Botanique des espaces de modules de courbes elliptiques : λ

P. Deligne

dédié à Gérard Laumon

Résumé. La courbe $X := \mathbb{P}^1 - \{0, 1, \infty\}$ est un espace grossier de modules pour les courbes elliptiques E munies d'un isomorphisme de $(\mathbb{Z}/2)^2$ avec le groupe E_2 de leurs points d'ordre divisant 2. Nous montrons que c'est aussi un espace fin de modules pour les courbes elliptiques munies d'une structure de niveau 4 convenable.

Abstract. The curve $X := \mathbb{P}^1 - \{0, 1, \infty\}$ is a coarse moduli space for elliptic curves E given with an isomorphism $\alpha : (\mathbb{Z}/2)^2 \xrightarrow{\sim} E_2$. We show it is also a fine moduli space for elliptic curves given with a suitable level 4 structure.

1. Espace grossier de modules

1.1. Soit E une courbe elliptique munie de $\alpha : (\mathbb{Z}/2)^2 \xrightarrow{\sim} E_2$. Notons e l'élément neutre de E. La donnée de α équivaut à celle d'une énumération $e_1,\ e_2,\ e_3$ des points d'ordre 2 de E : prendre pour $e_1,\ e_2,\ e_3$ les images par α de $(1,0),\ (0,1)$ et $(1,1)$. Le sous-groupe E_2 de E est le lieu des points fixes de l'involution $\sigma : E \to E : P \mapsto -P$. Le quotient Q de E par cette involution est de genre 0. On l'identifie à $\mathbb{P}^1$ en imposant que les images de e, e_1, et e_2 soient ∞, 0 et 1 et on définit $\lambda(E, \alpha)$ comme étant l'image de e_3 dans $X := \mathbb{P}^1 - \{0, 1, \infty\}$. En d'autres termes, la donnée de l'image de e dans Q fait de son complément une droite affine, dans laquelle les images $\bar{e}_i$ des e_i vérifient $\bar{e}_3 - \bar{e}_1 = \lambda(E, \alpha)(\bar{e}_2 - \bar{e}_1)$.

Cette construction garde un sens pour une famille de courbes elliptiques $E \to S$, paramétrée par un schéma S sur lequel 2 est inversible, et on sait qu'elle fait de X (sur $\mathrm{Spec}(\mathbb{Z}[\frac{1}{2}])$ un espace grossier de modules pour les (E, α). Ici, α est un isomorphisme de système locaux sur S (pour la topologie étale) entre le système local constant $(\mathbb{Z}/2)^2_S$, et E_2, et $\lambda(E, \alpha)$ est un morphisme de S dans X, i.e. une section s de $\mathcal{O}_S$ sur S, avec s et $s-1$ inversibles.

Le faisceau sur S des automorphismes de $(E, \alpha)/S$ est constant : c'est le faisceau constant $\mathbb{Z}/2$ engendré par l'involution σ. Grâce à ce fait, la courbe X est mieux qu'un espace grossier de modules : deux (E, α) et (E', α') sur S tels que $\lambda(E, \alpha) = \lambda(E', \alpha')$ sont localement isomorphes (pour la topologie étale), donc déduits l'un de l'autre par torsion par le $\mathbb{Z}/2$-torseur $Isom_S((E, \alpha), (E', \alpha'))$.

Dans la suite, nous nous exprimerons comme si E était une courbe sur un corps algébriquement clos de caractéristique $\neq 2$, sauf lorsque la généralisation au cas de familles, nécessaire et laissée au lecteur, présente une subtilité.

1.2 Soit $E_\lambda \subset \mathbb{P}^2$ la courbe cubique plane

(1.2.1) $\quad y^2 z = x(x-z)(x-\lambda z).$

Le point à l'infini $(0, 1, 0)$ est un point d'inflexion. On fait de E_λ une courbe elliptique en le prenant comme élément neutre e. Trois points de E_λ sont alignés si et seulement si leur somme est nulle, i.e. $=$ e.

La courbe E_λ est la complétée, dans $\mathbb{P}^2$, de la courbe affine

$$y^2 = x(x-1)(x-\lambda).$$

En coordonnées affines, l'involution est $(x, y) \mapsto (x, -y)$. Soit α donné par $e_1 = (0, 0)$, $e_2 = (1, 0)$. On a $\lambda(E_\lambda, \alpha) = \lambda$, et pour a inversible, la courbe

tordue de (E,α) par le groupe $\underline{\mathrm{Aut}}(E,\alpha) = \mathbb{Z}/2$—torseur des racines carrées de a est

$$y^2 = a\,x(x-1)(x-\lambda),$$

avec les mêmes e_i.

2. Niveau 4

Gardons les notations du n° 1. Quel que soit le point R de E, soit "$\frac{1}{2}R$" l'ensemble des points P tels que $2P = R$. C'est un espace principal homogène sous E_2, avec x dans E_2 agissant par $P \mapsto x + P$. [Sur une base S, R est une section de E/S, et "$\frac{1}{2}R$" est un E_2-torseur].

Prenons $R = e_2$. Noter que pour P dans "$\frac{1}{2}e_2$", on a $e_2 + P = -P$. Les deux orbites du sous-groupe $\{e, e_1\}$ de E_2 agissant sur "$\frac{1}{2}e_2$" sont donc échangées par l'involution σ.

La structure de niveau 4 qui nous intéresse est celle des choix de α et d'une des deux orbites, notée s, de l'action de $\{e, e_1\}$ sur "$\frac{1}{2}e_2$". Une fois α choisi, le choix de s "élimine l'automorphisme σ de (E,α)" et ne fait rien de plus : quel que soit (E,α) sur S, il existe localement sur S (pour la topologie étale) un (E',α',s) tel que (E,α) soit isomorphe à (E',α'), et (E',α',s) est unique à isomorphisme unique près. Les (E',α',s), définis localement, se recollent donc en (E,α',s) sur S, caractérisé par la propriété que (E',α') est localement isomorphe à (E,α).

En d'autres termes, quel que soit (E,α) sur S, il existe un recouvrement étale (U_i) de S tel que sur chaque U_i, l'image inverse de E_4 soit isomorphe à $(\mathbb{Z}/4)^2_S$. Ceci permet de choisir un s_i pour l'image inverse de (E,α) sur U_i. Sur $U_{ij} = U_i \times_S U_j$, il existe un unique isomorphisme φ_{ij} de (E,α,s_i) avec

(E, α, s_j), égal localement à l'identité ou à σ. Les φ_{ij} sont une donnée de descente, et (E', α', s) est la courbe recollée.

On peut voir (E', α', s) comme un représentant canonique pour les courbes (E_1, α_1) de même invariant λ que (E, α).

Des propriétés de l'espace grossier de modules X expliquées au n°1 résulte que X, muni de l'unique $(E^{\text{un}}, \alpha^{\text{un}}, s^{\text{un}})$ d'invariant la coordonnée λ de X, est un espace fin de modules pour les (E, α, s).

On peut décrire comme suit les structures de niveau 4 de type (α, s) en termes du sous-groupe H de $\mathrm{GL}(2, \mathbb{Z}/4)$ formé des matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + 2 \begin{pmatrix} * & * \\ * & 0 \end{pmatrix}.$$

Une base $\tilde{e}_1$, $\tilde{e}_2$ de E_4 définit la base $e_1 = 2\tilde{e}_1, \quad e_2 = 2\tilde{e}_2$ de E_2, et $s = \{\tilde{e}_2, \tilde{e}_2 + e_1\}$. Deux bases de E_4 donnent le même (α, s) si et seulement si on passe de l'une à l'autre par un élément de H. L'espace de modules des (E, α, s) est donc le quotient de l'espace de modules $X(4)$ des $\left(E, \tilde{\alpha} : (\mathbb{Z}/4)^2 \xrightarrow{\sim} E_4\right)$ par H, et H agit librement sur $X(4)$.

Soit $\Gamma(2)$ le sous-groupe de $\mathrm{GL}(2, \mathbb{Z}/4)$ formé des matrices congrues à 1 mod 2. Il est isomorphe à $(\mathbb{Z}/2)^4$. On pourrait répéter ce qui précède en partant de n'importe quel sous-groupe d'indice 2 de $\Gamma(2)$ ne contenant pas -1. Il existe 8 tels sous-groupes. Six d'entre eux sont les conjugués de H.

3. Lambda

Soit X le schéma $\mathbb{P}^1$-$\{0, 1, \infty\}$ sur $\mathrm{Spec}(\mathbb{Z}[\frac{1}{2}])$. On note λ sa coordonnée naturelle. Soit (E, α) la famille sur X de courbes elliptiques avec structure de niveau 2 définie en 1.2 : équation affine $y^2 = x(x-1)(x-\lambda)$, base des

points d'ordre 2 : $e_1 := (0,0)$, $e_2 := (1,0)$. Le sous-schéma "$\frac{1}{2}e_2$" de E est un E_2-torseur, donc fini étale de degré 4 sur X.

Théorème 3.1 *Le revêtement quadruple "$\frac{1}{2}e_2$" de X est somme disjointe de deux revêtements doubles, échangés par l'involution σ. Chacun est un torseur sous le sous-groupe $\{e, e_1\}$ de E_2 et définit donc une structure (α, s) sur E de type considéré au n°2.*

Chacun de ces revêtements doubles est isomorphe à celui des racines carrées de $1-\lambda$, d'équation $u^2 = 1-\lambda$. Pour l'un d'eux, on peut prendre comme isomorphisme

(3.1.1) $\quad u \mapsto (1+u,\ u+(1-\lambda))$.

Pour prouver 3.1, il s'agit de vérifier que l'image de (3.1.1) est bien dans E, et même dans "$\frac{1}{2}e_2$" et qu'elle est stable par $x \mapsto e_1 + x$, qui correspondra à $u \mapsto -u$. Pour que ce type d'énoncé soit vrai, X étant réduit, il suffit qu'il le devienne après changement de base de X à $\mathrm{Spec}(k)$ avec k algébriquement clos. Notre tâche devient de montrer que pour (E_λ, α) comme en 1.2 sur k algébriquement clos de caractéristique $\neq 2$, et pour $\sqrt{1-\lambda}$ une racine carrée de $1-\lambda$, le point $P = (1+\sqrt{1-\lambda},\ \sqrt{1-\lambda}+(1-\lambda))$ est sur E, vérifie $2P = e_2$, et que $e_1 + P$ est le point $\overline{P}$ obtenu en prenant l'autre racine carrée de $1-\lambda$. En d'autres termes, il faut vérifier que P est sur E, que la tangente à E en P passe par $e_2 = (1,0)$ et que $e_1 = (0,0)$, P et $\sigma\ \overline{P}$ sont alignés.

Les explications de n°2 fournissent le

Corollaire 3.2. *La courbe X est un espace fin de modules pour les courbes elliptiques munies d'une structure de niveau 4 de type (α, s). La famille (E, α, s) universelle est donnée par (E_λ, α) de 1.2, s étant une quelconque des deux composantes de $''\frac{1}{2}E_2''$ (les deux choix possibles donnent des (E, α, s) isomorphes).*

En effet, avec les notations de 1.2, le théorème montre que si (E'_λ, α', s) est attaché à (E_λ, α), (E'_λ, α') est isomorphe à (E_λ, α).

Preuve de 3.1. Pour plus de symétrie, considérons (sur k algébriquement clos) une courbe elliptique d'équation affine

(3.1.2) $\quad y^2 = (x-a)(x-b)(x-c)$

(a, b et c distincts). Comme précédemment, on prend pour élément neutre le point à l'infini, qui est un point d'inflection. Les points d'ordre 2 sont $A := (a, 0)$, $B := (b, 0)$ et $C := (c, 0)$.

Construction 3.3 On indexera les 4 points de "$\frac{1}{2}A$" par les choix de racines carrées de $a-b$ et de $a-c$.

Puisque "$\frac{1}{2}A$" est stable par l'involution σ, ses points (x, y) ne donnent lieu qu'à deux valeurs de x. Cherchons-les. La condition que la tangente à (x, y) passe par A s'écrit:

$$y\frac{d}{dy}(y^2) = (x-a)\frac{d}{dx}\left((x-a)(x-b)(x-c)\right).$$

À gauche, on a $2y^2 = 2(x-a)(x-b)(x-c)$. Éliminant la solution $x = a$ (la tangente par A passe par A), on obtient

(3.3.1) $\quad -(x-b)(x-c) + (x-a)(x-b) + (x-a)(x-c) = 0.$

Pour simplifier les notations, supposons provisoirement que $a = 0$. On peut se réduire à ce cas en observant que la translation $(x, y) \mapsto (x+a, y)$ envoie la courbe (3.1.2) sur la courbe $y^2 = x(x-(b-a))(x-(c-a))$.

Pour $a = 0$, l'équation (3.3.1) se réduit à

(3.3.2) $\quad x^2 = bc.$

Soient $\sqrt{-b}$ et $\sqrt{-c}$ des racines carrées de $-b$ et $-c$, et prenons $x = \sqrt{-b}\sqrt{-c}$. Cherchons les valeurs de y telles que (x, y) soit sur la courbe.

On a

$$y^2 = x(x-b)(x-c) = \sqrt{-b}\sqrt{-c}(\sqrt{-b}\sqrt{-c}+\sqrt{-b}\sqrt{-b})(\sqrt{-b}\sqrt{-c}+\sqrt{-c}\sqrt{-c})$$

$$= \left[\sqrt{-b}\sqrt{-c}(\sqrt{-b}+\sqrt{-c})\right]^2, \text{et}$$

$$P_0(\sqrt{-b},\sqrt{-c}) := \left(\sqrt{-b}\sqrt{-c}, \sqrt{-b}\sqrt{-c}(\sqrt{-b}+\sqrt{-c})\right)$$

est donc dans "$\frac{1}{2}A$". Les points $P_0(\sqrt{-b},\sqrt{-c})$ et $P_0(\sqrt{-b},-\sqrt{-c})$ ne sont pas échangés par σ. Ils sont donc alignés soit avec B, soit avec C. Ils sont alignés avec B. En d'autres termes,

$$B + P_0(\sqrt{-b},\sqrt{-c}) = \sigma P_0(-\sqrt{-b},\sqrt{-c}) = P_0(\sqrt{-b},-\sqrt{-c}).$$

En effet, le déterminant

$$\begin{vmatrix} \sqrt{-b}\sqrt{-c} & \sqrt{-b}\sqrt{-c}(\sqrt{-b}+\sqrt{-c}) & 1 \\ -\sqrt{-b}\sqrt{-c} & -\sqrt{-b}\sqrt{-c}(-\sqrt{-b}+\sqrt{-c}) & 1 \\ b & 0 & 1 \end{vmatrix}$$

est nul, car la somme de la première ligne, multipliée par $(-\sqrt{-b}+\sqrt{-c})$, et de la seconde, multipliée par $(\sqrt{-b}+\sqrt{-c})$, est la troisième ligne, multipliée par $2\sqrt{-c}$.

Les points de "$\frac{1}{2}A$" dans une orbite de $\{e, B\}$ correspondent donc à une même racine carrée de $-b$.

Ne supposons plus que $a = 0$. Par une translation de a sur x, on déduit de ce qui précède que, pour $\sqrt{a-b}$ et $\sqrt{a-c}$ des racines carrées de $a-b$ et $a-c$,

les points

$$P(\sqrt{a-b},\sqrt{a-c}) := \Big(a+\sqrt{a-b}\sqrt{a-c},\ \sqrt{a-b}\sqrt{a-c}(\sqrt{a-b}+\sqrt{a-c})\Big)$$

sont les points de "$\frac{1}{2}A$", et qu'à chaque orbite de $\{e,B\}$ correspond une racine carrée de $a-b$.

Prenons $a=1$, $b=0$, $c=\lambda$. On obtient 3.1 : une orbite de $\{e,e_1\}$ sur "$\frac{1}{2}e_2$" correspond à la racine carrée 1 de 1, l'autre à la racine carrée -1, et les points de l'orbite associée à 1 sont les

$$(1+\sqrt{1-\lambda},\ \sqrt{1-\lambda}(1+\sqrt{1-\lambda})).$$

Remarque 3.4 Si on prend $a=0$, $b=1$, $c=\lambda$, on voit que chaque orbite de $\{e,e_2\}$ sur "$\frac{1}{2}e_1$" correspond à une racine carrée i de -1. Une autre façon de le voir : si $s\subset E_4$ est une orbite de $\{e,e_1\}$ agissant sur "$\frac{1}{2}e_2$", et s' une de $\{e,e_2\}$ agissant sur "$\frac{1}{2}e_1$", l'accouplement de Weil sur E_4, à valeurs dans μ_4, est constant sur $s\times s'$, de valeurs i ou $-i$.

Tordant la courbe $y^2=x(x-1)(x-\lambda)$ par le $\mathbb{Z}/2$-torseur des racines carrées de -1, on obtient la courbe

$$y^2=-x(x-1)(x-\lambda),$$

α donné par les mêmes e_i, et pour celle-ci chaque orbite de $\{e,e_2\}$ sur "$\frac{1}{2}e_1$" correspond à 1 ou -1, de sorte que X, muni de cette courbe, est un espace fin de modules pour les (E,α,s), s une orbite de $\{e,e_2\}$ sur "$\frac{1}{2}e_1$".

Remarque 3.5. De même, si on pose $\overline{e}_1=0$, $\overline{e}_2=1$, $\overline{e}_3=\lambda$, alors

X, muni de la courbe

$$y^2 = (\overline{e}_i - \overline{e}_j)\, x\, (x-1)(x-\lambda),$$

tordue de la courbe (3.1.1) par le $\mathbb{Z}/2$-torseur des racines carrées de $(\overline{e}_i - \overline{e}_j)$, est un espace fin de modules pour les (E, α, s) avec s une orbite de $\{e, e_j\}$ sur "$\frac{1}{2}e_i$".

Ces problèmes de modules correspondent, avec les notations du n°2, à 6 sous-groupes d'indice 2 de $\Gamma(2)$ ne contenant pas -1. Ce sont les conjugués de H.

Les deux sous-groupes restants sont ceux qui contiennent l'intersection de $\Gamma(2)$ et du groupe dérivé de $SL(2, \mathbb{F}_4)$. Ou peut montrer que les espaces de modules correspondants sont X, muni d'une des courbes

$$y^2 = \pm\lambda(\lambda-1)\cdot x(x-1)(x-\lambda).$$