) \to G^n(T) \to G^m(T)$$

... qui réalise $G^M_{/S}$ comme le noyau d'un morphisme $G^n \to G^m$.

3) Le raisonnement précédent montre déjà que G^M est affine lorsque M est de type fini. Dans le cas général, on écrit M comme une limite inductive de O-modules de type fini, $M = \varinjlim M_i$, et alors $G^M = \varprojlim G^{M_i}$. □

10.1.2 Yoga du changement d'anneau

Soit $G \in {}_O\mathrm{Pref}_{/S}$, N un O-module à gauche. Soit également R un anneau agissant *à droite* O-linéairement sur N, et M un R-module à gauche. L'action de R sur N induit par fonctorialité une structure de S-préfaisceau en R-module sur le préfaisceau G^N, grâce à laquelle on peut former le préfaisceau $(G^N)^M$. Par définition, on a donc pour tout S-schéma T :

$$\begin{aligned}(G^N)^M(T) &= \mathrm{Hom}_R({}_RM, \mathrm{Hom}_O({}_ON_R, G(T)) \\ &= \mathrm{Hom}_O({}_ON_R \otimes_R M, G(T)) \\ &= G^{N \otimes_R M}(T)\end{aligned}$$

Exemple: Extension des scalaires.

Soit $O \to O'$ un morphisme d'anneau, et prenons $N = {}_O O'_{O'}$. $H = G^{O'}$ est alors un préfaisceau en O'-module, et pour tout O'-module M,

$$H^M = G^{({}_{[O]}O' \otimes_{O'} M)} = G^{{}_{[O]}M}$$

Exemple: Restriction des scalaires.

Soit $O'' \to O$ un morphisme d'anneau, et soit H le préfaisceau en O''-module déduit de G par restriction de scalaires à O''. Si N est un O''-module, on a donc pour tout S-schéma T :

$$\begin{aligned}H^N(T) &= \mathrm{Hom}_{O''}(N, G(T)) \\ &= \mathrm{Hom}_O(O \otimes_{O''} N, G(T)) \\ &= G^{O \otimes_{O''} N}(T)\end{aligned}$$

Si M est un O-module, et $N =_{[O'']} M$, le morphisme O-linéaire et surjectif $O \otimes_{O''} N \to M$ induit donc un monomorphisme de préfaisceau :

$$G^M \to G^{O \otimes_{O''} N} = H^N$$

Si F est un O''-préfaisceau, on a :

$$\mathrm{Hom}_{{}_O\mathrm{Pref}_{/S}}(G, F^O) = \mathrm{Hom}_{{}_{O''}\mathrm{Pref}_{/S}}(H, F)$$

Autrement dit, la restriction des scalaires ${}_O\mathrm{Pref}_{/S} \to {}_{O''}\mathrm{Pref}_{/S}$ est adjointe à gauche de l'extension des scalaires ${}_{O''}\mathrm{Pref}_{/S} \to {}_O\mathrm{Pref}_{/S}$. Comme d'autre part ces deux foncteurs préservent les faisceaux, la restriction des scalaires ${}_O\mathrm{Fais}_{/S} \to {}_{O''}\mathrm{Fais}_{/S}$ est adjointe à gauche de l'extension des scalaires ${}_{O''}\mathrm{Fais}_{/S} \to {}_O\mathrm{Fais}_{/S}$. Le foncteur de restriction est évidemment exact, et le foncteur d'extension envoie donc injectifs sur injectifs.

Appliquons ceci en particulier à $\mathbb{Z} \to O$. La catégorie des $\mathbb{Z}$-préfaisceaux (resp. faisceaux) est simplement la catégorie des préfaisceaux (resp. faisceaux) sur S en groupe abélien. Cette catégorie est abélienne et a assez d'injectif [17, III 1.1], et il en est donc de même des catégories ${}_O\mathrm{Pref}_{/S}$ et ${}_O\mathrm{Fais}_{/S}$ pour tout anneau O.

Exemple: Noyaux.

Soit a un idéal bilatère de O. En faisant opérer O à droite sur O/a et a on obtient une action à gauche de O sur $G^{O/a}$, ainsi que sur G^a. On notera $G[a] = G^{O/a}$ le préfaisceau en O-module ainsi obtenu. C'est un sous-préfaisceau en O-module de G, et c'est canoniquement un préfaisceau en O/a-module. Si M est un O-module tel que $a \cdot M = 0$, alors $G^M = G[a]^M$. On a une suite exacte de faisceaux en O-module :

$$0 \to G[a] \to G \to G^a.$$

En particulier, si $a = \mathrm{Ann}_O(M)$ pour un O-module M, a est un idéal bilatère et :

$$G^M = G[a]^M$$

De même, si α est un élément du centre $Z(O)$ de O et $\alpha \cdot M = 0$, alors :

$$G^M = G[\alpha]^M$$

Lemme 10.1.2 *Si $\varphi : O'' \to O$ est un morphisme d'anneau, et H le préfaisceau en O''-module déduit de G par restriction des scalaires, alors pour tout idéal I de O'', on a :*

$$H[I] = G[O\varphi(I)]$$

Preuve: Pour tout S-schéma T, $H[I](T) = \{x \in G(T) \mid \forall i \in I,\, \varphi(i) \cdot x = 0\}$. Or si $\varphi(I) \cdot x = 0$, à fortirori $O\varphi(I) \cdot x = 0$, donc $x \in G[O\varphi(I)](T)$. La réciproque est évidente. □

Dans la suite, on va essentiellement travailler avec des schémas.

10.2 Propriétés géométriques simples

Soit G un S-schéma *séparé* en O-module. On a alors vu que pour tout O-module de type fini M, $G^M_{/S}$ est un schéma.

Proposition 10.2.1 *Si $\mathcal{P}$ est l'une propriété de morphisme de schémas ci-dessous, alors : $\mathcal{P}(G_{/S}) \Rightarrow \mathcal{P}(G^M_{/S})$ pour tout O-module M de type fini.*

1. *quasi-compact (IV,1.1.2).*
2. *séparé (I,5.5.1).*
3. *localement de type fini (IV,1.3.4).*
4. *de type fini (IV,1.5.4).*
5. *localement de présentation finie (IV,1.4.3).*
6. *de présentation finie (IV,1.6.2).*
7. *propre (II,5.4.2).*
8. *entier (II,6.1.5).*
9. *fini (II,6.1.5).*
10. *quasi-fini (II, 6.2.4).*
11. *affine (II,1.6.2).*
12. *quasi-affine (II,5.1.10).*
13. *projectif (si S est quasi-compact) (II,5.5.5).*
14. *quasi-projectif (si S est quasi-compact) (II, 5.3.3 et 5.3.4).*

Preuve: Soit $O^m \to O^n \to M \to 0$ une présentation de M, de sorte que $G^M_{/S} = \ker(G^n \to G^m)$. $G_{/S}$ étant séparé, la section unité $S \to G^m$ est une immersion fermée, et le diagramme cartésien :

$$\begin{array}{ccc} G^M & \to & S \\ \downarrow & & \downarrow \\ G^n & \to & G^m \end{array}$$

montre alors que $G^M \to G^n$ est également une immersion fermée. Si donc $\mathcal{P}$ est une propriété des morphismes de schémas qui est vraie pour les immersions fermées, stable par changement de base et par composition, alors $\mathcal{P}(G_{/S}) \Rightarrow \mathcal{P}(G^M_{/S})$. C'est le cas pour toutes les propriétés ci-dessus, d'après les références indiquées dans [EGA], sauf pour : 5) et 6), car une immersion fermée n'est pas nécessairement localement de présentation finie ; 13) et 14), car le composé de deux morphismes quasi-projectifs (resp. projectifs) n'est pas nécessairement quasi-projectif (resp. projectif). Les références indiquées permettent néanmoins de conclure. □

Proposition 10.2.2

1. *Si $G_{/S}$ est plat (resp. lisse), $G^M_{/S}$ est plat (resp. lisse) pour tout O-module M de type fini et* projectif.
2. *Si $G_{/S}$ est étale, $G^M_{/S}$ est étale pour tout O-module M de type fini.*

Preuve: 1) M étant projectif, est facteur direct d'un module libre : $O^n = M \oplus N$, de sorte que $G^n = G^M \times_S G^N$. Si $s \in S$, on a donc $G^n_s = G^M_s \times_s G^N_s$, et la projection $G^n_s \to G^M_s$ est fidèlement plate. $G^n_{/S}$ étant plat, il résulte de [EGA, IV 11.3.11] que $G^n \to G^M$ est fidèlement plat, et $G^M_{/S}$ est plat. Si de plus $G_{/S}$ est lisse, il en est de même de $G^M_{/S}$ par [EGA, IV 17.7.7], compte tenu de ce que G et G^M sont alors localement de présentation finie sur S.

2) Si $G_{/S}$ est étale, $G^M_{/S}$ est localement de présentation finie puisque $G_{/S}$ l'est, et il reste donc à voir que $G^M_{/S}$ est formellement étale (cf. [EGA, IV 17.3.1]). Soit donc A un S-anneau et I un idéal nilpotent de A. Comme $G(A) \to G(A/I)$ est bijectif, $\mathrm{Hom}_O(M, G(A)) \to \mathrm{Hom}_O(M, G(A/I))$ l'est aussi, c'est-à-dire que $G^M(A) \to G^M(A/I)$ est bijectif ; donc $G^M_{/S}$ étale. □

10.3 Dimension relative, platitude et lissité

On suppose maintenant que $G_{/S}$ est un schéma en O-module, (séparé) et *de présentation finie* sur S.

10.3.1 Rappels sur les suites exactes

Proposition 10.3.1 *Soit $0 \to G' \to G \xrightarrow{f} G''$ une suite exacte de S-schémas en groupe de présentation finie sur S.*

1. *Si $G_{/S}$ est plat,*
   - *(a) $G_s \to G''_s$ est plat pour tout $s \in S \Leftrightarrow G \to G''$ est plat.*
   - *(b) Si tel est le cas, alors $G'_{/S}$ est plat et $G''_{/S}$ est plat aux points de $f(G)$.*
2. *Si $G_{/S}$ est lisse,*
   - *(a) $G_s \to G''_s$ est lisse pour tout $s \in S \Leftrightarrow G \to G''$ est lisse.*
   - *(b) Si tel est le cas, alors $G'_{/S}$ est lisse et $G''_{/S}$ est lisse aux points de $f(G)$.*
   - *(c) Si $G \to G''$ est plat, $G''_{/S}$ est lisse aux points de $f(G)$.*
3. *Dans* 1) *et* 2)*, on peut remplacer $s \in S$ par : s point géométrique de S.*
4. *Si S est le spectre d'un corps,*
   - *(a) $G \to G''$ est plat si G'' est réduit et $f(G^0) = G''^0$.*
   - *(b) $G \to G''$ est lisse si $G_{/k}$ est lisse et Lie(f) : Lie$(G)(k) \to$ Lie$(G'')(k)$ est surjectif.*

Preuve: 1) [EGA, IV 11.3.11]. 2) [EGA, IV 17.8.2] et [EGA, IV 17.7.7]. 3) résulte par exemple de [EGA, IV 2.3.13] pour 1), et de [EGA, IV 17.7.1] pour 2). 4) *a*) [DG, II §5.5.1], *b*) [DG, II §5.5.3]. □

10.3.2 Dimension additive

Définition *On dit que* la dimension relative de G est additive sur les suites exactes de O-modules *(ou plus simplement, que la dimension est additive), si pour tout point géométrique s de S, et toute suite exacte*

$$0 \to N \to P \to M \to 0$$

de O-modules, on a

$$dim(G_s^P) = dim(G_s^M) + dim(G_s^N).$$

Proposition 10.3.2 *Si $G_{/S}$ est plat, à dimension additive, et $G_{/S}^N$ est* lisse par fibre $\forall N \subset O^n$, *alors : $G_{/S}^M$ est plat pour tout M et $G_{/S}^N$ est lisse pour tout $N \subset O^n$.*

Preuve: Soit M un O-module de type fini, $0 \to N \to O^n \to M \to 0$ une suite exacte. Pour voir que $G_{/S}^M$ est plat, il suffit de voir que $G^n \to G^N$ est plat, et $G_{/S}^n$ étant plat, cela peut se tester sur les fibres géométriques. Soit donc $s = \mathrm{Spec}(k)$ un point géométrique de S. La catégorie des k-groupes algébriques étant abélienne ([TDTE, III 7.4]), on peut former le foncteur dérivé de $X \to G^X$. On obtient ainsi une suite *fppf* exacte :

$$0 \to G_k^M \to G_k^n \to G_k^N \to \mathrm{Ext}_O^1(N, G_k) \to 0.$$

L'additivité des dimensions montre alors que $\mathrm{Ext}_O^1(N, G_k)$ est de dimension 0, compte tenu de [DG, II §5.5.1]. Le morphisme $G_k^N \to \mathrm{Ext}_O^1(Q, G_k)$ est fidèlement plat, et G_k^N est lisse par hypothèse, donc $\mathrm{Ext}_O^1(Q, G_k)$ est lisse, et finalement étale ([DG, II §§5.1.4 et 5.2.1]). En particulier, le noyau G'_k de $G_k^N \to \mathrm{Ext}_O^1(Q, G_k)$ est *ouvert*, donc $G_k^n \to G'_k \to G_k^N$ est effectivement plat, puisque composé d'un morphisme fidèlement plat et d'une immersion ouverte.

Il en résulte donc que $G_{/S}^M$ est plat pour tout M. En particulier, si $N \subset O^n$, $G_{/S}^N$ est plat, donc également lisse puisque lisse par fibre ([EGA, IV 17.5.1]). $\square$

10.3.3 Un critère de dimension additive

Proposition 10.3.3 *Pour que $G_{/S}$ ait dimension additive sur les fibres, il faut et il suffit que, pour toute suite exacte*

$$0 \to M \to P \to Q \to 0$$

où P est un sous O-module d'un module libre*, pour tout point géométrique s de S, $dim(G_s^P) = dim(G_s^M) + dim(G_s^Q)$.*

Preuve: C'est clairement nécessaire. Montrons que c'est suffisant. Soit donc $0 \to Q' \to Q \to Q'' \to 0$ une suite exacte de O-module de type fini. Choisissons un début de résolution projective exacte :

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & M' & \to & M & \to & M'' & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & P' & \to & P & \to & P'' & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & Q' & \to & Q & \to & Q'' & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

où P', P, P'' sont O-projectifs, et M', M, M'' sont les noyaux, l'exactitude de la première ligne résultant du lemme du serpent. Sur un point géométrique s de S, on a donc :

$$\begin{array}{rcl}
\dim(G_s^{P'}) & = & \dim(G_s^{M'}) + \dim(G_s^{Q'}) \\
\dim(G_s^{P}) & = & \dim(G_s^{M}) + \dim(G_s^{Q}) \\
\dim(G_s^{P''}) & = & \dim(G_s^{M''}) + \dim(G_s^{Q''}) \\
\dim(G_s^{M}) & = & \dim(G_s^{M'}) + \dim(G_s^{M''}) \\
\dim(G_s^{P}) & = & \dim(G_s^{P'}) + \dim(G_s^{P''})
\end{array}$$

Ainsi :

$$\begin{array}{rcl}
\dim(G_s^{Q}) & = & \dim(G_s^{P}) - \dim(G_s^{M}) \\
 & = & \dim(G_s^{P'}) + \dim(G_s^{P''}) - \dim(G_s^{M'}) - \dim(G_s^{M''}) \\
 & = & \dim(G_s^{Q'}) + \dim(G_s^{Q'}).
\end{array}$$

$\square$

10.4 Exactitude

Soit G un S-schéma en O-module, de présentation finie sur S.

10.4.1 Le problème

Soit

$$0 \to N \to M \to P \to 0 \tag{10.1}$$

une suite exacte de O-modules. Elle induit donc une suite exacte :

$$0 \to G^P \to G^M \to G^N. \tag{10.2}$$

Plus précisément, on peut même former pour tout S-schéma T une suite exacte :

$$\begin{array}{l}
0 \to G^P(T) \to G^M(T) \to G^N(T) \to \\
\qquad \to \mathrm{Ext}^1_O(P, G(T)) \to \mathrm{Ext}^1_O(M, G(T)) \to \mathrm{Ext}^1_O(N, G(T)).
\end{array}$$

On a donc clairement : si P est O-projectif, (10.2) est exacte, et même scindée. Si $G(T)$ est O-injectif, (10.2)(T) est exacte. Au demeurant, l'exactitude d'une suite de schémas en groupe commutatif (ou de faisceaux) ne requiert pas cette exactitude, qui est même fausse en général, y compris pour les schémas en groupe finis, ou les schémas abéliens.

On s'intéresse à l'exactitude *fppf*, c'est-à-dire à l'exactitude de (10.2) dans la catégorie des faisceaux pour la topologie *fppf*. Cette exactitude signifie donc :

- pour tout S-schéma T et toute application O-linéaire $\alpha : N \to G(T)$, il existe un recouvrement *fppf* $T_i \to T$ et des morphismes O-linéaires $\alpha_i : M \to G(T_i)$, dont la restriction à N est le morphisme composé $\mathrm{res}\circ\alpha : N \to G(T) \to G(T_i)$.

Lorsque les O-modules N et M sont de type fini, on a vu que G^M et G^N était localement de présentation fini sur S, donc le morphisme $G^M \to G^N$ est également localement de présentation finie [EGA, IV 1.4.3]. Dire que $G^M \to G^N$ est *fppf* surjective revient alors juste à dire que c'est *un morphisme fidèlement plat.*

Définition *On dit que $G_{/S}$ est O-injectif si pour toute suite exacte (10.1) de O-module de type fini, la suite*

$$0 \to G^P \to G^M \to G^N \to 0$$

est fppf *exacte. Autrement dit : si $G^M \to G^N$ est un morphisme fidèlement plat.*

Proposition 10.4.1 *Si $G_{/S}$ est O-injectif, alors :*

1. *$G_{/S}$ a dimension additive.*
2. *$G^M_{/S}$ est plat pour tout O-module M.*
3. *Si $G_{/S}$ est lisse, $G^M_{/S}$ est lisse pour tout sous-module M d'un module libre de rang fini.*

Preuve: 1) est clair.

2) et 3) Soit $0 \to N \to O^n \to M \to 0$ une suite exacte de O-module. $G^n \to G^N$ est fidèlement plat par hypothèse, donc son noyau $G^M_{/S}$ est plat. Si de plus $G^n_{/S}$ est lisse, alors $G^N_{/S}$ est lisse d'après [EGA, IV 17.7.7]. $\square$

10.4.2 Critère de O-injectivité

Proposition 10.4.2 (Critère de Baer) *G est O-injectif si et seulement si pour tout idéal à gauche I de O, le morphisme $G \to G^I$ est fidèlement plat.*

Preuve: La condition est nécessaire. Montrons qu'elle est suffisante.

La suite (10.2) étant toujours exacte à gauche, il suffit de vérifier l'exactitude à droite. Soit donc $0 \to N \to M$, et posons

$$\wp = \left\{ N' \text{ sous } O - \text{module de } M \text{ contenant } N \mid G^{N'} \to G^N \text{ est fppf} \right\}.$$

Soit N' un élément de $\wp$ qui est maximal pour l'inclusion ($\wp \neq \emptyset$ car $N \in \wp$, et O est noethérien, donc il existe bien un tel N'). Supposons que $N' \neq M$ et soit

$m \in M \setminus N'$. Considérons alors $I = \{\alpha \in O \mid \alpha m \in N'\}$ et $N'' = N' + Om$. C'est un idéal (à gauche) de O. Par hypothèse, $G \to G^I$ est *fppf* surjective. D'autre part, m détermine un morphisme $f : G^{N'} \to G^I$ par la règle : si $x \in G^{N'}(S) = \mathrm{Hom}_O(N', G(S))$, $f(x) : I \to G(S)$ est $f(x)(\alpha) = x(\alpha m)$. Ce n'est autre que l'application induite par le morphisme O-linéaire évident : $I \to N'$. Formons alors le diagramme cartésien :

$$\begin{array}{ccc} G'' & \to & G \\ \downarrow & & \downarrow \\ G^{N'} & \to & G^I \end{array}$$

Un élément de $G''(S)$ est donc un couple (x,y) où $x : N' \to G(S)$ et $y \in G(S)$ sont tq $\forall \alpha \in I, \alpha y = x(\alpha m)$. Un tel couple définit alors un morphisme O-linéaire $x' : N'' \to G(S)$ par $x'(n'' = n' + om) = x(n') + oy$. x' est en effet bien défini, car si $n'' = n'_1 + o_1 m = n'_2 + o_2 m$, alors $n'_1 - n'_2 = (o_2 - o_1)m \in N'$ donc $o_2 - o_1 \in I$ et $(o_2 - o_1)y = x((o_2 - o_1)m) = x(n'_1) - x(n'_2)$. Inversement, une application O-linéaire $x' : N'' \to G(S)$ détermine $x : N' \to G(S)$ par restriction, et $y \in G(S)$ par $O \to Om \to N'' \to G(S)$, qui détermine bien un point de $G''(S)$. Donc $G'' \simeq G^{N''}$, le morphisme de projection $G'' \to G^{N'}$ s'identifiant au morphisme $G^{N''} \to G^{N'}$ déduit de l'inclusion $N' \hookrightarrow N''$. Or $G \to G^I$ étant fppf, $G'' \to G^{N'}$ l'est également, i.e., $G^{N''} \to G^{N'}$ est *fppf.* Le composé $G^{N''} \to G^{N'} \to G^N$ est donc *fppf*, et $N'' \in \wp$. Par maximalité de N', $N' = N''$, donc $m \in N'$: contradiction. Ainsi, $N' = M$ et $G^M \to G^N$ est *fppf.* □

Corollaire 10.4.3 *Si $G_{/S}$ est plat, alors $G_{/S}$ est O-injectif si et seulement si, pour tout point géométrique $\overline{s}$ de S, $G_{/\overline{s}}$ est O-injectif.*

Preuve: Cela résulte de ce que la fidèle platitude de $G \to G^I$ peut se tester par fibre. □

Corollaire 10.4.4 (Critère de Baer géométrique) *Si $G_{/S}$ est plat, les conditions suivantes sont équivalentes :*

1. *G est O-injectif et lisse.*
2. *Pour tout idéal I de O, G^I est géométriquement réduit et $G \to G^I$ est surjectif.*
3. *Pour tout idéal I de O, G^I est géométriquement réduit et pour tout point $s \in S$, il existe un corps algébriquement clos Ω sur $k(s)$ tel que $G(\Omega)$ soit O-injectif.*

De plus, on a alors : pour tout point géométrique $\overline{s}$ de S, $G(\overline{s})$ est O-injectif.

Preuve: 1) ⇒ 2) est immédiat.

2) ⇒ 1) Appliquons le critère de Baer : soit I un idéal de O, et montrons que $G \to G^I$ est un morphisme fidèlement plat. Comme $G_{/S}$ est plat, cela peut se vérifier par fibre ; par descente fpqc, il suffit de le vérifier sur les fibres géométriques. Mais si $\overline{s}$ est un point géométrique quelconque de S, notre hypothèse est : $G_{\overline{s}} \to G^I_{\overline{s}}$ est surjective et $G^I_{\overline{s}}$ est réduit, donc $G_{\overline{s}} \to G^I_{\overline{s}}$ est fidèlement plat par [DG, II §5.5.1].

2) $\Leftrightarrow$ 3) Cela résulte du critère usuel de Baer, cf. [13, I 3.7] : si

$$\mathrm{Hom}_O(O, G(\Omega)) \to \mathrm{Hom}_O(I, G(\Omega))$$

est surjective pour tout idéal I, alors $G(\Omega)$ est O-injectif. $\square$
On dira que "les points géométriques sont O-injectifs" si

$$\text{Pour tout } s \in S,\ G(\overline{k(s)})\,\text{est } O-\text{injectif.}$$

Remarque: Dans les deux critères ci-dessus, on peut se borner à tester le critère de Baer en se limitant à des idéaux dans un certain sous-ensemble d'idéaux $\wp$, pourvu que : pour tout idéal I de O différent de 0 et de O, $\exists \alpha \neq 0 \in O/I$ tel que $\mathrm{Ann}_O(\alpha) \in \wp$. Cela résulte en effet de la preuve.

10.5 Constructions standards

Soit $G_{/S}$ un schéma en O-module, M un O-module de type fini.

10.5.1 Algèbre de Lie

Proposition 10.5.1 *Pour tout S-schéma affine $T = \mathrm{Spec}(A)$,*

$$\begin{aligned} \mathrm{Lie}(G^M)(T) &= \mathrm{Hom}_O\left(M, \mathrm{Lie}\left(G\right)\left(T\right)\right) \\ &= \mathrm{Hom}_{O\otimes_{\mathbb{Z}}A}\left(M \otimes_{\mathbb{Z}} A, \mathrm{Lie}\left(G\right)\left(T\right)\right). \end{aligned}$$

Preuve: Découle des définitions. $\square$
Soit $0 \to N \to M \to P \to 0$ une suite exacte de O-module, $s = \mathrm{Spec}(k)$ un S-corps. On a une suite exacte :

$$0 \to \mathrm{Lie}\left(G^P\right)(k) \to \mathrm{Lie}\left(G^M\right)(k) \to \mathrm{Lie}\left(G^N\right)(k) \to \mathrm{Ext}^1_{O\otimes k}\left(P \otimes k, \mathrm{Lie}\left(G\right)(k)\right).$$

En particulier, si $\mathrm{Lie}\,(G)\,(k)$ est $O \otimes k$-injective ou si $P \otimes k$ est $O \otimes k$-projectif, $\mathrm{Lie}\left(G^M\right)(k) \to \mathrm{Lie}\left(G^N\right)(k)$ est surjective. Ce sera notamment le cas lorsque $O \otimes k$ est semi-simple.

10.5.2 Composantes connexes

On suppose ici que $S = \mathrm{Spec}(k)$ est le spectre d'un corps *parfait*, et que G est de type fini. La composante connexe G^0 de 1 dans G est alors un sous-schéma en groupe ouvert, et l'action de O sur G laisse G^0 stable : G^0 est donc canoniquement un schéma en O-module. Soit également $\pi_0(G)$ le quotient *fppf* G/G^0, de sorte que l'on a une suite exacte :

$$0 \to G^0 \to G \to \pi_0(G) \to 0 \tag{10.3}$$

de faisceau en O-module. Si M est un O-module, on en déduit une suite exacte :

$$0 \to (G^0)^M \to G^M \to \pi_0(G)^M.$$

Comme $\pi_0(G)$ est étale [DG, II §5.1.8], $\pi_0(G)^M$ l'est également par la proposition 10.2.2, et le noyau $(G^0)^M$ de $G^M \to \pi_0(G)^M$ est un sous-schéma en groupe ouvert de G^M. On a donc :

$$\left((G^0)^M\right)^0 = (G^M)^0. \tag{10.4}$$

On en déduit une suite exacte :

$$0 \to \pi_0\left((G^0)^M\right) \to \pi_0(G^M) \to \pi_0(G)^M. \tag{10.5}$$

Ceci permet dans l'étude de certaines questions (dimension, lissité...) de se ramener au cas où G est connexe. Lorsque G^0 est O-injectif, la suite (10.5) donne un *isomorphisme* :

$$\pi_0(G^M) \xrightarrow{\simeq} \pi_0(G)^M.$$

10.5.3 Passage au sous-schéma en groupe lisse sous-jacent

On suppose encore que $S = \mathrm{Spec}(k)$ est le spectre d'un corps *parfait*, et G est de type fini. On sait alors [DG, II §5.23] que G_{red} est un sous-schéma en groupe *lisse* de G. L'action de O sur G induit une action de O sur G_{red}, de sorte que l'immersion fermée $G_{\mathrm{red}} \to G$ soit O-linéaire.

Si $O^m \to O^n \to M \to 0$ est une présentation de M, on peut donc former un diagramme à lignes exactes :

$$\begin{array}{ccccccc} 0 & \to & G^M & \to & G^n & \to & G^m \\ & & \uparrow & & \uparrow & & \uparrow \\ 0 & \to & (G_{\mathrm{red}})^M & \to & (G_{\mathrm{red}})^n & \to & (G_{\mathrm{red}})^m \end{array}$$

et également un diagramme dont la *première ligne* est exacte, la seconde un complexe :

$$\begin{array}{ccccccc} 0 & \to & G^M & \to & G^n & \to & G^m \\ & & \uparrow & & \uparrow & & \uparrow \\ 0 & \to & (G^M)_{\mathrm{red}} & \to & (G^n)_{\mathrm{red}} & \to & (G^m)_{\mathrm{red}} \end{array}$$

Dans ces deux diagrammes, les flèches verticales sont des immersions fermées (utiliser [DG, II §5.5.1] pour le premier diagramme). Comme $(G^n)_{\mathrm{red}} = (G_{\mathrm{red}})^n$, on en déduit un morphisme $(G^M)_{\mathrm{red}} \to (G_{\mathrm{red}})^M$, qui est nécessairement une immersion fermée, et une bijection sur les points, de sorte que :

$$(G^M)_{\mathrm{red}} = ((G_{\mathrm{red}})^M)_{\mathrm{red}}.$$

Ceci permet dans l'étude des questions de nature topologique ou ensembliste de se ramener au cas où G est lisse.

10.5.4 Modèle de Néron

Supposons que S est un schéma de Dedekind connexe, donc intègre, de point générique $\xi = \mathrm{Sp}(K)$. Soit $A_{/K}$ un schéma en groupe lisse de type fini, muni d'une action de O. On suppose que $A_{/K}$ admet un modèle de Néron $\mathcal{A}_{/S}$. Par fonctorialité du modèle de Néron, l'action de O s'étend à une action sur $\mathcal{A}_{/S}$. Si M est un O-module de type fini, la fibre générique de $\mathcal{A}^M_{/S}$ est égale à $A^M_{/K}$.

De plus, pour tout point fermé x de S d'anneau local O_x, si O_x^{sh} dénote l'hensélisé strict de O_x et K_x^{sh} son corps des fractions, on sait que la spécialisation $\mathcal{A}(O_x^{\mathrm{sh}}) \to \mathcal{A}(K_x^{\mathrm{sh}})$ est bijective [3, 7.1.1] : c'est la propriété du "relèvement des points étales". Appliquant le foncteur $\mathrm{Hom}_O(M, \star)$ à cet isomorphisme de O-module, on voit donc que :

$$\mathcal{A}^M(O_x^{\mathrm{sh}}) \xrightarrow{\simeq} \mathcal{A}^M(K_x^{\mathrm{sh}}).$$

Autrement dit, $\mathcal{A}^M_{/S}$ satisfait à la propriété du relèvement des points étales.

Si $\mathrm{car}(K) = 0$, $A^M_{/K}$ est automatiquement lisse d'après [23]. Comme d'autre part $\mathcal{A}^M_{/S}$ est séparé, il résulte donc de [3, 7.1.5] que :

– Le modèle de Néron de $A^M_{/K}$ est le lissifié de $\mathcal{A}^M_{/S}$.

– $\mathcal{A}^M_{/S}$ est lisse $\Longleftrightarrow$ $\mathcal{A}^M_{/S}$ est le modèle de Néron de $A^M_{/K}$.

10.5.5 Suite connexe étale pour les schémas finis

Supposons maintenant que S est le spectre d'un anneau local hensélien, et $G_{/S}$ un schéma fini et plat en O-module. Soit

$$0 \to G^0 \to G \to G^{\mathrm{et}} \to 0 \tag{10.6}$$

la suite connexe étale de G [35, 3.7]. Alors :

Proposition 10.5.2 *Pour tout O-module M tel que $G^M_{/S}$ est fini et plat, la suite connexe étale de G^M est*

$$0 \to (G^0)^M \to G^M \to (G^{et})^M \to 0.$$

Preuve: Appliquant $\star^M$ à (10.6), on obtient déjà une suite exacte

$$0 \to (G^0)^M \to G^M \to (G^{\mathrm{et}})^M,$$

et $(G^{\mathrm{et}})^M_{/S}$ est étale d'après la proposition 10.2.2, donc $(G^0)^M_{/S}$ est un sous-schéma en groupe ouvert de $G^M_{/S}$, et en particulier plat. La composante connexe de $G^M_{/S}$ a une image triviale dans le schéma étale $(G^{\mathrm{et}})^M$, et est donc incluse dans $(G^0)^M$. Mais si k est le corps résiduel du point fermé s de S, $G^0(\overline{k}) = 0$; donc également $(G^0)^M(\overline{k}) = 0$, de sorte que $(G^0)^M$ est connexe, et $(G^0)^M = (G^M)^0$. Il en résulte que $(G^M)^{\mathrm{et}}$ s'identifie à un sous-schéma en groupe ouvert de $(G^{\mathrm{et}})^M$. Or

$$(G^{\mathrm{et}})^M(\overline{k}) = \mathrm{Hom}_O(M, G^{\mathrm{et}}(\overline{k})) = \mathrm{Hom}_O(M, G(\overline{k})) = G^M(\overline{k}) = (G^M)^{\mathrm{et}}(\overline{k}),$$

donc $(G^{\mathrm{et}})^M = (G^M)^{\mathrm{et}}$. □

Chapitre 11

Propriétés liées à l'anneau O

11.1 Dimension projective de O

Soit G un S-schéma en O-module, séparé, de présentation finie et *plat* sur S.

Proposition 11.1.1 *Si O est semi-simple, alors $G_{/S}$ est O-injectif. En particulier, $G^M_{/S}$ est plat pour tout M.*

Preuve: Compte tenu de la platitude de $G_{/S}$ cela résulte de 10.4.3 et du fait que toute suite exacte courte de O-module de type fini est scindée. $\square$

Proposition 11.1.2 *Si O est héréditaire, et $G_{/S}$ lisse, alors :*

1. *Pour tout sous-module N d'un module libre de rang fini, $G^N_{/S}$ est lisse.*
2. *Si $G_{/S}$ a dimension additive sur les fibres, alors $G^M_{/S}$ est plat pour tout O-module M.*
3. *$G_{/S}$ est O-injectif si et seulement si ses points géométriques le sont.*

Preuve: 1) Cela résulte de ce que M est alors projectif. 2) est alors une conséquence de la proposition 10.3.2, et 3) résulte enfin du corollaire 10.4.4 du critère de Baer. $\square$

11.2 Le cas d'un ordre

On suppose maintenant que :
- O est un ordre dans une $\mathbb{Q}$-algèbre séparable B de dimension finie (cf. [28, Chap. 2]).

On décompose B en produit de $\mathbb{Q}$-algèbres simples : $B = \prod_i B_i$. On note F_i le centre de B_i, et D_i le corps gauche $\mathrm{End}_{F_i}(B_i)$, de sorte qu'il existe un entier r_i tel que

$$B_i \simeq M_{r_i}(D_i)$$

(cf. [28, 7]). Soit également e_i l'idempotent central de B_i. Si X est un O-module de type fini, on note $X^0 = X \otimes \mathbb{Q}$ (un B-module), et X_i^0 la composante isotypique de X^0 correspondant à B_i, de sorte que $X_i^0 = X \otimes B_i = e_i.X^0$.

Si O est un ordre maximal, alors O est héréditaire [28, 21.2]. Si O est héréditaire, alors O admet une décomposition $O = \prod_i O_i$, où $O_i = e_i.O \subset B_i$ est un ordre héréditaire[28, 40.7]. Dans ce cas, tout module M se décompose en $M = \oplus_i M_i$, avec $M_i = e_i.M$, et cette décomposition est compatible avec les suites exactes de O-modules. En particulier, posant $G_i = G^{O_i}$, on a une décomposition

$$G = \underset{S}{\times}\ G_i,$$

et pour tout O-module M de type fini,

$$G^M = G^{\oplus M_i} = \underset{S}{\times}\ G^{M_i} = \underset{S}{\times}\ G_i^{M_i}.$$

Ceci nous permet (dans le cas où O est héréditaire) de nous ramener au cas où B est simple.

Si M est un O-module sans $\mathbb{Z}$-torsion, alors M est un sous-module d'un O-module libre (cf. [28, 10.6]). Si O est héréditaire, M est donc O-projectif (et plat). Partant d'un O-module M de type fini quelconque, on peut donc former la suite exacte de O-modules :

$$0 \to M_{\mathrm{tors}} \to M \to M/M_{\mathrm{tors}} \to 0.$$

Lorsque O est héréditaire, cette suite est scindée.

11.2.1 Dimension additive

On suppose que $G_{/S}$ est un schéma en O-module *séparé, de présentation finie.*

Proposition 11.2.1 *$G_{/S}$ a dimension additive si et seulement si $G[n]_{/S}$ est quasi-fini pour tout entier $n \geq 1$.*

Preuve: La condition est évidemment nécéssaire, comme il résulte de la considération de la suite exacte

$$0 \to O \xrightarrow{\times n} O \to O/nO \to 0,$$

laquelle implique, lorsque $G_{/S}$ a dimension additive, que pour tout point géométrique $\overline{s}$ de S, $\dim(G[n]_{\overline{s}}) = 0$. Inversement, supposons que $G[n]_{/S}$ est quasi-fini pour tout entier $n \geq 1$.

1) Soit

$$0 \to N \to M \to P \to 0 \tag{11.1}$$

une suite exacte de O-modules, et $\overline{s}$ un point géométrique de S. On veut montrer que

$$\dim(G^M_{\overline{s}}) = \dim(G^N_{\overline{s}}) + \dim(G^P_{\overline{s}}),$$

et on peut donc supposer directement que $S = \overline{s}$ est le spectre d'un corps algébriquement clos.

2) Notre hypothèse garantit déjà que $\dim(G^X) = 0$ pour tout O-module X qui est *fini*. En effet, un tel module est quotient d'une somme directe finie de copies de O/nO, et G^X est alors un sous-schéma fermé d'un produit (fini) de $G[n]$, et est donc également quasi-fini.

Il en résulte alors que si $f : X \to X'$ est une application O-linéaire à noyau et conoyau fini, alors $\dim(G^X) = \dim(G^{X'})$. En effet, on se ramène immédiatement aux deux cas suivants :

– f est surjective, de noyau K fini. La suite exacte $0 \to G^{X'} \to G^X \to G^K$ donne alors le résultat, compte tenu de [DG, II §5.5.1].
– f est injective de conoyau X'/X fini. Si $q = \#X'/X$, on a donc $qX' \subset f(X)$ et $f(X)/qX$ est fini. Les suites exactes :

$$0 \to G^{X'/X} \to G^{X'} \to G^X \quad \text{et} \quad 0 \to G^{f(X)/qX'} \to G^{f(X)} \to G^{qX'}$$

montrent alors que $\dim(G^{X'}) \leq \dim(G^X) = \dim(G^{f(X)}) \leq \dim(G^{qX'})$, et $\dim(G^{X'}) = \dim(G^{qX'})$ d'après le premier cas. Donc effectivement, $\dim(G^X) = \dim(G^{X'})$.

3) Soit O' un ordre maximal de B, contenant O. Tensorisant la suite exacte (11.1) par O', on obtient une suite exacte de O'-modules :

$$\mathrm{Tor}_O(O', P) \to O' \otimes_O N \to O' \otimes_O M \to O' \otimes_O P \to 0. \qquad (11.2)$$

D'autre part, la suite exacte de O-modules à droite $0 \to O \to O' \to O'/O \to 0$ donne la suite exacte :

$$0 \to \mathrm{Tor}_O(O', X) \to \mathrm{Tor}_O(O'/O, X) \to X \to O' \otimes_O X \to O'/O \otimes_O X \to 0,$$

où X est un O-module de type fini. En particulier, $\mathrm{Tor}_O(O', X)$ étant un O-module de type fini annulé par le cardinal de O'/O, est un ensemble fini.

Soit alors $H_{/S} = G^{O'}_{/S}$. C'est un S-schéma en O'-module, séparé et de présentation finie, et $H[n] \simeq G^{O'/nO'}$ est quasi-fini pour tout $n \geq 1$. Enfin, pour tout S-schéma T et tout O'-module X' :

$$\begin{aligned} H^{X'}(T) &= \mathrm{Hom}_{O'}(X', \mathrm{Hom}_O(O', G(T)) \\ &= \mathrm{Hom}_O({}_{[O]}X', G(T)) \\ &= G^{{}_{[O]}X'}(T). \end{aligned}$$

Si K est l'image de $O' \otimes_O N \to O' \otimes_O M$, on a donc une suite exacte de O'-modules :

$$0 \to K \to O' \otimes_O M \to O' \otimes_O P \to 0,$$

et

$$\begin{aligned}\dim(H^{O'\otimes_O M}) &= \dim(G^M)\\ \dim(H^K) &= \dim(G^N)\\ \dim(H^{O'\otimes_O P}) &= \dim(G^P).\end{aligned}$$

4) On est donc ramené au cas où O est *maximal*, et en particulier héréditaire. On peut alors décomposer P en $P = P_{\mathrm{tors}} \oplus P'$, où P' est O-projectif. Si M' est l'image réciproque de P' dans M, on a donc une suite exacte *scindée* :

$$0 \to N \to M' \to P' \to 0$$

De sorte qu'évidemment, $\dim(G^{M'}) = \dim(G^N) + \dim(G^{P'})$. P/P' et M/M' étant finis, on a également : $\dim(G^M) = \dim(G^{M'})$ et $\dim(G^P) = \dim(G^{P'})$, d'où le résultat. □

On dit d'un schéma en groupe $G_{/S}$ qu'il est semi-abélien s'il est lisse et si, pour tout point s de S, la composante connexe G_s^0 de G_s est une variété semi-abélienne [3, 7.3].

Corollaire 11.2.2 *Si $G_{/S}$ est semi-abélien, alors $G_{/S}$ a dimension additive sur les fibres.*

Preuve: Cf. [3, 7.3]. □

Remarque: Inversement, si $G_{/S}$ a dimension additive sur les fibres, alors pour tout point géométrique $\overline{s}$ de S *en caractéristique finie*, $G_{\overline{s}}$ est semi-abélien.

Corollaire 11.2.3 *Si $G_{/S}$ est semi-abélien à fibres géométriquement connexes, et O est héréditaire, alors $G_{/S}$ est O-injectif.*

Preuve: D'après le critère de Baer, il faut voir que pour tout idéal I de O, $f : G \to G^I$ est fidèlement plat. G étant plat, cela peut se tester par fibre, et on peut donc supposer que S est le spectre d'un corps. Comme on sait déjà que G^I est lisse, puisque I est projectif, il suffit de voir que $f : G \to G^I$ est surjectif. Les dimensions étant additives, on sait que $\dim(G) = \dim(G^{O/I}) + \dim(G^I)$, et il résulte alors de [DG, II §5.5.1] que $\dim f(G) = \dim(G^I)$. G étant connexe, il suffit donc de voir que G^I l'est également : cela résulte de ce que I est facteur direct d'un O-module libre, donc G^I est quotient d'un G^n. □

11.2.2 Lissité

On suppose maintenant que $G_{/S}$ est semi-abélien.

D'après (10.3.2), pour que $G^M_{/S}$ soit plat pour tout O-module M, il suffit que $G^N_{/S}$ soit lisse pour tout N O-module sans torsion. Si O est héréditaire, c'est effectivement le cas. On veut généraliser ce résultat.

Pour cela, on définit un entier $d(O)$ qui mesure le défaut d'hérédité : c'est le produit des nombres premiers p tels que le localisé de O en p ne soit *pas* héréditaire. Un ordre maximal étant héréditaire, et O étant maximal à presque toutes les places, le nombre $d(O)$ est bien défini. Comme un ordre global est héréditaire si et seulement si tous ses localisés le sont, on a : $d(O) = 1$ si et seulement si O est héréditaire.

Proposition 11.2.4 *Si toutes les caractéristiques résiduelles de S sont premières à $d(O)$, alors :*

1. *Pour tout O-module N sans torsion, $G^N_{/S}$ est lisse.*
2. *Pour tout O-module M, $G^M_{/S}$ est plat.*

Preuve: Par la proposition 10.3.2, il suffit de voir que pour tout O-module N sans torsion, $G^N_{/S}$ est lisse *par fibre*. Derechef, on peut donc supposer : S est le spectre d'un corps k, de caractéristique zéro ou première à $d(O)$.

Soit O' l'ordre de B défini par les conditions locales suivantes : pour tout premier q, $O_q = O'_q$ si $q \nmid d(O)$, et O'_q est un ordre maximal de B_q contenant O_q si $q \mid d(O)$. On a donc : O' est un ordre héréditaire puisque tous ses localisés le sont, et $\#O'/O = n$ divise une puissance de $d(O)$.

Si M est un O-module de type fini, $i : M \to O' \otimes_O M$ a un noyau et un conoyau finis, annulés par n. De même $O' \xrightarrow{n} O$ induit un morphisme j : $O' \otimes_O M \to M$, dont noyau et conoyau sont finis et annulés par n. On a donc :

$$\begin{array}{lrcl} i \otimes_k 1_k : & M \otimes_{\mathbb{Z}} k & \xrightarrow{\simeq} & (O' \otimes_O M) \otimes_{\mathbb{Z}} k \\ j \otimes_k 1_k : & (O' \otimes_O M) \otimes_{\mathbb{Z}} k & \xrightarrow{\simeq} & M \otimes_{\mathbb{Z}} k \end{array}$$

Supposons alors que l'un ou l'autre des k-schémas G^M et $G^{O' \otimes_O M}$ soit lisse, appelons le G^{M_1} et l'autre G^{M_2}, et soit $f : G^{M_1} \to G^{M_2}$ le morphisme induit par i ou j. Le morphisme induit sur les algèbres de Lie est :

$$\mathrm{Hom}_O(M_1, \mathrm{Lie}(G)(k)) \to \mathrm{Hom}_O(M_2, \mathrm{Lie}(G)(k))$$

ou encore :

$$\mathrm{Hom}_{O \otimes k}(M_1 \otimes k, \mathrm{Lie}(G)(k)) \to \mathrm{Hom}_{O \otimes k}(M_2 \otimes k, \mathrm{Lie}(G)(k))$$

C'est donc un isomorphisme. Il résulte alors de [DG, II §5.5.3] que f est lisse, et $G^{M_2}_{/k}$ est lisse (notons que par [DG, II §5.5.5] et [EGA, IV 17.6.2], f est même étale).

Appliquant ceci à $M = O$, on trouve donc d'abord que $H = G^{O'}$ est lisse puisque G est lisse ; le morphisme $G \to H$ est de plus étale, et fini d'après [3, 7.3.1]. Il en résulte aisément que H est également semi-abélienne. Or H est maintenant un O'-module, et O' est héréditaire, donc $H^{N'}$ est lisse pour tout O'-module N' sans torsion.

Soit alors N un O-module sans torsion, et $N' = O' \otimes_O N$. N' n'est pas nécessairement sans torsion, mais $\#N'_{\mathrm{tors}}$ est tué par n, donc $H^{N'_{\mathrm{tors}}} = H[n]^{N'_{\mathrm{tors}}}$ est étale : cela résulte en effet de ce que $H[n]$ est étale par [3, 7.3.2], et de la proposition 10.2.2. Ecrivant $N' = N'' \oplus N'_{\mathrm{tors}}$, de sorte que $H^{N'} = H^{N''} \times_S H^{N'_{\mathrm{tors}}}$, on voit que $H^{N'}$ est lisse. Or $H^{N'} = G^{O' \otimes_O N}$, donc G^N est lisse. $\square$

Corollaire 11.2.5 *Supposons S irréductible de point générique ξ, $G_{/S}$ abélien et O héréditaire en les caractéristiques de S. Alors :*

$$G_{/S} \textit{ est } O-\textit{injectif} \iff G_{/\xi} \textit{ est } O-\textit{injectif}$$

Preuve: D'après le critère de Baer, il faut voir que pour tout idéal I de O, $f : G \to G^I$ est fidèlement plat. G étant plat, cela peut se tester par fibre, et on peut donc supposer que S est le spectre d'un corps. G^I étant lisse par la proposition précédente, il suffit de voir que $f : G \to G^I$ est surjectif. Les dimensions étant additives, on sait déjà que $\dim(G) = \dim(G^{O/I}) + \dim(G^I)$, et il résulte alors de [DG, II §5.5.1] que $\dim f(G) = \dim(G^I)$, et $f(G)$ est connexe puisque G l'est : il reste donc à voir que G^I est également connexe. Mais $G^I_{/S}$ est propre (10.2), et sa fibre générique est géométriquement connexe, puisque $G_{/\xi}$ est O-injectif. Le corollaire résulte donc du théorème de connexion de Zariski ([EGA, III 4.3.1 ou IV 12.2.4 ou IV 15.5.7]). □

Remarque: La condition "O est héréditaire en les caractéristiques de S" est également *nécessaire* (pour la lissité), dans le cas des courbes elliptiques à multiplication complexe.

11.2.3 Dimension

On suppose maintenant que :
- O est un ordre dans une $\mathbb{Q}$-algèbre *simple* B.
- $G_{/S}$ est un schéma en O-module , de présentation finie, séparé, et tel que $G[n]_{/S}$ est quasi-fini pour tout entier $n \geq 1$.

Soit F le centre de B, $D^{\mathrm{opp}} = \mathrm{End}_F(B)$, de sorte qu'il existe un entier r tel que $B \approx M_r(D)$, et un entier d tel que $[D : F] = d^2$. Soit enfin $f = [F : \mathbb{Q}]$, de sorte que $\dim_{\mathbb{Q}}(B) = fd^2r^2$.

Si M est un O-module, $M \otimes \mathbb{Q}$ est un B-module, donc isomorphe à une somme directe de x copies de $I_0 = D^r$ (muni de sa structure de B-module simple). On dit que $\mathrm{rg}_O(M) = \frac{x}{r}$ est le O-rang de M. On a donc :

$$\dim_{\mathbb{Q}}(M \otimes \mathbb{Q}) = rfd^2\mathrm{rg}_O(M).$$

Si O' est un ordre de B contenant O, $\mathrm{rg}_{O'}(O' \otimes_O M) = \mathrm{rg}_O(M)$.

Pour tout point s de S, on note $\dim_s(G) = \dim(G_s)$: c'est "la dimension relative de G en s".

Proposition 11.2.6 *Pour tout O-module M,*

$$\forall s \in S : \qquad \dim_s(G^M) = \dim_s(G) \times \mathrm{rg}_O(M)$$

Preuve: M_{tors} est fini. Choisissant un isomorphisme B-linéaire

$$M/M_{\mathrm{tors}} \otimes \mathbb{Q} \approx (I_0)^x,$$

où $rx = \mathrm{rg}_O(M)$, on obtient un isomorphisme

$$M^r/M^r_{\mathrm{tors}} \approx (I_0)^{rx} \approx B^x.$$

Comme O^x est un réseau de B^x, on peut donc trouver une application O-linéaire

$$M^r \to O^x,$$

dont le noyau et le conoyau sont finis. On a alors :

$$\dim(G_s^{M^r}) = r \times \dim(G_s^M) = \dim(G_s^x) = x \times \dim(G_s)$$

donc $\dim_s(G^M) = \dim_s(G) \times \mathrm{rg}_O(M)$. $\square$

Corollaire 11.2.7 *r divise $\dim_s(G)$ pour tout point s de S.*

Preuve: Il suffit de voir qu'il existe un O-module M pour lequel $\mathrm{rg}_O(M) = 1/r$. On prend $M = Ox$ avec $x \neq 0 \in I_0$. $\square$

Bibliographie

[1] H. Bass, *On the ubiquity of Gorenstein Rings*. Math. Z., **82**. Band (1963).

[2] M. Bertolini, *Selmer groups and Heegner points in anticyclotomic $\mathbb{Z}_p$-extensions*. Comp. Math., **99** (1995), pp. 153-182.

[3] S. Bosch, W. Lütkebohmert et M. Raynaud, *Néron Models*. Ergebnisse der Mathematik, Springer-Verlag (1990).

[4] N. Bourbaki, *Algèbre Commutative, Chapitre 7 : Diviseurs*. Hermann (1961-65).

[DG] M. Demazure et P. Gabriel, *Groupes Algébriques*. Masson & cie, éditeurs - Paris, North-Holland Publishing Company - Amsterdam (1970).

[5] Deuring, *Die Typen der Multiplicatorenringe elliptischer Funcktionenkörper*. Abh. Math. Sem. Hamburg, Bd. **14** (1941), pp. 197-272.

[6] B.H. Gross, *Heights and the special values of L-series*. In *Number Theory* (H. Kisilevsky and J. Labute, eds), CMS Conference Proceedings, vol. **7**, Amer. Math. Soc. (1987), pp. 115-189.

[7] B.H. Gross and D. Zagier, *Heegner points and derivatives of L-series*. Invent. Math., **84** (1986), pp. 225-320.

[EGA] A. Grothendieck et J. Dieudonné, *Éléments de Géométrie Algébrique*. Publications Mathématiques de l'I.H.E.S., n°**4,8,11,17,20,24,28,32**.

[TDTE] A. Grothendieck, *Technique de descente et théorèmes d'existence en géométrie algébrique*. Séminaire Bourbaki, n°**190**,**195**,**212**,**221**,**232**,**236**.

[8] R. Hartshorne, *Algebraic Geometry*. GTM **52**, Springer-Verlag (1977).

[9] Y. Ihara, *On modular curves over finite fields*. Discrete subgroups of Lie groups and applications to moduli, Oxford University Press (1975), pp. 161-202.

[10] N. M. Katz et B. Mazur, *Arithmetic Moduli of Elliptic Curves*. Annals of Math. Studies, Princeton University Press (1985).

[11] V.A. Kolyvagin, *Euler Systems*. The Grothendieck Festschrift. Prog. in Math., Boston, Birkhauser (1990).

[12] S. Lang, *Algebra*. 2$^{\text{nd}}$ edition, Addison Wesley (1984).

[13] T.Y. Lam, *Lectures on Modules and Rings.* GTM n°**189**, Springer-Verlag (1998).

[14] S. Ling et J. Oesterlé, *The Shimura subgroup of* $J_0(N)$. Astérisque **196-197**, Société mathématique de France (1991).

[15] B. Mazur, *Modular Curves and Arithmetic.* Proceedings of the International Congress of Mathematicians, Warsaw 1983, PWN (1984), pp. 185-211.

[16] A. Mézard, *Fundamental Group.* Courbes semi-stables et groupe fondamental en géométrie algébrique (eds. J-B. Bost, F. Loeser et M. Raynaud), Progress in Math. vol. **187**, Birkhauser (2000).

[17] J.S. Milne, *Etale Cohomology.* Princeton University Press (1980).

[18] D. Mumford, *Geometric Invariant Theory.* Springer-Verlag (1965).

[19] J. P. Murre, *Représentation of unramified Functors. Applications*. Séminaire Bourbaki, 1964/65, n°**294**

[20] J. P. Murre, *Lectures on an Introduction to Grothendieck's Theory of the Fundamental Group.* Lecture notes, Tata Institute of Fundamental Research, Bombay (1967).

[21] J. Nekovář J. et N. Schappacher, *On the asymptotic behaviour of Heegner points.* Turk J. Math., **23** (1999), pp. 549-556.

[22] J. Nekovář, *On the parity of ranks of Selmer groups II.* Preprint, 2000.

[23] F. Oort, *Algebraic Group Schemes in Characteristic Zero are Reduced.* Inventiones **2** (1966).

[24] F. Oort, *Commutative group schemes.* LNM **15**, Springer-Verlag (1966).

[25] M. Ratner, *Raghunatan's conjectures for cartesian products of real and p-adic Lie groups.* Duke Math. J., **77 vol. 2** (1995), pp. 275-382.

[26] M. Raynaud, *Faisceaux amples sur les schémas en groupes et les espaces homogènes.* LNM **119**, Springer-Verlag (1970).

[27] M. Raynaud, *Schémas en groupes de type* $(p, \dots, p)$. Bull. Soc. math. France, **102** (1974), pp. 241-280.

[28] I. Reiner, *Maximal Orders.* Academic Press (1975).

[29] K. Ribet, *Congruence Relations between Modular Forms.* Proceedings of the International Congress of Mathematicians, Warsaw 1983, PWN (1984), pp. 503-514.

[30] J-P. Serre, *Complex Multiplication.* In *Algebraic Number Theory* (J.W.S. Cassels and A. Fröhlich, eds), Academic Press (1967), pp. 292-296.

[31] J-P. Serre, *Lie Algebras and Lie Groups.* LNM **1500**, Springer-Verlag (1992).

[32] J-P. Serre, *Arbres, amalgames,* SL_2. Astérisque **46**, Société mathématique de France (1977).

[33] J-P. Serre et J. Tate, *Good reduction of abelian varieties.* Ann. Math. **88** (1968), pp. 492-517.

[34] J. H. Silverman, *The Arithmetic of Elliptic Curves.* GTM **106**, Springer-Verlag (1986).

[35] J. Tate, *Finite Flat Group Schemes.* Modular Forms and Fermat's Last Theorem (G. Cornell, J.H. Silverman, G. Stevens eds.), Springer-Verlag (1997).

[36] J. Tate, *Global Class Field Theory.* Algebraic Number Theory (J.W.S Cassels, A. Fröhllich eds.), Academic Press (1967).

[37] V. Vatsal, *Uniform distribution of Heegner points.* Preprint, 2000.

[38] V. Vatsal, *Special values of anticylotomic L-functions.* Preprint, 2000.

[39] M-F. Vignéras, *Arithmétique des Algèbres de Quaternions.* LNM **800**, Springer-Verlag (1980).