

# Problèmes de modules pour les courbes elliptiques

Olivier Wittenberg

5 février 2002

## Résumé

Cet exposé est une introduction aux problèmes de modules des courbes elliptiques. Le but étant d'expliquer entièrement une preuve, on se restreint au cas le plus simple : celui des  $\Gamma(N)$ -structures. On démontre précisément l'existence d'un schéma de modules pour les courbes elliptiques relatives  $E \rightarrow S$  avec  $N$  inversible sur  $S$ , munies d'une  $\Gamma(N)$ -structure ; ainsi peut-on dire que la courbe modulaire  $Y(N)$  est définie sur  $\mathbb{Z}[1/N]$ .

## 1 Introduction et notations

Le problème auquel on s'intéresse dans cet exposé est celui de l'existence d'un schéma de modules pour les courbes elliptiques. En d'autres termes, il s'agit de la représentabilité du foncteur qui à un schéma  $S$  associe l'ensemble des classes d'isomorphisme de familles de courbes elliptiques paramétrées par  $S$  (cette notion sera précisément définie par la suite). En fait, ce foncteur n'est pas représentable ; ce n'est même pas un faisceau pour la topologie étale, comme on peut le voir avec l'exemple suivant.

Soient  $a, b, d \in \mathbb{Q}$  vérifiant  $4a^3 + 27b^2 \neq 0$ ,  $d > 0$ , et  $\sqrt{d} \notin \mathbb{Q}$ . Considérons les courbes elliptiques  $E_1$  et  $E_2$  sur  $\mathbb{Q}$  définies par les équations :

$$\begin{aligned} E_1 & : y^2 = x^3 + ax + b \\ E_2 & : dy^2 = x^3 + ax + b \end{aligned}$$

Une équation de Weierstrass pour  $E_2$  est  $y^2 = x^3 + ad^2x + bd^3$  (considérer  $(x, y) \mapsto (dx, d^2y)$ ). Les courbes elliptiques  $E_1$  et  $E_2$  sont clairement isomorphes après extension des scalaires à  $K = \mathbb{Q}(\sqrt{d})$ . Si le foncteur dont il est question était un faisceau étale,  $E_1$  et  $E_2$  devraient donc être  $\mathbb{Q}$ -isomorphes (la flèche  $\text{Spec}(K) \rightarrow \text{Spec}(\mathbb{Q})$  est un recouvrement pour la topologie étale). On peut constater que tel n'est pas le cas en calculant par exemple les discriminants des deux équations de Weierstrass. Leur quotient est  $d^6$ , or on sait que le quotient des discriminants de deux équations de Weierstrass définissant des courbes elliptiques isomorphes est une puissance douzième, ce qui contredit les hypothèse sur  $d$ .

L'existence de formes tordues, comme  $E_1$  et  $E_2$ , est expliquée par la présence d'automorphismes non triviaux des courbes elliptiques : les formes tordues d'un objet  $E$  s'identifient à des torsseurs sous le faisceau des automorphismes de  $E$ . Dans l'exemple ci-dessus, si l'on fixe un  $K$ -isomorphisme  $E_1 \times_{\mathbb{Q}} K \rightarrow E_2 \times_{\mathbb{Q}} K$ , on obtient deux  $(K \otimes_{\mathbb{Q}} K)$ -isomorphismes  $E_1 \times_{\mathbb{Q}} K \times_{\mathbb{Q}} K \rightarrow E_2 \times_{\mathbb{Q}} K \times_{\mathbb{Q}} K$  distincts en considérant les images réciproques de  $f$  par les deux projections  $K \times_{\mathbb{Q}} K \rightarrow K$ . Composons l'un avec l'inverse de l'autre ; on a maintenant un automorphisme qui est l'identité sur l'une des fibres géométriques et la multiplication par  $-1$  sur l'autre. On voit bien sur cet exemple que le problème provient de l'existence d'automorphismes des courbes elliptiques sur des corps algébriquement clos.

Ce problème peut être contourné de deux manières.

1. Au lieu de chercher à représenter ce foncteur par un schéma, on peut se poser la question de la représentabilité par un champ algébrique.
2. On peut imposer des structures supplémentaires aux courbes elliptiques, afin d'éliminer les automorphismes des objets que l'on classe, et espérer que les foncteurs obtenus sont représentables.

La première approche est celle adoptée par Deligne et Rapoport dans [2]. C'est la meilleure à plusieurs titres, notamment parce qu'elle est plus naturelle (on ne voit pas bien l'intérêt de forcer les objets que l'on étudie à être des schémas, excepté que les schémas nous sont plus familiers). Cependant, nous suivrons la seconde approche, plus classique, afin que l'exposé reste très élémentaire et puisse servir utilement d'introduction au sujet. Pour les mêmes raisons, nous ne nous embarrasserons pas des problèmes liés à la caractéristique, qui n'existent d'ailleurs qu'à cause de ces structures supplémentaires que l'on impose (en tout cas si l'on ne cherche pas à compactifier les espaces de modules obtenus).

### Notations

La catégorie opposée d'une catégorie  $\mathcal{C}$  sera notée  $\mathcal{C}^\circ$ . On note **Sch** la catégorie des schémas, **Ens** la catégorie des ensembles. Soit  $S$  un schéma. On note **Sch**/ $S$  la catégorie des  $S$ -schémas. Si  $G$  est un groupe,  $G_S$  désigne le schéma en groupes constant sur  $S$ , égal à  $G$ . On dit qu'un entier  $N$  est *inversible sur*  $S$  si c'est une section globale inversible de  $\mathcal{O}_S$ . Un schéma possède au plus une structure de  $\mathbb{Z}[1/N]$ -schéma ; on pourra donc considérer qu'être un  $\mathbb{Z}[1/N]$ -schéma est une *propriété* du schéma, et non une donnée supplémentaire. Un schéma est un  $\mathbb{Z}[1/N]$ -schéma si et seulement si  $N$  est inversible sur  $S$ . Le faisceau total des quotients de  $S$  est noté  $\mathcal{K}_S$  ; c'est le faisceau associé au préfaisceau dont l'anneau des sections sur un ouvert affine  $U = \text{Spec}(R)$  de  $S$  est le localisé de  $R$  en la partie multiplicative complémentaire de l'ensemble des diviseurs de zéro dans  $S$ . Le terme « diviseur » signifiera toujours « diviseur de Cartier ». Si  $i: D \rightarrow X$  est une immersion fermée, on notera  $\mathcal{I}_D$  ou  $\mathcal{I}_i$  le faisceau quasi-cohérent d'idéaux de  $X$  qui lui est associé, et, si de plus  $D$  est un diviseur de Cartier,  $\mathcal{O}_X(D)$  l'inverse de  $\mathcal{I}_D$  en tant que  $\mathcal{O}_X$ -module inversible. On considérera toujours  $\mathcal{O}_X(D)$  comme un sous- $\mathcal{O}_X$ -module de  $\mathcal{K}_X$  ; ainsi pourra-t-on dire qu'une fonction rationnelle sur  $X$  est une section globale de  $\mathcal{O}_X(D)$ .

Le lecteur est supposé familier avec les topologies de Grothendieck, ainsi qu'avec quelques résultats bien connus de descente fidèlement plate (consulter [SGA1] exposé VIII ou [1] pour une introduction à cette théorie).

## 2 Courbes elliptiques relatives

**Définition 2.1** — Soit  $S$  un schéma. On appelle courbe elliptique sur  $S$  la donnée d'un morphisme de schémas  $f: E \rightarrow S$  propre et lisse, dont les fibres sont des courbes connexes de genre 1, et d'une section  $\theta$  de ce morphisme.

La section  $\theta$  est appelée « section nulle », et elle sera la plupart du temps sous-entendue. Si  $E$  et  $E'$  sont deux courbes elliptiques sur  $S$ , on appelle morphisme de  $E$  vers  $E'$  tout morphisme de  $S$ -schémas préservant la section nulle.

**Remarque** — Les fibres d'une courbe elliptique relative sont géométriquement intègres (en effet, elles sont connexes et possèdent un point rationnel, donc sont géométriquement connexes ; de plus elles sont lisses). On pourrait donc remplacer « fibres » par « fibres géométriques » dans la définition.

**Définition 2.2** — Soit  $f: X \rightarrow S$  un morphisme propre et lisse, de dimension relative constante 1 (i.e. toutes les fibres sont de dimension 1). Si  $\mathcal{L}$  est un faisceau inversible sur  $X$ , on appelle degré de  $\mathcal{L}$  la fonction qui à  $s \in S$  associe le degré de la restriction de  $\mathcal{L}$  à la fibre de  $X$  en  $s$  (on suppose connue la notion de degré d'un faisceau inversible sur une courbe projective sur un corps). Si  $D$  est un diviseur de Cartier de  $X$  sur  $S$ , on appelle degré de  $D$  le degré du faisceau d'idéaux de  $D$ . Le degré en  $s$  se note  $\text{deg}_s(\cdot)$ .

On peut prouver que le degré est localement constant sur  $S$ . On le note  $\text{deg}(D)$  lorsqu'il est constant. On notera  $\text{Pic}(X/S)$  le conoyau de la flèche  $f^*: \text{Pic}(S) \rightarrow \text{Pic}(X)$ . Attention, il ne s'agit pas du groupe de Picard relatif ! Si  $s \in S$  est fixé, le degré en  $s$  est un morphisme de groupes  $\text{Pic}(X) \rightarrow \mathbb{Z}$ , dont on constate tout de suite qu'il se factorise par  $\text{Pic}(X/S)$ . Pour  $k \in \mathbb{Z}$ , on notera enfin  $\text{Pic}^{[k]}(X/S)$  l'image réciproque de  $\{k\}$  par cette flèche  $\text{Pic}(X/S) \rightarrow \mathbb{Z}$ .

**Proposition 2.3** — Soient  $S$  un schéma et  $X$  un  $S$ -schéma de dimension relative constante 1, lisse et séparé. Alors toute section de  $X$  sur  $S$  est un diviseur de Cartier effectif, propre et plat sur  $S$ , de degré 1.

Démonstration — Voir [3], Ch. 1, 1.2.2 et 1.2.3. L'idée est que si  $S$  est le spectre d'un corps algébriquement clos, l'assertion est presque évidente (c'est ici que l'on utilise la lissité); on se ramène à ce cas particulier à l'aide du critère de platitude fibre à fibre.  $\square$

Dans cette situation, le diviseur de Cartier défini par une section  $P \in X(S)$  sera noté  $[P]$ ; il est important de distinguer les deux, car sinon, lorsque  $X$  est un  $S$ -schéma en groupes, la notation  $P + Q$  serait ambiguë.

**Définition-proposition 2.4** — Soit  $E \rightarrow S$  une courbe elliptique relative avec  $S$  affine,  $S = \text{Spec}(R)$ . On dit que  $E$  possède une équation de Weierstrass s'il existe  $a_1, a_2, a_3, a_4, a_6 \in R$  tels que  $E$  soit  $S$ -isomorphe au sous-schéma fermé de  $\mathbb{P}_S^2$  défini par l'équation

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3,$$

la section nulle de  $E$  étant envoyée sur la section  $[x : y : z] = [0 : 1 : 0]$ . Dans ce cas,  $\Delta$  (donné par la formule habituelle) est inversible dans  $R$ . Inversement, à chaque fois que l'on se donne des  $a_i \in R$  tels que  $\Delta$  soit inversible, l'équation ci-dessus définit une courbe elliptique sur  $S$ . Enfin, si deux équations de Weierstrass définissent des courbes elliptiques  $S$ -isomorphes, on peut passer d'une équation à l'autre par un changement de coordonnées de la forme

$$\begin{aligned} x &\longmapsto u^2x + r \\ y &\longmapsto u^3y + u^2sx + t \end{aligned}$$

avec  $u, r, s, t \in R$  et  $u$  inversible dans  $R$  (et en simplifiant l'équation par  $u^6$ , bien entendu).

Attention, une courbe elliptique relative de base affine ne possède pas forcément d'équation de Weierstrass. On a cependant le résultat suivant.

**Théorème 2.5** — Soit  $E \rightarrow S$  une courbe elliptique avec  $S$  affine. Alors, localement sur  $S$  pour la topologie de Zariski,  $E$  possède une équation de Weierstrass. En d'autres termes, il existe un recouvrement  $(S_i)_{i \in I}$  de  $S$  par des ouverts affines tels que  $E \times_S S_i$  possède une équation de Weierstrass sur  $S_i$  pour tout  $i$ . Par ailleurs, si  $\text{Pic}(S) = 1$ ,  $E$  possède une équation de Weierstrass sur  $S$ .

Démonstration partielle — Notons  $f$  le morphisme  $E \rightarrow S$  et  $\theta$  la section nulle. On pose  $\mathcal{L} = \theta^* \mathcal{O}_E([\theta])$ ; c'est un faisceau inversible sur  $S$ . Comme  $\theta$  est une immersion fermée, on a la suite exacte de  $\mathcal{O}_E$ -modules :

$$0 \longrightarrow \mathcal{I}_\theta \longrightarrow \mathcal{O}_E \longrightarrow \theta_* \mathcal{O}_S \longrightarrow 0$$

En tensorisant par  $\mathcal{O}_E(n[\theta])$ , on en déduit la suite exacte suivante :

$$0 \longrightarrow \mathcal{O}_E((n-1)[\theta]) \longrightarrow \mathcal{O}_E(n[\theta]) \longrightarrow \theta_* \theta^* \mathcal{O}_E(n[\theta]) \longrightarrow 0$$

Ainsi,  $\mathcal{L}^{\otimes n} = f_*(\mathcal{O}_E(n[\theta])/\mathcal{O}_E((n-1)[\theta]))$  pour tout  $n \in \mathbb{Z}$ . On prouve facilement, à l'aide du théorème de Riemann-Roch et d'arguments de cohomologie cohérente (pour se restreindre à une fibre), que  $R^1 f_*(\mathcal{O}_E(n[\theta])) = 0$  pour  $n > 0$ . Ainsi, si l'on applique  $f_*$  à la suite exacte ci-dessus, elle reste exacte pour  $n > 1$ . Ensuite, l'exactitude se conserve si l'on passe aux sections globales, puisque  $S$  est affine. D'où la suite exacte, pour  $n > 1$  :

$$0 \longrightarrow \Gamma(E, \mathcal{O}_E((n-1)[\theta])) \longrightarrow \Gamma(E, \mathcal{O}_E(n[\theta])) \longrightarrow \Gamma(S, \mathcal{L}^{\otimes n}) \longrightarrow 0 \quad (1)$$

Comme  $\mathcal{L}$  est un faisceau inversible sur  $S$ , on peut supposer qu'il est libre, quitte à rétrécir  $S$ ; on n'a pas besoin de rétrécir  $S$  si  $\text{Pic}(S) = 1$ . Soit  $t \in \mathcal{L}(S)$  une base de  $\mathcal{L}$  sur  $\mathcal{O}_S$ . Pour tout  $n$ ,  $t^{\otimes n}$  est une base de  $\mathcal{L}^{\otimes n}$  sur  $\mathcal{O}_S$ . Considérons la suite exacte (1) pour  $n = 2$ . Soit  $x \in \Gamma(E, \mathcal{O}_E(2[\theta]))$  qui relève  $t^{\otimes 2}$ . Comme le  $R$ -module  $\Gamma(S, \mathcal{L}^{\otimes 2})$  est libre, la suite est scindée (canoniquement, maintenant que  $x$  est choisi). On prouve assez facilement que les flèches canoniques  $\mathcal{O}_S \rightarrow f_* \mathcal{O}_E \rightarrow f_* \mathcal{O}_E([\theta])$  sont des isomorphismes. Ainsi,  $\Gamma(E, \mathcal{O}_E(2[\theta])) = R \oplus Rx$ . Regardons maintenant le cas  $n = 3$  :

$$0 \longrightarrow R \oplus Rx \longrightarrow \Gamma(E, \mathcal{O}_E(3[\theta])) \longrightarrow \Gamma(S, \mathcal{L}^{\otimes 3}) \longrightarrow 0$$

Choisissons  $y \in \Gamma(E, \mathcal{O}_E(3[\theta]))$  qui relève  $t^{\otimes 3}$ . À nouveau, la suite est maintenant canoniquement scindée, d'où  $\Gamma(E, \mathcal{O}_E(3[\theta])) = R \oplus Rx \oplus Ry$ . Les faisceaux  $\mathcal{O}_E(n[\theta])$  s'identifient canoniquement à des sous- $\mathcal{O}_E$ -modules de  $\mathcal{K}_E$ ; on peut donc voir  $x$  et  $y$  comme des fonctions rationnelles sur  $E$ ; ainsi,  $x^2$  est une section globale de  $\mathcal{O}_E(4[\theta])$ . Regardons le cas  $n = 4$  de (1); on vérifie tout de suite que  $x^2$  s'envoie sur  $t^{\otimes 2}$ , d'où  $\Gamma(E, \mathcal{O}_E(4[\theta])) = R \oplus Rx \oplus Ry \oplus Rx^2$ . De même,  $\Gamma(E, \mathcal{O}_E(5[\theta])) = R \oplus Rx \oplus Ry \oplus Rx^2 \oplus Rxy$ . Pour  $n = 6$ , on se rend compte que  $y^2$  et  $x^3$  relèvent tous les deux  $t^{\otimes 6}$ ; ainsi,  $y^2 - x^3 \in R \oplus Rx \oplus Ry \oplus Rx^2 \oplus Rxy$ , d'où l'équation de Weierstrass. Il n'est ensuite pas difficile de prouver qu'elle définit une immersion fermée vers  $\mathbb{P}_S^2$ , en se servant du fait que c'est vrai sur les fibres.

Pour prouver l'énoncé sur les changements de coordonnées possibles entre équations de Weierstrass, il suffit de se rendre compte que la donnée d'une équation de Weierstrass détermine une base de  $\mathcal{L}$  sur  $\mathcal{O}_S$ ; en effet, l'image dans  $\Gamma(S, \mathcal{L})$  de la fonction rationnelle  $y/x$  (vue comme élément de  $\Gamma(E, \mathcal{O}_E([\theta]))$ ) est une base de  $\mathcal{L}$  sur  $\mathcal{O}_S$  (il suffit de le vérifier sur chaque fibre; c'est clair si  $S$  est le spectre d'un corps). Ainsi, toute équation de Weierstrass est obtenue de la manière que l'on vient de décrire, et les seuls changements de coordonnées possibles résident dans les libertés que l'on avait au moment du choix de  $t$ , de  $x$  et de  $y$ . On vérifie tout de suite qu'ils sont décrits par les formules annoncées ( $u$  correspond au changement  $t \mapsto ut$ ).  $\square$

**Théorème 2.6** — Soient  $S$  un schéma et  $E$  une courbe elliptique sur  $S$ , de section nulle  $\theta$ . L'application

$$\begin{aligned} E(S) &\longrightarrow \text{Pic}^{[0]}(E/S) \\ P &\longmapsto \mathcal{O}_E([P] - [\theta]) \end{aligned}$$

est bijective.

Démonstration — Ce théorème est prouvé dans [3] (« théorème d'Abel »).  $\square$

Ceci permet de munir  $E(S)$  d'une structure de groupe, par transport de structure, de manière fonctorielle. Ainsi,  $E$  est un  $S$ -schéma en groupes, et même un schéma abélien sur  $S$ , dont le neutre est  $\theta$ . On retrouve bien sûr la loi usuelle lorsque  $S$  est le spectre d'un corps. On pourrait donc définir une courbe elliptique relative comme étant un schéma abélien de dimension relative constante 1.

### 3 Structures de niveau et énoncé du théorème

Soit  $E$  une courbe elliptique sur un schéma  $S$ . Comme on l'a vu dans la section précédente,  $E$  est un  $S$ -schéma en groupes, et l'on peut donc parler de l'endomorphisme de multiplication par un entier  $N$ , que l'on note  $[N]$ . Le noyau de  $[N]$  est noté  $E[N]$ ; rappelons que c'est l'image réciproque du  $E$ -schéma  $S$  (vu comme  $E$ -schéma par la section nulle) par le changement de base  $[N]: E \rightarrow E$ . Les résultats classiques sur  $[N]$  et  $E[N]$  s'étendent aux courbes elliptiques relatives.

**Théorème 3.1** — Soient  $S$  un schéma,  $E$  une courbe elliptique sur  $S$  et  $N \in \mathbb{N}^*$ . L'endomorphisme  $[N]$  est fini et localement libre de rang  $N^2$ . Si  $N$  est inversible sur  $S$ ,  $E[N]$  est un  $S$ -schéma en groupes fini étale, localement isomorphe au schéma en groupes constant  $(\mathbb{Z}/N\mathbb{Z})_S^2$  sur  $S$  pour la topologie étale.

Démonstration — C'est un résultat bien connu sur les schémas abéliens.  $\square$

**Définition 3.2** — Soient  $E \rightarrow S$  une courbe elliptique,  $N \geq 1$  un entier inversible sur  $S$ . On appelle  $\Gamma(N)$ -structure sur  $E$  un isomorphisme de  $S$ -schémas en groupes  $(\mathbb{Z}/N\mathbb{Z})_S^2 \xrightarrow{\sim} E[N]$ . On appelle  $\Gamma'(N)$ -structure sur  $E$  un isomorphisme de  $S$ -schémas en groupes  $\mu_{N,S} \times_S (\mathbb{Z}/N\mathbb{Z})_S \xrightarrow{\sim} E[N]$ .

En d'autres termes, une  $\Gamma(N)$ -structure sur  $E$  consiste en la donnée d'un couple de sections de  $E$  sur  $S$  qui induisent une  $(\mathbb{Z}/N\mathbb{Z})$ -base de la  $N$ -torsion sur chaque fibre géométrique. Si  $T$  est un  $S$ -schéma et  $E$  une courbe elliptique sur  $S$ , une  $\Gamma(N)$ -structure sur  $E \rightarrow S$  induit par changement de base une  $\Gamma(N)$ -structure sur  $E \times_S T \rightarrow T$ ; de même pour les  $\Gamma'(N)$ -structures. Si  $\mathcal{O}_S(S)$  possède une racine primitive  $N$ -ème de l'unité,  $\mu_{N,S}$  et  $(\mathbb{Z}/N\mathbb{Z})_S$  sont isomorphes sur  $S$ , et une fois un isomorphisme fixé, il revient au même d'étudier les  $\Gamma(N)$ -structures ou les  $\Gamma'(N)$ -structures.

**Remarque** — L'existence même d'une  $\Gamma(N)$ -structure sur une courbe elliptique  $E$  est une condition restrictive sur  $E$ . Par exemple, pour  $N \geq 3$ , aucune courbe elliptique sur  $\mathbb{Q}$  ne possède de  $\Gamma(N)$ -structure ; en effet, d'après la surjectivité de l'accouplement de Weil,  $\mathbb{Q}$  devrait contenir une racine primitive  $N$ -ème de l'unité.

Énonçons maintenant le théorème qui est le but de cet exposé. Étant donné un  $\mathbb{Z}[1/N]$ -schéma  $S$ , on peut considérer la catégorie dont les objets sont les couples  $(E, \alpha)$  où  $E$  est une courbe elliptique sur  $S$  et  $\alpha$  une  $\Gamma(N)$ -structure sur  $E \rightarrow S$ , et dont les flèches  $(E, \alpha) \rightarrow (E', \alpha')$  sont les  $S$ -isomorphismes de courbes elliptiques  $E \rightarrow E'$  identifiant les  $\Gamma(N)$ -structures  $\alpha$  et  $\alpha'$ .

**Théorème 3.3** — Soit  $N \geq 3$  un entier. Le foncteur

$$\begin{aligned} F_N : (\mathbf{Sch}/\mathbb{Z}[1/N])^\circ &\longrightarrow \mathbf{Ens} \\ S &\longmapsto \text{ensemble des classes d'isomorphisme de courbes} \\ &\quad \text{elliptiques sur } S \text{ munies d'une } \Gamma(N)\text{-structure} \end{aligned}$$

est représenté par un  $\mathbb{Z}[1/N]$ -schéma affine, lisse, de dimension relative 1. De même pour le foncteur  $F'_N$  défini de la même manière, excepté que l'on considère  $\Gamma'(N)$  au lieu de  $\Gamma(N)$ .

Le théorème peut se reformuler ainsi : il existe un  $\mathbb{Z}[1/N]$ -schéma  $S_0$  affine, lisse, de dimension relative constante 1, une courbe elliptique  $E_0$  sur  $S_0$  et une  $\Gamma(N)$ -structure  $\alpha_0$  sur  $E_0$ , telles que pour tout  $\mathbb{Z}[1/N]$ -schéma  $S$ , toute courbe elliptique  $E$  sur  $S$  et toute  $\Gamma(N)$ -structure  $\alpha$  sur  $E$ , il existe un unique morphisme de schémas  $S \rightarrow S_0$  tel qu'il existe un  $S$ -isomorphisme  $E \rightarrow E_0 \times_{S_0} S$  envoyant  $\alpha_0$  sur  $\alpha$ . Autrement dit, toute  $\Gamma(N)$ -structure s'obtient par changement de base à partir de  $\alpha_0$  :  $\alpha_0$  est la  $\Gamma(N)$ -structure universelle.

## 4 Représentabilité, rigidité et représentabilité relative

La preuve du théorème repose de manière cruciale sur les notions de rigidité et de représentabilité relative.

**Définition 4.1** — Soient  $\mathcal{C}$  une catégorie et  $P: \mathcal{C}^\circ \rightarrow \mathbf{Ens}$  un foncteur. Si  $X$  est un objet de  $\mathcal{C}$ , on appelle  $P$ -structure sur  $X$  un élément de  $P(X)$ . On note  $\mathcal{C}/P$  la catégorie dont les objets sont les couples  $(X, \alpha)$  où  $X$  est un objet de  $\mathcal{C}$  et  $\alpha$  une  $P$ -structure sur  $X$ , et dont les flèches  $(X, \alpha) \rightarrow (Y, \beta)$  sont les flèches  $f: X \rightarrow Y$  telles que  $P(f): P(Y) \rightarrow P(X)$  envoie  $\beta$  sur  $\alpha$ .

Remarquons que cette notation est compatible avec la notation  $\mathcal{C}/X$  lorsque  $X$  est un objet de  $\mathcal{C}$  pour désigner la catégorie des « objets de  $\mathcal{C}$  au-dessus de  $X$  », si l'on convient d'identifier  $X$  à un foncteur par le plongement de Yoneda. Le lemme suivant est trivial, mais il est important de l'avoir à l'esprit.

**Lemme 4.2** — Le foncteur  $P$  est représentable si et seulement si la catégorie  $\mathcal{C}/P$  admet un objet final. Dans ce cas, si  $(X_0, \alpha_0)$  est un objet final,  $P$  est représenté par  $X_0$ , et  $\alpha_0$  est appelée la  $P$ -structure universelle.

**Définition 4.3** — On note  $\mathbf{Ell}_{\mathbb{Z}[1/N]}$  la catégorie dont les objets sont les courbes elliptiques relatives  $E \rightarrow S$  avec  $N$  inversible sur  $S$  (ce sont donc des couples  $(f, \theta)$  où  $f$  est un morphisme de schémas et  $\theta$  une section de  $f$ , vérifiant certaines propriétés), et dont les flèches sont les carrés cartésiens. En d'autres termes, si  $E \rightarrow S$  et  $E' \rightarrow S'$  sont des objets de  $\mathbf{Ell}_{\mathbb{Z}[1/N]}$ , une flèche entre eux est la donnée d'une flèche  $E \rightarrow E'$  et d'une flèche  $S \rightarrow S'$ , telles que le carré obtenu soit commutatif et cartésien.

**Définition 4.4** — Soit  $P: \mathbf{Ell}_{\mathbb{Z}[1/N]}^\circ \rightarrow \mathbf{Ens}$  un foncteur. On dit que  $P$  est rigide si pour toute courbe elliptique  $E \rightarrow S$  munie d'une  $P$ -structure  $\alpha$ , le seul  $S$ -automorphisme de  $E$  préservant  $\alpha$  est l'identité.

**Proposition 4.5** — Si  $P$  est représentable,  $P$  est rigide.

Démonstration — Notons  $\mathbb{E}_P \rightarrow \mathbb{S}_P$  une courbe elliptique relative représentant  $P$ . Soit  $E \rightarrow S$  une courbe elliptique, que l'on suppose munie d'une  $P$ -structure  $\alpha$ , c'est-à-dire que l'on fixe des flèches  $\alpha_1$  et  $\alpha_2$  telles

que le carré suivant soit cartésien :

$$\begin{array}{ccc} E & \xrightarrow{\alpha_1} & \mathbb{E}_P \\ f \downarrow & & \downarrow \\ S & \xrightarrow{\alpha_2} & \mathbb{S}_P \end{array}$$

Soit  $\sigma: E \rightarrow E$  un  $S$ -automorphisme de la courbe elliptique  $E$  préservant la  $P$ -structure  $\alpha$ , i.e. tel que  $\alpha_1 \circ \sigma = \alpha_1$ . Comme le carré ci-dessus est cartésien, pour vérifier que  $\sigma$  et  $\text{Id}_E$  coïncident, il suffit de vérifier que  $f \circ \sigma = f$  et que  $\alpha_1 \circ \sigma = \alpha_1$ , ce qui est bien vrai.  $\square$

L'intérêt de la notion de rigidité apparaît dans la situation où l'on a deux courbes elliptiques  $E$  et  $E'$  au-dessus d'un schéma  $S$ , munies de  $P$ -structure  $\alpha$  et  $\alpha'$ , et que l'on sait que les couples  $(E, \alpha)$  et  $(E', \alpha')$  sont  $S$ -isomorphes : la rigidité de  $P$  entraîne alors qu'il existe un *unique* isomorphisme entre eux.

Lorsque  $P: \mathbf{Ell}_{\mathbb{Z}[1/N]}^\circ \rightarrow \mathbf{Ens}$  est un foncteur, on note  $\tilde{P}: (\mathbf{Sch}/\mathbb{Z}[1/N])^\circ \rightarrow \mathbf{Ens}$  le foncteur qui à un  $\mathbb{Z}[1/N]$ -schéma  $S$  associe l'ensemble des classes de  $S$ -isomorphisme de courbes elliptiques sur  $S$  munies d'une  $P$ -structure. Si l'on veut,  $\tilde{P}(S)$  est l'ensemble des classes d'isomorphisme des objets de la catégorie fibre<sup>1</sup> en  $S$  du foncteur  $\mathbf{Ell}_{\mathbb{Z}[1/N]}/P \rightarrow \mathbf{Sch}/\mathbb{Z}[1/N]$  qui à  $(E \rightarrow S, \alpha)$  associe  $S$ .

**Proposition 4.6** — *Soit  $P: \mathbf{Ell}_{\mathbb{Z}[1/N]}^\circ \rightarrow \mathbf{Ens}$  un foncteur. Il est représentable si et seulement s'il est rigide et si  $\tilde{P}$  est représentable.*

Démonstration — Si  $P$  est représentable, on vérifie tout de suite que  $\tilde{P}$  est représenté par  $\mathbb{S}_P$ . Supposons  $\tilde{P}$  représentable et rigide, représenté par un schéma  $S_0$ . La  $\tilde{P}$ -structure universelle  $\alpha_0$  sur  $S_0$  est la donnée d'une courbe elliptique  $E_0$  sur  $S_0$ , munie d'une  $P$ -structure (le tout à isomorphisme près ; on en choisit une). Montrons que  $E_0 \rightarrow S_0$  représente  $P$ . Soit  $E \rightarrow S$  une courbe elliptique,  $N$  inversible sur  $S$ , munie d'une  $P$ -structure  $\alpha$ . Le schéma  $S$  est alors naturellement muni d'une  $\tilde{P}$ -structure ; il existe donc une unique flèche  $f: S \rightarrow S_0$  telle qu'il existe un  $S$ -isomorphisme  $g: E \rightarrow E_0 \times_{S_0} S$  tel que  $P(g)$  envoie  $\alpha_0$  sur  $\alpha$ , et  $g$  est unique par rigidité de  $P$ . Autrement dit, il existe une unique flèche  $E \rightarrow E_0$  rendant le carré évident cartésien :  $(E_0 \rightarrow S_0, \alpha_0)$  est bien un objet final de  $\mathbf{Ell}_{\mathbb{Z}[1/N]}/P$ .  $\square$

En commettant un léger abus, on notera  $\Gamma(N)$  (resp.  $\Gamma'(N)$ ) le foncteur  $\mathbf{Ell}_{\mathbb{Z}[1/N]}^\circ \rightarrow \mathbf{Ens}$  qui à une courbe elliptique relative associe l'ensemble de ses  $\Gamma(N)$ -structures (resp.  $\Gamma'(N)$ -structures). Ainsi, le foncteur  $F_N$  (resp.  $F'_N$ ) n'est autre que  $\widetilde{\Gamma(N)}$  (resp.  $\widetilde{\Gamma'(N)}$ ).

**Définition 4.7** — *On dit qu'un foncteur  $P: \mathbf{Ell}_{\mathbb{Z}[1/N]}^\circ \rightarrow \mathbf{Ens}$  est relativement représentable si, pour toute courbe elliptique  $E \rightarrow S$  avec  $N$  inversible sur  $S$ , le foncteur*

$$\begin{array}{ccc} [E \rightarrow S]_P: \mathbf{Sch}/S & \longrightarrow & \mathbf{Ens} \\ T & \longmapsto & P(E \times_S T) \end{array}$$

*est représentable.*

En d'autres termes,  $P$  est relativement représentable si toute courbe elliptique  $E \rightarrow S$  avec  $N$  inversible sur  $S$  acquiert une  $P$ -structure universelle après un changement de base approprié. Quelques notations supplémentaires seront commodes. Si  $P$  est représentable, on notera  $\mathbb{E}_P \rightarrow \mathbb{S}_P$  une courbe elliptique le représentant ; si  $P$  est relativement représentable et que  $E \rightarrow S$  est une courbe elliptique, on notera  $\mathbb{E}_{[E \rightarrow S]_P} \rightarrow \mathbb{S}_{[E \rightarrow S]_P}$  une courbe elliptique représentant  $[E \rightarrow S]_P$ . Dans ce cas,  $\mathbb{S}_{[E \rightarrow S]_P}$  est canoniquement un  $S$ -schéma.

On peut maintenant esquisser la preuve de la représentabilité de  $F_N$  (ou de  $F'_N$ ) pour  $N \geq 3$ . La première étape est de prouver la rigidité de  $\Gamma(N)$  pour  $N \geq 3$ , ce qui n'est pas difficile, et la représentabilité relative de  $\Gamma(N)$ . Ensuite, on montre que  $\Gamma(3)$  et  $\Gamma(4)$  sont représentables, en donnant explicitement les équations de courbes elliptiques qui les représentent. Il existe ainsi une courbe elliptique  $\mathbb{E}_{\Gamma(3)} \rightarrow \mathbb{S}_{\Gamma(3)}$  possédant une  $\Gamma(3)$ -structure universelle. Soit  $E \rightarrow S$  une courbe elliptique avec  $N$  inversible sur  $S$ . Que signifie « se donner une

1. La catégorie fibre n'est pas une sous-catégorie pleine de  $\mathbf{Ell}_{\mathbb{Z}[1/N]}/P$  : les flèches de la catégorie fibre en  $S$  sont celles au-dessus de  $\text{Id}_S$ .

$\Gamma(N)$ -structure sur  $E$  » ? Pour fixer les idées, prenons  $N = 5$ . Supposons d'abord 3 inversible sur  $S$ . On voit facilement que la donnée d'une  $\Gamma(15)$ -structure est canoniquement équivalente à celle d'une  $\Gamma(3)$ -structure et d'une  $\Gamma(5)$ -structure. Les  $\Gamma(3)$ -structures sur  $E \rightarrow S$  sont en bijection avec les carrés cartésiens

$$\begin{array}{ccc} E & \longrightarrow & \mathbb{E}_{\Gamma(3)} \\ \downarrow & & \downarrow \\ S & \longrightarrow & \mathbb{S}_{\Gamma(3)}, \end{array}$$

par rigidité de  $\Gamma(3)$ . Une fois un tel carré fixé, la donnée d'une  $\Gamma(5)$ -structure sur  $E \rightarrow S$  équivaut, d'après la représentabilité relative de  $\Gamma(5)$ , à la donnée d'un morphisme de  $\mathbb{S}_{\Gamma(3)}$ -schémas  $S \rightarrow \mathbb{S}_{[\mathbb{E}_{\Gamma(3)} \rightarrow \mathbb{S}_{\Gamma(3)}]_{\Gamma(5)}}$ . Ainsi,  $F_{15}$  est représenté par le schéma  $\mathbb{S}_{[\mathbb{E}_{\Gamma(3)} \rightarrow \mathbb{S}_{\Gamma(3)}]_{\Gamma(5)}}$ , que l'on note donc  $\mathbb{S}_{\Gamma(15)}$ . Le foncteur  $F_{15}$  possède une action naturelle de  $\mathrm{GL}_2(\mathbb{Z}/15\mathbb{Z})$ , et donc de  $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ . On montre par des arguments classiques que le schéma quotient  $\mathbb{S}_{\Gamma(15)}/\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$  existe. On est alors en droit d'espérer qu'il représente  $F_5$ , ou plutôt sa restriction à  $\mathbf{Sch}/\mathbb{Z}[1/15]$ . Par le même raisonnement, mais en remplaçant 3 par 4, on obtient la représentabilité de la restriction de  $F_5$  à  $\mathbf{Sch}/\mathbb{Z}[1/10]$ ; on vérifie alors facilement que par recollement au-dessus de  $\mathbb{Z}[1/5]$ , on obtient un schéma qui représente  $F_5$ .

## 5 Représentabilité de $F_3$ et $F_4$

On va directement prouver que les foncteurs  $\Gamma(3)$  et  $\Gamma(4)$  sont représentables. Ici on ne s'intéresse qu'aux  $\Gamma(N)$ -structures, pas aux  $\Gamma'(N)$ -structures; on verra que c'est suffisant, même pour traiter le cas de  $F'_N$ . Soit  $\mathbf{EllW}_{\mathbb{Z}[1/N]}$  la sous-catégorie pleine de  $\mathbf{Ell}_{\mathbb{Z}[1/N]}$  dont les objets sont les courbes elliptiques  $E \rightarrow S$ ,  $N$  inversible sur  $S$ , avec  $S$  affine, qui possèdent une équation de Weierstrass. Notons

$$\Gamma(N)|_{\mathbf{EllW}_{\mathbb{Z}[1/N]}} : (\mathbf{EllW}_{\mathbb{Z}[1/N]})^\circ \rightarrow \mathbf{Ens}$$

la restriction du foncteur  $\Gamma(N)$ .

**Lemme 5.1** — *Soit  $N \geq 1$ . Soit  $E_0 \rightarrow S_0$  un objet de  $\mathbf{EllW}_{\mathbb{Z}[1/N]}$  qui représente  $\Gamma(N)|_{\mathbf{EllW}_{\mathbb{Z}[1/N]}}$ . Alors, en tant qu'objet de  $\mathbf{Ell}_{\mathbb{Z}[1/N]}$ , il représente  $\Gamma(N)$ .*

Démonstration — Notons  $\alpha_0$  la  $\Gamma(N)|_{\mathbf{EllW}_{\mathbb{Z}[1/N]}}$ -structure universelle sur  $E_0 \rightarrow S_0$ . Soit  $E \rightarrow S$  une courbe elliptique avec  $N$  inversible sur  $S$ , munie d'une  $\Gamma(N)$ -structure  $\alpha$ . Il faut voir que  $\alpha$  provient de  $\alpha_0$  par un unique morphisme dans  $\mathbf{Ell}_{\mathbb{Z}[1/N]}$ . Commençons par l'unicité; on se donne donc deux carrés cartésiens

$$\begin{array}{ccc} E & \xrightarrow{e_k} & E_0 \\ \downarrow & & \downarrow \\ S & \xrightarrow{s_k} & S_0 \end{array}$$

avec  $k = 1$  ou  $k = 2$ , qui envoient  $\alpha_0$  sur  $\alpha$ . Si  $(e_1, s_1) \neq (e_2, s_2)$ , on peut remplacer  $S$  par un ouvert arbitrairement petit contenant un point où  $s_1$  et  $s_2$  ne coïncident pas, ou bien l'image d'un point où  $e_1$  et  $e_2$  ne coïncident pas. On peut donc supposer que  $S$  est affine et que  $E$  possède une équation de Weierstrass, auquel cas le résultat est acquis.

Montrons maintenant l'existence d'un tel carré cartésien. Il existe un recouvrement de  $S$  par une famille d'ouverts affines  $(S_i)$ , tel que  $E \times_S S_i \rightarrow S_i$  possède une équation de Weierstrass. Notons  $E_i = E \times_S S_i$  et  $\alpha_i$  la  $\Gamma(N)$ -structure induite par  $\alpha$  sur  $E_i \rightarrow S_i$ . Elle provient de  $\alpha_0$  par un unique carré cartésien de la forme :

$$\begin{array}{ccc} E_i & \xrightarrow{e_i} & E_0 \\ \downarrow & & \downarrow \\ S_i & \xrightarrow{s_i} & S_0 \end{array}$$

Notons  $S_{ij} = S_i \cap S_j$ ,  $E_{ij} = E \times_S S_{ij}$  et  $\alpha_{ij}$  la  $\Gamma(N)$ -structure déduite de  $\alpha$ . La courbe elliptique  $E_{ij} \rightarrow S_{ij}$  n'est pas forcément un objet de  $\mathbf{EllW}_{\mathbb{Z}[1/N]}$  ( $S_{ij}$  peut ne pas être affine), mais on a déjà montré l'unicité d'un carré cartésien

$$\begin{array}{ccc} E_{ij} & \longrightarrow & E_0 \\ \downarrow & & \downarrow \\ S_{ij} & \longrightarrow & S_0 \end{array}$$

envoyant  $\alpha_0$  sur  $\alpha$ . Ainsi, les  $s_i$  (resp. les  $e_i$ ) coïncident deux à deux sur l'intersection de leurs domaines de définition, et définissent donc un carré commutatif

$$\begin{array}{ccc} E & \xrightarrow{e} & E_0 \\ \downarrow & & \downarrow \\ S & \xrightarrow{s} & S_0 \end{array}$$

dont on vérifie tout de suite qu'il est cartésien. Il reste à voir qu'il envoie  $\alpha_0$  sur  $\alpha$ , mais cela découle de la remarque évidente que le foncteur  $[E \rightarrow S]_{\Gamma(N)}$  est un faisceau pour la topologie de Zariski (c'est le seul endroit de la démonstration qui soit spécifique à  $\Gamma(N)$ ).  $\square$

Ainsi, on pourra se contenter d'étudier les courbes elliptiques sur une base affine, possédant une équation de Weierstrass, pour montrer la représentabilité de  $F_3$  et de  $F_4$ ; et on pourra même se contenter de les étudier localement sur la base.

## 5.1 $\Gamma(3)$ -structures

Soit  $E \rightarrow S = \text{Spec}(R)$  un objet de  $\mathbf{EllW}_{\mathbb{Z}[1/3]}$ , muni d'une  $\Gamma(3)$ -structure  $\alpha: (\mathbb{Z}/3\mathbb{Z})_S^2 \xrightarrow{\sim} E[3]$ . Notons respectivement  $P$  et  $Q$  les images des sections globales  $(1, 0)$  et  $(0, 1)$  de  $(\mathbb{Z}/3\mathbb{Z})_S^2$  par  $\alpha$ . Lorsqu'on fixe une  $S$ -immersion fermée  $i: E \rightarrow \mathbb{P}_S^2$ , on conviendra de noter  $x(A)$  et  $y(A)$  les coordonnées affines d'une section  $A \in E(S)$  arrivant dans l'ouvert où  $z$  est inversible. Ce sont donc des éléments de  $R$ . Notons  $\theta$  la section nulle.

**Proposition 5.2** — *Quitte à remplacer  $S$  par un ouvert affine contenant un point donné, l'affirmation suivante est vraie : il existe d'uniques  $B, C \in R$  tels qu'il existe un  $S$ -isomorphisme de  $E$  vers le sous-schéma fermé de  $\mathbb{P}_S^2$  défini par l'équation*

$$y^2z + (3C - 1)xyz + (-3C^2 - B - 3BC)yz^2 = x^3,$$

la section  $\theta$  étant envoyée sur  $[x : y : z] = [0 : 1 : 0]$ , vérifiant :

- $x(P) = 0$  et  $y(P) = 0$ ;
- $x(Q) = C$  et  $y(Q) = B + C$ ;
- $C$  est inversible;
- on a  $B^3 = (B + C)^3$ .

L'énoncé sous-entend que  $P$  et  $Q$  arrivent dans l'ouvert où  $z$  est inversible, ce qui est clairement nécessaire.

Démonstration — Soit une équation de Weierstrass pour  $E$  :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

D'après 2.4, il suffit de montrer qu'il existe d'uniques  $u, r, s, t \in R$ , avec  $u$  inversible, tels que l'équation de Weierstrass obtenue en remplaçant  $x$  par  $u^2x + r$  et  $y$  par  $u^3y + u^2sx + t$  et en simplifiant par  $u^6$  vérifie les propriétés indiquées ( $y$  compris la forme de l'équation de Weierstrass), avec  $C = x(Q)$  et  $B = y(Q) - x(Q)$ . Comme 3 est inversible dans  $R$ , on peut fixer  $r$  par la condition  $a_2 = 0$  (i.e. pour tous  $u, s, t$ , il existe un unique  $r$  tel que le coefficient  $a_2$  de la nouvelle équation soit nul); cette condition est évidemment nécessaire pour que les propriétés ci-dessus soient vérifiées. Comme  $P$  est d'ordre 3, le  $\mathcal{O}_E$ -module inversible

$\mathcal{O}_E(3[P] - 3[\theta])$  provient de  $\text{Pic}(S)$ , d'après 2.6. Ainsi, quitte à rétrécir  $S$ , on peut le supposer libre. Soit  $f \in \Gamma(E, \mathcal{O}_E(3[\theta] - 3[P]))$  une base sur  $\mathcal{O}_E$ ;  $f$  est uniquement déterminée à multiplication par un inversible de  $\mathcal{O}_E(E)$  près, donc à un inversible de  $R$  près (puisque la flèche canonique  $\mathcal{O}_S \rightarrow p_*\mathcal{O}_E$  est un isomorphisme, si  $p$  désigne le morphisme structural  $E \rightarrow S$ ). Rappelons que l'on a vu, au cours de la démonstration du théorème 2.5, que l'on peut supposer que  $\Gamma(E, \mathcal{O}_E(3[\theta])) = R \oplus Rx \oplus Ry$  quitte à remplacer  $S$  par un ouvert affine. Ainsi,  $f = \alpha_0 + \alpha_1x + \alpha_2y$  pour d'uniques  $\alpha_i \in R$ . Le coefficient  $\alpha_2$  est nécessairement inversible; en effet, sinon, quitte à se restreindre à une fibre, on pourrait le supposer nul, et le pôle de  $f$  en  $[\theta]$  serait d'ordre au plus 2, ce qui n'est pas. Par conséquent, il existe d'uniques  $\beta_0, \beta_1 \in R$  tels que  $y + \beta_1x + \beta_0$  soit une base de  $\mathcal{O}_E(3[\theta] - 3[P])$  sur  $\mathcal{O}_E$ . On peut alors fixer  $s$  et  $t$  par la condition  $\beta_0 = \beta_1 = 0$ ; cette condition est bien nécessaire pour que  $a_4 = a_6 = 0$ .

Ainsi,  $y$  est une base de  $\mathcal{O}_E(3[\theta] - 3[P])$  sur  $\mathcal{O}_E$ . Cela signifie, en notant  $I$  l'idéal de

$$R_0 = R[x, y]/(y^2 + a_1xy + a_3y - x^3 - a_4x - a_6)$$

engendré par  $y - y(P)$  et  $x - x(P)$ , que  $y \in I^3$ . En particulier,  $y \in I$ , donc  $y(P) \in I$ , et donc  $y(P) = 0$  puisque  $y(P) \in R$  et  $R_0/I = R$ . L'hypothèse que  $y$  est une base de  $\mathcal{O}_E(3[\theta] - 3[P])$  sur  $\mathcal{O}_E$  entraîne que  $(x - x(P))^3 \in Ry$ ; par conséquent  $(x - x(P))^3$  est nul dans  $R_0/(y) = R[x]/(x^3 + a_4x + a_6)$ , c'est-à-dire que  $(x - x(P))^3 = (x^3 + a_4x + a_6)f(x)$  dans  $R[x]$  pour un  $f(x) \in R[x]$ . Nécessairement,  $f(x) = 1$ , puis  $3x(P) = 0$ ; comme 3 est inversible dans  $R$ ,  $x(P) = 0$  et donc  $a_4 = a_6 = 0$ .

De même pour  $Q$ : quitte à remplacer  $S$  par un ouvert affine, on peut supposer  $\mathcal{O}_E(3[\theta] - 3[Q])$  libre sur  $\mathcal{O}_E$ ; il existe alors d'uniques  $A, B \in R$  tels que  $y - Ax - B \in \Gamma(E, \mathcal{O}_E(3[\theta] - 3[Q]))$  en soit une base. Notons  $C = x(Q)$ . La fonction  $(x - C)^3$  est une section globale de  $\mathcal{O}_E(3[\theta] - 3[Q])$ , donc  $(x - C)^3 \in (y - Ax - B)R$ , et donc  $(x - C)^3 = 0$  dans  $R_0/(y - Ax - B)$ , c'est-à-dire que

$$(x - C)^3 = ((Ax + B)^2 + a_1x(Ax + B) + a_3(Ax + B) - x^3)f(x)$$

dans  $R[x]$  pour un  $f(x) \in R[x]$ . Nécessairement,  $f(x) = -1$ . On en déduit, coefficient par coefficient :

$$3C = A^2 + a_1A \quad (2)$$

$$-3C^2 = 2AB + a_1B + a_3A \quad (3)$$

$$C^3 = B^2 + a_3B \quad (4)$$

Remarquons que  $C$  est nécessairement inversible. En effet, si ce n'était pas le cas, on pourrait le supposer nul, quitte à se restreindre à une fibre; on aurait alors  $x(P) = 0$  et  $x(Q) = 0$ , donc  $P = Q$  ou  $P = -Q$ , ce qui contredit l'hypothèse que  $P$  et  $Q$  forment une base de la 3-torsion. L'équation (2) permet d'en déduire que  $A$  est inversible. Lorsqu'on change de coordonnées,  $y - Ax - B$  devient  $u^3(y + (s - A)x/u) + t - Ar - B$ , ce qui montre que l'on peut fixer  $u$  par la condition  $A = 1$ , et cette condition est bien sûr nécessaire pour que  $y(Q) - x(Q) = B$ . On déduit tout de suite des équations (2), (3) et (4) que  $a_1 = 3C - 1$ ,  $a_3 = -3C^2 - B - 3BC$  et que  $B^3 = (B + C)^3$ . Enfin, comme  $y - x - B$ ,  $y - y(Q)$  et  $x - C$  sont des sections globales de  $\mathcal{O}_E(3[\theta] - [Q])$ ,  $y(Q) - B - C$  en est aussi une, mais c'est un élément de  $R$ , d'où  $y(Q) = B + C$ .  $\square$

**Corollaire 5.3** — *On voit maintenant  $B$  et  $C$  comme des indéterminées. Définissons les éléments suivants de  $\mathbb{Z}[B, C]$  :*

$$a_1 = 3C - 1 \quad ; \quad a_3 = -3C^2 - B - 3BC \quad ; \quad \Delta = (a_1^3 - 27a_3)a_3$$

Soit  $S_0 = \text{Spec}(\mathbb{Z}[B, C, (3\Delta C)^{-1}]/(B^3 - (B + C)^3))$ . Soit  $E_0$  le sous-schéma fermé de  $\mathbb{P}_{S_0}^2$  défini par l'équation

$$y^2z + a_1xyz + a_3yz^2 = x^3,$$

et soit  $\theta_0 \in E_0(S_0)$  la section  $[0 : 1 : 0]$ . Soient  $P$  et  $Q$  les sections arrivant dans l'ouvert où  $z$  est inversible, telles que  $x(P) = 0$ ,  $y(P) = 0$ ,  $x(Q) = C$ ,  $y(Q) = B + C$ . Alors, toutes ces données définissent une courbe elliptique munie d'une  $\Gamma(3)$ -structure,  $E_0 \rightarrow S_0$  représente  $\Gamma(3)$ , et  $(P, Q)$  est la  $\Gamma(3)$ -structure universelle.

Démonstration — En combinant le lemme 5.1, la proposition 5.2 et le fait que  $[E \rightarrow S]_{\Gamma(3)}$  est un faisceau pour la topologie de Zariski, on voit que la seule chose à montrer est que  $(E_0, (P, Q))$  est bien une courbe

elliptique sur  $S_0$  munie d'une  $\Gamma(3)$ -structure. Comme  $\Delta$  est inversible,  $E_0$  est une courbe elliptique sur  $S_0$ . Le fait que  $(P, Q)$  définit une  $\Gamma(3)$ -structure se teste sur chaque fibre géométrique, ce que l'on peut faire en reprenant les calculs de la démonstration précédente à l'envers (ou bien en utilisant les formules de multiplication par 2 et par  $-1$ ).  $\square$

## 5.2 $\Gamma(4)$ -structures

Soit  $E \rightarrow S = \text{Spec}(R)$  un objet de  $\mathbf{EllW}_{\mathbb{Z}[1/2]}$ , muni d'une  $\Gamma(4)$ -structure  $\alpha: (\mathbb{Z}/4\mathbb{Z})_S^2 \xrightarrow{\sim} E[4]$ . Notons respectivement  $P$  et  $Q$  les images des sections globales  $(1, 0)$  et  $(0, 1)$  de  $(\mathbb{Z}/4\mathbb{Z})_S^2$  par  $\alpha$ , et  $\theta$  la section nulle.

**Proposition 5.4** — *Quitte à remplacer  $S$  par un ouvert affine contenant un point donné, l'affirmation suivante est vraie : il existe d'uniques  $\sigma, i \in R$  avec  $\sigma$  inversible, tels qu'il existe un  $S$ -isomorphisme de  $E$  vers le sous-schéma fermé de  $\mathbb{P}_S^2$  défini par l'équation*

$$y^2 z = x(x-z) \left( x - \frac{1}{4} \left( \sigma + \frac{1}{\sigma} \right)^2 z \right),$$

la section  $\theta$  étant envoyée sur  $[x : y : z] = [0 : 1 : 0]$ , et vérifiant :

- $i^2 = -1$  ;
- $x(2P) = 0$ ,  $x(2Q) = 1$  et  $x(2P + 2Q) = x(P)^2$  ;
- $x(P) = \frac{1}{2} \left( \sigma + \frac{1}{\sigma} \right)$  et  $y(P) = -\frac{i(\sigma^2 + 1)(\sigma - 1)^2}{4\sigma^2}$  ;
- $x(Q) = 1 - \frac{i}{2} \left( \sigma - \frac{1}{\sigma} \right)$  et  $y(Q) = \frac{(\sigma^2 - 1)(\sigma + i)^2}{4\sigma^2}$ .

Démonstration — Soit une équation de Weierstrass pour  $E$  :

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

Elle est uniquement déterminée modulo les choix de  $u, r, s, t \in R$  avec  $u$  inversible (cf. le cas des  $\Gamma(3)$ -structures). Comme 2 est inversible dans  $R$ , on peut fixer  $s$  et  $t$  par la condition  $a_1 = a_3 = 0$ . On obtient ainsi une équation

$$y^2 = x^3 + a_2 x^2 + a_4 x + a_6,$$

uniquement déterminée modulo le choix de  $u$  et  $r$ . Notons que la nullité de  $a_1$  et de  $a_3$  entraîne que pour tout point  $G \in E(S)$  arrivant dans l'ouvert où  $z$  est inversible,  $x(-G) = x(G)$  et  $y(-G) = -y(G)$ , et donc  $y(G) = 0$  si et seulement si  $G$  est d'ordre 2. En particulier,  $y(2P) = y(2Q) = y(2P + 2Q) = 0$ , et pour  $G$  tel que  $2G \neq 0$ ,  $x(G) - x(2P)$ ,  $x(G) - x(2Q)$  et  $x(G) - x(2P + 2Q)$  sont inversibles dans  $R$  (puisqu'ils le sont sur chaque fibre). On peut donc poser

$$i = \frac{y(P)y(Q)}{(x(P) - x(2P))(x(P) - x(2Q))(x(Q) - x(2P + 2Q))} \quad (5)$$

et

$$\sigma = x(P) + i(x(Q) - 1).$$

On vérifie tout de suite qu'il est nécessaire que  $i$  et  $\sigma$  aient ces valeurs, en remplaçant  $x(P)$ ,  $x(Q)$ ,  $y(P)$ ,  $y(Q)$ ,  $x(2P)$ ,  $x(2Q)$  et  $x(2P + 2Q)$  par leurs expressions en fonction de  $\sigma$  et  $i$ , et en utilisant la relation  $i^2 = -1$ . On veut donc montrer qu'il existe d'uniques  $u$  et  $r$  dans  $R$ , avec  $u$  inversible, tels que l'équation de Weierstrass obtenue en remplaçant  $x$  par  $u^2 x + r$  et  $y$  par  $u^3 y$  et en simplifiant par  $u^6$  vérifie les propriétés indiquées avec ces valeurs de  $i$  et de  $\sigma$  (y compris la forme de l'équation de Weierstrass). On fixe  $r$  par la condition  $x(2P) = 0$ .

**Lemme 5.5** — *On a les égalités de fonctions rationnelles suivantes (i.e. de sections globales de  $\mathcal{X}_E$  ;  $G$  est la variable) :*

$$x(G + 2Q)(x(G) - x(2Q)) = (x(G) - x(2P + 2Q))x(2Q) \quad (6)$$

$$x(G + 2P)x(G) = x(2P + 2Q)x(2Q) \quad (7)$$

Démonstration — Pour prouver une égalité  $f = g$ , où  $f$  et  $g$  sont des sections globales de  $\mathcal{K}_E^*$ , on commence par prouver que  $f$  et  $g$  ont même diviseur (i.e. même image dans  $\Gamma(E, \mathcal{K}_E^*/\mathcal{O}_E^*)$ ). Cela implique que  $f/g$  est une section globale de  $\mathcal{O}_E^*$ , or on a vu que  $\Gamma(E, \mathcal{O}_E^*) = R^*$ . Ainsi, il suffit de trouver une section  $M \in E(S)$  telle que  $f$  et  $g$  soient définies en  $M$ , que  $g(M)$  soit inversible dans  $R$ , et que  $f(M) = g(M)$ , pour prouver que  $f = g$ . Pour la première équation, on vérifie sans difficulté que les deux membres de l'égalité ont pour diviseur  $2[2P+2Q] - 2[\theta]$  et valent tous les deux  $-x(2Q)x(2P+2Q)$  en  $G = 2P$ . Pour montrer que  $x(2Q)$  est inversible dans  $R$ , on peut supposer que  $R$  est un corps ; si l'on avait  $x(2Q) = 0$ , on aurait alors  $2Q = 2P$ , ce qui contredit l'hypothèse que  $(P, Q)$  est une  $\Gamma(4)$ -structure. De même pour  $x(2P+2Q)$ . Les deux membres de la deuxième égalité ont pour diviseur 0 et valent  $x(2P+2Q)x(2Q)$ , qui est inversible, en  $G = 2Q$ .  $\square$

**Lemme 5.6** — *L'égalité de polynômes de  $R[x]$  suivante est vraie :*

$$x^3 + a_2x^2 + a_4x + a_6 = x(x - x(2Q))(x - x(2P + 2Q))$$

Démonstration — Notons  $f(x)$  le polynôme de gauche. Comme  $y(2P) = 0$  et  $x(2P) = 0$ ,  $f(0) = 0$  et donc  $f(x) = xg(x)$  avec  $g \in R[x]$ . Comme  $y(2Q) = 0$ ,  $f(x(2Q)) = 0$ , mais  $x(2Q)$  est inversible dans  $R$  (car non nul sur chaque fibre, car sinon on aurait  $2P = 2Q$ ), donc  $g(x(2Q)) = 0$  :  $g(x) = (x - x(2Q))h(x)$  avec  $h \in R[x]$ . Enfin, l'inversibilité de  $x(2P+2Q) - x(2Q)$  permet de conclure.  $\square$

**Lemme 5.7** — *On a  $i^2 = -1$ .*

Démonstration — On déduit du lemme précédent que

$$i^2 = \frac{x(Q)(x(Q) - x(2Q))(x(P) - x(2P + 2Q))}{x(P)(x(P) - x(2Q))(x(Q) - x(2P + 2Q))}.$$

Appliquons le lemme 5.5 avec  $G = Q$  pour la première équation,  $G = P$  pour la seconde. On obtient

$$x(2Q)(x(Q) - x(2P + 2Q)) = x(Q)(x(Q) - x(2Q)) \quad (8)$$

et

$$x(2Q)(x(P) - x(2P + 2Q)) = x(P)(x(2Q) - x(P)), \quad (9)$$

ce qui permet d'éliminer les occurrences de  $x(2P + 2Q)$  dans l'expression de  $i^2$  ci-dessus.  $\square$

Il existe un unique  $u \in R$ , inversible, tel que  $y(P) = i(x(P) - x(2P + 2Q))$ . On vérifie par le calcul que cette condition est nécessaire pour obtenir celles de l'énoncé, en remplaçant  $y(P)$ ,  $x(P)$  et  $x(2P + 2Q)$  par leurs valeurs en fonction de  $i$  et  $\sigma$ . Montrons maintenant qu'elle est suffisante. Tout d'abord, comme  $y(P)^2 = x(P)(x(P) - x(2Q))(x(P) - x(2P + 2Q))$ , on a  $x(P)(x(P) - x(2Q)) = -(x(P) - x(2P + 2Q))$ . L'équation (9) permet d'en conclure que  $x(2Q) = 1$  (on n'insiste pas sur les conditions d'inversibilité, qui se testent sur les fibres). L'équation (7) avec  $G = P$  donne  $x(2P + 2Q) = x(P)^2$ . Il ne reste plus qu'à vérifier les expressions des coordonnées de  $P$  et de  $Q$ .

**Lemme 5.8** —  *$\sigma$  est inversible dans  $R$ , et  $\frac{1}{\sigma} = x(P) - i(x(Q) - 1)$ .*

Démonstration — Comme  $i^2 = -1$ , il suffit de vérifier que  $x(P)^2 + (x(Q) - 1)^2 = 1$ , mais cela découle de l'équation (8) et des relations  $x(P)^2 = x(2P + 2Q)$  et  $x(2Q) = 1$ .  $\square$

De la définition de  $\sigma$  et du lemme précédent, on déduit les expressions de  $x(P)$  et de  $x(Q)$ . L'expression de  $y(P)$  s'obtient grâce à la relation  $y(P) = i(x(P) - x(2P + 2Q)) = ix(P)(1 - x(P))$ . Enfin, l'expression de  $y(Q)$  en fonction de  $i$  et  $\sigma$  se déduit de l'équation (5).  $\square$

**Corollaire 5.9** — *On voit maintenant  $\sigma$  et  $i$  comme des indéterminées. Soit*

$$S_0 = \text{Spec}(\mathbb{Z}[\sigma, i, (2\sigma(\sigma^4 - 1))^{-1}]/(i^2 + 1)).$$

Soit  $E_0$  le sous-schéma fermé de  $\mathbb{P}_{S_0}^2$  défini par l'équation

$$y^2 z = x(x-z) \left( x - \frac{1}{4} \left( \sigma + \frac{1}{\sigma} \right)^2 z \right),$$

et soit  $\theta_0 \in E_0(S_0)$  la section  $[0 : 1 : 0]$ . Soient  $P$  et  $Q$  les sections arrivant dans l'ouvert où  $z$  est inversible, telles que  $x(P)$ ,  $y(P)$ ,  $x(Q)$  et  $y(Q)$  soient donnés par les expressions de la proposition 5.4. Alors, toutes ces données définissent une courbe elliptique munie d'une  $\Gamma(4)$ -structure,  $E_0 \rightarrow S_0$  représente  $\Gamma(4)$ , et  $(P, Q)$  est la  $\Gamma(4)$ -structure universelle.

Démonstration — L'inversibilité de  $\sigma^4 - 1$  équivaut à l'inversibilité du discriminant. Tout ce qu'il reste à montrer est donc que  $(P, Q)$  est une  $\Gamma(4)$ -structure sur  $E_0$ , i.e. que  $4P = 0$ ,  $4Q = 0$ ,  $2P \neq 0$ ,  $2Q \neq 0$ ,  $2P \neq 2Q$ , ce qui peut se faire sur chaque fibre à l'aide de la formule de duplication.  $\square$

## 6 Représentabilité relative de $\Gamma(N)$ et $\Gamma'(N)$

Soit  $N \in \mathbb{N}^*$ . Le foncteur  $\Gamma(N)$  est naturellement muni d'une action de  $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ .

**Proposition 6.1** — *Les foncteurs  $\Gamma(N)$  et  $\Gamma'(N)$  sont relativement représentables. De plus, pour toute courbe elliptique  $E \rightarrow S$  avec  $N$  inversible sur  $S$ , le morphisme  $\mathbb{S}_{[E \rightarrow S]_{\Gamma(N)}} \rightarrow S$  est fini étale, et est un toreur sous  $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$  (pour l'action induite par celle de  $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$  sur  $\Gamma(N)$ ).*

Démonstration — Soit  $E \rightarrow S$  une courbe elliptique avec  $N$  inversible sur  $S$ . Il s'agit de prouver la représentabilité du foncteur suivant :

$$\begin{aligned} (\mathbf{Sch}/S)^\circ &\longrightarrow \mathbf{Ens} \\ T &\longmapsto \mathrm{Isom}_{T\text{-sch. en gr.}}((\mathbb{Z}/N\mathbb{Z})_T^2, E[N]_T) \end{aligned}$$

Ce foncteur est un faisceau pour la topologie étale. De plus, comme  $E[N]$  est localement (sur  $S$ ) isomorphe à  $(\mathbb{Z}/N\mathbb{Z})_S^2$  pour la topologie étale, il est localement isomorphe au faisceau constant

$$\underline{\mathrm{Isom}}_{S\text{-faisc. en gr.}}((\mathbb{Z}/N\mathbb{Z})_S^2, (\mathbb{Z}/N\mathbb{Z})_S^2) = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})_S,$$

et de manière compatible à l'action de  $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ . En d'autres termes c'est un faisceau étale localement constant, à tiges finies. Il est donc bien représentable par un  $S$ -schéma fini étale (cette implication est bien connue ; elle découle du fait que l'on peut descendre, par un morphisme fidèlement plat, tout schéma affine sur la base muni d'une donnée de descente, et que les propriétés « fini » et « étale » descendent aussi), qui est un toreur sous  $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ .

Le cas de  $\Gamma'(N)$  ne pose pas plus de difficulté. Après un changement de base étale,  $\mu_{N,S}$  et  $(\mathbb{Z}/N\mathbb{Z})_S$  deviennent isomorphes, donc le faisceau étale  $[E \rightarrow S]_{\Gamma'(N)}$  est localement isomorphe à  $[E \rightarrow S]_{\Gamma(N)}$  ; en particulier, il est localement constant et à tiges finies, et il est donc représentable.  $\square$

## 7 Rigidité de $\Gamma(N)$ et $\Gamma'(N)$ pour $N \geq 3$

**Proposition 7.1** — *Pour  $N \geq 3$ , les foncteurs  $\Gamma(N)$  et  $\Gamma'(N)$  sont rigides.*

Soit  $E \rightarrow S$  une courbe elliptique avec  $N$  inversible sur  $S$ , munie d'une  $P$ -structure  $\alpha$  où  $P = \Gamma(N)$  ou  $P = \Gamma'(N)$ . Soit  $\sigma$  un  $S$ -automorphisme de  $E$  préservant  $\alpha$ . Il faut voir que  $\sigma = \mathrm{Id}_E$  ; quitte à se restreindre à une fibre, on peut supposer que  $S$  est le spectre d'un corps  $k$ . Quitte ensuite à remplacer  $k$  par une extension séparable, on peut supposer que  $k$  contient les racines  $N$ -èmes de l'unité ; par conséquent, on peut supposer que  $P = \Gamma(N)$ . Dire que  $\sigma$  préserve  $\alpha$  signifie exactement que  $\sigma$  induit l'identité sur  $E[N]$ . Ainsi, le résultat à prouver est le suivant.

**Lemme 7.2** — *Soit  $N \geq 3$ ,  $k$  un corps dont la caractéristique ne divise pas  $N$ . Soit  $E$  une courbe elliptique sur  $k$ , et  $\sigma \in \mathrm{Aut}_k(E)$  qui induise l'identité sur  $E[N]$ . Alors  $\sigma = \mathrm{Id}_E$ .*

Démonstration — L'hypothèse signifie que  $\sigma - 1$  s'annule sur  $E[N]$ ; il existe donc  $\tau \in \text{End}_k(E)$  tel que  $\sigma = 1 + N\tau$ . Notons respectivement  $\text{Tr}(f)$ ,  $\deg(f)$  et  $\chi_f$  la trace, le degré et le polynôme caractéristique d'un  $k$ -endomorphisme  $f$  de  $E$ ; on a  $\chi_f(T) = T^2 - \text{Tr}(f)T + \deg(f)$  et  $\deg(mf - n) = m^2\chi_f(n/m)$  pour  $n, m \in \mathbb{N}$ ,  $m \neq 0$ . Comme  $\deg(mf - n) \geq 0$  pour tous  $m$  et  $n$ ,  $\chi_f(t) \geq 0$  pour tout  $t \in \mathbb{R}$  et donc  $(\text{Tr}(f))^2 \leq 4\deg(f)$ . Appliquons ceci à  $\sigma$  :  $\deg(\sigma) = 1$  donc  $|\text{Tr}(\sigma)| \leq 2$ . Comme  $\text{Tr}(\sigma) = 2 + N\text{Tr}(\tau)$ , on en déduit que  $|\text{Tr}(\tau)| \leq 4$ . Par ailleurs  $1 = \deg(\sigma) = N^2\chi_\tau(1/N) = 1 + N\text{Tr}(\tau) + N^2\deg(\tau)$ , d'où  $\deg(\tau) \leq 4/N^2 < 1$ , et donc  $\tau = 0$ , c'est-à-dire  $\sigma = \text{Id}_E$ .  $\square$

**Remarque** — On peut aussi prouver ce lemme en utilisant la structure du groupe des automorphismes d'une courbe elliptique sur un corps algébriquement clos, qui est bien connue.

**Remarque** — Le lemme reste vrai en remplaçant « courbe elliptique » par « variété abélienne » dans l'énoncé. Voir [4] pour une preuve.

## 8 Fin de la preuve

### 8.1 Rappels sur les quotients

Si  $\mathcal{C}$  est une catégorie,  $X$  un objet de  $\mathcal{C}$ ,  $G$  un groupe agissant à gauche sur  $X$  (i.e. muni d'un morphisme de groupes  $G \rightarrow \text{Aut}_{\mathcal{C}}(X)$ ), on appelle *quotient de  $X$  par  $G$*  un objet initial dans la catégorie des objets  $Y$  de  $\mathcal{C}$  munis d'une flèche  $X \rightarrow Y$  invariante par l'action de  $G$ . Rappelons aussi que si  $X$  est un  $Y$ -schéma et  $G$  un schéma en groupes sur  $Y$  agissant à gauche sur  $X$ , on dit que  $X$  est un *torseur* sous  $G$  si  $G \times_Y X \rightarrow X \times_Y X$ ,  $(g, x) \mapsto (gx, x)$  est un isomorphisme. Si  $G$  est seulement un groupe agissant sur  $X$ , on dira que  $X$  est un torseur sous  $G$  (sous-entendu : sur  $Y$ ) si c'en est un sous le schéma en groupes constant  $G_Y$ . Enfin, si  $G$  est un groupe agissant sur un  $S$ -schéma  $X$ , on dit qu'il agit *librement* si son action sur  $X(T)$  est libre pour tout  $S$ -schéma  $T$ .

**Théorème 8.1** — Soient  $X = \text{Spec}(A)$  un schéma affine et  $G$  un groupe fini agissant sur  $X$ . Notons  $p: X \rightarrow \text{Spec}(A^G)$  le morphisme déduit de l'inclusion de  $A^G$  dans  $A$ ,  $A^G$  désignant le sous-anneau des invariants par  $G$ . Alors  $p$  est un quotient de  $X$  par  $G$  dans **Sch**, et  $p$  est entier et surjectif. Supposons que  $A$  possède une structure de  $R$ -algèbre compatible à l'action de  $G$ ;  $A^G$  est alors naturellement une  $R$ -algèbre, et  $p$  est un quotient dans **Sch**/ $R$ . Supposons  $R$  noethérien et  $X$  de type fini sur  $R$ . Alors  $Y$  est de type fini sur  $R$  et  $p$  est un morphisme fini. Si de plus  $G$  agit librement sur  $X$ ,  $p$  est étale et est un torseur sous  $G$ .

Démonstration — Ceci découle des énoncés 1.1, 1.5 et 2.6 de [SGA1] exposé V.  $\square$

**Proposition 8.2** — Soient  $X$  et  $Y$  des schémas,  $G$  un groupe fini agissant sur  $X$ ,  $p: X \rightarrow Y$  un morphisme fppf invariant sous l'action de  $G$ . Si  $p$  est un torseur sous  $G$ , c'est un quotient de  $X$  par  $G$  dans la catégorie des schémas.

Démonstration — Il suffit de voir que  $p$  est un quotient dans la catégorie des faisceaux fppf sur  $Y$ , ce qui est une question locale sur  $Y$  pour la topologie fppf. On peut donc supposer que  $p$  possède une section, auquel cas le résultat est clair.  $\square$

### 8.2 Théorème de représentabilité

Le but de cette section est de prouver le théorème suivant.

**Théorème 8.3** — Soit  $N \in \mathbb{N}^*$ . Soit  $P: (\mathbf{Ell}_{\mathbb{Z}[1/N]})^\circ \rightarrow \mathbf{Ens}$  un foncteur relativement représentable et rigide. On suppose que pour toute courbe elliptique  $E \rightarrow S$ ,  $N$  inversible sur  $S$ , le morphisme de schémas  $\mathbb{S}_{[E \rightarrow S]_P} \rightarrow S$  est affine. Alors  $P$  est représentable, et  $\mathbb{S}_P$  est un schéma affine. Supposons de plus que pour toute  $E \rightarrow S$ ,  $N$  inversible sur  $S$ , le morphisme  $\mathbb{S}_{[E \rightarrow S]_P} \rightarrow S$  est étale; alors  $\mathbb{S}_P$  est un  $\mathbb{Z}[1/N]$ -schéma lisse de dimension relative constante 1.

Pour  $k \geq 1$ , notons  $\tilde{P}[1/kN]: (\mathbf{Sch}/\mathbb{Z}[1/kN])^\circ \rightarrow \mathbf{Ens}$  la restriction du foncteur  $\tilde{P}$ . Si  $X$  est un schéma et  $k \geq 1$ , on note  $X[1/k]$  l'ouvert de  $X$  où  $k$  est inversible, autrement dit  $X[1/k] = X \times_{\mathrm{Spec}(\mathbb{Z})} \mathrm{Spec}(\mathbb{Z}[1/k])$ .

**Lemme 8.4** — *Pour prouver le théorème 8.3, il suffit de traiter le cas où  $N$  est un multiple de 2 ou de 3.*

Démonstration — Supposons  $\tilde{P}[1/2N]$  et  $\tilde{P}[1/3N]$  représentables. Pour  $k = 2$  ou  $k = 3$ , il existe alors une courbe elliptique  $\mathbb{E}_k \rightarrow \mathbb{S}_{\tilde{P}[1/kN]}$  munie d'une  $P$ -structure  $\alpha_k$ , telle que toute courbe elliptique  $E \rightarrow S$  munie d'une  $P$ -structure, où  $S$  est un  $\mathbb{Z}[1/kN]$ -schéma, s'obtienne à  $S$ -isomorphisme près par un unique changement de base  $S \rightarrow \mathbb{S}_{\tilde{P}[1/kN]}$  à partir de  $\mathbb{E}_k$  et  $\alpha_k$ .

Les  $\mathbb{Z}[1/6N]$ -schémas  $\mathbb{S}_{\tilde{P}[1/2N]}[1/6]$  et  $\mathbb{S}_{\tilde{P}[1/3N]}[1/6]$  sont canoniquement isomorphes (ils représentent tous les deux  $\tilde{P}[1/6N]$ ); appelons  $\mathbb{S}$  le schéma que l'on obtient en recollant  $\mathbb{S}_{\tilde{P}[1/2N]}$  et  $\mathbb{S}_{\tilde{P}[1/3N]}$  selon ces ouverts. On a tautologiquement  $\mathbb{S}_{\tilde{P}[1/2N]} = \mathbb{S}[1/2]$  et  $\mathbb{S}_{\tilde{P}[1/3N]} = \mathbb{S}[1/3]$  (en tant qu'ouverts de  $\mathbb{S}$ ). Ainsi,  $\mathbb{S}[1/6]$  représente  $\tilde{P}[1/6N]$ ; il existe donc un isomorphisme  $f: \mathbb{E}_2[1/6] \rightarrow \mathbb{E}_3[1/6]$  de courbes elliptiques sur  $\mathbb{S}[1/6]$ , compatible aux  $P$ -structures induites par  $\alpha_2$  et  $\alpha_3$ . En recollant  $\mathbb{E}_2$  et  $\mathbb{E}_3$  selon  $f$ , on obtient un schéma  $\mathbb{E}$ , naturellement muni d'une structure de courbe elliptique sur  $\mathbb{S}$ .

Par représentabilité relative de  $P$ ,  $\alpha_2$  et  $\alpha_3$  correspondent respectivement à des  $\mathbb{S}$ -morphisms

$$\beta_2: \mathbb{S}[1/2] \rightarrow \mathbb{S}_{[\mathbb{E} \rightarrow \mathbb{S}]_P}$$

et

$$\beta_3: \mathbb{S}[1/3] \rightarrow \mathbb{S}_{[\mathbb{E} \rightarrow \mathbb{S}]_P}.$$

Comme  $f$  envoie la restriction de  $\alpha_3$  sur celle de  $\alpha_2$ ,  $\beta_2$  et  $\beta_3$  coïncident sur  $\mathbb{S}[1/6]$ , et définissent donc une  $P$ -structure  $\alpha$  sur  $\mathbb{E} \rightarrow \mathbb{S}$ . On vérifie sans difficulté que  $(\mathbb{E} \rightarrow \mathbb{S}, \alpha)$  est la  $\tilde{P}$ -structure universelle. Ainsi,  $\mathbb{S}$  représente  $\tilde{P}$ ;  $P$  étant rigide, il est lui aussi représentable.

Le morphisme  $\mathbb{S} \rightarrow \mathrm{Spec}(\mathbb{Z}[1/N])$  est affine, puisqu'il l'est localement sur la base;  $\mathbb{S}$  est donc un schéma affine. La lissité et la dimension relative se testent localement sur la base, donc les assertions les concernant sont vérifiées par  $\mathbb{S} \rightarrow \mathrm{Spec}(\mathbb{Z}[1/N])$ .  $\square$

Pour prouver la représentabilité de  $\tilde{P}$  lorsque  $N$  est multiple de 2 ou de 3, nous allons employer la stratégie décrite précédemment : on montre que le produit de  $P$  et d'un certain foncteur auxiliaire représentable  $Q$ , muni d'une action d'un groupe fini  $G$ , est représentable, puis on essaie de retrouver  $P$  en quotientant par l'action de  $G$  sur le produit. Le théorème suivant l'exprime en termes précis.

**Hypothèse 8.5** — *On suppose qu'il existe un foncteur  $Q: (\mathbf{Ell}_{\mathbb{Z}[1/N]})^\circ \rightarrow \mathbf{Ens}$  représentable et relativement représentable<sup>2</sup>, un groupe fini  $G$  et une action (à gauche) de  $G$  sur  $Q$ , tels que pour toute courbe elliptique  $E \rightarrow S$  avec  $N$  inversible sur  $S$ , le morphisme  $\mathbb{S}_{[E \rightarrow S]_Q} \rightarrow S$  soit fini étale et fasse de  $\mathbb{S}_{[E \rightarrow S]_Q}$  un torseur sous  $G_S$ . On suppose enfin que  $\mathbb{S}_Q$  est un  $\mathbb{Z}[1/N]$ -schéma affine, lisse de dimension relative constante 1.*

On fait bien sûr agir  $G$  sur le foncteur  $[E \rightarrow S]_Q: (\mathbf{Sch}/S)^\circ \rightarrow \mathbf{Ens}$  (et donc sur le  $S$ -schéma  $\mathbb{S}_{[E \rightarrow S]_Q}$ ) par son action sur  $Q$  (rappelons que  $[E \rightarrow S]_Q(T) = Q(E \times_S T \rightarrow T)$ ).

**Théorème 8.6** — *Sous l'hypothèse 8.5, le foncteur  $\tilde{P}$  est représentable, représenté par un  $\mathbb{Z}[1/N]$ -schéma affine. De plus, si pour toute courbe elliptique  $E \rightarrow S$  avec  $N$  inversible sur  $S$ , le morphisme  $\mathbb{S}_{[E \rightarrow S]_P} \rightarrow S$  est étale, alors  $\tilde{P}$  est représenté par un  $\mathbb{Z}[1/N]$ -schéma lisse de dimension relative constante 1.*

D'après 5.3, 5.9 et 6.1, l'hypothèse 8.5 est vérifiée pour  $N$  multiple de 3 (prendre pour  $Q$  la restriction de  $\Gamma(3)$  à  $\mathbf{Ell}_{\mathbb{Z}[1/3]}$ ) et pour  $N$  pair (prendre pour  $Q$  la restriction de  $\Gamma(4)$  à  $\mathbf{Ell}_{\mathbb{Z}[1/2]}$ ). Ainsi, d'après le lemme 8.4, le théorème 8.3 est prouvé.

Démonstration — Tout d'abord, montrons que le foncteur  $P \times Q: (\mathbf{Ell}_{\mathbb{Z}[1/N]})^\circ \rightarrow \mathbf{Ens}$  est représentable. Comme  $Q$  est représentable, il existe une courbe elliptique  $\mathbb{E}_Q \rightarrow \mathbb{S}_Q$  munie d'une  $Q$ -structure universelle; de plus,  $P$  étant relativement représentable, il existe un  $\mathbb{S}_Q$ -schéma  $\mathbb{S}_{[\mathbb{E}_Q \rightarrow \mathbb{S}_Q]_P}$  sur lequel  $\mathbb{E}_Q$  acquiert une

2. On peut prouver qu'un foncteur représentable  $(\mathbf{Ell}_{\mathbb{Z}[1/N]})^\circ \rightarrow \mathbf{Ens}$  est automatiquement relativement représentable, mais ce n'est pas trivial et ne nous servira pas.

$P$ -structure universelle pour les courbes elliptiques déduites de  $\mathbb{E}_Q$  par changement de base. Il est maintenant immédiat que la courbe elliptique

$$\mathbb{E}_Q \times_{\mathbb{S}_Q} \mathbb{S}_{[\mathbb{E}_Q \rightarrow \mathbb{S}_Q]_P} \longrightarrow \mathbb{S}_{[\mathbb{E}_Q \rightarrow \mathbb{S}_Q]_P}$$

représente  $P \times Q$ . On la note donc  $\mathbb{E}_{P \times Q} \rightarrow \mathbb{S}_{P \times Q}$ ; elle est munie d'une  $(P \times Q)$ -structure universelle  $(\alpha_{P \times Q}, \beta_{P \times Q})$ . Faisons agir  $G$  sur  $\mathbb{S}_{P \times Q}$  de la manière suivante : pour  $g \in G$ , la  $(P \times Q)$ -structure  $(\alpha_{P \times Q}, g\beta_{P \times Q})$  sur  $\mathbb{E}_{P \times Q} \rightarrow \mathbb{S}_{P \times Q}$  provient de  $(\alpha_{P \times Q}, \beta_{P \times Q})$  par un unique carré cartésien

$$\begin{array}{ccc} \mathbb{E}_{P \times Q} & \xrightarrow{e(g)} & \mathbb{E}_{P \times Q} \\ \downarrow & & \downarrow \\ \mathbb{S}_{P \times Q} & \xrightarrow{s(g)} & \mathbb{S}_{P \times Q}, \end{array}$$

et on fait agir  $g$  sur  $\mathbb{S}_{P \times Q}$  par  $s(g)$ . On a  $s(hg) = s(g)s(h)$  et  $e(hg) = e(g)e(h)$ , par unicité. Par hypothèse, le morphisme  $\mathbb{S}_{[\mathbb{E}_Q \rightarrow \mathbb{S}_Q]_P} \rightarrow \mathbb{S}_Q$  est affine et fini ; par hypothèse aussi,  $\mathbb{S}_Q$  est un schéma affine et de type fini sur  $\mathbb{Z}[1/N]$ . Ainsi,  $\mathbb{S}_{P \times Q}$  est lui aussi affine et de type fini sur  $\mathbb{Z}[1/N]$ , ce qui permet d'appliquer le théorème 8.1 : d'où l'existence d'un quotient  $\mathbb{S}_{P \times Q}/G$ , qui est un  $\mathbb{Z}[1/N]$ -schéma affine, et tel que la projection  $\mathbb{S}_{P \times Q} \rightarrow \mathbb{S}_{P \times Q}/G$  soit finie étale (l'action est libre, d'après l'hypothèse 8.5).

Le  $\mathbb{S}_{P \times Q}$ -schéma  $\mathbb{E}_{P \times Q}$  possède une donnée de descente relativement à la projection  $\mathbb{S}_{P \times Q} \rightarrow \mathbb{S}_{P \times Q}/G$  : comme on vient de le voir,  $\mathbb{E}_{P \times Q} \rightarrow \mathbb{S}_{P \times Q}$  s'identifie à l'image réciproque d'elle-même par  $s(g)$  (à l'aide de  $e(g)$ ), et on choisit l'identité comme  $\mathbb{S}_{P \times Q}$ -isomorphisme entre les images réciproques de  $\mathbb{E}_{P \times Q} \rightarrow \mathbb{S}_{P \times Q}$  par  $s(g)$  et par Id. La compatibilité trois à trois de ces isomorphismes (i.e. la commutativité du triangle obtenu en considérant les images réciproques par Id, par  $s(g)$ , et par  $s(hg)$ ) découle immédiatement de la relation  $e(hg) = e(g)e(h)$ .

De plus, le faisceau inversible  $\mathcal{O}_{\mathbb{E}_{P \times Q}}([\theta])$  est ample relativement à  $\mathbb{S}_{P \times Q}$  (cela signifie qu'il existe un recouvrement de  $\mathbb{S}_{P \times Q}$  par des ouverts affines tels que la restriction de ce faisceau inversible à l'image réciproque de chacun de ces ouverts affines soit ample — cette propriété est vérifiée ici d'après l'existence d'équations de Weierstrass localement sur la base) et est compatible à la donnée de descente. On sait que l'on peut toujours descendre, par un morphisme fidèlement plat, un schéma quasi-compact sur la base muni d'une donnée de descente et d'un faisceau inversible relativement ample et compatible à la donnée de descente (c'est un critère d'effectivité classique ; voir [SGA1], exposé VIII, prop. 7.8).

Il existe donc une courbe elliptique  $\mathbb{E}_0$  sur  $\mathbb{S}_{P \times Q}/G$  et un diagramme cartésien :

$$\begin{array}{ccc} \mathbb{E}_{P \times Q} & \longrightarrow & \mathbb{E}_0 \\ \downarrow & & \downarrow \\ \mathbb{S}_{P \times Q} & \longrightarrow & \mathbb{S}_{P \times Q}/G \end{array}$$

Essayons de descendre la  $P$ -structure  $\alpha_{P \times Q}$ . Par représentabilité relative de  $P$ ,  $\alpha_{P \times Q}$  correspond à un unique  $\mathbb{S}_{P \times Q}/G$ -morphisme  $\mathbb{S}_{P \times Q} \rightarrow \mathbb{S}_{[\mathbb{E}_0 \rightarrow \mathbb{S}_{P \times Q}/G]_P}$ , lequel est invariant sous l'action de  $G$  puisque  $\alpha_{P \times Q}$  l'est. Il se factorise donc par  $\mathbb{S}_{P \times Q}/G$  (propriété universelle du quotient), et l'on obtient ainsi une  $P$ -structure  $\alpha_0$  sur  $\mathbb{E}_0$  qui est envoyée sur  $\alpha_{P \times Q}$  par le carré cartésien ci-dessus.

Nous allons maintenant montrer que  $\mathbb{S}_{P \times Q}/G$  représente  $\tilde{P}$ , et que la  $\tilde{P}$ -structure universelle sur  $\mathbb{S}_{P \times Q}/G$  est la classe d'isomorphisme de  $(\mathbb{E}_0, \alpha_0)$ .

Soit  $E \rightarrow S$  une courbe elliptique munie d'une  $P$ -structure  $\alpha$ , où  $S$  est un  $\mathbb{Z}[1/N]$ -schéma. Il s'agit de montrer que la classe d'isomorphisme de  $(E, \alpha)$  provient de  $(\mathbb{E}_0, \alpha_0)$  par un unique changement de base  $S \rightarrow \mathbb{S}_{P \times Q}/G$ . Commençons par l'existence. La représentabilité relative de  $Q$  nous donne un  $S$ -schéma  $\mathbb{S}_{[E \rightarrow S]_Q}$  ; la courbe elliptique  $E \times_S \mathbb{S}_{[E \rightarrow S]_Q} \rightarrow \mathbb{S}_{[E \rightarrow S]_Q}$  est munie d'une  $P$ -structure (celle induite par  $\alpha$ ) et d'une  $Q$ -structure (celle qui est universelle), d'où une flèche canonique  $\mathbb{S}_{[E \rightarrow S]_Q} \rightarrow \mathbb{S}_{P \times Q}$ . On vérifie tout de suite que cette flèche commute à l'action de  $G$ . Par hypothèse, comme  $N$  est inversible sur  $S$ ,  $\mathbb{S}_{[E \rightarrow S]_Q} \rightarrow S$  est un torseur fini étale sous  $G$ , et  $S$  est donc le quotient de  $\mathbb{S}_{[E \rightarrow S]_Q}$  par  $G$  (d'après 8.2). Ainsi, par la propriété universelle du quotient, la flèche  $\mathbb{S}_{[E \rightarrow S]_Q} \rightarrow \mathbb{S}_{P \times Q}/G$  se factorise par  $S$ . On obtient le diagramme

commutatif suivant :

$$\begin{array}{ccc} \mathbb{S}_{[E \rightarrow S]_Q} & \longrightarrow & \mathbb{S}_{P \times Q} \\ \downarrow & & \downarrow \\ S & \xrightarrow{f} & \mathbb{S}_{P \times Q}/G \end{array}$$

Notons  $E' = S \times_{\mathbb{S}_{P \times Q}/G} \mathbb{E}_0$  et  $\alpha'$  la  $P$ -structure sur  $E' \rightarrow S$  induite par  $\alpha_0$ . Il faut montrer que les couples  $(E', \alpha')$  et  $(E, \alpha)$  sont isomorphes sur  $S$ . Ces deux couples induisent la même  $\tilde{P}$ -structure sur  $\mathbb{S}_{[E \rightarrow S]_Q}$  ; il existe donc un  $\mathbb{S}_{[E \rightarrow S]_Q}$ -isomorphisme

$$E \times_S \mathbb{S}_{[E \rightarrow S]_Q} \xrightarrow{t} E' \times_S \mathbb{S}_{[E \rightarrow S]_Q}$$

compatible aux  $P$ -structures induites. Comme  $P$  est rigide, il ne peut y avoir qu'un isomorphisme de courbes elliptiques sur  $\mathbb{S}_{[E \rightarrow S]_Q} \times_S \mathbb{S}_{[E \rightarrow S]_Q}$

$$E \times_S \mathbb{S}_{[E \rightarrow S]_Q} \times_S \mathbb{S}_{[E \rightarrow S]_Q} \longrightarrow E' \times_S \mathbb{S}_{[E \rightarrow S]_Q} \times_S \mathbb{S}_{[E \rightarrow S]_Q}$$

compatible aux  $P$ -structures induites par  $\alpha$  et  $\alpha'$ . Les deux que l'on obtient à partir de  $t$ , par changement de base par les deux projections, sont donc égaux :  $t$  est compatible aux données de descente. Le morphisme  $\mathbb{S}_{[E \rightarrow S]_Q} \rightarrow S$  étant fidèlement plat (il est surjectif car fini de rang constant égal au cardinal de  $G$ ), on en déduit que  $t$  descend en un  $S$ -isomorphisme  $t_S : E \rightarrow E'$ . On peut maintenant utiliser la représentabilité relative de  $P$  pour vérifier que  $t_S$  est compatible aux  $P$ -structures  $\alpha$  et  $\alpha'$ , ce qui découle à nouveau de la fidèle platitude de  $\mathbb{S}_{[E \rightarrow S]_Q} \rightarrow S$ . Ainsi, le changement de base  $f$  convient.

Reste à montrer l'unicité. Soit  $g : S \rightarrow \mathbb{S}_{P \times Q}/G$  un morphisme compatible aux  $\tilde{P}$ -structures  $(E, \alpha)$  et  $(\mathbb{E}_0, \alpha_0)$ . Posons  $T = S \times_{\mathbb{S}_{P \times Q}/G} \mathbb{S}_{P \times Q}$ . Dans le diagramme suivant, le petit carré est commutatif et cartésien, et d'après la propriété universelle de  $f$ , tout ce qu'il faut montrer est que le diagramme est entièrement commutatif :

$$\begin{array}{ccc} \mathbb{S}_{[E \rightarrow S]_Q} & & \\ & \searrow & \\ & & T \longrightarrow \mathbb{S}_{P \times Q} \\ & \searrow & \downarrow \\ & & S \xrightarrow{g} \mathbb{S}_{P \times Q}/G \end{array}$$

Par rigidité de  $P$ , il existe un unique isomorphisme

$$i : E \times_S T \longrightarrow \mathbb{E}_{P \times Q} \times_{\mathbb{S}_{P \times Q}} T$$

de courbes elliptiques sur  $T$ , compatible aux  $P$ -structures  $\alpha$  et  $\alpha_{P \times Q}$ . On munit ainsi la première de ces courbes elliptiques d'une  $Q$ -structure en transportant  $\beta_{P \times Q}$  par  $i$ , d'où un  $S$ -morphisme  $u : T \rightarrow \mathbb{S}_{[E \rightarrow S]_Q}$ . On vérifie tout de suite que  $u$  commute à l'action de  $G$ . De plus, il est immédiat que les deux triangles du diagramme suivant dont  $u$  est un bord sont commutatifs :

$$\begin{array}{ccc} \mathbb{S}_{[E \rightarrow S]_Q} & & \\ & \searrow & \\ & & T \longrightarrow \mathbb{S}_{P \times Q} \\ & \searrow & \downarrow \\ & & S \xrightarrow{g} \mathbb{S}_{P \times Q}/G \end{array}$$

On en déduit qu'il suffit de montrer que  $u$  est un isomorphisme. Le morphisme  $\mathbb{S}_{P \times Q} \rightarrow \mathbb{S}_{P \times Q}/G$  est un torseur sous  $G$ , d'après 8.1. Ainsi,  $u$  est un morphisme  $G$ -équivariant de  $G$ -torseurs, ce qui implique que  $u$  est un isomorphisme.

Il reste à démontrer que  $\mathbb{S}_{P \times Q}/G$  est un  $\mathbb{Z}[1/N]$ -schéma lisse de dimension relative constante 1, sous l'hypothèse que  $\mathbb{S}_{[E \rightarrow S]_P} \rightarrow S$  est étale pour toute courbe elliptique  $E \rightarrow S$  avec  $N$  inversible sur  $S$ . Cette hypothèse dit en particulier que  $\mathbb{S}_{P \times Q} \rightarrow \mathbb{S}_Q$  est étale. D'après 8.5,  $\mathbb{S}_Q$  est un  $\mathbb{Z}[1/N]$ -schéma lisse de dimension relative constante 1 ; il en va donc de même pour  $\mathbb{S}_{P \times Q}$ . Finalement,  $\mathbb{S}_{P \times Q} \rightarrow \mathbb{S}_{P \times Q}/G$  étant un torseur fini étale, on en déduit le résultat voulu.  $\square$

### 8.3 Conclusion

**Corollaire 8.7** — *Pour  $N \geq 3$ , les foncteurs  $\Gamma(N)$  et  $\Gamma'(N)$  sont représentables, et sont représentés par des courbes elliptiques relatives dont la base est un  $\mathbb{Z}[1/N]$ -schéma affine, lisse, de dimension relative constante 1.*

Démonstration — Il suffit d'emboîter les énoncés 8.3, 7.1 et 6.1.  $\square$

Le théorème 8.3 est très général ; il permet de prouver l'existence de nombreux autres schémas de modules<sup>3</sup> (par exemple pour les courbes elliptiques munies d'un point d'ordre  $N$ , les courbes elliptiques munies d'un sous-groupe cyclique d'ordre  $N$ , ou encore les courbes elliptiques munies d'une  $\Gamma'(N)$ -structure vérifiant la « condition de déterminant 1 » — cette condition permet d'obtenir un schéma de modules géométriquement connexe). Cela dit, il faut souvent travailler un peu plus pour obtenir la représentabilité relative du foncteur considéré (notons toutefois que le problème des  $\Gamma'(N)$ -structures de déterminant 1 se traite exactement de la même manière que celui des  $\Gamma(N)$ -structures).

Le présent exposé n'a abordé que la question de l'existence des schémas de modules ; mentionnons quelques sujets qu'il est intéressant d'étudier ensuite :

- la comparaison avec la théorie transcendante sur  $\mathbb{C}$  ;
- la compactification desdits schémas de modules, et l'interprétation des points à l'infini par les courbes elliptiques généralisées ;
- la notion de base de Drinfeld, qui conduit à de bonnes généralisations des  $\Gamma(N)$ -structures lorsque  $N$  n'est pas inversible sur la base (si  $E \rightarrow S$  est une courbe elliptique relative avec  $N$  non inversible sur  $S$ , il ne peut pas exister d'isomorphisme entre  $E[N]$  et  $(\mathbb{Z}/N\mathbb{Z})_S^2$ ) ;
- l'étude de la réduction modulo  $p$  des schémas de modules ainsi obtenus, pour  $p$  divisant  $N$ .

Tout ceci est fait en détail dans [2] et [3]. Notons que la théorie des bases de Drinfeld n'était pas disponible au moment de l'écriture de [2] ; il vaut donc mieux consulter [3] pour ce qui concerne la réduction modulo  $p$ .

## Bibliographie

- [1] BOSCH, S., LÜTKEBOHMERT, W., RAYNAUD, M., Néron models, *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*, 21, Springer-Verlag, Berlin, 1990.
- [2] DELIGNE, P., RAPOPORT, M., *Les schémas de modules des courbes elliptiques*, in *Modular functions of one variable, II, Lecture Notes in Math.*, Vol. 349, Springer, Berlin, 1973.
- [3] KATZ, N., MAZUR, B., *Arithmetic moduli of elliptic curves*, *Annals of Mathematics Studies*, 108, Princeton University Press, Princeton, NJ, 1985.
- [4] SERRE, J.-P., *Rigidité du foncteur de Jacobi d'échelon  $n \geq 3$ , appendice à l'exposé 17 du séminaire Cartan 1960–1961*.
- [SGA1] GROTHENDIECK, A., RAYNAUD, M., *Revêtements étales et groupe fondamental, Séminaire de Géométrie Algébrique du Bois Marie 1960–1961 (SGA 1), Lecture Notes in Math.*, Vol. 224, Springer, Berlin, 1971.

---

3. C'est la base de la courbe elliptique universelle pour les  $P$ -structures que l'on appelle le schéma de modules de  $P$  (il s'agit donc en fait du schéma qui représente  $\tilde{P}$ ).