LES SCHÉMAS DE MODULES DE COURBES ELLIPTIQUES

par P. Deligne[1] et M. Rapoport[2]

(1) Research on this paper was partially supported by NSF grant GP 36418X.

(2) Le deuxième auteur pense que les activités politiques de l'OTAN sont incompatibles avec l'activité pacifique du mathématicien et regrette pour cette raison que ce congrès a été partiellement financé par cette organisation.

International Summer School on Modular Functions
Antwerp 1972

SOMMAIRE

Introduction

1. Soit X le demi-plan de Poincaré

$$X = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\} \quad .$$

Le groupe $SL(2, \mathbb{R})$ agit sur X par transformations homographiques

$$z \mapsto \frac{az+b}{cz+d} \quad .$$

Si Γ est un sous-groupe de $SL(2, \mathbb{Z})$ défini par des conditions de congruence, la surface de Riemann X/Γ est le complément d'un ensemble fini de points ("à l'infini") dans une surface de Riemann compacte. C'est donc une courbe algébrique. Ses points sont en correspondance bijective avec les classes d'isomorphie de courbes elliptiques munies d'une "structure de niveau" d'espèce convenable. On sait qu'il résulte de cette interprétation qu'elle admet pour corps de définition un sous-corps d'un corps cyclotomique. Dans cet article, nous étudions la structure à l'infini et la réduction modulo p de X/Γ .

Concentrons-nous sur le cas où Γ est le sous-groupe de $SL(2, \mathbb{Z})$ formé des matrices congrues modulo n à la matrice identité. Supposons que $n \geq 3$, auquel cas Γ agit sur X sans point fixe.

Pour $z \in X$, notons E_z le quotient de $\mathbb{C}$ par le réseau $\mathbb{Z} + \mathbb{Z}z$. La loi d'addition dans $\mathbb{C}$ passe au quotient et munit E_z d'une structure de courbe elliptique (= variété abélienne de dimension un). Les courbes elliptiques E_z et $E_{z'}$ sont isomorphes si et seulement si z et z' sont conjugués sous $SL(2, \mathbb{Z})$. Le noyau $E(z)_n$ de la multiplication par n dans $E(z)$ est l'image de $\frac{1}{n}(\mathbb{Z} + \mathbb{Z}z)$; nous noterons $\alpha(z)$ l'isomorphisme

$$E(z)_n \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^2 \quad : \quad (a+bz)/n \mapsto (a,b) \quad .$$

Pour que les couples $(E(z),\alpha(z))$ et $(E(z'),\alpha(z'))$ soient isomorphes, il faut et il suffit que z et z' soient conjugués sous Γ .

Pour toute courbe elliptique E sur un corps algébriquement clos k de caractéristique p ne divisant par n , le groupe E_n est muni d'une forme alternée non dégénérée e_n à valeurs dans les racines $n^{\text{ièmes}}$ de l'unité de k . Une <u>structure de niveau</u> n sur E est un isomorphisme $\alpha: E_n \xrightarrow{\sim} (\mathbb{Z}/n)^2$.
Si α est une structure de niveau n , nous noterons $\zeta(\alpha)$ la racine primitive $n^{\text{ième}}$ de l'unité

$$\zeta(\alpha) = e_n(\alpha^{-1}((1,0)),\alpha^{-1}((0,1))) \quad .$$

Faisons $k = \mathbb{C}$, et posons $\zeta_n = \exp(\frac{2\pi i}{n})$. Un couple (E,α) est isomorphe à un couple $(E(z),\alpha(z))$ $(z \in X)$ si et seulement si

$$\zeta(\alpha) = \zeta_n$$

(ou ζ_n^{-1} , selon la convention de signe utilisée dans la définition de e_n) .

2. Ce qui précède se généralise aux familles de courbes elliptiques, paramétrées par un schéma S . On trouve que X/Γ représente le foncteur F_n suivant sur les schémas sur $\mathbb{C}$: $F_n(T)$ est l'ensemble des classes d'isomorphie de familles algébriques paramétrées par T de courbes elliptiques E munies d'une structure de niveau n telle que $\zeta(\alpha) = \zeta_n$.

La définition de $F_n(T)$ garde un sens lorsque T est seulement supposé être un schéma sur $\mathbb{Z}[\zeta_n, \frac{1}{n}]$. Igusa a prouvé dans [11] que le foncteur F_n obtenu est représentable par un schéma $M_n^*[1/n]$ sur $\mathbb{Z}[\zeta_n,1/n]$. La méthode d'Igusa est la suivante.

a) Si $M_n^\circ[1/n]$ existe, alors $M_{nm}^\circ[1/nm]$ existe. Si E est une courbe elliptique sur un corps algébriquement clos, la multiplication par m induit un isomorphisme de E_{nm}/nE_{nm} avec E_n ; une structure de niveau nm : $\alpha : E_{nm} \xrightarrow{\sim} (\mathbb{Z}/nm)^2$ définit ainsi par réduction modulo n une structure de niveau n . Ceci se transpose au cas d'un schéma de base quelconque et définit un morphisme de foncteurs $F_{nm} \to F_n$ Ce morphisme est relativement représentable. Il fait de $M_{nm}^\circ[1/nm]$ un revêtement galoisien non ramifié de groupe $\mathrm{Ker}(SL(2, \mathbb{Z}/nm) \to SL(2, \mathbb{Z}/n))$ de $M_n^\circ[1/nm] \otimes_{\mathbb{Z}[\zeta_n]} \mathbb{Z}[\zeta_{nm}]$ ($\otimes$ désigne une extension des scalaires).

b) Si $M_{nm}^\circ[1/nm]$ existe, $M_n^\circ[1/nm]$ existe. On obtient $M_n^\circ[1/nm]$ par un passage au quotient.

c) $M_3^\circ[1/3]$ et $M_4^\circ[1/4]$ existent. Explicitement, on a

$$M_3^\circ[1/3] = \mathrm{Spec}(\mathbb{Z}[\zeta_3, 1/3, \mu, (\mu^3-1)^{-1}]) \quad ,$$

avec pour courbe elliptique universelle la cubique plane d'équation

$$X^3 + Y^3 + Z^3 = 3\mu XYZ \quad .$$

La section neutre est $(1,-1,0)$ et la base du groupe des points d'ordre 3 est $((-1,0,1)\ ,\ (-1,\zeta_3,0))$.

En niveau 4, on a

$$M_4^\circ[1/4] = \mathrm{Spec}(\mathbb{Z}[i, 1/2, \sigma, (\sigma(\sigma^4-1))^{-1}]) \quad ,$$

où on a posé $i = \zeta_4$, avec pour courbe elliptique universelle la cubique plane d'équation non homogène

$$y^2 = x(x-1)(x-\lambda) \quad , \text{ pour}$$

$$\lambda = \frac{1}{4}(\sigma + 1/\sigma)^2 \quad .$$

La section neutre est le point à l'infini, et la base (r,s) du groupe des points

d'ordre 4 est donnée par

$$r = (\frac{1}{2}(\sigma + 1/\sigma) \ , \ \frac{i(\sigma^2+1)(\sigma-1)^2}{4\cdot\sigma^2} \ )$$

$$s = (-\frac{i}{2}(\sigma - 1/\sigma) + 1, \ -\frac{(\sigma^2-1)(\sigma+i)^2}{4\cdot\sigma^2} \ )$$

Les formules ci-dessus pour $M_4^\circ[1/4]$ sont copiées de Shioda [31]. Igusa utilisait non pas $M_4^\circ[1/4]$ mais le schéma de modules des courbes elliptiques munies d'une structure intermédiaire entre une structure de niveau 4 et une de niveau 2.

d) $M_n^\circ[1/n]$ s'obtient en recollant $M_n^\circ[1/3n]$ et $M_n^\circ[1/4n]$.

3. La surface de Riemann X/Γ est non compacte. Géométriquement, ce fait se traduit comme suit : si E_η est une courbe elliptique munie d'une structure de niveau n sur $\mathbb{C}((T))$, il arrive que le modèle minimal de E_η sur $\mathbb{C}[[T]]$ ait mauvaise réduction. Dans ce cas, la fibre spéciale E'_o du modèle de Néron E' de E_η sur $\mathbb{C}[[T]]$ est isomorphe à $\mathbb{C}^* \times \mathbb{Z}/kn$ pour k convenable. Soit E_o le sous-groupe de E'_o réunion des composantes de E'_o dont l'ordre dans $\pi_o(E'_o)$ divise n . Ce sous-groupe est isomorphe à $\mathbb{C}^* \times \mathbb{Z}/n$. Il présente sur E'_o l'avantage suivant: après extension des scalaires de $\mathbb{C}((T))$ à $\mathbb{C}((T^{1/\ell}))$, le nombre de composantes connexes de E'_o est multiplié par ℓ , tandis que E_o ne change pas.

La forme alternée e_n définit par spécialisation une forme alternée, encore notée e_n , sur $(E_o)_n$. La structure α de niveau n définit par spécialisation

$$\alpha_o : (E_o)_n \xrightarrow{\sim} (\mathbb{Z}/n)^2 \ ,$$

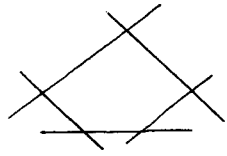
et $\zeta(\alpha_o) = e_n(\alpha^{-1}((1,0)),\alpha^{-1}((0,1))) = \zeta_n$.

Cette discussion suggère que les points à l'infini de X/Γ correspondent

aux classes d'isomorphisme de systèmes (E_o, e_n, α_n) comme ci-dessus. Tel est bien le cas.

Dans le texte, nous précisons cette interprétation modulaire de l'ensemble des points à l'infini de X/Γ en une interprétation modulaire de la courbe projective X/Γ^- compactifiée de X/Γ . En voici le principe.

Pour E_η sur $\mathbb{C}((T))$ comme plus haut, la fibre spéciale $\bar{E}'_o$ du modèle minimal $\bar{E}'_o$ de E_η sur $\mathbb{C}[[T]]$ est un cycle de kn droites projectives :



Soit $\bar{E}$ déduit de $\bar{E}'$ en contractant en un point les composantes irréductibles de $\bar{E}'_o$ dont l'ordre ne divise pas n . La fibre spéciale $\bar{E}_o$ de $\bar{E}$ est un cycle de n droites projectives se coupant transversalement, et est une compactification de E_o (E_o s'identifie au lieu lisse $\bar{E}_o^{reg}$ de $\bar{E}_o$) . Par spécialisation, + et α définissent une loi de groupe sur le lieu lisse $\bar{E}_o^{reg}$ de $\bar{E}_o$, une action de $\bar{E}_o^{reg}$ sur $\bar{E}_o$ et un isomorphisme

$$\alpha_o : (\bar{E}_o^{reg})_n \xrightarrow{\sim} (\mathbb{Z}/n)^2 \quad .$$

Soit T un schéma de type fini sur $\mathbb{C}$. Inspirés par les remarques ci-dessus, nous définissons une <u>courbe elliptique généralisée</u> munie d'une structure α de niveau n , telle que $\zeta(\alpha) = \zeta_n$, sur T comme consistant en :

a) un morphisme propre et plat $p : E \to T$;

b) une structure de schéma en groupes commutatif sur l'ouvert E^{reg} de E où p est lisse; on suppose que l'addition se prolonge en une action

$$+ : E^{reg} \times_T E \to E \quad ;$$

c) un isomorphisme de schémas en groupes $(E^{reg})_n \xrightarrow{\sim} (\mathbb{Z}/n)^2_T$. On suppose que les fibres géométriques de p sont soit des courbes elliptiques munies d'une structure de niveau n telle que $\zeta(\alpha) = \zeta_n$, soit sont isomorphes à l'un des systèmes $(\bar{E}_o, \alpha_o)$ construits ci-dessus.

Nous prouvons que la courbe X/Γ^- représente le foncteur $\bar{F}_n$ suivant sur les schémas de type fini sur $\mathbb{C}$. $\bar{F}_n(T)$ est l'ensemble des classes d'isomorphie de courbes elliptiques généralisées E sur T , munie d'une structure α de niveau n telle que $\zeta(\alpha) = \zeta_n$.

Pour rendre viable la définition des courbes elliptiques généralisées, nous faisons un usage intensif de techniques de Grothendieck (théorèmes de changement de base (EGA III) et de dualité ([10]) en cohomologie des faisceaux cohérents). Ces techniques fournissent un moyen systématique pour ramener des énoncés relatifs, concernant des schémas sur un schéma de base S , au cas où S est le spectre d'un corps algébriquement clos.

Pour prouver que le foncteur $\bar{F}_n$ est représentable, nous utilisons le critère général de M. Artin [3]. La vérification des hypothèses de ce critère présente le point délicat suivant. La donnée b) dans la définition d'une courbe elliptique généralisée est un morphisme de schémas sur T $+ : E^{reg} \times_T E \to E$, dont l'un $(E^{reg} \times_T E)$ n'est pas nécessairement propre sur T . Ceci nous contraint à prouver la prorepresentabilité <u>effective</u> de F_n par une voie détournée, le théorème d'existence de Grothendieck n'étant pas directement applicable.

Les chapitres II, III et le §1 de IV contiennent les outils requis pour surmonter ces difficultés. Ci-dessus, nous avons travaillé sur $\mathbb{C}$. Dans le texte, nous travaillons sur $\mathbb{Z}$ ou $\mathbb{Z}[\zeta_n]$, selon le cas, et obtenons une courbe $M_n[1/n]$, projective et lisse sur $\mathbb{Z}[\zeta_n, \frac{1}{n}]$, solution d'un problème de module, et telle que X/Γ^- s'en déduise par extension des scalaires à $\mathbb{C}$.

4. Parler de la "réduction mod p de X/Γ^-" présuppose le choix d'un modèle M_n de X/Γ^- sur $\mathbb{Z}[\zeta_n]$. La définition de M_n donnée dans le texte équivaut à la suivante : M_n est le normalisé, dans le corps des fonctions de $M_n^\circ[1/n]$, de la droite de j (la droite projective sur $\mathbb{Z}[\zeta_n]$, dans laquelle M_n s'envoye par l'application "invariant modulaire de la courbe elliptique universelle"). Soit encore M_n° la courbe affine d'anneau de coordonnées le normalisé de $\mathbb{Z}[\zeta_n][j]$ dans l'anneau des coordonnées de M_n°. On montre dans le texte que

$$M_n[1/n] = M_n \otimes_{\mathbb{Z}[\zeta_n]} \mathbb{Z}[\zeta_n, 1/n] \quad \text{et}$$

$$M_n^\circ[1/n] = M_n^\circ \otimes_{\mathbb{Z}[\zeta_n]} \mathbb{Z}[\zeta_n, 1/n] \ .$$

Nous prouvons les résultats suivants :

a) La courbe modulaire M_n est projective sur $\mathbb{Z}[\zeta_n]$, et lisse en dehors d'un ensemble fini de points de M_n°, les points supersinguliers de caractéristique divisant n.

b) Il existe une famille finie de points f_i de M_n à valeurs dans $\mathbb{Z}[\zeta_n]$ (= des sections du morphisme de schéma $M_n \to \mathrm{Spec}(\mathbb{Z}[\zeta_n]))$, telles que

b1) les sections f_i sont disjointes (= les points f_i sont incongruents modulo tout idéal premier de $\mathbb{Z}[\zeta_n]$) ;

b2) M_n° est le complément dans M_n de la réunion des "sections à l'infini" f_i.

c) Soit $\underline{\underline{p}}$ un idéal premier de $\mathbb{Z}[\zeta_n]$, divisant le facteur premier p de n. Nous déterminons l'ensemble des composantes irréductibles de la réduction de M_n modulo $\underline{\underline{p}}$. Pour décrire le résultat, nous supposerons que n est le produit de deux entiers ≥ 3 premiers entre eux, n' et n''. Sous cette hypothèse, $M_n[1/n']$ est le normalisé dans $M_n^\circ[1/n]$ du schéma $M_{n'}[1/n']$, dont nous connaissons une interprétation modulaire. Les images réciproques sur $M_n^\circ[1/n']$ et $M_n^\circ[1/n'']$ des

courbes elliptiques universelles sur $M^\circ_{n'}[1/n']$ et $M^\circ_{n''}[1/n'']$ se recollent et fournissent une courbe elliptique universelle E sur M°_n. La structure de niveau $\alpha : E_n \xrightarrow{\sim} (\mathbb{Z}/n)^2$ sur $M^\circ_n[1/n]$ se prolonge en un morphisme de schéma en groupes sur M°_n

$$\alpha^{-1} : (\mathbb{Z}/n)^2 \to E_n \quad .$$

La composante p-primaire de α^{-1} est un morphisme

$$\beta(p) : (\mathbb{Z}/p^k)^2 \to E_{p^k} \quad .$$

Les points supersinguliers de caractéristique p de M_n $(p|n)$ sont ceux en lesquels $\beta(p)$ est nul. Les composantes irréductibles de la réduction de M_n modulo p sont en correspondance biunivoque avec les sous-groupes cycliques d'ordre p^k de $(\mathbb{Z}/p^k)^2$ (les points de $\mathbb{P}^1(\mathbb{Z}/p^k)$) : aux points non supersinguliers de la composante d'indice $A \subset (\mathbb{Z}/p^k)^2$, le noyau de $\beta(p)$ est A. Nous prouvons que ces composantes irréductibles sont unibranches, et que deux quelconques d'entre elles se recoupent en tous les points supersinguliers.

Les composantes irréductibles de la réduction de M_n modulo p avaient été déterminées par Pjateckii-Shapiro (voir son article dans ce volume). Il travaille malheureusement avec $PGL(2)$ plutôt qu'avec $GL(2)$, de sorte que ses résultats sont plus embrouillés que les nôtres.

Sous la même hypothèse sur n que ci-dessus, l'un de nous (P. Deligne) a récemment prouvé que ces composantes irréductibles sont en fait lisses, et que M_n est un schéma régulier.

Pour étudier M_n, la première étape est de recouvrir par des ouverts ayant une interprétation modulaire l'ouvert M^h_n de M_n obtenu en ôtant les points supersinguliers de caractéristique divisant n. On y arrive en étudiant le schéma de modules qui classifie les courbes elliptiques munies d'un isomorphisme

$\alpha : E_n \xrightarrow{\sim} \mu_n \times \mathbb{Z}/n$. Une interprétation modulaire permet

a) de déterminer l'ensemble des points de M_n sur un corps algébriquement clos;

b) de prouver la lissité de M_n^h sur $\mathbb{Z}[\zeta_n]$. Il reste, et c'est le point le plus délicat, à étudier les points supersinguliers.

5. Il est sans doute possible d'étudier la structure à l'infini de M_n par voie rigide-analytique, à l'aide de la théorie de la courbe de Tate, sans donner au préalable de l'infini une description modulaire. Une telle approche risque même d'être la seule praticable dans l'étude à l'infini de schémas de modules de dimension supérieure. Elle nous a souvent servi de guide heuristique (voir ci-dessous). Toutefois, pour être rendue précise, elle requiert des préliminaires rigides-analytiques dont nous avons voulu nous dispenser.

Ceci explique que la courbe de Tate n'apparaisse que dans l'ultime chapitre VII. Nous l'utilisons pour déduire des propriétés à distance finie des M_n et de leur réduction modulo p des résultats sur le développement des formes modulaires en série de Fourier. Nous prouvons notamment les résultats suivants.

- L'algèbre graduée des formes modulaires sur X/Γ dont le développement à toutes les pointes est à coefficients dans $\mathbb{Z}[\zeta_n]$ est une algèbre de type fini sur $\mathbb{Z}[\zeta_n]$.

- Si l'idéal premier $\underline{p}$ de $\mathbb{Z}[\zeta_n]$ ne divise pas n , et qu'en une pointe le développement en série de Fourier d'une forme modulaire φ sur X/Γ est à coefficients dans $\mathbb{Q}[\zeta_n]$ et $\underline{p}$-entier , le développement de φ aux autres pointes a les mêmes propriétés.

On donne aussi des indications fragmentaires sur le cas où $\underline{p}$ divise n .

6. Notre usage heuristique de la courbe de Tate repose sur les principes suivants.

a) A l'aide de la courbe de Tate, on peut deviner ou démontrer ce qui se passe au voisinage de l'infini.

b) En dehors des points supersinguliers, la situation est partout la même, et en particulier la même qu'au voisinage de l'infini.

A ces principes s'ajoute le suivant.

c) Géométriquement, i.e. après extension des scalaires (ou du corps résiduel) à $\overline{\mathbb{F}}_p$, la situation est la même aux divers points supersinguliers de caractéristique p.

La théorie locale (formelle) de M_n au voisinage des points géométriques correspondant à une courbe elliptique E sur $\overline{\mathbb{F}}_p$ est gouvernée par le groupe p-divisible $D_p(E)=\bigcup E_{p^n}$, soit essentiellement par le groupe formel complété de E à l'origine. Ceci résulte du théorème de Serre-Tate selon lequel E et ce groupe p-divisible ont même théorie des déformations. Les principes b) et c) en résultent, car ce groupe p-divisible ne dépend, à isomorphisme près, que du caractère ordinaire ou supersingulier de E.

7. Soient H une algèbre de quaternions indéfinie, de discriminant D, sur $\mathbb{Q}$ et Δ un sous-groupe de congruence du groupe des unités de H. Le groupe Δ est un sous-groupe discret à quotient compact de $SL(2, \mathbb{R})$. La courbe complète X/Δ paramétrise des variétés abéliennes de dimension 2, A munies d'un homomorphisme d'un ordre de H dans $End(A)$ (des "fausses courbes elliptiques", dans la terminologie de Serre). Nos méthodes s'appliquent à l'étude de X/Δ et de sa réduction mod p, pour autant que p soit premier à D.

Les remarques suivantes permettent même de déduire de théorèmes pour M_n des théorèmes sur la structure locale de X/Δ.

d) Soient $\mathcal{O}$ un ordre de H, avec $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq GL(2, \mathbb{Z}_p)$, et e un idempotent non trivial de $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Si A est un schéma abélien de dimension 2 sur un corps algébriquement clos k de caractéristique p, muni de $\mu : \mathcal{O} \to End(A)$, le complété $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ agit sur le groupe p-divisible $D_p(A) = \bigcup A_{p^n}$, et $D_p A) = e.D_p(A) \oplus (1-e)D_p(A)$. Le schéma abélien A, muni de μ, et le groupe p-divisible $eD_p(A)$, ont même théorie des déformations.

e) le groupe p-divisible $eD_p(A)$ est isomorphe à $D_p(E)$ pour E une courbe elliptique soit ordinaire, soit supersingulière.

La réduction modulo p de X/Δ a été étudiée par Morita. Il obtient aussi des résultats dans le cas bien plus difficile où $p \mid D$.

8. Dans la littérature des schémas de modules, le langage des Foundations de Weil est parfois utilisé. Selon qu'on utilise ce langage, ou celui de Grothendieck, on met l'accent sur l'une des deux visions suivantes de ce qu'est un schéma X sur un corps de nombres K.

a) C'est un schéma X, muni d'un morphisme $X \to Spec(K)$. Cette vision est celle qui domine nos notations.

b) C'est un schéma $\overline{X}$ sur la clôture algébrique $\overline{K}$ de K, qui est défini sur K. Cette vision transparaît dans la technique de démonstration qui consiste à ramener un énoncé relatif à un S-schéma X à un énoncé relatif à ses fibres géométriques $X_{\overline{s}}$, obtenue par extension des scalaires de S à un corps algébriquement clos $k(\overline{s})$.

La "restriction des scalaires à la Grothendieck" de K à $\mathbb{Q}$ prend un aspect très différent selon la vision adoptée.

a) Au K-schéma X on associe le $\mathbb{Q}$-schéma défini par X et le morphisme composé $X \to Spec(K) \to Spec(\mathbb{Q})$. On ne le distingue pas de X dans la notation. Un schéma est d'abord un $\mathbb{Q}$-schéma; si c'est un K-schéma, il est muni d'un $\mathbb{Q}$-morphisme $X \to Spec(K)$.

b) Soit I l'ensemble des plongements de K dans $\overline{\mathbb{Q}}$. Pour $\sigma \in I$, posons

$\overline{X}_\sigma = X \otimes_{K,\sigma} \overline{\mathbb{Q}}$. On a $X \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} = \sum_{\sigma \in I} \overline{X}_\sigma$. Le $\mathbb{Q}$-schéma déduit comme en a) d'un K-schéma apparaît comme la somme disjointe des conjugués $\overline{X}_\sigma$ de $\overline{X}$, cette somme étant en outre définie sur $\mathbb{Q}$. Le $\mathbb{Q}$-morphisme $X \to \mathrm{Spec}(K)$ s'interprète comme l'application de cette somme dans l'ensemble d'indices $I = \mathrm{Spec}(K) \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$.

Pour $M_n^\circ[1/n]$, la situation est la suivante : le schéma $M_n^\circ[1/n]$ représente le foncteur des classes d'isomorphie de courbes elliptiques E/T , munies d'un isomorphisme $\alpha : E_n \xrightarrow{\sim} (\mathbb{Z}/n)^2$. Un tel couple (E,α) définit (par la théorie de la forme alternée e_n) une racine primitive $n^{\text{ième}}$ de l'unité $\zeta(\alpha)$ sur T , d'où un morphisme de schémas

$$(E,\alpha) \mapsto \zeta(\alpha) \quad : \quad M_n^\circ[1/n] \to \mathrm{Spec}(\mathbb{Z}[\zeta_n, \tfrac{1}{n}]) \quad .$$

Vu comme $\mathbb{Z}[\zeta_n,\frac{1}{n}]$ - schéma, $M_n^\circ[1/n]$ classifie les $(E,\alpha)/T$, T un $\mathbb{Z}[\zeta_n,\frac{1}{n}]$ - schéma , avec $\zeta(\alpha) = \zeta_n$.

On a

$$M_n^\circ[1/n] \otimes_{\mathbb{Z}[\zeta_n]} \mathbb{C} \simeq X/\Gamma \ ;$$

tandis que, si l'on pose $X^{\pm} = \mathbb{C} - \mathbb{R}$,

$$M_n^\circ[1/n] \otimes_{\mathbb{Z}} \mathbb{C} = X^{\pm} \times GL(2, \mathbb{Z}/n) \ / \ GL(2, \mathbb{Z})$$

est somme de $\varphi(n)$ copies de X/Γ .

9. Une courbe elliptique sur un corps algébriquement clos k a un ou des automorphismes non triviaux. Ceci exclut que le foncteur qui à un schéma T associe l'ensemble des classes d'isomorphie de courbes elliptiques E sur T soit représentable : ce n'est pas même un faisceau. On peut y obvier de deux manières.

a) Systématiquement imposer des structures de niveau additionnelles, qui éliminent ces automorphismes. C'est ce que nous avons fait dans cette introduction.

b) Employer le langage des champs algébriques, pour lequel nous renvoyons à [8] et [17] . C'est ce que nous faisons dans le texte, pour les raisons suivantes.

1. Imposer une structure de niveau additionnelle modifie le comportement à l'infini des objets étudiés (M_{nm} se ramifie sur M_n le long de l'infini) .

2. Les calculs et démonstrations deviennent plus simples lorsqu'on n'a pas à se préoccuper de structures additionnelles importunes.

Au chapitre VI, nous déduisons de nos résultats sur les champs modulaires des résultats sur les schémas grossiers de modules (= coarse modular schemes), habituellement considérés.

10. Nous renvoyons à la table des matières et aux introductions des divers chapitres pour une description plus précise de leur contenu.

Nous remercions N. Katz de l'aide qu'il nous a apportée.

Notations

Le travail est divisé en chapitres; chaque chapitre est divisé en paragraphes. Les références internes à un même chapitre ne mentionnent pas le numéro de ce chapitre.

Nous utiliserons librement les définitions et notations de la théorie des champs algébriques telles qu'elles sont exposées dans [8] §4. Toutefois, contrairement à la terminologie de loc. cit., un morphisme de catégories fibrées en groupoïdes

$$\varphi : \mathcal{M}_1 \to \mathcal{M}_2$$

sera dit <u>représentable</u> si pour chaque morphisme $x : X \to \mathcal{M}_2$ d'un schéma X vers $\mathcal{M}_2$, le produit fibré $\mathcal{M}_1 \times_{\mathcal{M}_2} X$ est un espace algébrique.

Un schéma en groupes G sur un schéma S est parfois appelé un S-groupe. Le sous-schéma en groupes, noyau de la multiplication par n dans G, est noté G_n.

Soit X un S-schéma. Si T est un S-schéma, nous noterons par X_T le produit fibré $X \times_S T$. Si $S = \mathrm{Spec}(A)$ et $T = \mathrm{Spec}(B)$, X_B, ou $X \otimes_A B$ ont la même signification. Pour $n \in \mathbb{N}$, on pose $X[1/n] = X \otimes_{\mathbb{Z}} \mathbb{Z}[1/n]$.

On pose $\zeta_n = \exp(\frac{2\pi i}{n})$.

Pour les principes qui gouvernent nos notations pour les champs modulaires, nous référons au §0 du chapitre III.

I Préliminaires

Ce chapitre rassemble des résultats bien connus dont nous aurons à faire usage. Le lecteur est invité à ne s'y reporter qu'en cas de besoin.

1. Schémas en courbes.

1.0. Dans ce paragraphe, on appelle schéma en courbes sur un schéma S un morphisme propre et plat de présentation finie de dimension relative au plus 1.

1.1. Si C/S est un schéma en courbes sur S, la caractéristique d'Euler-Poincaré $\chi(\mathcal{O}_{C_s})$ des fibres est localement constante (EGA III, 7.9.). On définit le genre arithmétique g de C_s par

$$1 - g_s = \chi(C_s, \mathcal{O}_{C_s}) \quad .$$

Si la caractéristique d'Euler-Poincaré des fibres est constante de valeur $1 - g$, on appelle $C|S$ un schéma en courbes de genre g ou simplement une courbe de genre g sur S.

1.2. Un morphisme $p : X \to S$ est dit de Cohen-Macaulay s'il est plat de présentation finie et que ses fibres (géométriques) sont des schémas de Cohen-Macaulay.

Un schéma en courbes de Cohen-Macaulay sur S est un schéma en courbes $p : C \to S$ qui est de Cohen-Macaulay et dont les fibres géométriques sont purement de dimension un. De même, quand on parlera de courbes lisses, ou réduites, ou intégres, on sous-entendra "purement de dimension un".

Pour $S = \mathrm{Spec}(A)$, on parlera indifféremment de courbes sur S ou de courbes sur A.

2. Dualité en cohomologie des faisceaux cohérents.

2.1. Nous nous proposons de rappeler ce que fournit la théorie de dualité de Grothendieck pour un morphisme $p : X \to S$ lorsque

a) p est de Cohen-Macaulay purement de dimension relative d ; et que

b) S est noethérien.

Dans les applications que nous avons en vue, nous pourrions toujours nous ramener au cas où p est de plus quasi-projectif.

Le complexe dualisant relatif $Rp^! \mathcal{O}_S$ [10] n'a qu'un seul faisceau de cohomologie non nul, celui de degré $-d$; c'est le faisceau des différentielles régulières

$$\omega_{X/S} = \underline{H}^{-d}(Rp^! \mathcal{O}_S) \tag{2.1.1.}$$

([10] V. 9.7.). Ce faisceau est plat sur S . Sa formation commute à tout changement de base $S' \to S$ et à la localisation étale sur X (voir [10] ou [34]).

2.2. Si p est de plus propre, on définit un morphisme "trace"

$$Tr : R^d p_*(\omega_{X/S}) \to \mathcal{O}_S \tag{2.2.1}$$

de formation compatible à tout changement de base. Le théorème de dualité affirme que, pour tout complexe borné de faisceaux cohérents K , la flèche déduite de Tr

$$Rp_* R \underline{\mathrm{Hom}}_{\mathcal{O}_X}(K, \omega_{X/S})[-d] \xrightarrow{\sim} R \underline{\mathrm{Hom}}_{\mathcal{O}_S}(Rp_* K, \mathcal{O}_S) \tag{2.2.2.}$$

est un isomorphisme.

Si K est réduit à un faisceau localement libre F placé en degré 0 et que les faisceaux $R^i p_*(F)$ sont localement libres, (2.2.2.) devient

(2.2.3.) $$R^{d-j}p_*(F^\vee \otimes \omega_{X/S}) \xrightarrow{\sim} R^j p_*(F)^\vee$$

(où le $^\vee$ désigne le dual d'un $\mathcal{O}_X$-module resp. d'un $\mathcal{O}_S$-module).

$\omega_{X/S}$ est un faisceau inversible si et seulement si p est de Gorenstein [10] .

Pour S non nécessairement noethérien, on définit $\omega_{X/S}$ et Tr par passage à la limite; pour K un complexe borné de faisceaux localement libres, (2.2.2) reste valable, et se prouve par passage à la limite.

Pour S le spectre d'un corps k , $\omega_{X/S}$ se notera encore $\omega_{X/k}$, voire simplement ω_X .

2.3. Soient X une courbe réduite sur un corps algébriquement clos k , et $\pi : \widetilde{X} \to X$ la normalisée de X . Le faisceau ω_X s'identifie au sous-faisceau suivant de l'image directe par π du faisceau des différentielles méromorphes sur X . Les sections de ω_X sur U sont les différentielles méromorphes ω sur $\pi^{-1}(U)$ telles que, pour tout $P \in U$ et tout $f \in \mathcal{O}_{X,P}$,

$$\sum_{R \mapsto P} \mathrm{Res}_R(f \cdot \omega) = 0$$

Si X n'a comme singularités que des points doubles ordinaires P_i , et que $\pi^{-1}(P_i) = \{P_i', P_i''\}$, les différentielles régulières sur X s'identifient aux formes différentielles méromorphes ω sur $\widetilde{X}$ régulières en dehors des P_i', P_i'' , ayant au pis un pôle simple en les P_i' et P_i'' et qui vérifient

$$\mathrm{Res}_{P_i'}(\omega) + \mathrm{Res}_{P_i''}(\omega) = 0$$

([27] , Chapitre IV).

3. Rappels sur le foncteur de Picard.

3.1. Soit $p : X \to S$ un morphisme propre plat et de présentation finie. On appelle foncteur de Picard relatif de X au-dessus de S et on note $\mathrm{Pic}_{X/S}$ le faisceau fppf associé au préfaisceau

(3.1.1) $S' \mapsto \mathrm{Pic}(X \times_S S')$ = groupe des classes d'isomorphie de faisceaux inversibles sur

$$X \times_S S' \ .$$

Le morphisme canonique $\mathrm{Pic}(X)/\mathrm{Pic}(S) \to \mathrm{Pic}_{X/S}(S)$ est injectif si $p_*\mathcal{O}_X = \mathcal{O}_S$. Il est bijectif si de plus p possède une section (TDTE V.2.4.).

3.2. On dit que p est <u>cohomologiquement plat en dimension 0</u> (EGA III, 7.), ou simplement <u>cohomologiquement plat</u>, si la formation de $p_*\mathcal{O}_X$ commute à tout changement de base $S' \to S$. Un théorème fondamental de M. Artin affirme que, si p est propre, plat de présentation finie et cohomologiquement plat, alors $\mathrm{Pic}_{X/S}$ est représentable par un espace algébrique localement de présentation finie sur S ([2] Thm. 7.3). Si de plus, $p : X \to S$ est un schéma en courbes, $\mathrm{Pic}_{X/S}$ est lisse sur S.

Si $\mathrm{Pic}_{X/S}$ est représentable par un espace algébrique, on note $\mathrm{Pic}^0_{X/S}$ le sous-foncteur en groupes de $\mathrm{Pic}_{X/S}$ composante neutre de $\mathrm{Pic}_{X/S}$. Si $p : X \to S$ est un schéma en courbes, il est représentable par un espace algébrique.

3.3. Soit C un courbe propre sur un corps k. Si $\mathcal{L}$ est un faisceau inversible sur C, on définit son <u>degré</u> $\deg_C(\mathcal{L})$ par la formule (de Riemann-Roch) :

(3.3.1) $$\chi(\mathcal{L}) = \deg_C(\mathcal{L}) + \chi(\mathcal{O}_C)$$

On a alors (cf. [15])

(3.3.2) $$\deg_C(\mathcal{L}_1 \otimes \mathcal{L}_2) = \deg_C(\mathcal{L}_1) + \deg_C(\mathcal{L}_1)$$

(3.3.3) Si C a pour composantes irréductibles réduites les sous-schémas D_i, et si D_i est de multiplicité (= longueur de l'anneau local de C au point maximal de D_i) n_i, alors

$$\deg_C(\mathcal{L}) = \Sigma\, n_i \deg_{D_i}(\mathcal{L}) \quad , \text{ où on a posé}$$

(3.3.4) $$\deg_{D_i}(\mathcal{L}) = \deg_{D_i}(\mathcal{L} \otimes \mathcal{O}_{D_i}) \quad .$$

3.4. Soit $p : C \to S$ une courbe sur S et $\mathcal{L}$ un faisceau inversible sur C. Le degré de $\mathcal{L}$ sur les fibres C_s ($s \in S$) de C est localement constant et définit un morphisme de faisceaux abéliens (pour la topologie fppf) :

(3.4.1) $$\deg : \mathrm{Pic}_{C/S} \to \mathbb{Z} \quad .$$

On désigne par $\mathrm{Pic}^{[o]}_{C/S}$ le noyau de (3.4.1). (Voir 3.7. pour la relation entre Pic^o et $\mathrm{Pic}^{[o]}$ dans un cas spécial).

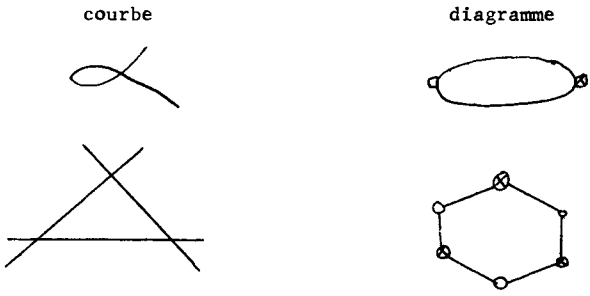
3.5. Soit C une courbe réduite sur un corps algébriquement clos k. Le <u>diagramme des composantes irréductibles de</u> C est le graphe non orienté $\Gamma(C)$ suivant, dans lequel on distingue deux espèces de sommets.

(3.5.1) L'ensemble $\Gamma^o = {}'\Gamma^o \amalg {}''\Gamma^o$ des sommets de $\Gamma(C)$ est somme de l'ensemble ${}'\Gamma^o$ des composantes irréductibles de C et de l'ensemble ${}''\Gamma^o$ des points singuliers de C.

(3.5.2) Pour $p \in C(k)$, appelons <u>branches</u> de C en p les points de la normalisée $\tilde{C}$ de C d'image p. L'ensemble Γ^1 des arrêtes de $\Gamma(C)$ est l'ensemble des couples (p,b) formés d'un point singulier p et d'une branche b de C en p.

(3.5 3) Une arrête (p,b) joint $p \in {}''\Gamma^o$ à celle des composantes irréductibles de C, identifiée à une composante irréductible de $\tilde{C}$, qui contient b.

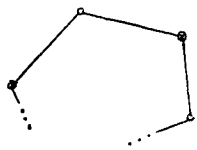
Exemples 3.5.4. Notons o les points de $'\Gamma^o$ et $\otimes$ ceux de $''\Gamma^o$. Les courbes suivantes ont les diagrammes suivants :



Si C est purement de dimension un, non nécessairement réduite, on pose $\Gamma(C) = \Gamma(C_{red})$.

3.6. On note $Aut(\Gamma(C))$ le groupe des automorphismes du graphe $\Gamma(C)$ qui transforment $'\Gamma^o(C)$ en $'\Gamma^o(C)$ et $''\Gamma^o(C)$ en $''\Gamma^o(C)$.

Dans le cas où $\Gamma(C)$ est un cycle à $2n$ sommets et $2n$ arrêtes :



nous dirons qu'un élément de $Aut(\Gamma(C))$ est une rotation, ou qu'il préserve l'orientation de $\Gamma(C)$ s'il induit l'identité sur le premier groupe de cohomologie entière $H^1(\Gamma(C), \mathbb{Z})$. Le sous-groupe distingué $Aut^+(\Gamma(C))$ de $Aut(\Gamma(C))$ formé des rotations est cyclique d'ordre n et $Aut(\Gamma(C))$ est le groupe dihédral produit semi-direct d'une "réflexion" par $Aut^+(\Gamma(C)) \simeq \mathbb{Z}/n\mathbb{Z}$.

3.7. Soient k un corps algébriquement clos, et C une courbe propre et réduite sur k , dont les singularités sont formellement isomorphes à celle de la réunion des axes de coordonnées dans un espace affine A^n .

Le schéma de Picard $\mathrm{Pic}_{C/k}$ se dévisse comme suit. Soient $(D_i)_{i\in I}$ les composantes irréductibles de C, $\widetilde{D}_i$ la normalisée de D_i et $\widetilde{C} = \coprod \widetilde{D}_i$ la normalisée de C.

a) Le morphisme "degré total" :

$$\deg_I = (\deg_{D_i})_{i\in I} : \mathrm{Pic}_{C/k} \to \mathbb{Z}^I$$

et surjectif, de noyau $\mathrm{Pic}^o_{C/k}$.

b) Le morphisme

$$\mathrm{Pic}^o_{C/k} \to \mathrm{Pic}^o_{\widetilde{C}/k} = \overline{\prod} \mathrm{Pic}_{\widetilde{D}_i/k}$$

est surjectif, d'image le plus grand quotient de $\mathrm{Pic}^o_{C/k}$ qui soit un schéma abélien. Son noyau est un tore, canoniquement isomorphe à

$$H^1(\Gamma(C), \mathbb{Z}) \otimes \mathbb{G}_m .$$

Pour D propre et purement de dimension un sur k, il existe une et une seule courbe C comme plus haut, munie d'un morphisme radiciel $C \to D$; l'application

$$\mathrm{Pic}_{D/k} \to \mathrm{Pic}_{C/k}$$

est surjective de noyau unipotent connexe.

4. Sous-schéma de non-lissité.

Soit $f : X \to S$ un morphisme plat de présentation finie purement de dimension relative d.

Il résulte du critère jacobien de lissité que le sous-schéma X^{sing} de X défini par l'idéal jacobien, i.e. par le d-ième idéal déterminantiel de $\Omega^1_{X/S}$

(Bourbaki; Alg. Comm. Chap. 7, §4, ex. 10) a pour espace topologique sous-jacent l'ensemble des points de X où f est non-lisse. Nous l'appelerons le sous-schéma de non-lissité de X [SGA 7, VI]. Le lien où f est lisse est noté X^{reg}

5. Rappels sur la théorie des déformations.

5.1. Soit Λ un anneau local noethérien complet de corps résiduel k. Deux cas particulièrement utiles sont les suivants.

a) $\Lambda = k$.

b) k est parfait de caractéristique $p > 0$ et Λ est l'anneau des vecteurs de Witt $W(k)$ (l'unique anneau de valuation discrète complet de corps résiduel k et d'idéal maximal (p)) .

On désigne par C_Λ la catégorie des Λ - algèbres locales artiniennes de corps résiduel k et par $\hat{C}_\Lambda$ la catégorie des Λ-algèbres noethériennes locales complètes de corps résiduel k. Un foncteur covariant F de C_Λ vers (Ens) est dit pro-représentable s'il existe $R \in \mathrm{Ob}\, \hat{C}_\Lambda$ et un isomorphisme de foncteurs sur C_Λ .

(5.1.1) $$\hat{\xi} : \mathrm{Hom}(R,A) \xrightarrow{\sim} F(A) \quad .$$

L'algèbre R est alors uniquement déterminée.

Un foncteur covariant F de $\hat{C}_\Lambda$ dans (Ens) induit par restriction un foncteur $F|C_\Lambda : C_\Lambda \to (\mathrm{Ens})$. Si $F|C_\Lambda$ est proreprésentable, on dit qu'il est effectivement proreprésentable s'il existe $\xi \in F(R)$ (R comme ci-dessus) qui définisse (5.1.1) .

5.2. Considérons les systèmes (M,B,α) du type suivant

a) M est une Λ-algèbre locale noethérienne complète de corps résiduel k ;

b) B est une M-algèbre locale noethérienne complète plate, de corps résiduel k, munie d'un isomorphisme

$$\alpha : B \otimes_M k \simeq k[[X,Y]] / (XY) \quad .$$

Un tel système $(\Lambda[[t]], A, \alpha_o)$ est fourni par la $\Lambda[[t]]$ - algèbre

$$A = \Lambda[[t,X,Y]] / (XY-t) \quad .$$

On démontre dans [8] §1 que ce dernier système est versel. Pour tout (B,M,α), il existe un homomorphisme $\Lambda[[t]] \to M$ tel que (B,α) se déduise de (A,α_o) par extension des scalaires : $B = A \otimes_{\Lambda[[t]]} M$.

On en déduit facilement l'énoncé suivant :

Proposition 5.3. Soit $p : C \to S$ un schéma en courbes sur un schéma noethérien S. Soient $s \in S$, et $x \in C_s(s)$. On suppose que C_s présente en x un point double ordinaire à tangentes rationnelles. Alors, le complété $\hat{C}_x$ de C en x est $\hat{S}_s$-isomorphe à $\hat{S}_s[[X,Y]] / (XY-t)$ pour un $t \in \Gamma(\hat{S}_s, \mathcal{O})$ convenable.

On a mieux :

Théorème 5.3. Soient $p : C \to S$ un schéma en courbes, $s \in S$ et $x \in C_s(s)$ tel que C_s présente en x un point double ordinaire. Alors, localement pour la topologie étale (au voisinage de x et s), C est S-isomorphe à

$$X = S[u,v] / (uv-t) \subset \mathbb{A}^2_S$$

pour t convenable. Si les tangentes de C_s en x sont rationnelles sur $k(s)$, l'hensélisé $C^h_{(x)}$ de C en x est $S^h_{(s)}$-isomorphe à l'hensélisé de X en le

point (0,0) d'image s , pour $t \in \Gamma(S^h_{(s)}, \mathcal{O})$ convenable .

Ce théorème résulte aussitôt du cas particulier où S est supposé de type fini sur $\mathbb{Z}$. Il résulte de 5.2 et de la théorie de R. Elkik de l'algébrisation des modules des singularités isolées.

6. Points de division des courbes elliptiques.

Soit E une courbe elliptique (variété abélienne de dimension un) sur un corps algébriquement clos k .

Pour tout entier $n \geq 1$, on sait que le schéma en groupes E_n , noyau de la multiplication par n , est le spectre d'une algèbre de Hopf de dimension n^2 sur k Si n est inversible dans k , on a $E_n \simeq (\mathbb{Z}/n)^2$.

Si k est de caractéristique $p > 0$, le noyau du morphisme de Frobenius $F : E \to E^{(p)}$ est de rang p . Il est isomorphe à μ_p ou à α_p . S'il est isomorphe à μ_p , on dit que E est ordinaire, et $E_n \simeq \mathbb{Z}/n \times \mu_n$. Sinon, on dit que E est supersingulière.

Dans la suite exacte

$$0 \to \mathrm{Ker}(F) \to E_p \to E_p/\mathrm{Ker}(F) \to 0 \ ,$$

les deux termes extrêmes sont en dualité de Cartier. Si E est supersingulière, E_p est donc isomorphe à α_{p^2} , l'unique extension non triviale annulée par p de α_p par α_p .

Les courbes elliptiques supersingulières sur k sont toutes isogènes, et forment un nombre fini de classes d'isomorphie (cf. [32]) .

7. Rappels d'algèbre commutative.

Nous utiliserons souvent les résultats suivants d'algèbre commutative, pour la démonstration desquels nous renvoyons aux EGA.

(7.1) Soit $f : X \to Y$ un morphisme de type fini de schémas noethériens. Si Y est de Cohen-Macaulay et f plat, alors X est de Cohen-Macaulay si et seulement si les fibres de f le sont. Par exemple, si Y est de Cohen-Macaulay et f quasi-fini et plat, X est de Cohen-Macaulay.

Si Y est régulier, X de Cohen-Macaulay et que, au point $x \in X$ d'image $y \in Y$, on a

(7.1 1) $$\dim(\mathcal{O}_{X,x}) = \dim(\mathcal{O}_{Y,y}) + \dim(\mathcal{O}_{X,x} \otimes_{\mathcal{O}_{Y,y}} k(y)) ,$$

alors f est plat en x. La condition (7.1.1) est vérifiée si f est quasi-fini dominant et X irréductible.

EGA IV 6.3.5 et EGA IV 6.1.5.

(7.2) Soit Y noethérien de dimension deux. Pour que Y soit normal, il faut et il suffit que Y soit de Cohen-Macaulay, et régulier sauf en des points de codimension deux.

EGA IV. 5.8.6. (Critère de normalité de Serre).

(7.3) Soit Y noethérien de dimension un et génériquement réduit. Pour que Y soit réduit, il faut et il suffit que Y soit de Cohen-Macaulay.

EGA IV. 5.8.5.

(7.4) Soit $f : X \to Y$ un morphisme de S-schémas plats de présentation finie. Pour que f vérifie l'une des conditions suivantes : être plat, lisse, étale, une immer-

sion ouverte, un isomorphisme, plat d'intersection complète relative, il faut et il suffit que pour tout point géométrique $\overline{s}$ de S, $f_{\overline{s}} : X_{\overline{s}} \to Y_{\overline{s}}$ vérifie la dite condition.

Pour "plat", c'est EGA IV 11.3.10. Les propriétés "lisse", "étale", "plat d'intersection complète relative" équivalent à "plat" + une propriété des fibres. Enfin, "immersion ouverte" équivaut à "étale et radiciel" (EGA IV.17.9.1), (où "radiciel" est une propriété des fibres), et "isomorphisme" équivaut à "immersion ouverte et surjectif".

8. Schémas grossiers de modules

Soit $\mathfrak{M}$ un champ algébrique sur un schéma de base S.

Définition 8.1. Un espace grossier de $\mathfrak{M}$ est un espace algébrique M sur S, muni d'un S-morphisme $\pi : \mathfrak{M} \to M$ ayant les propriétés suivantes :

(i) Tout S-morphisme de $\mathfrak{M}$ vers un espace algébrique X sur S se factorise de façon unique par π.

(ii) Si $\overline{s} : \mathrm{Spec}(k) \to S$ est un point géométrique de S (k algébriquement clos), π induit une bijection de l'ensemble de classes d'isomorphie d'objets de $\mathfrak{M}$ sur $\overline{s}$ (= S-morphisme de s dans $\mathfrak{M}$) avec $M(\overline{s})$

8.2. Si S est noethérien et $\mathfrak{M}$ séparé de type fini sur S, on peut montrer que $\mathfrak{M}$ admet un espace grossier M. Voici quelques-unes de ses propriétés.

(8.2.1) Soient $m : \mathrm{Spec}(k) \to \mathfrak{M}$ un point géométrique de $\mathfrak{M}$, $\mathcal{O}^{h}_{\mathfrak{M},m}$ l'henselisé strict de $\mathfrak{M}$ en m, $\mathcal{O}^{h}_{M,\pi(m)}$ l'henselisé strict de M en $\pi(m)$ et $\mathrm{Aut}(m)$ le groupe des automorphismes de l'objet m de $\mathfrak{M}$ sur $\mathrm{Spec}(k)$. L'application π induit un isomorphisme

$$\mathrm{Spec}(\mathcal{O}^h_{\mathfrak{M},m}) \,/\, \mathrm{Aut}(m) \xrightarrow{\sim} \mathrm{Spec}(\mathcal{O}^h_{M,\pi(m)}) \quad .$$

Soit $H \subset \mathrm{Aut}(m)$ le sous-groupe des automorphismes de l'objet m de $\mathfrak{M}$ sur k qui se prolongent en un automorphisme de l'objet $\mathrm{Spec}(\mathcal{O}^h_{\mathfrak{M},m}) \to \mathfrak{M}$ de $\mathfrak{M}$ sur $\mathrm{Spec}(\mathcal{O}^h_{\mathfrak{M},m})$. Le groupe $\mathrm{Aut}(m)/H$ agit effectivement sur $\mathcal{O}^h_{\mathfrak{M},m}$.

(8.2.2) Si $u : X \to \mathfrak{M}$ est étale surjectif, M est le quotient de X par la relation d'équivalence $X \times_{\mathfrak{M}} X$. En particulier, pour $\mathfrak{M} = [X/G]$ (voir [8] § 4), on a $M = X/G$.

(8.2.3) Pas plus que le passage au quotient, la formation du schéma grossier ne commute en général pas aux changements de base. Toutefois, il commute aux changements de base plat, et à tout changement de base lorsque π est étale. De plus, si M' est le schéma grossier de $\mathfrak{M} \otimes_S S'$, l'application

$$M' \to M \otimes_S S'$$

est radicielle

II Courbes elliptiques généralisées.

Dans ce chapitre, nous définissons les courbes elliptiques généralisées sur un schéma de base quelconque, et prouvons les théorèmes qui rendent viable la définition adoptée.

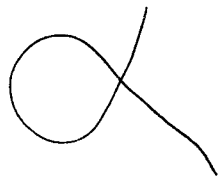
1. Polygones de Néron.

1.1 Soit $\tilde{C} = \mathbb{P}^1 \times \mathbb{Z}/n$ la somme disjointe de n copies de $\mathbb{P}^1$, indexées par $\mathbb{Z}/n$ ($n \geq 1$). En recollant la i-ième copie de $\mathbb{P}^1$ avec la $(i+1)$-ième, par identification de la section 0 de la i-ième copie avec la section ∞ de la $(i+1)$-ième, on obtient une courbe de genre un C sur $\mathrm{Spec}(\mathbb{Z})$, de normalisée $\tilde{C}$.

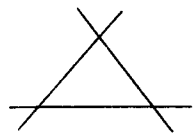
Pour tout schéma S, on appelle polygone de Néron à n côtés standard sur S, ou simplement n-gone standard sur S, le schéma sur S qui s'en déduit par extension des scalaires. Un polygone de Néron (resp. un n-gone) sur un corps algébriquement clos k est un schéma sur k isomorphe à l'un des polygones standards (resp. au n-gone standard).

Exemples.

$n = 1$



$n = 3$



Lemme 1.2. Soit C un polygone de Néron sur un corps algébriquement clos k.

(i) $H^0(C,\mathcal{O}_C) = k$.

(ii) $H^0(C,\omega_C)$ est de dimension 1 sur k et le morphisme canonique

$$H^0(C,\omega_C) \otimes_k \mathcal{O}_C \to \omega_C$$

est un isomorphisme. En particulier $\omega_C \simeq \mathcal{O}_C$.

Preuve : (i) résulte de ce que C est réduit et connexe.

(ii) On peut supposer que C est le n-gone standard.

Soit η la forme différentielle sur le normalisé $\tilde{C} = \mathbb{P}^1 \times \mathbb{Z}/n$ dont la restriction à la i-ième copie de $\mathbb{P}^1$ est $\frac{dx}{x}$. Il est clair que η a des pôles simples au plus, et des résidues $+1$ resp. -1 au "0" resp. "∞" de la i-ième copie de $\mathbb{P}^1$. La forme η définit donc une section globale de $\omega_{C/s}$ (cf. I. 2.3.). Elle engendre ω_C en chaque point de C.

Lemme 1.3. Soit C une courbe réduite, connexe de genre un sur un corps algébriquement clos, ayant comme seules singularités de points doubles ordinaires et telle que $\omega_C \simeq \mathcal{O}$. Alors C est lisse ou un polygone de Néron.

Preuve : Soient $\pi : \tilde{C} \to C$ la normalisée de C, de composantes irréductibles $(C_i)_{1 \le i \le a}$, $g_i \ge 0$ le genre de C_i et b le nombre de points doubles de C. La suite exacte longue de cohomologie déduite de

$$0 \to \mathcal{O}_C \to \pi_* \mathcal{O}_{\tilde{C}} \to \text{conoyau} \to 0$$

et 1.2 (i) fournissent

$$a = \Sigma\, g_i + b \qquad \text{et}$$

$$b \ge a - 1 \ge 0 \quad .$$

Soit $b_i \ge 0$ le nombre de points de C_i d'image un point singulier de C.
On a

$$2\, b = \sum_1^a b_i \quad .$$

L'existence de ω non nul sur chaque composante fournit

$$g_i = 0 \Rightarrow b_i \ge 2 \quad .$$

La connexité fournit

$$a > 0 \Rightarrow b_i \ge 1 \quad .$$

Ces inéquations ont pour solutions

a) $a = 1$, $b = 0$, $g = 1$ (cas non singulier)

b) $a = n$, $b = n$, $g_i = 0$, $b_i = 2$ $(n \geq 1)$: les C_i sont $\simeq \mathbb{P}^1$,

et sur chaque C_i deux points ont pour image un point double de C . La courbe C , étant connexe, est un polygone de Néron.

Définition 1.4. Une courbe stable de genre un C sur un schéma S (ou espace algébrique S , ou champ algébrique S) est un schéma en courbes sur S (cf. I.1.0.) dont toute fibre géométrique est soit une courbe propre lisse et connexe de genre un soit un polygone de Néron.

Proposition 1.5. : Soit $p : C \to S$ un morphisme propre et plat de présentation finie. L'ensemble des points $s \in S$ tel que C_s soit une courbe stable de genre un est un sous-schéma ouvert dans S .

Preuve : Les conditions $C_{\bar{s}}$ réduit, réduit et connexe, réduit et purement de dimension un, de genre un, n'ayant pour singularités que des points quadratiques ordinaires, sont toutes ouvertes. Que la condition $\omega \simeq \mathcal{O}$ de 1.3 soit ouverte résulte de la démonstration de 1.6 ci-dessous.

Proposition 1.6. Soit $p : C \to S$ une courbe stable de genre un.

(i) $p_* \mathcal{O}_C = \mathcal{O}_S$ universellement .

(ii) $\omega_{C|S}$ et $p_*(\omega_{C|S})$ sont inversibles et l'application canonique

$$p^* p_*(\omega_{C|S}) \to \omega_{C|S} \tag{1.6.1}$$

est un isomorphisme.

Preuve. On se ramène aussitôt au cas où S est noethérien. Puisque les fibres géométriques de p sont connexes et réduites, (i) résulte de EGA III. 7.8.8. Puisque les fibres géométriques de p sont des intersections complètes locales, p est d'intersection complète locale relative et $\omega_{C|S}$ est inversible. De (i) et de

ce que $R^2p_*\mathcal{G} = 0$, on tire que $R^1p_*\mathcal{G}$ est localement libre de formation compatible à tout changement de base $S' \to S$ (EGA III. 7.8.) . Il résulte alors de la dualité des faisceaux cohérents (I.2.) que $p_*(\omega_{C/S})$ est localement libre de formation compatible avec tout changement de base. Comme $(\omega_{C/S})_s = \omega_{C_s/s}$, on est réduit à démontrer (ii) dans le cas où S est le spectre d'un corps algébriquement clos. Dans ce cas, 1.6.1 est bien connu pour C lisse et résulte de 1.2 pour un polygone de Néron.

Le lemme 1.7 suivant est un cas particulier de I 3.7.

Lemme 1.7. Soit C un polygone de Néron sur un corps algébriquement clos k .

(i) $\mathrm{Pic}^\circ(C) = \mathbb{G}_m \otimes H^1(\Gamma(C), \mathbb{Z})$ est isomorphe à $\mathbb{G}_m$.

(ii) Un automorphisme g de C induit l'identité sur $\mathrm{Pic}^\circ(C)$ si et seulement si g agit par rotations sur le diagramme $\Gamma(C)$ des composantes irréductibles de C .

Lemme 1.8. Soit $\widetilde{C}$ le n-gone standard sur $\mathbb{Z}$. On a une suite exacte de groupes algébriques

$$0 \to \mathbb{G}_m^n \xrightarrow{a} \underline{\mathrm{Aut}}(C) \xrightarrow{b} \underline{\mathrm{Aut}}(\Gamma(C)) \to 0$$

Soit $\widetilde{C} = \mathbb{P}^1 \times \mathbb{Z}/n$; C est défini par recollement à partir de $\widetilde{C}$, d'où $\pi : \widetilde{C} \to C$. Un calcul local montre que $\widetilde{C}$ se déduit de C en éclatant le sous-schéma de non lissité C^{sing} , et ceci reste vrai après tout changement de base. La réunion des sections marquées "0" et "∞" des composantes de $\widetilde{C}$ est l'image réciproque du sous-schéma de non lissité. Dès lors, après tout changement de base, tout automorphisme de C induit un automorphisme de $\widetilde{C}$ qui respecte la réunion des sections marquées. Ceci permet de définir b et montre que $\mathrm{Ker}(b)$ s'identifie au sous-groupe $\mathbb{G}_m^n$ de $\mathrm{Aut}(C)$ formé des automorphismes transformant chaque composante $\mathbb{P}^1 \times \{i\}$ en elle-même, et respectant les sections $(0,i)$ (∞,i) . Après tout changement de base, une section $\lambda = (\lambda_i)$ de $\mathbb{G}_m^n$ agit sur $\mathbb{P}^1 \times \{i\}$ comme l'homothétie de rapport λ_i .

Il reste à prouver que b est surjectif; nous le ferons en exhibant des automorphismes de C , compatibles à la donnée de recollement, et définissant des

des automorphismes de C dont l'image par b engendre le groupe dihédral $\mathrm{Aut}(\Gamma(C))$. Ce sont

$$\tau : (x,i) \longmapsto (x^{-1},-i)$$

$$\sigma_j : (x,i) \longmapsto (x,i+j) \qquad (j \in \mathbb{Z}/n) \ .$$

1.9. Soit C le n-gone standard sur $\mathrm{Spec}(\mathbb{Z})$. Identifions le normalisé $\tilde{C}$ de C avec $\mathbb{P}^1 \times \mathbb{Z}/n\mathbb{Z}$ et l'image réciproque de C^{reg} dans $\tilde{C}$ avec $\mathbb{G}_m \times \mathbb{Z}/n\mathbb{Z}$. On obtient une action de $\mathbb{G}_m \times \mathbb{Z}/n\mathbb{Z}$ sur $\tilde{C} = \mathbb{P}^1 \times \mathbb{Z}/n\mathbb{Z}$ en posant

$$(a,i) + (b,j) = (a\cdot b, i+j)$$

où $a\cdot b$ dénote l'action naturelle de $\mathbb{G}_m$ sur $\mathbb{P}^1$.

Cette action passe au quotient et définit un morphisme

(1.9.1) $$+ : C^{reg} \times C \to C \ .$$

La restriction de $+$ à $C^{reg} \times C^{reg}$ définit une structure de schéma en groupes commutatifs sur C^{reg}, et $+$ est une action du groupe C^{reg} sur C.

On définit comme suit des automorphismes de $(C,+)$:

a) l'automorphisme de $\tilde{C} = \mathbb{P}^1 \times \mathbb{Z}/n$ $\quad \tau : (x,i) \longmapsto (x^{-1},-1)$ passe au quotient et définit un automorphisme τ de $(C,+)$;

b) pour tout schéma S et tout $\zeta \in \mu_n(S)$, l'automorphisme $u(\zeta)$ de C_S $u(\zeta) : (x,i) \longmapsto (x.\zeta^i,i)$ passe au quotient et définit un automorphisme de $(C_S,+)$.

De a) et b) on déduit une action sur C du schéma en groupe produit semi-direct du groupe à deux éléments $\{e,\tau\}$ par μ_n.

Proposition 1.10. Soit C le n-gone standard sur $\mathrm{Spec}(\mathbb{Z})$. La construction précédente identifie le foncteur $\mathrm{Aut}(C,+)$ des automorphismes de C compatibles à $+$ avec le produit semi-direct $\{e,\tau\} \times\cdot \mu_n$. Le sous-groupe $\mathrm{Aut}^+(C,+)$ des automorphismes agissant trivialement sur $\mathrm{Pic}^o_{C/\mathbb{Z}}$ s'identifie au sous-groupe μ_n.

On a $\mathrm{Pic}^o_{C/\mathbb{Z}} \xrightarrow{\sim} \mathbb{G}_m$, et τ agit sur Pic^o par l'automorphisme $x \mapsto x^{-1}$

de $\mathbb{G}_m$. Puisque $\mathrm{Aut}(\mathbb{G}_m) \simeq \mathbb{Z}/2$, le diagramme

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mu_n & \longrightarrow & \{e,\tau\}\times\mu_n & \longrightarrow & \{e,\tau\} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \underline{\mathrm{Aut}}^+(C,+) & \longrightarrow & \underline{\mathrm{Aut}}(C,+) & \longrightarrow & \underline{\mathrm{Aut}}(\mathbb{G}_m) & & \end{array}$$

montre qu'il suffit de vérifier que $\mu_n \xrightarrow{\sim} \underline{\mathrm{Aut}}^+(C,+)$.

Soit $g \in \mathrm{Aut}^+(C,+)(S)$. On déduit de 1.8 et 1.7 (ii) qu'il existe $\lambda = (\lambda_i) \in \mathbb{G}_m^n$ tel que g soit $a(\lambda)$ (notation de 1.8). Que g commute à $+$ signifie alors que $\lambda_i\lambda_j = \lambda_{i+j}$: λ définit un homomorphisme de $\mathbb{Z}/n$ dans $\mathbb{G}_m$, et g est défini par une section de μ_n .

1.11. Soient k un corps algébriquement clos, et $(C,+)$ déduit de la courbe 1.10 par extension des scalaires de $\mathbb{Z}$ à k . On vérifie que, pour $x \in C^{reg}(k)$, la translation $y \mapsto x + y$ agit par rotations sur le diagramme des composantes irréductibles $\Gamma(C)$.

Définition 1.12. Une courbe elliptique généralisée (sur une base S) est une courbe stable de genre un

$$p : C \to S ,$$

munie d'un morphisme

$$(1\ 12.1) \qquad + : C^{reg} \times_S C \to C$$

tel que

a) La restriction de (1.1 .1) à C^{reg} fait de C^{reg} un schéma en groupes commutatif.

b) (1.12.1) définit une action du schéma en groupes C^{reg} sur C .

c) Pour tout point géométrique $\bar{s}$ de S tel que $C_{\bar{s}}$ soit singulier, les translations $y \mapsto x+y$ de $C_{\bar{s}}$ $(x \in C_s^{reg}(\bar{s}))$ agissent par rotations sur $\Gamma(C_s)$.

Bien entendu, une courbe elliptique généralisée lisse n'est d'autre qu'une courbe elliptique au sens usuel.

Proposition 1.13. Soit $(C,+)$ vérifiant 1.12 a) et b) . L'ensemble U des $s \in S$ tels que C_s/s vérifie c) est ouvert et fermé dans S . Au-dessus de U, C^{reg} agit trivialement sur $\mathrm{Pic}^0_{C/S}$.

Preuve : Soit x un point géométrique de $C_{\bar{s}}$. La translation $y \mapsto x+y$ agit par translation si et seulement si elle agit trivialement sur $\mathrm{Pic}^0_{C_s}$. Appliquons le lemme suivant (une variation sur un thème de SGA 3) à $\mathrm{Pic}^0_{C/S} \times_S C^{reg}$ sur C^{reg} .

Lemme 1.14. Soit $p : A \to S$ un schéma en groupes sur S de fibres des extensions de variétés abéliennes par des tores. Soient g et h deux endomorphismes de A . Il existe une partie ouverte et fermée de S tel que, pour tout S-schéma T , $g_T = h_T$ si et seulement si T se factorise par V .

Le lemme montre que U de 1.13 est fermé, car son complément est image d'une partie ouverte (et fermée) $C^{reg}-V$ de C^{reg} . Il prouve aussi que si $S = U$, C^{reg} agit trivialement sur $\mathrm{Pic}^0_{C/S}$. Nous prouverons que U est ouvert en même temps que 1.15 ci-dessous.

Preuve de 1.14. Si S est artinien local, de point s , et que $g_s = h_s$, alors $g = h$ sur A_n , pour n invertible, car ce groupe est fini étale. La réunion des A_n est schématiquement dense, et donc $g = h$.

On peut se ramener au cas où S est noethérien. Si $s \in S$, et que $g_s = h_s$, il résulte que $\mathrm{Ker}(g-h)$ à même complété formel que A en $0 \in A_s \subset A$, puis que $g = h$ dans un voisinage de s . Il existe donc V ouvert comme en 1.14 Soit $\bar{V}$ l'adhérence de V . On a $\overline{A_V} = A_{\bar{V}}$, donc $g = h$ au-dessus de $\bar{V}$ et $V \supset \bar{V}$ est fermé .

Proposition 1.15 : Soit $(p : C \to S , +)$ une courbe elliptique généralisée. Il existe une famille localement finie de sous-schémas $(S_n)_{n\geq 1}$ fermés et disjoints de S telle que

a) $\bigcup_n S_n$ = image du sous-schéma de non-lissité C^{sing} (I. 4.)

b) Sur S_n , localement pour la topologie fppf , C est isomorphe à l'image

réciproque de la courbe elliptique généralisée à n cotés standard 1.9.

Preuve : Le problème est local sur S, et trivial au voisinage des points de S où C_s est lisse. Soit donc $\bar{s}$ un point géométrique de S, localisé en $s \in S$, tel que la courbe $C_{\bar{s}}$ soit un n-gone. Soit α un isomorphisme entre $C_{\bar{s}}$ et le polygone standard, tel que $\alpha(e)$ soit le point 1 de la composante d'indice $0 \in \mathbb{Z}/n$, et indexons les composantes de $C_{\bar{s}}$ par $\mathbb{Z}/n$, à l'aide de α. La translation par $x \in C_{\bar{s}}^{reg}$, dans la composante d'indice i, induit la rotation de $\Gamma(C_{\bar{s}})$ qui amène la composante d'indice 0 sur celle d'indice i : l'addition induit sur $\pi_o(C_s^{reg}) \simeq \mathbb{Z}/n$ l'addition dans $\mathbb{Z}/n$, et si x est dans la composante d'indice un de $C_{\bar{s}}^{reg}$, la translation par x permute transitivement les points singuliers de $C_{\bar{s}}$. Dans un voisinage étale de $\bar{s}$, C_{reg}/S admet des sections x telles que $x(\bar{s})$ soit dans la composante d'indice un de $C_{\bar{s}}$. L'automorphisme $g = x +$ de C/S vérifie alors l'hypothèse du lemme suivant.

Lemme 1.16. Soient C/S une courbe stable de genre un sur S, g un S-automorphisme de C et $\bar{s}$ un point géométrique de S localisé en $s \in S$. On suppose que $C_{\bar{s}}$ est un n-gone, et que g permute transitivement les points singuliers de C_s. Soit $T \subset S$ l'image du sous-schéma de non lissité C^{sing}. Au-dessus d'un voisinage de s, la courbe C_T/T est isomorphe, localement pour la topologie étale, au n-gone standard.

On vérifie fibre par fibre que C^{sing} est non ramifié sur S. Au voisinage étale de $\bar{s}$, C^{sing} est donc somme disjointe de n sous-schémas F_i, $F_i \to S$ étant un plongement fermé. Puisque g est un automorphisme, $g(\cup F_i) = \cup F_i$. En $\bar{s}$, donc au voisinage étale de $\bar{s}$, g permute transitivement les F_i et ceux-ci ont tous la même image T.

Pour prouver le lemme, on peut supposer que $S = T$. Ce qui précède montre que C^{sing} est alors fini étale sur S ; on peut le supposer somme de sections disjointes x_i. D'après I 5.3, pour tout $s \in S$, $(C,x_i(s))/(S,s)$ est localement pour la topologie étale isomorphe au sous-schéma de A_S^2 d'équation $xy = t$ (t section convenable de $\mathfrak{O}_S$, nulle en s). L'image du lieu de non lissité $x = y = 0$ de ce

schéma est le sous-schéma $t = 0$ de S ; le lieu de non lissité ne peut être étale que si $t \equiv 0$ au voisinage de s . Localement pour la topologie étale, $(C,x_i(s))/(S,s)$ est donc isomorphe au sous-schéma de A^2_S d'équation $xy = 0$.

Eclatons C^{sing} dans C pour obtenir $\widetilde{C}$. Un calcul local montre que $\widetilde{C}$ est lisse sur S , de fibres isomorphes aux normalisées des fibres de C , et que l'image réciproque dans $\widetilde{C}$ de C^{sing} est étale sur S .

Soit $\pi : \widetilde{C} \to S'$ la factorisation de Stein de $\widetilde{C}$. S' est fini étale sur S et les fibres géométriques de π sont isomorphes à $\mathbb{P}^1$. Localement sur S (pour la topologie étale), $\widetilde{C}$ est donc somme de n copies de $\mathbb{P}^1$. Au voisinage étale de s , C se déduit de $\widetilde{C}$ comme $C_{\overline{s}}$ de $\widetilde{C}_{\overline{s}}$, donc est un polygone de Néron standard.

Variante : On se réduit facilement à supposer S noethérien. On peut alors remplacer l'argument de localisation étale utilisé par un passage aux complétés; on se dispense ainsi du délicat théorème 5.3, remplacé par 5.2, mais on doit vérifier une compatibilité entre éclatements et complétions.

Fin de la preuve de 1.13. Soient $U \subset S$ et $V \subset C^{reg}$, ouvert et fermé comme dans 1.13 et sa démonstration. Il faut prouver U ouvert. Puisque le complément de l'image du lieu de non lissité de C est dans U , on se ramène au cas où S est égal à cette image. Soit $x \in U$. Quitte à se localiser près de U pour la topologie étale, il existe une translation g vérifiant l'hypothèse de 1.16, et on peut supposer que la courbe C/S est isomorphe au n-gone standard. On vérifie alors que l'image d'une partie ouverte et fermée de C^{reg} (ici, $= V$) est ouverte et fermée.

Fin de la preuve de 1.15 (dont on reprend les notations).

On prend pour S_n le schéma T de (1.16) . On peut supposer $S_n = T$; il existe alors localement un isomorphisme de courbes α de C avec l'image inverse sur S du polygone de Néron standard. Il se relève en $\widetilde{\alpha} : \widetilde{C} \xrightarrow{\sim} \mathbb{P}^1 \times \mathbb{Z}/n$, et on peut supposer que $\widetilde{\alpha}(e) = (1,0)$. Via α et $\widetilde{\alpha}$, $(C^{reg})^o$ agit sur $\mathbb{P}^1 = \mathbb{P}^1 \times \{0\}$ en fixant les sections 0 et ∞ , et s'identifie à $\mathbb{P}^1 - \{0\} - \{\infty\}$. On a donc

$(C^{reg})^o \simeq \mathbb{G}_m$ (compatible à +) . Au voisinage de s , on peut normaliser α de sorte que $\tilde{\alpha}(x^i) = (1,i)$ $(0 \leq i < n)$. Si $x^n = 1$, α est alors un isomorphisme de $(C,+)$ avec la courbe (1.9) . Dans le cas général , $x^n = a \in \mathbb{G}_m(S)$, a admet une racine $n^{ième}$ localement pour la topologie fppf de S (pour la topologie étale si n est inversible sur S) et on remplace x par $x.a^{-1/n}$.

La proposition suivante jouera un rôle technique clef dans les questions de représentabilité.

Proposition 1.17. Soit X/S une courbe elliptique généralisée sur S , de section unité $e \in X(S)$, et soit $u : Y \to X$ un revêtement fini étale de X , muni de $e \in Y(S)$ au-dessus de e . On suppose que les fibres géométriques de Y/S sont connexes. Il existe alors une et une seule structure de courbe elliptique généralisée sur Y , d'unité e , telle que le diagramme

(1.17.1)
$$\begin{array}{ccc} Y^{reg} \times_S Y & \xrightarrow{+} & Y \\ \downarrow & & \downarrow u \\ X^{reg} \times_S Y & \xrightarrow{+} & X \end{array}$$

soit commutatif.

Soit $t \in Y^{reg}(S)$. Soit F' le foncteur qui à T/S associe l'ensemble des $\tau : Y_T \to Y_T$ rendant commutatif le diagramme

$$\begin{array}{ccc} Y_T & \xrightarrow{\tau} & Y_T \\ \downarrow & & \downarrow \\ X_T & \xrightarrow{u(t)+} & X_T \end{array}$$

Ce foncteur est représenté par un revêtement étale S' de S (ouvert et fermé dans le revêtement défini par la factorisation de Stein de $Y_T \times_{X_T} Y_T$ (morphismes $(u(t)+)\circ u$ et u) . L'application $e \to \tau(e)$ envoie S' dans $u^{-1}ut(S)$, fini étale sur S . Le sous foncteur F' de F correspondant aux τ tels que $\tau(e_T) = t_T$ est donc encore représenté par un S" fini et étale sur S . Prouvons que $S'' \xrightarrow{\sim} S$. Il suffit de vérifier que pour S spectre d'un corps algébriquement clos, il existe un et un seul τ relevant u(t)+ tel que $\tau(e) = t$.

Ceci revient à montrer que le revêtement Y de X, et son image réciproque par $u(t)+ : X \to X$, sont isomorphes. Pour X lisse, cela résulte de ce que $u(t)$ est dans la composante neutre de X^{reg}. Pour X un polygone de Néron, on observe que X n'a qu'un seul revêtement irréductible de degré donné.

L'unique section de S'' sur S définit un morphisme $t+ : Y \to Y$. Cette construction, étant compatible aux changements de base, définit

$$+ : Y^{reg} \times Y \to Y ,$$

rendant (1.17.1) commutatif, tel que $t + e = t$, et caractérisé par ces propriétés. Reste à prouver que $+$ fait de Y une courbe elliptique généralisée, ie. que diverses identités, telles $x+y = y+x$ $(x,y \in Y^{reg}(S)$ sont vérifiées. Puisque $u(x+y) = u(x) + u(y) = u(y) + u(x) = u(y+x)$, $x+y$ est une section de $u^{-1}(u(y+x)(S))$, étale sur S, et il suffit de vérifier que $x+y = y+x$ pour les fibres géométriques. Pour les fibres propres et lisses, une loi de composition à unité est automatiquement une loi de groupe abélien. Pour les autres, le polygone de Néron à n côtés, avec sa loi $+$ standard, n'a pour revêtements que les polygones de Néron à nk côtés, avec leur loi $+$ standard.

Les autres identités à vérifier se prouvent de même.

1.18. Soit $(C,+)$ une courbe elliptique généralisée sur S. On vérifie fibre par fibre que le morphisme

$$n : x \to nx : C^{reg} \to C^{reg}$$

est plat. Son noyau C_n est donc plat sur S.

Supposons que S soit le spectre d'un corps algébriquement clos k.

a) si C est lisse, on sait que C_n est fini de rang n^2

b) si C est un m-gone, on a $C^{reg} \simeq \mathbb{G}_m \times \mathbb{Z}/m$.

Notant (n,m) le pgcd de n et m, on a donc

$$C_n \simeq \mu_n \times \mathbb{Z}/((n,m))$$

En particulier, C_n est fini de rang $n.(n,m)$.

Rappelons le lemme suivant.

Lemme 1.19. Soit $f : X \to S$ un morphisme quasi-fini plat et séparé, avec S noethérien. Si le rang des fibres de f est constant, alors f est fini.

Preuve : Prouvons que f est propre. D'après le critère valuatif de propreté, on peut supposer que S est un trait. D'après le Main theorem de Zariski, X est un ouvert d'un schéma $\overline{X}$ fini sur S qu'on peut même prendre plat sur S . Comparant les rangs des fibres spéciales et génériques de X et $\overline{X}$, on trouve que $X = \overline{X}$, d'où 1.19.

Corollaire 1.20. Soient $p : C \to S$ une courbe elliptique généralisée sur S et n un entier. On suppose que, pour tout point géométrique $\bar{s}$ de S , $C_{\bar{s}}$ est lisse, ou un m-gone, avec $n|m$. Alors, C_n est fini localement libre sur S de rang n^2.

On se ramène à supposer S noethérien, et on applique 1.18, 1.19.

2. Courbes stables irréductibles.

Dans ce §, nous prouvons que, pour C/S une courbe stable de genre un, de fibres géométriques irréductibles, et pour $e \in C^{reg}(S)$, il existe sur C une et une seule structure de courbe elliptique généralisée d'unité e .

2.1 Certains résultats préliminaires vaudront pour un morphisme propre et plat de présentation finie $p : C \to S$ vérifiant la condition suivante.

(2.1.1) C est une courbe de Cohen-Macaulay de genre un sur S , $p_*\mathcal{O}_C = \mathcal{O}_S$ universellement et $p^* p_* \omega_{C/S} \xrightarrow{\sim} \omega_{C/S}$.

Une courbe stable de genre un sur S vérifie (2 1.1) (1.6). Si une fibre géométrique $C_{\bar{s}}$ de p vérifie (2.1.1), alors C/S vérifie (2.1.1) dans un voisinage de s (pour la condition : "Cohen-Macaulay", voir EGA IV 12.2.1.; pour

$p_*\mathcal{O}_C = \mathcal{O}_S$, voir EGA III. 7.8.8.; si $p_*\mathcal{O}_C = \mathcal{O}_S$ universellement, $p_*\omega_{C/S}$ est localement libre de formation compatible à tout changement de base, et on conclut comme en 1.6). Les fibres spéciales des modèles de Néron de courbes elliptiques vérifient (2.1.1)(SGA 7 X 1.15).En particulier, les courbes $p : C \to S$ de genre un à fibres géométriques intègres (= elliptiques, cubiques planes nodales ou cubiques planes cuspidales) vérifient (2 1.1).

Pour toute section t de C/S on désignera par $m(t)$ le faisceau d'idéaux qui définit le sous-schéma $t(S)$.

Proposition 2.2. Soient S un schéma noethérien, $\bar{s}$ un point géométrique de S localisé en $s \in S$, $p : C \to S$ vérifiant (2.1.1) et $\mathcal{F}$ un faisceau cohérent sur C plat sur S . On suppose que le faisceau $\mathcal{F}_{\bar{s}}$ sur $C_{\bar{s}}$ est isomorphe à un faisceau $m(t_{\bar{s}})$, pour $t_{\bar{s}} \in C_{\bar{s}}(\bar{s})$. Alors, au-dessus d'un voisinage U de s dans S , il existe une et une seule section $t \in C(U)$ telle que $\mathcal{F}|p^{-1}(U)$ soit isomorphe à $m(t)$.

La démonstration repose sur le lemme suivant

Lemme 2.2.1. Il existe un voisinage U de s au-dessus duquel $p_* \mathrm{Hom}(\mathcal{F},\mathcal{O}_C)$ est localement libre de rang un de formation compatible à tout changement de base $U' \to U$.

Déduisons 2.2 de 2.2.1. Quitte à restreindre S , on peut supposer que $P_*\mathrm{Hom}(\mathcal{F},\mathcal{O}_C)$ admet une section globale e qui, après tout changement de base, définit un isomorphisme $\mathcal{O}_S \xrightarrow{\sim} p_*\mathrm{Hom}(\mathcal{F},\mathcal{O}_C)$. Vu l'hypothèse, après changement de base de S à $\bar{s}$, $e : \mathcal{F} \to \mathcal{O}_C$ définit un isomorphisme $\mathcal{F}_s \xrightarrow{\sim} m(t_{\bar{s}})$.

Comme $e \otimes_{\mathcal{O}_S} k(s) : \mathcal{F}_s \to \mathcal{O}_{C_s}$ est injectif, il résulte de EGA IV.11.3.7 que $(\mathrm{Ker}\ e)_x = 0$ et que $(\mathrm{Coker}\ e)_x$ est p-plat en chaque point x de C_s , donc que $\mathrm{Ker}\ e = 0$ et $K = \mathrm{Coker}\ e$ est plat sur un voisinage U de s . Quitte à restreindre S , on peut supposer que $U = S$. Comme $K_{\bar{s}}$ est de support fini, K est de support fini sur S. La flèche $\mathcal{O}_S \to p_*(K)$, qui vient de $\mathcal{O}_C \to K$, est après tensorisation avec $k(s)$ un isomorphisme.Donc,en appliquant le lemme de Nakayama (ce qui est

loisible, car le support de K est finie sur S) ce morphisme est surjectif et, parce que K est plat sur S , il est aussi injectif.

Quitte à restreindre S , on peut donc supposer que e est injectif et que $\mathcal{O}_S \simeq p_*(K)$. Le sous-schéma de C défini par $e(\mathcal{J})$ est donc isomorphe à S et définit la seule section t telle que $\mathcal{J} \simeq m(t)$.

Prouvons 2.2.1. La suite exacte longue de cohomologie associée à

$$0 \longrightarrow m(t_{\bar{s}}) \longrightarrow \mathcal{O}_{C_{\bar{s}}} \longrightarrow \mathcal{O}(t_{\bar{s}}) \longrightarrow 0$$

et (2 1.1) fournissent

$$H^0(C_{\bar{s}}, m(t_{\bar{s}})) = 0 \tag{2.2.2}$$

$$\dim_{k(\bar{s})} H^1(C_{\bar{s}}, m(t_{\bar{s}})) = 1 \tag{2.2.3}$$

Il suffit donc de démontrer le lemme suivant :

Lemme 2.3. Avec les notations de 2.2, supposons que $H^0(C_{\bar{s}}, \mathcal{J}_{\bar{s}}) = 0$ et que $\dim_{k(\bar{s})} H^1(C_{\bar{s}}, \mathcal{J}_{\bar{s}}) = 1$. Il existe alors un voisinage U de s dans S au-dessus duquel $p_* \mathrm{Hom}(\mathcal{J}, \mathcal{O}_C)$ est localement libre de rang un, de formation compatible à tout changement de base $U' \to U$.

Preuve : Par hypothèse, $H^i(C_{\bar{s}}, \mathcal{J}_{\bar{s}}) = 0$ pour $i \neq 1$, et $H^1(C_s, \mathcal{J}_s)$ est de rang un. Il en résulte que, dans un voisinage de s , $R^i p_*(\mathcal{J})$ est nul pour $i \neq 1$, le reste après tout changement de base, et que $R^1 p_* \mathcal{J}$ est localement libre de rang un de formation compatible à tout changement de base.

Dans le théorème de dualité (I.2.2),

$$Rp_* \, R\,\mathrm{Hom}(\mathcal{J}, \omega_{C/S})[-1] \xrightarrow{\sim} R\,\mathrm{Hom}(Rp_* \mathcal{J}, \mathcal{O}_S) ,$$

prenons les faisceaux de cohomologie de degré -1 . On obtient

$$p_* \, \mathrm{Hom}(\mathcal{J}, \omega_{C/S}) \xrightarrow{\sim} (R^1 p_* \mathcal{J})^\vee$$

(où $^{\vee}$ désigne le $\mathcal{O}_S$-module dual). En particulier, $p_* \underline{\mathrm{Hom}}(\mathfrak{F}, \omega_{C/S})$ est localement libre de rang un compatible à tout changement de base. Il résulte de (2.1.1) que $p_* \omega_{C/S}$ est localement libre de rang un de formation compatible à tout changement de base. De (2.1.1) résulte donc encore que, localement sur S, $\omega_{C/S}$ est isomorphe à $\mathcal{O}_C$, et 2.3 en résulte.

Corollaire 2.4. : Soit $p : C \to S$ une courbe de genre un sur S qui vérifie (2.1.1). Soit $\mathfrak{L}$ un faisceau inversible sur C qui définisse un élément de $\mathrm{Pic}^o_{C/S}(S)$ (cf. I 3.2). Pour toute section t de C sur S, il existe une et une seule section t' telle que localement sur S, $m(t')$ soit isomorphe à $m(t) \otimes \mathfrak{L}$.

Preuve : On se ramène à supposer S noethérien. D'après 2.2 on peut supposer que S est le spectre d'un corps algébriquement clos. Nous allons traiter un cas "universel". Faisons le changement de base de S à $T = C \times_S \mathrm{Pic}^o_{C/S}$, prenons pour t la section universelle et pour $\mathfrak{L}$ le faisceau inversible universel. Pour chaque point de la forme $(x, 1_{\mathrm{Pic}})$ $(x \in C)$ de T l'assertion est trivialement vérifiée. Donc, par 2.2, l'assertion est vraie sur un voisinage de $C \times 1_{\mathrm{Pic}} \subset T$. La courbe C étant propre, il existe un voisinage ouvert U de 1_{Pic} dans $\mathrm{Pic}^o_{C/S}$ tel que l'assertion soit vraie au-dessus de $C \times U \subset T$. L'assertion est donc valable sur le produit de C par le groupe engendré par U, qui est $\mathrm{Pic}^o_{C/S}$ tout entier, donc sur $T = C \times_S \mathrm{Pic}^o_{C/S}$.

2.5. Nous noterons $+$ le morphisme

$$+ : \mathrm{Pic}^o_{C/S} \times C \to C \quad ,$$

tel que pour $t \in C(S)$ et pour $\lambda \in \mathrm{Pic}^o_{C/S}(S)$, représenté par un faisceau inversible $\mathfrak{L}$, on ait

$$m(\lambda + t) \simeq m(t) \otimes \mathfrak{L}^{\otimes -1} \qquad \text{(localement sur } S\text{)}. \tag{2.5.1}$$

Pour $t \in C^{\mathrm{reg}}(S)$, $\mathcal{O}(t) = m(t)^{\otimes -1}$ est faisceau inversible, d'où un morphisme

$$\varpi : C^{\mathrm{reg}} \to \mathrm{Pic}_{C/S} : t \mapsto \mathcal{O}(t) \quad . \tag{2.5.2}$$

On a

$$\varphi(\lambda + t) = \lambda + \varphi(t) \quad . \tag{2.5.3}$$

Théorème 2.6. *Soit* $p : C \to S$ *une courbe de genre un qui vérifie (2.1.1)*

(i) φ *est une immersion ouverte.*

(ii) *Si* p *est à fibres géométriques intègres , l'image de* φ *est un torseur sous* $\mathrm{Pic}^{o}_{C/S}$.

(iii) *Si* p *est à fibres géométriques réduites, l'action* $+$ *de* $\mathrm{Pic}^{o}_{C/S}$ *sur* C *induit l'action triviale de* $\mathrm{Pic}^{o}_{C/S}$ *sur* $\mathrm{Pic}^{[o]}_{C/S}$.

Preuve. Il suffit de prouver (i) et (ii) lorsque S est le spectre d'un corps algébriquement clos k (EGA IV. 17.8.2.). Les images par φ des diverses composantes connexes de C^{reg} sont alors disjointes. Soient D l'une d'elles, et $e \in D(k)$. Les applications $\lambda \mapsto \lambda + e$ et $t \mapsto \varphi(t) - \varphi(e)$ sont des isomorphismes inverses l'un de l'autre entre D et Pic^{o} . En particulier, φ est un isomorphisme $D \xrightarrow{\sim} \varphi(e) + \mathrm{Pic}^{o}$ et (i), (ii) en résultent.

Prouvons (iii). Soit λ dans Pic^{o} , représenté par un faisceau inversible $\mathcal{L}$. Localement pour la topologie fppf , tout élément de $\mathrm{Pic}^{[o]}$ se met sous la forme $\mathcal{O}(\Sigma\, n_i t_i) =_{\mathrm{dfn}} \bigotimes_i m(t_i)^{\otimes(-n_i)}$, avec $\Sigma\, n_i = 0$, pour des sections t_i convenables de C^{reg} . Le transformé par $\lambda +$ de $\mathcal{O}(\Sigma\, n_i t_i)$ est

$$\mathcal{O}(\Sigma\, n_i(\lambda + t_i)) = \bigotimes_i m(\lambda + t_i)^{\otimes(-n_i)} \sim \bigotimes_i [m(t_i)^{\otimes(n_i)} \otimes \mathcal{L}^{\otimes n_i}] \simeq \bigotimes_i m(t_i)^{\otimes(-n_i)} \otimes$$

$$\otimes \bigotimes_i \mathcal{L}^{\otimes n_i} \simeq \mathcal{O}(\Sigma\, n_i t_i) \quad ,$$

et l'assertion en résulte.

Voici une variante de 2.2.

Proposition 2.6.1. *Soient* S *un schéma noethérien,* $\bar{s}$ *un point géométrique de* S *localisé en* $s \in S$, $p : C \to S$ *un schéma en courbes de genre un sur* S *et* $\mathcal{F}$ *un faisceau cohérent sur* C *plat sur* S . *On suppose que* $C_{\bar{s}}$ *est une courbe intègre,*

que $\mathcal{F}_s$ est sans torsion et génériquement de rang un et que $\chi(C_{\bar{s}},\mathcal{F}_{\bar{s}}) = -1$. Alors, au-dessus d'un voisinage U de s , il existe une et une seule section $t \in C(U)$ telle que $\mathcal{F}|p^{-1}(U)$ soit isomorphe à $m(t)$.

Comme observé en 2.1, C/S vérifie (2.1.1) au voisinage de s ; d'après 2.2, il suffit donc de traiter le cas où S est spectre d'un corps algébriquement clos : $S = \bar{s}$.

Sous cette hypothèse, prouvons que $H^0(C,\mathcal{F}) = 0$. Si $f \in H^0(C,\mathcal{F})$ est non nul, la suite

$$0 \longrightarrow \mathcal{O}_C \xrightarrow{f} \mathcal{F} \longrightarrow \mathcal{F}/\mathcal{O}_C.f \longrightarrow 0$$

est exacte, puisque $\mathcal{F}$ est sans torsion sur C intègre.

On déduit que

$$\chi(C,\mathcal{F}) = \chi(C,\mathcal{O}_C) + \chi(C,\mathcal{F}/\mathcal{O}_C\cdot f) = 0 + \chi(C,\mathcal{F}_{/f\cdot\mathcal{F}}) \geq 0 \ ,$$

ce qui contredit l'hypothèse.

Puisque $\chi = -1$, les hypothèses de 2.3 sont vérifiées : il existe $e : \mathcal{F} \to \mathcal{O}_C$, avec $e \neq 0$. Puisque $\mathcal{F}$ est sans torsion génériquement de rang un, et C intègre, la suite

$$0 \longrightarrow \mathcal{F} \xrightarrow{e} \mathcal{O}_C \longrightarrow \mathcal{O}_C/e\mathcal{F} \longrightarrow 0$$

est exacte, et le support de $\mathcal{O}_C/e\mathcal{F}$ est fini. On a

$$\chi(C,\mathcal{O}_C/e\mathcal{F}) = \chi(C,\mathcal{O}_C) - \chi(C,\mathcal{F}) = 0 - (-1) = 1 \ ,$$

i.e. $\dim H^0(C,\mathcal{O}_C/e\mathcal{F}) = 1$: l'idéal $e(\mathcal{F})$ définit un point t de C , et $\mathcal{F} \simeq m(t)$.

Proposition 2.7. (i) Soient $p : C \to S$ une courbe de genre un à fibres géométriques intègres et $e \in C^{reg}(S)$. Il existe une et une seule loi $+ : C^{reg} \times C \to C$ telle que, sur S et après tout changement de base, pour $x \in C^{reg}(S)$ et $y \in C(S)$, on ait

(2.7.1) $\qquad m(x+y) \simeq m(x) \otimes m(y) \otimes m(e)^{\otimes -1}$ localement sur S

(ii) Cette loi fait de C^{reg} un schéma en groupe commutatif d'unité e agissant sur C ; pour cette action, C^{reg} agit trivialement sur $Pic^{o}_{C/S}$.

(iii) La symétrie $x \mapsto -x$ de C^{reg} se prolonge à C et, pour $t \in C(S)$, on a localement sur S

$$m(-t) \simeq \underline{Hom}(m(t), \mathcal{O}(-2(e))) \quad . \tag{2.7.2}$$

(iv) Si C/S est stable, + est l'unique structure de courbe elliptique généralisée sur C d'unité e .

Preuve : On peut supposer S noethérien. D'après 2.1, la condition (2.1.1) est vérifiée. L'assertion (i) résulte alors de 2.4. D'après 2.6, le morphisme

$$\varphi_e : C^{reg} \to Pic^{o}_{C/S} : x \mapsto \varphi(x) - \varphi(e)$$

est un isomorphisme de S-schémas. On a

$$\varphi_e(x+y) = \varphi(x+y) - \varphi(e) = (\varphi(x) + \varphi(y) - \varphi(e)) - \varphi(e) = \varphi_e(x) - \varphi_e(y) ,$$

de sorte que φ_e est un isomorphisme de groupes. Pour $x \in C^{reg}(S)$ et $y \in C(S)$, on a $x+y = \varphi_e(x) + y$. L'assertion (ii) en résulte.

Si C/S est stable, (C,+) est une courbe elliptique généralisée d'après (ii). Si + est une autre loi de courbe elliptique généralisée d'unité e , et que $x \in C^{reg}(S)$, on sait que la translation $x +$ agit trivialement sur $Pic^{o}_{C/S}$ (1.13). On a donc, pour $y \in C^{reg}(S)$ et $z \in C(S)$,

$$x + (y+z) = x +(\varphi_e(y) + z) = \varphi_e(y) + (x + z) = y + (x + z) \quad .$$

Pour $z = e$, ceci donne $x + y = y+x = x+y$, et + coincide avec + sur $C^{reg} \times C^{reg}$. Par passage à l'adhérence schématique, on a $+ = +$ partout, d'où (iv).

Prouvons (iii). Pour $t \in C^{reg}(S)$, on a $\varphi_e(-t) = - \varphi_e(t)$, donc localement sur S

$$\mathcal{O}((-t))\mathcal{O}(-(e)) \simeq \mathcal{O}(-(t))\mathcal{O}((e)) \quad , \quad \text{ie.}$$

$$m(-t) \simeq m(t)^{\otimes -1} \otimes \mathcal{O}(-2(e)) \quad .$$

Il reste à prouver que pour t quelconque, le second membre de (2.7.2) est, localement sur S, de la forme $m(x)$. La suite exacte

$$0 \longrightarrow m(t) \longrightarrow \mathcal{O}_C \longrightarrow t_*\mathcal{O}_S \longrightarrow 0 \tag{2.7.3}$$

donne la suite exacte

$$0 \longrightarrow \mathrm{Hom}(t_*\mathcal{O}_S, \mathcal{O}(-2(e)) \longrightarrow \mathrm{Hom}(\mathcal{O}_C, \mathcal{O}(-2(e)) \longrightarrow$$
$$\longrightarrow \mathrm{Hom}(m(t), \mathcal{O}(-2(e)) \longrightarrow \mathrm{Ext}^1(t_*\mathcal{O}_S, \mathcal{O}(-2(e)) \longrightarrow 0 \quad . \tag{2.7.4}$$

Comme $\omega_{C/S}$ est un faisceau inversible sur C (cf. 1.6.1), $\mathcal{O}(-2(e))$ est, localement sur C, isomorphe à $\omega_{C/S}$. Donc localement sur C $\mathrm{Ext}^1(t_*\mathcal{O}_S, \mathcal{O}(-2(e)) \simeq \mathrm{Ext}^1(t_*\mathcal{O}_S, \omega_{C/S})$. On applique maintenant la formule de dualité des faisceaux cohérents <u>pour le morphisme</u> $t : S \to C$:

$$Rt_*R\,\mathrm{Hom}_{\mathcal{O}_S}(\mathcal{O}_S, t^!\omega_{C/S}) \xrightarrow{\sim} R\,\mathrm{Hom}_{\mathcal{O}_C}(Rt_*\mathcal{O}_S, \omega_{C/S}) \quad . \tag{2.7.5}$$

On remarque que $t^!\omega_{C/S} = t^!p^!\mathcal{O}_S[1] \simeq (p\circ t)^!\mathcal{O}_S[1] = \mathcal{O}_S[1]$. De plus, $R^1t_*\mathcal{O}_S = 0$. En prenant les H^0 des deux membres de (2.7.5) on obtient

$$\mathrm{Ext}^1(t_*\mathcal{O}_S, \omega_{C/S}) \simeq t_*\mathcal{O}_S \quad .$$

De plus, il est facile à voir que $\mathrm{Hom}(t_*\mathcal{O}_S, \mathcal{O}(-2(e)) = 0$. La suite exacte obtenue

$$0 \longrightarrow \mathcal{O}(-2(e)) \longrightarrow \mathrm{Hom}(m(t), \mathcal{O}(-2(e)) \longrightarrow t_*\mathcal{O}_S \longrightarrow 0 \tag{2.7.6}$$

montre que $\mathrm{Hom}(m(t), \mathcal{O}(-2(e))$ est plat sur S, que sa formation commute à tout changement de base $S' \to S$ et que ses fibres sont génériquement de rang 1 et sans torsion. Pour voir que ce faisceau est, localement sur S', de la forme $m(t')$, il suffit de voir que pour chaque point géométrique $\bar{s}$ de S' on a que $\chi(C_{\bar{s}}, \mathrm{Hom}(m(t), \mathcal{O}(-2(e))) = -1$ (cf. 2.6). Mais $\deg_{C_{\bar{s}}}(\mathcal{O}(-2(e)) = -2$, donc $\chi(C_{\bar{s}}\ \mathcal{O}(-2(e)) = -2$, et $\chi(C_{\bar{s}}, t_*\mathcal{O}_{\bar{s}}) = 1$. On a donc bien

$\chi(C_{\bar{s}}, \mathrm{Hom}(m(t), \mathcal{O}(-2(e))) = -1$ et par suite que $\mathrm{Hom}(m(t), \mathcal{O}(-2(e)) = m(t')$ pour une section t', ce qui achève la démonstration.

Corollaire 2.8. Soit $p : C \to S$ une courbe elliptique généralisée sur S. L'application $x \to -x : C^{reg} \to C^{reg}$, se prolonge en un automorphisme de C/S.

L'extension cherchée est unique, car C^{reg} est schématiquement dense dans C. Le problème est donc local pour la topologie fpqc. Le problème est trivial au-dessus de l'ouvert où C est lisse. Soit $\bar{s}$ un point géométrique de S, localisé en $s \in S$, tel que $C_{\bar{s}}$ soit un n-gone. Au voisinage de ce point, C_n est fini et plat et, localement pour la topologie fppf, admet une section t telle que les multiples de t rencontrent les diverses composantes de $C_{\bar{s}}$. Au voisinage de s, t engendre un sous-groupe H de C_n, isomorphe à $\mathbb{Z}/n$. Le groupe $H_{\bar{s}}$ agit librement sur $C_{\bar{s}}$, et $C_{\bar{s}}/H$ est un 1-gone. Dans un voisinage de s, on a alors

a) H agit librement sur C, et C/H est une courbe elliptique généralisée sur S.

b) C/H est à fibres géométriques irréductibles (appliquer 1.15 à C/H)

c) C est un revêtement fini étale de C/H.

On sait que C/H admet une involution $x \to -x$ (2.7(iii)). On procède alors comme en 1.17 pour relever cette involution en une involution de C.

3. Construction de courbes elliptiques généralisées.

Ce § ne servira pas dans la suite de cet article et nous recommandons au lecteur de l'omettre en première lecture.

Nous y démontrons le théorème suivant 3.2 ci-dessous.

3.1. Soit $p : C \to S$ une courbe stable de genre un munie d'une section $e \in C^{reg}(S)$. Soit G un S-schéma en groupes commutatifs plat localement de présentation finie qui agit sur C. Soient les conditions suivantes.

(3.1.1) G agit trivialement sur $\mathrm{Pic}^{o}_{C/S}$.

(3.1.2) Pour chaque point géométrique $\bar{s}$ de S , $G(\bar{s})$ agit transitivement sur l'ensemble des composantes irréductibles de $C_{\bar{s}}$.

Dans le cas particulier important où G est le schéma en groupes constant $\mathbb{Z}$, l'action ζ de G est définie par l'automorphisme $g = \zeta(1)$ de C et (3.1.1) (3.1.2) deviennent

(3.1.3) g agit trivialement sur $\mathrm{Pic}^{o}_{C/S}$

(3.1.4) Pour chaque point géométrique $\bar{s}$ de S , g permute transitivement les composantes irréductibles de $S_{\bar{s}}$.

Théorème 3.2. Soit G agissant sur C comme en 3.1. Si les conditions (3.1 1) et (3.1.2) sont vérifiées, il existe sur C une et une seule structure de courbe elliptique généralisée d'unité e telle que G agisse sur C par translations. De plus, tout automorphisme de C sur S qui commute à G et vérifie (3.1.1) est une translation.

Plan de la démonstration. Nous prouverons les énoncés suivants.

(A) Soit s un point géométrique de S tel que $G_{\bar{s}}$ agissant sur $C_{\bar{s}}$ vérifie (3.1.1) et (3.1.2). Il existe un voisinage fppf U de $\bar{s}$ et $g \in G(U)$ tel que l'action de g sur C_U vérifie (3.1.3) (3.1.4).

(B) 3.2 pour $G = \mathbb{Z}$

Montrons déjà que (A) et (B) impliquent 3.2. Les problèmes sont locaux pour la topologie fppf . Si $G_{\bar{s}}$ agissant sur $C_{\bar{s}}$ vérifié (3.1.1) (3.1.2), on peut donc supposer qu'il existe $g \in G(S)$ comme en (A). D'après (B), il existe une et une seule structure de courbe elliptique généralisée d'unité e telle que g soit une translation. De plus, puisque G et g commutent et que G vérifie (3.1.1), G agit par translations. Enfin, tout automorphisme vérifiant (3.1.1) qui commute à G commute à g , donc est une translation.

Preuve de (A) Si $C_{\bar{s}}$ est lisse, on prend pour U l'ouvert de S au-dessus duquel C est lisse, et $g = e$. Sinon, $C_{\bar{s}}$ est un n-gone et l'image de $G(\bar{s})$ dans le groupe des automorphismes du diagramme $\Gamma(C_{\bar{s}})$ des composantes irréductibles de $C_{\bar{s}}$ est d'ordre $\geq n$. D'après (3.1.1), $G(\bar{s})$ agit par rotations sur $\Gamma(C_{\bar{s}})$. Le groupe $\mathrm{Aut}^+(\Gamma(C_{\bar{s}}))$ des rotations de $\Gamma(C_{\bar{s}})$ étant cyclique d'ordre n, il existe $g_{\bar{s}} \in G(s)$ d'image un générateur de ce groupe, et $g_{\bar{s}}$ permute transitivement les composantes irréductibles de $C_{\bar{s}}$. Localement fppf, il existe une section g de G qui induise $g_{\bar{s}}$. On peut appliquer 1.16 à g pour vérifier (3.1.4) dans un voisinage de $\bar{s}$. Que 3.1.3 soit vérifié par g dans un voisinage de $\bar{s}$ résulte de 1.13.

Preuve de 3.2 pour $G = \mathbb{Z}$.

Soient ζ l'action de G sur C et $g = \zeta(1)$. En appliquant 1.16 à g, on se ramène à supposer que les fibres géométriques de C sont toutes lisses ou des n-gones (n fixe). Dans ce cas, $g^n e$ est fibre par fibre dans la même composante connexe de C que e et g^n est justiciable du lemme suivant.

Lemme 3.3. Soit h un automorphisme de C qui commute à g et vérifie (3.1.3). Si he est fibre par fibre dans la même composante irréductible de C que e, alors h est de la forme $x \mapsto \lambda + x$ pour λ une section de $\mathrm{Pic}^o_{C/S}$.

Preuve : On aura $\lambda =$ classe de $\mathcal{O}(he - e)$. L'hypothèse 3.1.3 assure que $x \mapsto \lambda + x$ commute à g. Remplaçant h par $h(x - \lambda)$, on se ramène à supposer que $he = e$. Puisque h vérifie (3 1.3), pour toute section μ de $\mathrm{Pic}^o_{C/S}$, on a $h(g^k(\mu+e)) = g^k(\mu+e)$. Toute section de C^{reg} étant localement pour la topologie fppf de la forme $g^k(\mu+e)$, h agit trivialement sur C^{reg}, donc sur C.

Preuve de 3.2 (suite) : On a $g^n x = \lambda + x$. Soit μ tel que $\lambda = \mu^{-n}$ et $g_1 = g \circ (x \mapsto \mu + x)$. Alors, $g_1^n = \mathrm{Id}$ et g_1 définit une action de $\mathbb{Z}/n$ sur C. Cette action est libre et les fibres géométriques de $C/(\mathbb{Z}/n)$ sont intègres. Sur $C/(\mathbb{Z}/n)$, il existe donc une et une seule structure de courbe elliptique généralisée de section neutre e (2.7). Sur C, il existe une et une seule structure de courbe elliptique généralisée d'unité e telle que g_1 soit une translation

(cf. 1.17) . D'après 3.3, pour λ une section de Pic^{o} , et pour toute structure de courbe elliptique généralisée, $(\lambda + e) + x$ est $\lambda + x$. La loi obtenue est donc aussi la seule telle que g soit une translation. Enfin, si h commute à g et vérifie (3.1.3) , il existe localement k tel que hg^{k} soit justiciable de 3.3, et h est une translation.

Remarque 3.4 . Si C est une courbe elliptique généralisée sur S , on peut montrer qu'il existe un et un seul homomorphisme

$$u : \mathrm{Pic}^{[0]}_{C/S} \to C^{reg}$$

tel que, après tout changement de base, pour toute section t de C^{reg} sur S , on ait

$$u(\mathcal{O}((t)-(e))) = t \quad .$$

III Théorèmes de représentabilité.

0. Introduction et notations.

Dans ce chapitre et les suivants, nous définissons et étudions divers champs algébriques, classifiant les courbes elliptiques généralisées munies de diverses structures additionnelles.

0.1. Notons $\mathcal{M}$ la catégorie fibrée en groupoïde sur la catégorie (Sch) des schémas suivante : $\mathcal{M}(S)$ est la catégorie dont les objets sont les courbes elliptiques généralisées sur S, et les morphismes les S-isomorphismes; le foncteur "image réciproque par $u : S \to T$" est $E \mapsto E \times_T S$. La catégorie $\mathcal{M}$ est un champ sur (Sch) pour la topologie fpqc (2.1) mais n'est pas un champ algébrique.

0.2. Soit $\mathcal{M}_*$ le sous-champ suivant de $\mathcal{M}$: $\mathcal{M}_*$ classifie les courbes elliptiques généralisées C/S telles que, pour tout point géométrique $\bar{s}$ de S, la caractéristique de $k(\bar{s})$ ne divise pas le nombre de composantes irréductibles de la fibre géométrique C_s. Le résultat principal 2.5 de ce chapitre est que $\mathcal{M}_*$ est un champ algébrique. De ce théorème technique résulteront les théorèmes de représentabilité des chapitres suivants. Nous le déduirons des critères généraux de M. Artin. Pour pouvoir appliquer ceux-ci, le point essentiel sera de prouver la prorepréśentabilité effective de certains foncteurs; ce sera fait au § 1.

0.3. Nous adopterons les principes de notation suivants.

a) $\mathcal{M}$, affecté d'un indice, désigne le champ algébrique classifiant les courbes elliptiques généralisées, soumises à certaines restrictions, ou munies de structures additionnelles, dont l'espèce dépend de l'indice.

b) L'exposant $^\circ$ indique le sous-champ ouvert correspondant aux courbes elliptiques proprement dites.

c) L'exposant ^{h} indique le sous-champ ouvert obtenu en ôtant les points correspondant aux courbes elliptiques supersingulières de caractéristique $p|n$, où n dépend du contexte.

d) L'exposant $^\infty$ indique le sous-champ fermé image du lieu singulier de la courbe

universelle.

e) Une notation $\mathcal{M}[1/n]$ indique soit qu'on considère un champ sur $\mathbb{Z}[1/n]$, soit, si $\mathcal{M}$ a déjà été défini, désigne $\mathcal{M} \otimes \mathbb{Z}[1/n]$.

f) Le schéma grossier de modules défini par un champ algébrique (I.8) se note par le même symbole, avec $\mathcal{M}$ remplacé par M .

Nous étendrons ces notations à certains champs au-dessus de $\mathcal{M}$, non nécessairement définis par un "problème de module" stricto sensu.

1. Un théorème de proreprésentabilité.

1.1 Soient Λ un anneau local complet de corps résiduel k et C_0 une courbe elliptique généralisée sur k . On suppose que C_0 est lisse ou l'image réciproque sur k de la courbe elliptique généralisée standard à n côtés (II.1.9). Soit D le foncteur des déformations de C_0 : pour A une Λ-algèbre noethérienne locale complète de corps résiduel k , $D(A)$ est l'ensemble des classes d'isomorphie de courbes elliptiques généralisées $C/\mathrm{Spec}(A)$, munies d'un isomorphisme $C \otimes_A k \simeq C_0$. Ce § est consacré à la démonstration du théorème suivant.

Théorème 1.2. *Supposons C_0 lisse ou n premier à l'exposant caractéristique p de k On a alors*

(i) *$(C_0,+)$ n'a pas d'automorphismes infinitésimaux (non nuls).*

(ii) *Le foncteur des déformations D de $(C_0,+)$ est effectivement proreprésentable.*

(iii) *D est proreprésenté par une courbe C sur $\mathrm{Spec}(\Lambda[[t]])$,*

(iv) *Si C_0 est non lisse, on peut choisir t de sorte que $t = 0$ soit l'image du sous-schéma de non lissité.*

Les automorphismes infinitésimaux de $(C_0,+)$ forment le groupe Lie $\mathrm{Aut}(C_0,+)$, de sorte que (i) résulte de (II.1.10). Il résulte de (i) et de [25] que D est proreprésentable.

1.3. Le cas où C_o est irréductible.

Dans ce cas, le foncteur des déformations de $(C_o,+)$ s'identifie par II.2.7 au foncteur D' des déformations de (C_o,e), le couple formé de la courbe C_o et de la section marquée e. Ce dernier foncteur est effectivement proreprésentable, un schéma formel en courbes complètes étant toujours projectif, donc algébrisable. Que D' vérifie (iii) résulte des deux formules suivantes :

$$\dim \mathrm{Ext}^1(\Omega^1_{C_o}(e), \mathcal{O}_{C_o}) = 1 \tag{1.3.1}$$

$$\dim \mathrm{Ext}^2(\Omega^1_{C_o}(e), \mathcal{O}_{C_o}) = 0 \quad . \tag{1.3.2}$$

En effet, le Ext^2 est le groupe où vivent les obstructions aux déformations. S'il s'annule, D' est proreprésenté par un algèbre de séries formelles sur Λ. Le Ext^1 s'identifie à $D'(k[\varepsilon]/(\varepsilon^2))$, et détermine la dimension relative.

Prouvons (1.3.1) et (1.3.2). Puisque ω_{C_o} est isomorphe à $\mathcal{O}_{C_o}$, on a par dualité (I.2.2)

$$\dim \mathrm{Ext}^i(\Omega^1_{C_o}(e), \mathcal{O}_{C_o}) = \dim H^{1-i}(\Omega^1_{C_o}(e)) .$$

La formule (1.3.2) en résulte trivialement. Pour (1.3.1), on peut supposer k algébriquement clos.

Si C_o est lisse, $\Omega_{C_o}(e) \simeq \omega_{C_o}(e) \simeq \mathcal{O}_{C_o}(e)$ est un faisceau inversible de degré 1, d'où $\dim H^0(C_o, \Omega_{C_o}(e)) = 1$ dans ce cas.

Sinon, le normalisé $\pi : \tilde{C}_o \to C_o$ de C_o est isomorphe à $\mathbb{P}^1$ et un calcul local montre que le morphisme canonique

$$\Omega_{C_o}(e) \longrightarrow \pi_* \Omega_{\tilde{C}_o}(e)$$

est surjectif à noyau de longueur un, concentré au seul point singulier de C_o. L'assertion dans ce cas résulte de la suite exacte de cohomologie : on utilise que

$$H^0(C,\pi_*\Omega_C(e)) \simeq H^0(\mathbb{P}^1,\Omega_{\mathbb{P}^1}(e)) = 0 \quad (\text{car } \deg_{\mathbb{P}^1}(e)) = -1).$$

Cela démontre (iii).

Prouvons (iv). La courbe C_o est ici polygone de Néron à un côté. La théorie des déformations des points quadratiques ordinaires montre qu'il existe $u \in \Lambda[[t]]$ tel que $u = 0$ soit l'image du lieu de non lissité de C. D'après (II.1.15.), sur $\mathrm{Spec}(\Lambda[[t]]/(u))$, C est isomorphe à l'image réciproque du polygone de Néron à un côté standard (1.1). La propriété universelle de $\Lambda[[t]]$ implique alors que $\mathrm{Spec}(\Lambda[[t]]/(u))$ est non ramifié sur $\mathrm{Spec}(\Lambda)$, donc que $\Lambda[[t]] \simeq \Lambda[[u]]$. Ceci achève la démonstration pour C_o irréductible.

1.4 Le cas général.

On peut supposer que C_o est le polygone de Néron standard à n côtés sur k, déduit de $P^1 \times \mathbb{Z}/n$ par recollement. Soit H_o le sous-groupe cyclique d'ordre n de C_o, image de $\{1\} \times \mathbb{Z}/n$.

Soit D'' le foncteur des déformations de $(C_o, +, H_o)$: $D''(A)$ est l'ensemble des classes d'isomorphie de systèmes $(C,+,H)$ ($(C,+)$ courbe elliptique généralisée sur A, H sous-groupe de C^{reg} isomorphe à $\underline{\mathbb{Z}/n}$), munis d'un isomorphisme de leur fibre spéciale avec $(C_o,+,H_o)$.

Lemme 1.4.1. On a $D'' \xrightarrow{\sim} D$.

Cela résulte de ce que C_n^{reg} est fini étale sur A (car n est premier à p).

1.4.2 Dans la fin de la démonstration, on ne suppose plus que n est premier à p (cette hypothèse ne servira que via 1.4.1). Soit $(C,+,H)$ comme plus haut (sur A local complet). Le groupe H agit librement sur C (car H_o agit librement sur C_o), de sorte que C/H (qui existe car C est projectif) est plat sur A. La loi $+$ passe au quotient, et $(C/H,+)$ est une déformation du polygone de Néron à un côté $(C_o/H_o,+)$. Notant D_1 le foncteur des déformations de $(C_o/H_o,+)$, on obtient

ainsi un morphisme de D'' dans D_1 .

Lemme 1.4.3. Le morphisme 1.4.2 de D'' dans D_1 est un isomorphisme (on ne suppose pas ici n premier à p)

D'après EGA IV. 18.1.2 pour A artinien, joint au théorème d'existence en géométrie formelle EGA III.5. pour A local complet, pour toute déformation $(C,+)$ de $(C_o/H_o,+)$ sur A , il existe une et une seule déformation C de la courbe C_o sur A , munie de $\pi_o : C_o \to C_o/H_o$. On applique alors II.1.17.

Achevons la démonstration de 1.2. D'après 1.4.1 et 1.4.3, D est isomorphe à D_1 étudié en 1.3 et vérifié donc 1.2 (ii) (iii). L'assertion (iv) résulte de l'assertion analogue pour D_1 , car l'image du sous-schéma de non lissité est la même pour C et C/H (notations de 1.4.2).

2. Construction de $\mathfrak{M}_*$.

Lemme 2.1. : $\mathfrak{M}$ (défini en 0.1) est un champ pour la topologie fpqc .

Preuve : Soit $S' \to S$ un morphisme fpqc et $p' : C' \to S'$ une courbe elliptique généralisée munie d'une donnée de descente. Les sous-schémas S'_n de S' définis en II.1.15 se descendent en des sous-schémas S_n de S (descente fpqc de sous-schémas fermés). Par localisation sur S , pour la topologie de Zariski, on peut donc supposer que les fibres géométriques de C' sont lisses ou ont n composantes irréductibles. Le sous-schéma C'_n de C' est alors fini sur S' (cf. II.1.20.) et rencontre chaque composante irréductible de chaque fibre géométrique de C' . Le faisceau inversible $\mathcal{L} = \mathcal{O}_{C'}(C'_n)$ est relativement ample ; il est muni d'une donnée de descente. L'assertion résulte donc de la descente des schémas quasi-projectifs (SGA 1, VIII.7.8 et SGA 1, VIII.5.2).

Rappellons que pour $\mathcal{S}$ un champ sur (Sch/S) , on identifie les 1-morphismes $\xi : X \to \mathcal{S}$ d'un S-schéma X dans $\mathcal{S}$ aux objets de $\mathcal{S}(X)$ ([8]).

2.2. M. Artin a démontré un critère maniable pour prouver qu'un foncteur est représentable par un espace algébrique ([2] , [3]). La même démonstration fournit le critère suivant pour vérifier qu'un champ est algébrique.

Théorème 2.3. (M. Artin). Soit S un schéma de type fini sur un corps ou sur un anneau excellent de Dedekind. Soit $\mathcal{S}$ une catégorie fibrée en groupoïdes sur (Sch/S).

$\mathcal{S}$ est un champ algébrique localement de type fini sur S si (et seulement si)

(0) $\mathcal{S}$ est un champ pour la topologie étale.

(1) $\mathcal{S}$ est localement de présentation finie, (i.e. pour chaque système projectif filtrant de S-schémas affines $\mathrm{Spec}(A_i)$, le foncteur canonique

$$\varinjlim_i \mathcal{S}(\mathrm{Spec}(A_i)) \longrightarrow \mathcal{S}(\varprojlim_i \mathrm{Spec}(A_i))$$

définit une équivalence des catégories.).

(2) Soient $\xi, \eta \in \mathrm{Ob}(\mathcal{S}(X))$ deux 1-morphismes d'un S-schéma X de type fini sur S vers $\mathcal{S}$. Alors $\underline{\mathrm{Isom}}\,(X; \xi, \eta)$ est un espace algébrique localement de type fini sur S .

(3) Soit k_o un $\mathcal{O}_S$-corps de type fini (i.e. $\mathrm{Spec}(k_o)$ est de type fini sur S), et soit ξ_o un 1-morphisme de $\mathrm{Spec}(k_o)$ vers $\mathcal{S}$. Il existe un anneau local complet R , un morphisme u du spectre d'une extension séparable finie k'_o de k_o dans le point fermé s de $\mathrm{Spec}(R)$, et un diagramme commutatif

$$\begin{array}{ccc} \mathrm{Spec}(k'_o) & \longrightarrow & \mathrm{Spec}(k_o) \\ \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle \xi_o} \\ \mathrm{Spec}(R) & \xrightarrow{\xi} & \mathcal{S} \end{array}$$

avec ξ formellement étale en s .

(4) Si ξ est un 1-morphisme d'un S-schéma de type fini X dans $\mathcal{S}$ et que ξ est formellement étale en un point x de type fini sur S , alors ξ est formellement étale en chaque point de type fini sur S dans un voisinage ouvert de x .

Remarques 2.4.

(i) Si les corps résiduels de type fini de S sont parfaits, pour établir que $\mathcal{S}$ est un champ algébrique on peut remplacer (0) - (4) par (0),(1),(2),(3'),(4), où (3') est la condition suivante :

(3') Soient $s \in S$ et k_o une extension finie de $k(s)$. On suppose que $u : \mathrm{Spec}(k_o) \to S$ est de type fini. Par hypothèse, $k(s)$ est alors parfait et $k_o/k(s)$ séparable. Il existe donc un unique anneau local complet $\Lambda(k_o)$ de corps résiduel k_o, muni de $\bar{u} : \mathrm{Spec}(\Lambda(k_o)) \to S$ formellement étale et prolongeant u. Pour $\xi_o \in \mathrm{Ob}\, \mathcal{S}(k_o)$, nous noterons $\underline{\mathrm{Def}}(\xi_o)$ la catégorie suivante sur la duale de $\hat{C}_{\Lambda(k_o)}$: pour $A \in \mathrm{Ob}\, \hat{C}_{\Lambda(k_o)}$, un objet de $\underline{\mathrm{Def}}(\xi_o)(A)$ est un objet ξ de $\mathcal{S}(A)$, muni d'un isomorphisme $\xi_o \xrightarrow{\sim}$ (image de ξ dans $\mathcal{S}(k_o)$). La condition (3') est la conjonction de (3'a) et (3'b) :

(3'a) Les objets de $\mathcal{S}$ n'ont pas d'automorphismes infinitésimaux; plus précisément pour k_o et ξ_o comme ci-dessus, et ξ_o' l'image réciproque de ξ_o sur $k_o[\varepsilon]$ ($\varepsilon^2 = 0$), on a $\mathrm{Aut}(\xi_o') \xrightarrow{\sim} \mathrm{Aut}(\xi_o)$. Cette condition, et (2), implique que les objets de $\underline{\mathrm{Def}}(\xi_o)(A)$ n'ont pas d'automorphismes non triviaux.

(3'b) Pour k_o et ξ_o comme plus haut, le foncteur

$$A \to \text{l'ensemble des classes d'isomorphies dans } \mathrm{Def}(\xi_o)(A)$$

est effectivement prorepréstentable (par un anneau local complet R et $\xi \in \mathcal{S}(R)$ se réduisant selon ξ_o).

Il suffit même de vérifier (3'b) après extension des scalaires à une extension finie de k_o.

(ii) Si S est de type fini sur un corps ou sur un anneau excellent de Dedekind ayant un nombre infini de points et si les anneaux locaux complets R qui apparaissent dans la condition (3'b) sont tous normaux et de même dimension de Krull, on peut supprimer la condition (4).

(Pour le lecteur familier avec [2], (i) est facile à prouver. Pour (ii), voir ([2], Thm. 3.9).

Le polygone de Néron à n côtés standard définit un morphisme

$$f_n : \mathrm{Spec}(\mathbb{Z}[\tfrac{1}{n}]) \longrightarrow \mathfrak{M}^*$$

Théorème 2.5. :

(i) $\mathfrak{M}_*$ (défini en 0.2) est un champ algébrique lisse sur $\mathrm{Spec}(\mathbb{Z})$.

(ii) L'image $\mathfrak{M}_*^\infty$ du schéma de non-lissité de la courbe elliptique généralisée universelle au-dessus de $\mathfrak{M}_*$ est réunion des images de f_n $(n \geq 1)$.

Preuve. Pour prouver que $\mathfrak{M}_*$ est un champ algébrique, nous utilisons le critère 2.3 (avec $S = \mathrm{Spec}(\mathbb{Z})$) . Passons en revue les conditions (0) à (4) .

(0) résulte de 2.1.

(1) résulte par des arguments standard de EGA IV.8.8.

(2) Soient X un S-schéma de type fini et $(p_i : C_1 \to X,+)$, $(p_2 : C_2 \to X,+)$ deux courbes elliptiques généralisées. Prouvons que $\mathrm{Isom}_X((C_1,+),(C_2,+))$ est représentable. Ce foncteur est un faisceau fpqc (2.1) de sorte que le problème est local. On peut donc supposer que les fibres géométriques de C_1 sont lisses ou à n côtés (n convenable) et qu'il existe $\varphi : \underline{\mathbb{Z}/n} \hookrightarrow C_1$ dont l'image rencontre chaque composante irréductible de chaque fibre géométrique de C_1 . Le morphisme $f \to f\circ\varphi(1)$ envoye Isom dans le sous-schéma ouvert de C_n^{reg} formé des g tels que les g^k rencontrent toutes les composantes des fibres géométriques. Il résulte de l'assertion suivante que ce morphisme est relativement représentable, donc Isom représentable.

(*) Pour C_i à fibres lisses ou à n côté, et muni de $H_i \subset C_i^{reg}$, H_i isomorphe à $\underline{\mathbb{Z}/n}$, rencontrant toutes les composantes de toutes les fibres géométriques (i=1,2), $\mathrm{Isom}((C_1,H_1,+),(C_2,H_2,+))$ est représentable.

D'après II 1.17, le morphisme

$$\mathrm{Isom}((C_1,H_1,+),(C_2,H_2,+)) \to \mathrm{Isom}((C_1/H_1,e),(C_2/H_2,e))$$

est en effet représentable par un morphisme étale, tandis qu'il résulte de la théorie du foncteur de Hilbert que $\mathrm{Isom}((C_1/H_1,e)(C_2/H_2,e))$ est représentable.

(3') Soit k_o un $\mathrm{Spec}(\mathbb{Z})$-corps de type fini; c'est donc un corps fini.

(3')a) résulte de 1.2.(i).

(3')b) résulte de 1.2.(ii).

(4) D'après 1.2 (iii), les foncteurs de déformations sont proreprésentés par des anneaux réguliers de dimension 2. D'après 2.4 (ii), la condition (4) est automatiquement vérifiée.

La lissité de $\mathfrak{M}_*$ résulte de sa lissité formelle 1.2.(iii). La seconde assertionde 2.5. résulte de II 1.15. et de 1.2.(iv).

Remarque 2.6. $\mathfrak{M}_*$ est horriblement non séparé! Il résultera de (IV.2.2) que le sous-champ ouvert $\mathfrak{M}_1$ de $\mathfrak{M}_*$ classifiant les courbes elliptiques généralisées C/S à fibres géométriques intègres est propre et lisse sur $\mathbb{Z}$. Le "fourre-tout" $\mathfrak{M}_*$ nous sera utile pour compactifier des modules de courbes elliptiques avec niveau.

Le sous-champ ouvert $\mathfrak{M}_{(n)}[1/n]$ de $\mathfrak{M}_*[1/n]$ qui classifie les courbes elliptiques généralisées C/S (n inversible sur S) à fibres géométriques lisses ou des polygones de Néron à n côtés est lui aussi propre et lisse sur $\mathrm{Spec}(\mathbb{Z}[1/n])$. Il est toutefois moins naturel que $\mathfrak{M}_1[1/n]$.

IV. Structures de niveau.

Dans ce chapitre, nous définissons et étudions les schémas de module de courbes elliptiques dont les points de division par n sont munis de structures additionnelles. Nous étudions en détail la structure à l'infini de ces schémas. Leur réduction modulo p, pour $p|n$, ne sera considérée sérieusement qu'au chapitre suivant.

1. Contractions.

1.1. Soit $p : C \to S$ une courbe stable de genre un et $H \subset C^{reg}$ un sous-schéma fini localement libre sur S de l'ouvert de lissité de C. On vérifie fibre par fibre que H est automatiquement un diviseur de Cartier sur C. On suppose que les fibres de H sont non vides.

Proposition 1.2. *Il existe un et un seul S-schéma $\overline{C}$, muni de $u : C \to \overline{C}$, tel que*

(a) *$\overline{C}$ est une courbe stable de genre un sur S ;*

(b) *pour tout point géométrique $\overline{s}$ de S, $\overline{C}_{\overline{s}}$ se déduit de $C_{\overline{s}}$ en contractant en un point chacune des composantes irréductibles de $C_{\overline{s}}$ qui ne rencontrent pas H_s*

A. Existence. Un argument de passage à la limite nous ramène à supposer S noethérien. Pour tout $\overline{s}$ et tout $n > 0$, on a $H^0(C_{\overline{s}}, \mathcal{O}(-nH_{\overline{s}})) = 0$. Par dualité (I 2.2 et II 1.2), on a donc $H^1(C_{\overline{s}}, \mathcal{O}(nH_{\overline{s}})) = 0$. D'après EGA III 7.8, les $p_*\mathcal{O}(nH)$ ($n > 0$) sont localement libres de formation compatible à tout changement de base. Le même énoncé vaut pour $n = 0$ (II.1.6). Soit $\mathcal{G}$ l'algèbre homogène

$$\mathcal{G} = \bigoplus_{n>0} p_* \mathcal{O}(nH) .$$

Pour $C_{\overline{s}}$ irréductible, $\mathcal{O}(H_{\overline{s}})$ est ample, et $\mathcal{G}_{\overline{s}}$ engendré par $\bigoplus_{n \leq A} H^0(\mathcal{O}(nH_{\overline{s}}))$, avec A indépendant de s.

Supposons que $C_{\overline{s}}$ soit un polygone de Néron, et soit $\overline{C}_{\overline{s}}$ le polygone de Néron qui s'en déduit en contractant en un point chaque composante irréductible qui

ne rencontre pas H . On vérifie que

$$H^0(\overline{C}_{\overline{s}}, \mathcal{O}(nH_{\overline{s}})) \xrightarrow{\sim} H^0(C_{\overline{s}}, \mathcal{O}(nH_{\overline{s}})) \quad .$$

Sur $\overline{C}_{\overline{s}}$, $\mathcal{O}(nH_{\overline{s}})$ est ample, et $G_{\overline{s}}$ est engendré par $\bigotimes_{n\leq B} H^0(\mathcal{O}(nH_{\overline{s}}))$ avec B indépendant de s .

L'algèbre homogène $G = \bigoplus_n p_* \mathcal{O}(nH)$ est donc de type fini, et son spectre homogène $\overline{C}$ est propre et plat sur S , de formation compatible à tout changement de base. Le morphisme naturel $u : C \to \overline{C}$ vérifie (a) et (b) .

B. Unicité. Soit

$$\begin{array}{ccc} C & \xrightarrow{u} & \overline{C} \\ & {\scriptstyle p}\searrow \quad \swarrow{\scriptstyle \overline{p}} & \\ & S & \end{array}$$

vérifiant (i) et (ii). On vérifie fibre par fibre que u induit un isomorphisme $u^{-1}(\overline{C}^{reg}) \xrightarrow{\sim} C^{reg}$ (EGA IV 17.8.2). Les arguments de A. montrent que $\mathcal{O}_{\overline{C}}(H)$ est ample et que $\overline{G} = \bigoplus \overline{p}_* \mathcal{O}_{\overline{C}}(nH)$ est plat et commute à tout changement de base. On vérifie fibre par fibre que $\overline{G} \xrightarrow{\sim} G$, et $\overline{C} = \mathrm{Sp}\ h(G)$.

Proposition 1.3. *Soit $p : C \to S$ une courbe elliptique généralisée dont les fibres géométriques sont lisses ou sont des nm-gones. Il existe une et une seule courbe elliptique généralisée $\overline{p} : \overline{C} \to S$, munie de $u : C \to \overline{C}$, telle que*

(i) *Les fibres géométriques de $\overline{C}$ sont lisses ou des n-gones. $\overline{C}_{\overline{s}}$ se déduit de $C_{\overline{s}}$ en contractant en un point les composantes irréductibles de $C_{\overline{s}}$ adhérence de celles des composantes connexes de $C^{reg}_{\overline{s}}$ dont l'ordre dans $\pi_0(C^{reg}_{\overline{s}})$ ne divise pas n .*

(ii) *Le diagramme suivant est commutatif*

$$\begin{array}{ccc} u^{-1}(\overline{C}^{reg}) \times_S C & \xrightarrow{+} & C \\ \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle u} \\ \overline{C}^{reg} \times_S \overline{C} & \xrightarrow{+} & \overline{C} \end{array}$$

Localement pour la topologie fppf de S, il existe $H \subset C$ comme en 1.1, qui rencontre exactement celles des composantes irréductibles des $C_{\bar{s}}$ qu'on ne désire pas contracter (on peut prendre $H = C_n$, fini et plat d'après (II.1.20)). D'après 1.2, il existe une et une seule courbe stable de genre un $\overline{C}$, munie de $u : C \to \overline{C}$, qui vérifie (i). Le sous-groupe $u^{-1}(\overline{C}^{reg})$ de C^{reg} agit sur $\overline{C}$ par transport de structure; puisque $u^{-1}(\overline{C}^{reg}) \xrightarrow{\sim} C^{reg}$, ceci fournit la structure de courbe elliptique généralisée voulue sur $\overline{C}$.

Exemple 1.4. Soit C/S une courbe elliptique généralisée, et appliquons 1.3 avec $n = 1$. Localement sur S, l'hypothèse de 1.3 est vérifiée, pour m convenable (II.1.15). Il existe donc une et une seule courbe elliptique généralisée $c(C)$ sur S, à fibres géométriques irréductibles, munie de $u : C \to c(C)$ et telle que u induise un isomorphisme

$$(C^{reg})^0 \xrightarrow{\sim} c(C)^{reg} \quad . \tag{1.4.1}$$

D'après la démonstration de 1.3.4, la courbe $c(C)$ est en effet uniquement déterminée par la condition (i) de 1.3, qui résulte de (1.4.1), tandis que la structure de courbe généralisée est uniquement déterminée par la section neutre (II.2.7), implicite dans 1.4.1.

1.5. Soit S le spectre d'un anneau de valuation discrète complet à corps résiduel algébriquement clos, et η, s ses points génériques et spéciaux. Pour toute extension finie $k(\eta')$ de $k(\eta)$, nous noterons (S', η', s') le trait normalisé de S dans $k(\eta')$. Soit C_η une courbe elliptique sur η. Nous disons que C_η à réduction stable si le modèle minimal de C_η sur S est une courbe stable de genre un.

Proposition 1.6. (i) *Il existe une extension finie $k(\eta')$ de $k(\eta)$ telle que la courbe $C_{\eta'} = C_\eta \otimes_\eta \eta'$ ait réduction stable sur η'.*

(ii) *Si C_η à réduction stable, le modèle minimal $\widetilde{C}$ de C_η sur S admet une unique structure de courbe elliptique généralisée prolongeant celle de C_η.*

(iii) *Si de plus les points d'ordre n de C_η sont définis sur $k(\eta)$, soit le modèle minimal $\widetilde{C}$ de C est lisse, soit $\widetilde{C}_s$ est un m-gone, avec $n|m$, et il*

existe une courbe elliptique généralisée C sur S, de fibre spéciale lisse ou un n-gone et un isomorphisme α de sa fibre générique avec C_η.

(iv) Le couple (C,α) est unique à isomorphisme unique près.

Preuve. (i). C'est un théorème de Néron et Kodaira ([4] ou [20] ou [14]).

(ii). La propriété universelle du modèle de Néron assure que $e \in C_\eta(\eta)$ se prolonge en une section de $\widetilde{C}^{reg}$ sur S. Si $u \in \widetilde{C}^{reg}(S)$, la translation $u+$ de C_η se prolonge par transport de structure en un automorphisme de $\widetilde{C}$; de même, $x \to -x$ se prolonge à $\widetilde{C}$.

Soit U le plus grand ouvert de $\widetilde{C}$ tel que la loi $+$ de C_η se prolonge en $+ : U \times C \to C$. Il suffit de prouver que $U = C^{reg}$: ceci acquis, les identités exprimant que $+$ est une structure de courbe elliptique généralisée résulterons de la densité schématique de C_η dans $\widetilde{C}$. Pour $v \in \widetilde{C}^{reg}(S)$, U est stable par translation par v : on prolonge $+$ à $v+U$ par $(v+u) + x = v+(u+x)$. Puisque U est aussi stable par localisation étale sur S (on le vérifie par un argument de descente; rappelons que la formation du modèle minimal est compatible à la localisation étale sur S), il suffit de montrer que $U_s \neq \phi$.

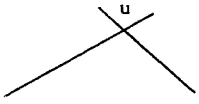
Soit x un point maximal (= générique) de $\widetilde{C}_s$, et soit S_1 le trait spectre de l'anneau local de $\widetilde{C}$ en x. Puisque $\widetilde{C}$ est lisse sur S en x, $\widetilde{C}_1 = C \times_S S_1$ est encore un modèle minimal sur S_1. Soit $u \in C_1(S)$ défini par l'inclusion $S_1 \hookrightarrow \widetilde{C}$. Par transport de structure, la translation $u+$ de la fibre générique de $\widetilde{C}_1$ se prolonge en un automorphisme de C_1, d'où

$$+ : S_1 \times_S \widetilde{C} \longrightarrow \widetilde{C} .$$

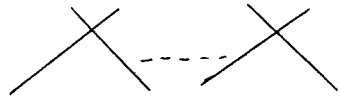
Ecrivant S_1 comme limite projective des voisinages de x, on trouve que le morphisme $+ : C_\eta \times C_\eta \to C_\eta$ se prolonge en $+ : U \times_S \widetilde{C} \to \widetilde{C}$, avec $x \in U$.

(iii). On sait que $\widetilde{C}_n$ est quasi-fini et plat. Puisque d'après l'hypothèse et la propriété universelle du modèle de Néron, tous les points géométriques de $(\widetilde{C}_\eta)_n$ proviennent de sections de $\widetilde{C}_n$ sur S, ce groupe est même fini sur S, et $(\widetilde{C}_s)_n$ est de rang n^2. La fibre spéciale $\widetilde{C}_s$ est donc lisse ou un m-gone, avec $n|m$ (cf II 1.18), et on applique 1.3. pour obtenir C par contraction.

(iv). Soit C une courbe elliptique généralisée sur S, de fibre générale C_η, et telle que C_s soit lisse ou un polygone à n côtés. En un point de non lissité u de C, C est formellement isomorphe au complété à l'origine de la courbe affine dans A^2_S d'équation $xy = t^k$, pour k convenable. Par homogénéité, k ne dépend pas du point choisi. Pour $k > 1$, C est singulier en u. Ces singularités se résolvent en éclatant de façon itérée les points singuliers, ce procès aboutissant à remplacer u par $k-1$ droites projectives:



donne



(cf. [8]). Soit $\tilde{C}$ la courbe résolue. Il n'existe pas de courbe exceptionnelle de première espèce contenue dans $\tilde{C}_s$, de sorte que $\tilde{C}$ est le modèle minimal de C_η. La courbe C est lisse si et seulement si le modèle minimal $\tilde{C}$ de C_η est lisse, auquel cas $C = \tilde{C}$. Sinon, $\tilde{C}_s$ est un polygone de Néron à nk côtés, et C s'en déduit par contraction de la façon utilisée dans la preuve de l'existence.

2. Structures de niveau n.

2.1. Soit n un entier. Nous ne considérerons dans ce § que des schémas S sur lesquels n est inversible.

Dans ce §, nous noterons $\mathcal{M}_{(n)}$ le champ algébrique sur $\mathbb{Z}[1/n]$ qui classifie les courbes elliptiques généralisées C/S, de fibres géométriques lisses ou des polygones de Néron à n côtés. D'après (II.1.15), $\mathcal{M}_{(n)}$ est un ouvert de $\mathcal{M}_*$, donc un champ algébrique (III.2.5) lisse sur $\mathbb{Z}[1/n]$. Soit f_n la section de $\mathcal{M}_{(n)}$ définie par la courbe 1.9 sur $\mathbb{Z}[1/n]$.

Proposition 2.2. *Le champ algébrique $\mathcal{M}_{(n)}$ est propre et lisse sur $\mathbb{Z}[1/n]$. Son lieu à l'infini $\mathcal{M}^\infty_{(n)} = \mathcal{M}_{(n)} \cap \mathcal{M}^\infty_*$ est l'image de f_n.*

La seconde assertion n'est mise que pour rappel. Elle résulte de III.2.5. et implique que $\mathcal{M}^0_{(n)}$ est dense dans $\mathcal{M}_{(n)}$. La propreté résulte alors de 1.6 et du critère valuatif de propreté [8].

DeRa-68

2.3. Pour C/S du type considéré, C_n^{reg} est fini étale de rang n^2 (II.1.20), donc localement isomorphe à $(\mathbb{Z}/n)^2$ (pour la topologie étale). Une structure de niveau n sur C est un isomorphisme

$$\alpha : C_n \xrightarrow{\sim} (\mathbb{Z}/n)^2$$

Définition 2.4. $\mathcal{M}_n[1/n]$ est le champ algébrique sur $\mathbb{Z}[1/n]$ suivant : pour S un schéma sur lequel n est inversible, $\mathcal{M}_n[1/n](S)$ est la catégorie des courbes elliptiques généralisées C/S, de fibres géométriques lisses ou des polygones de Néron à n côtés, munies d'une structure de niveau n.

Il est clair que $\mathcal{M}_n[1/n]$ est fini étale et représentable sur $\mathcal{M}_{(n)}$, et même un espace principal homogène de groupe $GL(2, \mathbb{Z}/n)$. On note $\mathcal{M}_n^{\infty}[1/n]$ l'image réciproque de $\mathcal{M}_{(n)}^{\infty}$, image du sous-schéma de non lissité de la courbe universelle sur $\mathcal{M}_n[1/n]$. Le théorème suivant résulte aussitôt de 2.2.

Théorème 2.5. $\mathcal{M}_n[1/n]$ est propre et lisse sur $\mathbb{Z}[1/n]$, et $\mathcal{M}_n^{\infty}[1/n]$ est fini étale sur $\mathbb{Z}[1/n]$.

2.6. Rappelons qu'un champ algébrique $\mathcal{S}$ "est" un espace algébrique si les objets qu'il classifie n'ont pas d'automorphismes. Plus précisément, si pour tout corps algébriquement clos, k, les objets de $\mathcal{S}(k)$ n'ont pas d'automorphisme non trivial, alors

a) pour tout schéma S, les objets de $\mathcal{S}(S)$ n'ont pas d'automorphisme non trivial;

b) le foncteur $S \mapsto$ (l'ensemble des classes d'isomorphie dans $\mathcal{S}(S)$) est représentable par un espace algébrique.

Théorème 2.7. Si $n \geq 3$, $\mathcal{M}_n[1/n]$ est un espace algébrique.

Soient C une courbe elliptique généralisée sur un corps algébriquement clos k, lisse ou un polygone de Néron à n côtés. Il faut prouver qu'un automorphisme σ de C, trivial sur C_n, est l'identité. Pour C une courbe elliptique, on applique ([26], app. à Exp. 17). Pour C un polygone de Néron, on vérifie sur II.1.10 que $\mathrm{Aut}(C)$ agit fidèlement sur C_n.

Variante 2.8. Cet argument, et III.2.1 , impliquent aussitôt que le foncteur F_n : $S \mapsto$ (l'ensemble des classes d'isomorphie de courbes elliptiques généralisées sur S munies d'une structure de niveau n) est un faisceau pour la topologie fpqc . Les arguments de III.2.5. montrent alors que ce foncteur vérifie le critère de représentabilité de M. Artin. Pour prouver que F_n est représentable par un espace algébrique ($n \geq 3$) , il n'est donc pas nécessaire de généraliser au préalable le critère de M. Artin au cas des champs algébriques.

Corollaire 2.9. Si $n \geq 3$, $\mathfrak{M}_n[1/n]$ est un schéma projectif et lisse sur $\mathbb{Z}[1/n]$.

Un espace algébrique régulier en courbes sur $\mathbb{Z}$ est en effet toujours quasi-projectif, donc un schéma. Voici une démonstration plus constructive : par voie transcendante (cf. §5), on vérifie qu'après extension des scalaires à $\mathbb{C}$, $\mathfrak{M}_n^\infty$ rencontre chaque composante irréductible de $\mathfrak{M}_n$. Par spécialisation, on en déduit que le diviseur $\mathfrak{M}_n^\infty$ rencontre chaque composante irréductible de chaque fibre géométrique de $\mathfrak{M}_n$ (utiliser que $\mathfrak{M}_n$ est propre et lisse). Dès lors, $\mathcal{O}(\mathfrak{M}_n^\infty)$ est un faisceau inversible relativement ample.

3. Structures de niveau H

3.1 Soient n un entier et H un sous-groupe de $GL(2, \mathbb{Z}/n)$. Soient S un schéma sur lequel n est inversible et C une courbe elliptique sur S . Pour tout S-schéma T , soit $F(T)$ l'ensemble des structures de niveau n sur C_T , l'image réciproque de C sur T . Le foncteur F est représenté par un revêtement fini étale de S qui est un espace principal homogène de groupe $GL(2, \mathbb{Z}/n)$. Soit F_H le faisceau pour la topologie étale engendré par le préfaisceau

$$T \longmapsto F_H(T) = F(T)/H$$

(H agissant à gauche,il vaudrait peut-être mieux écrire $H\backslash F(T)$) . Dans le langage canonique,

$$F_H = \underline{\mathrm{Hom}}(C_n, (\mathbb{Z}/n)^2)/H \quad .$$

Ce foncteur est représenté par un revêtement fini étale de S .

Une structure de niveau H sur C est un élément de $F_H(S)$. Un isomorphisme $\alpha : C_n \xrightarrow{\sim} (\mathbb{Z}/n)^2$ définit une structure de niveau H , et deux tels isomorphismes définissent la même structure si et seulement si, localement sur S , il existe $g \in H$ tel que $g\alpha = \beta$ Ce g est uniquement déterminé, donc constant sur chaque composante connexe de S . On prendra garde qu'une structure de niveau H ne provient en général pas d'un $\alpha : C_n \xrightarrow{\sim} (\mathbb{Z}/n)^2$. Elle ne provient de tels α que localement pour la topologie étale. Par exemple, pour $H = GL(2, \mathbb{Z}/n)$, C a une et une seule structure de niveau H ; elle ne vient d'un α que si C_n est isomorphe à $(\mathbb{Z}/n)^2$ sur S .

Définition 3.2. $\mathcal{M}_H^0[1/n]$ est le champ algébrique suivant : pour S un schéma sur lequel n est inversible, $\mathcal{M}_H^0[1/n]$ (S) est la catégorie des courbes elliptiques C/S , munies d'une structure de niveau H (les morphismes sont les isomorphismes).

Il est clair que $\mathcal{M}_H^0[1/n]$ est fini étale et localement représentable sur $\mathcal{M}_1^0[1/n]$.

Définition 3.3. Le champ algébrique $\mathcal{M}_H$ est le normalisé de $\mathcal{M}_1$ dans $\mathcal{M}_H^0[1/n]$.

Théorème 3.4. (i) $\mathcal{M}_H$ est propre sur $\mathrm{Spec}(\mathbb{Z})$.

(ii) $\mathcal{M}_H[1/n]$ est lisse sur $\mathrm{Spec}(\mathbb{Z}[1/n])$, et $\mathcal{M}_H^0[1/n]$ est le complément d'un sous-champ $\mathcal{M}_H^\infty[1/n]$ fini et étale sur $\mathrm{Spec}(\mathbb{Z}[1/n])$.

Preuve (i) Par définition, $\mathcal{M}_H$ est fini et relativement représentable sur $\mathcal{M}_1$ Sa propreté résulte donc de celle de $\mathcal{M}_1$.

(ii) L'assertion résulte du lemme d'Abhyankhar (SGA 1,XIII5.) appliquable ici parce que $\mathcal{M}_1[1/n]$, est lisse sur $\mathbb{Z}[1/n]$, que $\mathcal{M}_1^\infty[1/n]$ est un diviseur de $\mathcal{M}_1[1/n]$, lisse sur $\mathbb{Z}[1/n]$, et dont le point générique est de caractéristique 0 , et que $\mathcal{M}_H^0[1/n]$ est fini étale sur $\mathcal{M}_1[1/n] - \mathcal{M}_1^\infty[1/n]$.

En 6.7, nous donnerons de 3.4 une démonstration "modulaire" .

Pour $H = \{e\}$, nous poserons $\mathcal{M}_n = \mathcal{M}_H$. Cette notation est légitimée par la proposition suivante.

Proposition 3.5. Pour $H = \{e\}$, $\mathcal{M}_H[1/n]$ est le champ $\mathcal{M}_n[1/n]$ de 2.4.

La construction 1.4 définit un morphisme de champs

$$c : \mathcal{M}_n[1/n] \to \mathcal{M}_1[1/n] : (C,\alpha) \mapsto c(C) \quad .$$

Puisque $\mathcal{M}_n[1/n]$ est normal (même lisse sur $\mathbb{Z}[1/n]$) , propre sur $\mathbb{Z}[1/n]$, et que clairement $\mathcal{M}_n^o[1/n] \simeq \mathcal{M}_H^o[1/n]$, il nous suffit de prouver que c est fini et localement représentable. Il est clair que les fibres de c sont finies. Pour tester la représentabilité locale, il suffit dès lors de vérifier (cf. 2.6):

Lemme 3.5.1. Pour k un corps algébriquement clos, C un objet de $\mathcal{M}_n[1/n]$ (k) et $c(C)$ son image dans $\mathcal{M}_1(k)$, l'application naturelle $i : \mathrm{Aut}(C) \to \mathrm{Aut}(c(C))$ est injective.

Pour $n \geq 3$, $\mathrm{Aut}(C)$ est trivial (cf.2.7) . Pour $n = 2$, $\mathrm{Aut}(C) = \{\pm 1\}$. Enfin, pour $n = 1$, i est l'identité.

3.6. Soient n et m deux entiers, avec $n|m$. Soient $H \subset GL(2, \mathbb{Z}/n)$, et H' son image réciproque dans $GL(2, \mathbb{Z}/nm)$. Pour E une courbe elliptique sur S , une structure de niveau nm $E_{nm} \xrightarrow[\alpha']{\sim} (\mathbb{Z}/nm)^2$ définit une structure de niveau n , α , rendant commutatif le diagramme

$$\begin{array}{ccc} E_{nm} & \xrightarrow[\alpha']{\sim} & (\mathbb{Z}/nm)^2 \\ \Big\downarrow{\scriptstyle x^m} & & \Big\downarrow \\ E & \xrightarrow[\alpha]{\sim} & (\mathbb{Z}/n)^2 \end{array}$$

Pour nm invertible sur S , cette construction définit un isomorphisme du faisceau des H'-structures sur E avec celui des H-structures. On a

$$\mathcal{M}_{H'}^o[1/nm] \simeq \mathcal{M}_H^o[1/n][1/m] \quad .$$

Puisque $\mathcal{M}_H^o[1/n]$ est fini et étale sur $\mathcal{M}_1^o[1/n]$, c'est le normalisé de $\mathcal{M}_1^o[1/n]$ dans $\mathcal{M}_{H'}^o[1/nm]$. On en déduit un isomorphisme

$$\mathcal{M}_{H'} \simeq \mathcal{M}_H \ .$$

Le champ $\mathcal{M}_H$ ne dépend donc que du sous-groupe ouvert K de $GL(2, \hat{\mathbb{Z}})$ image réciproque de H . Nous le noterons parfois $\mathcal{M}_K$.

3.7. Soient n et m deux entiers premiers entre eux , $H \subset GL(2, \mathbb{Z}/n)$ et $I \subset GL(2, \mathbb{Z}/m)$. Soient K et L les images réciproques de H et I dans $GL(2, \hat{\mathbb{Z}})$. Les morphismes de réduction mod n et m induisent un isomorphisme $GL(2, \mathbb{Z}/nm) \xrightarrow{\sim} GL(2, \mathbb{Z}/n) \times GL(2, \mathbb{Z}/m)$. Via cet isomorphisme, $K \cap L$ est l'image réciproque de $H \times I \subset GL(2, \mathbb{Z}/n) \times GL(2, \mathbb{Z}/m)$.

Construction 3.8. Avec les notations précédentes,

$$\mathcal{M}_K^o[1/n] \times_{\mathcal{M}_1} \mathcal{M}_L^o[1/m] \xrightarrow{\sim} \mathcal{M}_{K\cap L}^o[1/nm] \ .$$

Soit C/S une courbe elliptique. Les application $x \to x^m$ et $x \to x^n$ définissent un isomorphisme

$$C_{nm} \xrightarrow{\sim} C_n \times C_m \ . \tag{3.8.1}$$

Si $\bar{\alpha}$ (resp. $\bar{\beta}$) est une structure de niveau H (resp. I) sur C , localement représentée par $\alpha : C_n \xrightarrow{\sim} (\mathbb{Z}/n)^2$ (resp. $\beta : C_m \to (\mathbb{Z}/m)^2$) , on définit la structure $\bar{\alpha} \times \bar{\beta}$ de niveau $H \times I$ sur C comme étant la classe de l'isomorphisme $\alpha \times \beta$ rendant commutatif le diagramme

$$\begin{array}{ccc} C_{nm} & \xrightarrow{\alpha \times \beta} & (\mathbb{Z}/nm)^2 \\ \downarrow & & \downarrow \text{réduction} \\ C_n \times C_m & \xrightarrow{(\alpha,\beta)} & (\mathbb{Z}/n)^2 \times (\mathbb{Z}/m)^2 \end{array} \tag{3.8.1}$$

L'isomorphisme 3.8 est défini par

$$(C.\bar{\alpha}.\bar{\beta}) \longmapsto (C, \bar{\alpha} \times \bar{\beta})$$

Proposition 3.9. Avec les notations de 3.7., l'isomorphisme 3.8 se prolonge en

(3.9.1) $$\mathcal{M}_K \times_{\mathcal{M}_1} \mathcal{M}_L \xrightarrow{\sim} \mathcal{M}_{K\cap L}$$

Preuve. Il suffit de prouver que $\mathcal{M}_K \times_{\mathcal{M}_1} \mathcal{M}_L$ est normal. Prouvons-le au-dessus de $\mathbb{Z}[1/m]$. Au-dessus de $\mathbb{Z}[1/n]$, la démonstration est symétrique. $\mathcal{M}_L[1/m]$ est lisse sur $\mathbb{Z}$, donc plat sur $\mathcal{M}_1$ (I 7.1). $\mathcal{M}_K \times_{\mathcal{M}_1} \mathcal{M}_L[1/m]$ est donc plat sur $\mathcal{M}_K$, et de Cohen-Macaulay (I 7.2 et 7.1) $\mathcal{M}_L^o[1/m]$ est même étale sur $\mathcal{M}_1$, donc $\mathcal{M}_K \times_{\mathcal{M}_1} \mathcal{M}_L^o[1/m]$, étale sur $\mathcal{M}_K$, est normal.

D'après le lemme d'Abhyankar, la ramification de $\mathcal{M}_K[1/n]$ sur $\mathcal{M}_1[1/n]$ (resp. $\mathcal{M}_L[1/m]$ sur $\mathcal{M}_1[1/m]$) est modérée. Les indices de ramifications pour $\mathcal{M}_K$ et $\mathcal{M}_L$ sont donc premiers entre eux (en fait, des diviseurs de n et m). Il en résulte que $\mathcal{M}_K[1/mn] \times_{\mathcal{M}_1} \mathcal{M}_L[1/mn]$ est lisse, et il ne reste plus qu'à appliquer le critère de Serre (I.7.2).

Corollaire 3.9.2. Si n est le produit de deux entiers premiers entre eux et ≥ 3, alors $\mathcal{M}_n$ est un schéma.

Soit $n = n'.n''$. Le champ $\mathcal{M}_n[1/n']$ est un schéma, car représentable sur $\mathcal{M}_{n'}[1/n']$. De même, $\mathcal{M}_n[1/n'']$, donc $\mathcal{M}_n$, est un schéma.

Proposition 3.10. (i) L'espace grossier M_H défini par $\mathcal{M}_H$ est propre et plat sur $\mathrm{Spec}(\mathbb{Z})$

(ii) C'est le normalisé dans $M_H^o[1/n]$ de M_1 (isomorphe à $\mathbb{P}^1$: voir VI 1.1).

(iii) On a $M_H = M_n/H$.

(iv) Les fibres géométriques de $M_H[1/n] \to \mathrm{Spec}(\mathbb{Z}[1/n])$ sont géométriquement unibranches.

Preuve La propreté de M_H résulte de celle de $\mathcal{M}_H$. De la description de l'hensélisé strict d'un anneau local de M_H donnée en I.8.2, et de la normalité de $\mathcal{M}_H$, il résulte que M_H est normal. De même, M_H est plat sur $\mathbb{Z}$. Puisque $\mathcal{M}_H \to \mathcal{M}_1$, donc $M_H \to M_1$ est fini, (ii) résulte de (i) et de la normalité.

Il suffit de prouver (iii) et (iv) lorsque $n \geq 3$ (cf. 3.6) auquel cas $M_n^o[1/n] = \mathfrak{M}_n^o[1/n]$. Avec les notations de [8] §4 on a alors

$$M_H^o[1/n] = [M^o[1/n] \,/\, H] \quad ,$$

de sorte que $M_H^o[1/n] = M_n^o[1/n]/H$. Ceci étant, (iii) résulte de (ii).

L'application

$$(M_n \otimes \overline{\mathbb{F}}_p)/H \longrightarrow (M_n/H) \otimes \overline{\mathbb{F}}_p = M_H \otimes \overline{\mathbb{F}}_p$$

est radicielle. Si $p \nmid n$, $M_n \otimes \overline{\mathbb{F}}_p$, donc $(M_n \otimes \overline{\mathbb{F}}_p)/H$ est lisse, et (iv) en résulte.

3.11. La catégorie des courbes elliptiques à isogénie près sur un schéma S est la catégorie déduite de celle des courbes elliptiques en inversant les isogénies. Notant $E \otimes \mathbb{Q}$ la courbe elliptique à isogénie près sur S sous-jacente à E/S, on a

$$\mathrm{Hom}_S(E \otimes \mathbb{Q} \,,\, F \otimes \mathbb{Q}) = \mathrm{Hom}_S(E,F) \otimes \mathbb{Q} \quad .$$

3.12. Plaçons nous sur un corps algébriquement clos de caractéristique 0 k. Pour toute courbe elliptique E sur k, soit

$$\hat{T}(E) = \varprojlim E_n \qquad \text{(isomorphe à } \hat{\mathbb{Z}}^2 \text{)}$$

$$\hat{V}(E) = \hat{T}(E) \otimes \mathbb{Q} \qquad \text{(isomorphe à } \hat{\mathbb{Z}}^2 \otimes \mathbb{Q} = (\mathbb{A}^f)^2 \text{)} \quad .$$

Le groupe des points de division de E est canoniquement isomorphe à $\hat{V}(E)/\hat{T}(E)$: à $x \in \frac{1}{n}\hat{T}(E)/\hat{T}(E)$, on associe l'image dans E_n de $nx \in \hat{T}(E)$.

Une isogénie $E \to F$ induit un isomorphisme $\hat{V}(E) \xrightarrow{\sim} \hat{V}(F)$. Ceci permet de définir $\hat{V}(E_o)$ pour E_o une courbe elliptique à isogénie près. Si $f : E \to F$ est une isogénie, on a

$$\mathrm{Ker}(f) = \mathrm{Ker}(\hat{V}(E)/\hat{T}(E) \to \hat{V}(F)/\hat{T}(F)) = \mathrm{coker}(\hat{T}(E) \to \hat{T}(F)) \quad .$$

L'application $f \mapsto \hat{T}(F) \subset \hat{V}(E)$ identifie les isogénies de source E aux "réseaux" $\hat{T}'$ contenant $\hat{T}(E)$. On en déduit que le foncteur

$$E \to (E \otimes \mathbb{Q},\ \hat{T}(E) \subset \hat{V}(E \otimes \mathbb{Q}))$$

(courbes elliptiques) → (courbes elliptiques à isogénie près E_o , munies d'un "réseau" $\hat{T} \subset \hat{V}(E)$

est une équivalence de catégories.

3.13. Soit E_o une courbe elliptique à isogénie près sur k . Un réseau $\hat{T} \subset \hat{V}(E_o)$ peut s'interpréter comme une classe mod $GL(2, \hat{\mathbb{Z}})$ d'isomorphismes

$$\beta : \hat{V}(E_o) \longrightarrow (\mathbb{A}^f)^2 \quad :$$

à β on associe $\beta^{-1}(\hat{\mathbb{Z}}^2)$.

Soit $K \subset GL(2, \hat{\mathbb{Z}})$ l'image réciproque de $H \subset GL(2, \mathbb{Z}/n)$. Si $(E_o, \hat{T})$ correspondent à une courbe E , à une structure de niveau H sur E on associe l'ensemble des $\beta : \hat{V}(E_o) \xrightarrow{\sim} \mathbb{A}^{f^2}$ tels que $\beta^{-1}(\hat{\mathbb{Z}}^2) = \hat{T}$ et que $\beta_n : E_n = \hat{T}/n\hat{T} \xrightarrow{\sim} \hat{\mathbb{Z}}^2/n\hat{\mathbb{Z}}^2 = (\mathbb{Z}/n\mathbb{Z})^2$ définisse la structure de niveau H . Les β forment une classe latérale sous K , et l'ensemble des courbes elliptiques munies d'une structure de niveau H $(E, \bar{\alpha})$, avec $E \otimes \mathbb{Q} = E_o$, s'identifie à

$$K \backslash \mathrm{Isom}(\hat{V}(E_o)\ ,\ \mathbb{A}^{f^2}) \quad .$$

3.14. Soit $g \in GL(2, \mathbb{A}^f)$ tel que $gKg^{-1} \subset GL(2, \hat{\mathbb{Z}})$. Si on identifie une courbe elliptique avec structure de niveau K (= de niveau H) à (E_o, β) , avec $\beta \in K \backslash \mathrm{Isom}(\hat{V}(E_o)\ ,\ \mathbb{A}^{f^2})$, l'application $(E_o, \beta) \mapsto (E_o, g\beta)$ associe à une courbe de niveau K une courbe de niveau gKg^{-1} .

Ces constructions gardent un sens sur un schéma de caractéristique 0 quelconque et définissent

$$(3.14.1) \qquad g : \mathfrak{M}^o_K \otimes \mathrm{Spec}(\mathbb{Q}) \xrightarrow{\sim} \mathfrak{M}^o_{gKg^{-1}} \otimes \mathrm{Spec}(\mathbb{Q}) \quad ,$$

et un isomorphisme $[g]$ entre l'image réciproque par g de la courbe universelle sur $\mathfrak{M}^o_{gKg^{-1}} \otimes \mathrm{Spec}(\mathbb{Q})$ à isogénie près avec la courbe universelle sur $\mathfrak{M}^o_K \otimes \mathrm{Spec}(\mathbb{Q})$, à isogénie près.

Par passage à la limite sur K, on en déduit une action de $GL(2, \mathbb{A}^f)$ sur le schéma $\varprojlim_K \mathcal{M}_K^o \otimes \mathrm{Spec}(\mathbb{Q})$, et sur la courbe elliptique universelle à isogénie près.

3.15. Explicitons l'application composée

$$(3.15.1) \qquad \mathcal{M}_K^o \otimes \mathbb{Q} \xrightarrow{\sim} \mathcal{M}_{gKg^{-1}}^o \otimes \mathbb{Q} \xrightarrow{c} \mathcal{M}_1^o \otimes \mathbb{Q} \quad .$$

Prenons n, et soit m tels que

$$\hat{\mathbb{Z}}^2 \subset \frac{1}{m} g^{-1}(\hat{\mathbb{Z}}^2) \subset \frac{1}{n}\hat{\mathbb{Z}}^2 \quad .$$

Soit B le sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^2$ image de $\frac{1}{m} g^{-1}(\hat{\mathbb{Z}}^2)/\hat{\mathbb{Z}}^2$ par la multiplication par n : $\frac{1}{n}\hat{\mathbb{Z}}^2/\hat{\mathbb{Z}}^2 \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^2$.

A une courbe elliptique avec structure de niveau H $(E,\bar{\alpha})$, on associe la courbe elliptique $E/\alpha^{-1}(B)$, pour $\alpha : E_n \xrightarrow{\sim} (\mathbb{Z}/n)^2$ un quelconque représentant de $\bar{\alpha}$. L'isogénie $[g]$ est $1/m$ fois la projection $E \to E/\alpha^{-1}(B)$.

Proposition 3.16. *L'isomorphisme 3.14.1 se prolonge en un isomorphisme*

$$g : \mathcal{M}_K^o \xrightarrow{\sim} \mathcal{M}_{gKg^{-1}}^o$$

L'isomorphisme $[g]$ *se prolonge en un isomorphisme*

$$[g] : g^* (\text{courbe elliptique sur } \mathcal{M}_{gKg^{-1}}^o) \otimes \mathbb{Q} \simeq (\text{courbe elliptique sur } \mathcal{M}_K) \otimes \mathbb{Q} \, .$$

Preuve. Montrons tout d'abord que (3.15.1) se prolonge en

$$cg : \mathcal{M}_K^o \to \mathcal{M}_1^o \quad .$$

Soit b l'ordre de B comme en 3.15 et soit I le champ relativement représentable sur $\mathcal{M}_1^o$ qui représente le foncteur des sous-schémas en groupes localement libres de rang b de la courbe elliptique universelle E. La théorie des schémas de Hilbert montre que la projection $I \to \mathcal{M}_1^o$ est un morphisme propre et représentable. En vertu du lemme suivant, il est fini.

Lemme 3.17. Soient E une courbe elliptique sur k algébriquement clos et b un entier Il n'y a qu'un nombre fini de sous-schémas en groupes de rang b de E .

Preuve de 3.17. On procède par récurrence sur b .

a) il n'y a qu'un nombre fini de sous-schémas étales de rang b de E : ils s'identifient aux sous-groupes d'ordre b de $E_b(k)$

b) si $H \subset E$ n'est pas étale, k est de caractéristique $p > 0$ et $H \supset \mathrm{Ker}(F)$ Les sous-groupes non étales de rang b de E correspondent donc aux sous-groupes de rang b/p de $E^{(p)} = E/\mathrm{Ker}(F)$, et on conclut par l'hypothèse de récurrence.

Preuve de 3.16. (suite). La construction 3.14 définit une section s sur $\mathfrak{M}_K^o \otimes \mathrm{Spec}(\mathbb{Q})$ de $I \times_{\mathfrak{M}_1} \mathfrak{M}_K^o$.

Il résulte du Main Theorem de Zariski et de la normalité de $\mathfrak{M}_K^o$ que cette section se prolonge sur $\mathfrak{M}_K^o$, définissant un sous-groupe B de l'image inverse E par c de la courbe elliptique universelle sur $\mathfrak{M}_1^o$; le prolongement cg voulu est défini par E/B ; l'isomorphisme [g] est défini comme en 3.15.

Le morphisme cg ainsi défini est quasi-fini et représentable. Il identifie donc $\mathfrak{M}_K^o$ à un ouvert du normalisé $\mathfrak{M}^o_{gKg^{-1}}$ de $\mathfrak{M}_1^o$ dans $\mathfrak{M}_K^o \otimes \mathrm{Spec}(\mathbb{Q}) \overset{g}{\simeq} \mathfrak{M}^o_{gKg^{-1}} \otimes \mathrm{Spec}(\mathbb{Q})$, d'où

$$g : \mathfrak{M}_K^o \hookrightarrow \mathfrak{M}^o_{gKg^{-1}} \quad .$$

Ce morphisme est un isomorphisme, d'inverse g^{-1} .

3.18. On peut montrer que g se prolonge en un isomorphisme

$$\mathfrak{M}_K \xrightarrow{\sim} \mathfrak{M}_{gKg^{-1}} \quad .$$

Nous nous contenterons de montrer le résultat analogue pour les schémas grossiers.

Proposition 3.19. Le morphisme de schémas grossiers déduit de 3.16 se prolonge en

$$g : M_K \xrightarrow{\sim} M_{gKg^{-1}} \quad .$$

Soit $\Gamma \subset M_K \times M_{gKg^{-1}}$ l'adhérence du graphe G de $g : M_K^o \xrightarrow{\sim} M_{gKg^{-1}}^o$. On a, ensemblistement,

$$\Gamma = G \cup (\Gamma \cap (M_K^\infty \times_{\mathbb{Z}} M_{gKg^{-1}}^\infty)) \quad .$$

Dès lors, Γ est fini sur M_K et $M_{gKg^{-1}}$ et, d'après le Main theorem et 3.10 $\Gamma \to M_K$ et $\Gamma \to M_{gKg^{-1}}$ sont des isomorphismes. 3.19 en résulte.

3.20. Soit C une courbe elliptique sur S, avec n inversible sur S. Il est bien connu que le "e_n-pairing" définit un isomorphisme.

$$(3.20.1) \qquad e_n : \overset{2}{\Lambda} C_n \xrightarrow{\sim} \mu_n \quad .$$

Une structure de niveau n $\alpha : C_n \xrightarrow{\sim} (\mathbb{Z}/n)^2$ définit donc un isomorphisme $\det(\alpha)^{-1} : \mathbb{Z}/n \xrightarrow{\sim} \mu_n$, i.e. une racine primitive $n^{\text{ième}}$ de l'unité $d(\alpha) = \det(\alpha)^{-1}(1)$ sur S

Notons $\mathbb{Z}[\zeta_n]$ l'anneau des entiers du corps des racines $n^{\text{ièmes}}$ de l'unité. La construction $\alpha \mapsto d(\alpha)$ définit un morphisme

$$d : \mathfrak{M}_n^o[1/n] \to \mathrm{Spec}(\mathbb{Z}[\zeta_n]) \quad .$$

Ce morphisme se prolonge au normalisé et définit

$$(3.20.2) \qquad d : \mathfrak{M}_n \to \mathrm{Spec}(\mathbb{Z}[\zeta_n]) \quad .$$

De même, une structure de niveau H α définit

$$d(\alpha) \in \underline{\mathrm{Isom}}(\mathbb{Z}/n, \mu_n)/\det(H) \quad .$$

Le groupe $(\mathbb{Z}/n)^*$ agit sur $\mathbb{Z}[\zeta_n]$ par $\zeta_n \mapsto \zeta_n^i$; si $\mathbb{Z}[\zeta_n]^{\det H}$ est le sous-anneau des invariants de $\mathbb{Z}[\zeta_n]$ sous l'action de $\det H \subset (\mathbb{Z}/n)^*$, on trouve comme plus haut

$$(3.20.3) \qquad d : \mathfrak{M}_H \longrightarrow \mathrm{Spec}(\mathbb{Z}[\zeta_n]^{\det H}) \quad ,$$

définissant

(3.20.4) $$d : M_H \to \mathrm{Spec}(\mathbb{Z}[\zeta]^{\det H}) \quad .$$

3.21. Plaçons-nous sur $\mathbb{M}_{(m)}[1/m]$ avec $n|m$. Si C est la courbe elliptique généralisée universelle, le e_n-pairing se prolonge en un isomorphisme

$$\overset{2}{\Lambda}\, C_n \simeq \mu_n \quad .$$

En particulier, pour le polygone de Néron à m côtés standard , on trouve un isomorphisme

(3.21.1) $$e_n : \overset{2}{\Lambda}\, (\mathbb{G}_m \times \mathbb{Z}/m)_n \simeq \mu_n \quad .$$

Identifions $\mathbb{Z}/n$ à $(\mathbb{Z}/m)_n$ par $i \mapsto (m/n)i$. On a

(3.21.2) $$\overset{2}{\Lambda}\, (\mathbb{G}_m \times \mathbb{Z}/m)_n = \overset{2}{\Lambda}\, (\mu_n \times \mathbb{Z}/n) \xrightarrow{\sim} \mu_n \quad .$$

Selon les conventions de signe utilisées pour définir e_n , (3.21.1) et (3.21.2) sont égaux ou opposés.

4. Exemples.

4.1. Nous noterons $\Gamma_0(n)$, $\Gamma_{00}(n)$, $\Gamma'_{00}(n)$ et $\Gamma(n)$ les sous-groupes de $GL(2, \hat{\mathbb{Z}})$ formé des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ telles que :

$\Gamma_0(n)$: $c \equiv 0 \pmod n$;

$\Gamma_{00}(n)$: $c \equiv 0 \pmod n$, $a \equiv 1 \pmod n$;

$\Gamma'_{00}(n)$: $c \equiv 0 \pmod n$, $a \equiv d \equiv 1 \pmod n$;

$\Gamma(n)$: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod n$.

Ces sous-groupes sont chacun image réciproque de sous-groupes H de $GL(2, \mathbb{Z}/n)$.

4.2. Pour $\Gamma_0(n)$, H est le sous-groupe de $GL(2, \mathbb{Z}/n)$ qui stabilise le sous-groupe $\mathbb{Z}/n \times \{0\}$ de $(\mathbb{Z}/n)^2$. Si C est une courbe elliptique sur S , et que

$\bar{\alpha}$ est une structure de niveau H sur C, représentée par $\alpha : C_n \xrightarrow{\sim} (\mathbb{Z}/n)^2$, le sous-schéma en groupes $\alpha^{-1}(\mathbb{Z}/n \times \{0\})$ de C_n ne dépend donc que de $\bar{\alpha}$. Si n est inversible sur S, cette construction établit un isomorphisme du faisceau des structures de niveau H sur C avec le faisceau des sous-schémas en groupes de C localement isomorphes à $\mathbb{Z}/n$. En d'autres termes :

Construction 4.3. $\mathfrak{M}^o_{\Gamma_o(n)}[1/n]$ s'identifie au champ algébrique classifiant les courbes elliptiques C/S, avec n inversible sur S, munies d'un sous-schéma en groupes A localement isomorphe à $\mathbb{Z}/n$.

4.4. Pour C/S et A comme en 4.3, le sous-groupe C_n/A de C/F est localement isomorphe à $\mathbb{Z}/n$, d'où un morphisme

$$w : \mathfrak{M}^o_{\Gamma_o(n)}[1/n] \to \mathfrak{M}^o_{\Gamma_o(n)}[1/n] : \quad (C,A) \mapsto w(C,A) = (C/A,\ C_n/A) \quad .$$

La multiplication par n se factorise par un isomorphisme $C/C_n \xrightarrow{\sim} C$; celui-ci définit un isomorphisme

$$ww(C,A) = ((C/A)/(C_n/A)\ ,\ (C/A)_n/(C_n/A)) = (C/C_n,\ ..) \xrightarrow{\sim} (C,A) \quad ,$$

d'où un isomorphisme $w^2 \simeq Id$: w est une involution. On vérifie que w est du type 3.16, pour $g = \begin{pmatrix} 0 & 1 \\ n & 0 \end{pmatrix}$.

4.5. Voici une description plus symétrique du champ et de w. Associons à (E,A) l'isogénie $E \to E/A$. On trouve que $\mathfrak{M}^o_{\Gamma_o(n)}[1/n]$ est encore le champ classifiant les isogénies

$$a : E_1 \to E_2 \quad ,$$

de noyau cyclique d'ordre n.

Si (E,A) définit $a : E_1 \to E_2$, $w(E,A)$ définit une isogénie $E_2 \to E_1/(E_1)_n$, qui, via l'isomorphisme 4.4 de $E_1/(E_1)_n$ avec E_1, s'identifie au dual de Cartier de a : dans le langage des isogénies,

$$w(a : E_1 \to E_2) \quad \text{est} \quad (a^* : E_2 \to E_1) \quad .$$

4.6. Soient C/S et A comme en 4.3. Pour chaque facteur premier p de n, soit A_p la composante p-primaire de A : $A = \prod_{p|n} A_p$, et soit $n(p)$ l'ordre de A_p : $n = \prod p^{n(p)}$. On pose $w_p(E,A) = (E/A_p\ ,\ A + E_{p^{n(p)}}/A_p)$. Les w_p définissent des involutions de $\mathcal{M}^o_{\Gamma_o(n)}[1/n]$, celles-ci commutent deux à deux, et w est leur composé.

4.7. Le sous-groupe $\Gamma_{oo}(n)$ de $GL(2,\hat{\mathbb{Z}})$ est l'image réciproque du sous-groupe H de $GL(2,\mathbb{Z}/n)$ qui fixe l'élément $(1,0)$ de $(\mathbb{Z}/n)^2$ ou, ce qui revient au même, le morphisme $\beta : \mathbb{Z}/n \to (\mathbb{Z}/n)^2 : x \mapsto (x,0)$. Raisonnant comme en 4.2, on obtient :

Construction 4.8. $\mathcal{M}^o_{\Gamma_{oo}(n)}[1/n]$ s'identifie au champ algébrique classifiant les courbes elliptiques C/S, avec n inversible sur S, munies d'un plongement $\beta : \underline{\mathbb{Z}/n} \hookrightarrow C_n$, i.e. d'une section $\beta(1)$ partout d'ordre exactement n.

4.9. $\Gamma'_{oo}(n)$ est l'image réciproque du sous-groupe H de $GL(2,\mathbb{Z}/n)$ qui fixe $(1,0) \in (\mathbb{Z}/n)^2$ et la classe de $(0,1)$ dans $(\mathbb{Z}/n)^2/\mathbb{Z}/n \times \{0\}$. Dès lors, $\mathcal{M}^o_{\Gamma'_{oo}(n)}[1/n]$ s'identifie au champ algébrique classifiant les courbes elliptiques C/S, avec n inversible sur S, munies de $\beta : \underline{\mathbb{Z}/n} \hookrightarrow C_n$ et de $\gamma : \underline{\mathbb{Z}/n} \xrightarrow{\sim} C_n/\mathrm{Im}(\beta)$. Le produit extérieur définit un isomorphisme

$$C_n/\mathrm{Im}(\beta) \xleftarrow{\sim} (\mathbb{Z}/n) \otimes C_n/\mathrm{Im}(\beta) \xrightarrow{\beta} \mathrm{Im}(\beta) \otimes C_n/\mathrm{Im}(\beta) \xrightarrow{\wedge} \overset{2}{\wedge} C_n \xrightarrow{e_n} \mu_n .$$

Via cet isomorphisme, se donner γ revient donc à se donner un isomorphisme de $\mathbb{Z}/n$ avec μ_n, i.e une racine primitive $n^{\text{ième}}$ de l'unité sur S. Dès lors

Construction 4 10. $\mathcal{M}^o_{\Gamma'_{oo}(n)}[1/n] \simeq \mathcal{M}^o_{\Gamma_{oo}(n)}[1/n] \otimes \mathbb{Z}[\zeta_n]$.

Cet isomorphisme est le produit fibré, sur $\mathrm{Spec}(\mathbb{Z})$, du morphisme d'oubli: $\mathcal{M}^o_{\Gamma'_{oo}(n)} \to \mathcal{M}^o_{\Gamma_{oo}(n)}[1/n]$ (défini parce que $\Gamma'_{oo}(n) \subset \Gamma_{oo}(n)$) et du morphisme d (3.20.3).

Définition 4.11. $'\mathcal{M}_{\Gamma_o(n)}[1/n]$ est le champ algébrique classifiant les courbes elliptiques généralisées C/S, avec n inversible sur S, munie d'un sous-schéma en groupe A, localement isomorphe à $\mathbb{Z}/n$, et rencontrant chaque composante irréductible de chaque fibre géométrique de C.

(On verra dans un instant que $'\mathcal{M}_{\Gamma_0(n)}[\frac{1}{n}] \simeq \mathcal{M}_{\Gamma_0(n)}[\frac{1}{n}]$.)

Si un m-gone est classifié par $'\mathcal{M}_{\Gamma_0(n)}$, on a $m|n$. L'application "oubli de A" envoye donc $'\mathcal{M}_{\Gamma_0(n)}[1/n]$ dans $\mathcal{M}_4$. Elle est étale de sorte que $'\mathcal{M}_{\Gamma_0(n)}[1/n]$ est un champ algébrique lisse.

4.12. Comme en 3.5, on définit un morphisme "oubli de A et contraction (1.3)"

$$c : '\mathcal{M}_{\Gamma_0(n)}[1/n] \to \mathcal{M}_1[1/n] .$$

Pour k un corps algébriquement clos et C un objet de $'\mathcal{M}_{\Gamma_0(n)}[1/n](k)$, l'application $\mathrm{Aut}(C) \to \mathrm{Aut}(c(C))$ est injective : pour C lisse, c'est trivial; pour C un m-gone, muni de $A \subset C$, on vérifie sur II.1.10. que $x \to -x$ est le seul automorphisme non trivial de (C,A) . On vérifie comme en 3.4 que $'\mathcal{M}_{\Gamma_0(n)}[1/n]$ est propre sur $\mathbb{Z}[1/n]$. Comme en 3.5, on en déduit le résultat suivant

Construction 4.13. On a $\mathcal{M}_{\Gamma_0(n)}[1/n] \simeq '\mathcal{M}_{\Gamma_0(n)}[1/n]$.

Des arguments analogues fournissent la

Construction 4.14. $\mathcal{M}_{\Gamma_{00}(n)}[1/n]$ est le champ algébrique classifiant les courbes généralisées C/S , avec n inversible sur S , munies d'un plongement $\beta : \mathbb{Z}/n \hookrightarrow C$, dont l'image rencontre chaque composante irréductible de chaque fibre géométrique de C .

Puisque $\mathbb{Z}[\zeta_n][1/n]$ est étale sur $\mathbb{Z}[1/n]$, on déduit par ailleurs de 4.10 par normalisation la

Construction 4.15. $\mathcal{M}_{\Gamma'_{00}(n)}[1/n] \simeq \mathcal{M}_{\Gamma_{00}(n)}[1/n] \otimes \mathbb{Z}[\zeta_n]$.

4.16. Soit A le sous-groupe de $GL(2, \mathbb{Z}/n)$ formé des homothéties. Nous appelerons structures projectives de niveau n les structures de niveau A . Elles jouent un rôle important dans les travaux d'Ihara. Plus généralement :

Définition 4.17. Soit C/S une courbe elliptique généralisée sur S, avec n inversible sur S. On suppose que les fibres géométriques singulières de C sont des n-gones. Une structure projective de niveau n sur C est une section de $\mathrm{Isom}(C_n, (\mathbb{Z}/n)^2)/A$.

Lemme 4.18. Soit (C,α) une courbe elliptique généralisée sur un corps algébriquement clos, munie d'une structure projective de niveau n. Si $n \geq 2$, le seul automorphisme non trivial de C qui respecte α est $x \mapsto -x$.

Si C est un n-gone, le lemme résulte facilement de II.1.10, et vaut même si $n = 1$. Si C est lisse, c'est un cas particulier du lemme suivant.

Lemme 4.19. Soient $n \geq 2$ et g un automorphisme d'ordre fini d'une variété abélienne X sur un corps algébriquement clos k. Si g induit une homothétie sur X_n, alors $g^2 = 1$.

Par hypothèse, il existe $r \in \mathbb{Z}/n$ tel que $g - r$ soit nul sur X_n. Il existe donc un endomorphisme h de X tel que $g-r = n.h$. Si ζ est une racine du polynôme caractéristique de g, ζ est une racine de l'unité et l'entier algébrique $\zeta-r$ est divisible par n. Si R est l'anneau des entiers du corps $\mathbb{Q}(\zeta)$, l'image de ζ dans R/nR est donc égale à celle de r. Puisque $R = \mathbb{Z}[\zeta]$, c'est absurde si $\zeta \neq \pm 1$. Puisque g est semi-simple, 4.19 en résulte.

Du lemme 4.18 pour les n-gones, et d'arguments maintenant familiers, on déduit le résultat suivant.

Construction 4.20. Pour A comme en 4.16, $\mathcal{M}_A[1/n]$ est le champ algébrique classifiant les courbes elliptiques généralisées munies d'une structure projective de niveau n.

Pour (C,α) classifié par $\mathcal{M}_A[1/n]$, et $n \geq 2$, il résulte de 4.18 que $\mathrm{Aut}(C,\alpha)$ est constant. On en déduit la proposition suivante (1.8).

Proposition 4.21. Pour A comme en 4.16, et $n \geq 2$, l'application

$$\mathfrak{M}_A[1/n] \longrightarrow M_A[1/n]$$

est étale.

Remarque 4.22. Pour $n = 2$, $\mathfrak{M}_A$ n'est autre que $\mathfrak{M}_2$, et l'application $\mathfrak{M}_2[1/2] \to M_2[1/2]$ est donc étale.

5. Théorie transcendante (rappels).

5.1 Soit E une courbe elliptique sur $\mathbb{C}$. L'application exponentielle définit une suite exacte de groupes analytiques

$$0 \to H_1(E, \mathbb{Z}) \xrightarrow{\iota} \mathrm{Lie}(E) \xrightarrow{\exp} E(\mathbb{C}) \to 0 \quad .$$

Si $\beta : \mathbb{Z}^2 \xrightarrow{\sim} H_1(E, \mathbb{Z})$ est une base de E, nous poserons

$$z(\beta) = \iota(\beta(1,0))/\iota(\beta(0,1)) \in \mathbb{C} - \mathbb{R}$$

(pour ι_1 et ι_2 deux éléments de $\mathrm{Lie}(E)$, avec $\iota_2 \neq 0$, on note ι_1/ι_2 le nombre complexe λ tel que $\iota_1 = \lambda\iota_2$).

Si $\gamma = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in GL(2, \mathbb{Z})$, on a

$$z(\beta\gamma) = \frac{a\, z(\beta) + b}{c\, z(\beta) + d} \quad .$$

5.2. L'application $x \to \exp(\frac{1}{n}\, \iota(x))$ induit un isomorphisme

$$H_1(E, \mathbb{Z}) \otimes \mathbb{Z}/n \xrightarrow{\sim} E_n \quad . \tag{5.2.1}$$

Posons $X^{\pm} = \mathbb{C} - \mathbb{R}$, et soit X le demi-plan supérieur. Si $\alpha : E_n \xrightarrow{\sim} (\mathbb{Z}/n)^2$ est une structure de niveau n, la classe du couple $(z(\beta), \alpha\circ\beta) : z(\beta) \in X^+$, $\alpha\circ\beta \in GL(2, \mathbb{Z}/n)$, dans

$$X^{\pm} \times GL(2, \mathbb{Z}/n) \,/\, GL(2, \mathbb{Z})$$

ne dépend que de (E,α).

5.3. Soient H et K comme en 3.6. . La construction 5.2 définit un isomorphisme

$$M_H^o(\mathbb{C}) \xrightarrow{\sim} X^{\pm} \times (H \backslash GL(2, \mathbb{Z}/n)/GL(2, \mathbb{Z}) \quad .$$

On a d'ailleurs des isomorphismes

$$X \times (H \backslash GL(2, \mathbb{Z}/n))/SL(2, \mathbb{Z}) \xrightarrow{\sim} X^{\pm} \times (H \backslash GL(2, \mathbb{Z}/n))/GL(2, \mathbb{Z})$$
$$\xrightarrow{\sim} K \backslash X^{\pm} \times GL(2, \mathbb{A}^f)/GL(2, \mathbb{Q}) \quad .$$

5.4. On sait que le morphisme de réduction : $SL(2, \mathbb{Z}) \to SL(2, \mathbb{Z}/n)$ est surjectif. Il en résulte que les composantes connexes de $M_H^o(\mathbb{C})$ s'identifient aux fibres de l'application

$$(5.4.1) \qquad X \times (H \backslash GL(2, \mathbb{Z}/n))/SL(2, \mathbb{Z}) \xrightarrow{\det} \det H \backslash (\mathbb{Z}/n)^* \quad .$$

Soit $\mu_n^*(\mathbb{C})$ l'ensemble des racines primitives $n^{\text{ièmes}}$ de l'unité dans $\mathbb{C}$. Par extension des scalaires de $\mathbb{Z}$ à $\mathbb{C}$, (3.20.4) définit une application.

$$(5.4.2) \qquad M_H(\mathbb{C}) \xrightarrow{d} \det H \backslash \mu_n^*(\mathbb{C}) \quad .$$

Via la bijection $x \mapsto \exp(\frac{2\pi i x}{n}) : \mathbb{Z}/n \xrightarrow{\sim} \mu_n(\mathbb{C})$, (5.4.1) s'identifie à la restriction de cette application à $M_H^o(\mathbb{C})$. Les fibres géométriques de caractéristiques 0 de (3.20.3) (3.20.4) sont donc irréductibles. Le corollaire suivant résulte dès lors du théorème de connexion de Zariski.

Corollaire 5.5. En toute caractéristique, les fibres géométriques de (3.20.4) : $M_H \to \mathrm{Spec}(\mathbb{Z}[\zeta_n]^{\det H})$ sont connexes.

Corollaire 5.6. En caractéristique p première à n, les fibres géométriques de (3.20.4) sont irréductibles.

Elles sont connexes et géométriquement unibranches (3.10 (iv)).

6. Structures de niveau H : étude à l'infini.

Ce § ne servira pas dans la suite de cet article. Nous recommandons au lecteur de l'omettre en première lecture.

Soit H un sous-groupe de $GL(2, \mathbb{Z}/n)$. Nous nous proposons de donner une interprétation modulaire de $\mathcal{M}_H[1/n]$ qui généralise 3.5, 4.13, 4.14, 4.15 et 4.20. Nous définirons tout d'abord par voie modulaire un champ $\mathcal{M}'_H[1/n]$, propre et lisse sur $\mathbb{Z}[1/n]$, et dont $\mathcal{M}^o_H[1/n]$ soit un sous-champ ouvert dense. Nous définirons comme en 3.5 un morphisme fini $c : \mathcal{M}'_H[1/n] \to \mathcal{M}_1[1/n]$. Nous prouverons ensuite l'analogue de (3.5.1). La démonstration de 3.5 donne alors $\mathcal{M}'_H[1/n] = \mathcal{M}_H[1/n]$; c'est l'interprétation modulaire cherchée.

6.1. Soient A un groupe isomorphe à $(\mathbb{Z}/n)^2$, $A' \subset A$ un sous-groupe isomorphe à $\mathbb{Z}/n$ et B un sous-groupe contenant A'. Le système (A,A',B) est donc isomorphe à un système $((\mathbb{Z}/n)^2, \mathbb{Z}/n \times \{0\}, \mathbb{Z}/n \times m\mathbb{Z}/n\mathbb{Z})$, pour $m|n$ convenable. Soit de plus μ un groupe isomorphe à $\mathbb{Z}/n$ et $\beta_o : \overset{2}{\Lambda} A \xrightarrow{\sim} \mu$. Nous noterons β_1 la restriction de β_o à $\overset{2}{\Lambda} B$.

L'exemple essentiel d'une telle situation est le suivant. Soient C une courbe elliptique généralisée sur un trait complet S, de points η et s, $\bar{\eta}$ le spectre d'une clôture algébrique de $k(\eta)$ et $\bar{s}$ le spectre de la clôture algébrique correspondante de $k(s)$. Si n est inversible sur S, que C_η est lisse et que $C_{\bar{s}}$ est un polygone de Néron à $m|n$ côtés, on prend

$$\mu = \mu_n(\bar{\eta}) \simeq \mu_n(\bar{s}),\ A = C_n(\eta),\ A' = C^o_n(s),\ B = (C^{reg}_s)_n(\bar{s}) \text{ et } \beta_o = e_n .$$

La restriction β_1 de β_o à $\overset{2}{\Lambda} B$ ne dépend que de la fibre spéciale $C_{\bar{s}}$ (cf. 3.21).

6.2. Avec les notations de 6.1, soient I l'ensemble des isomorphismes $\alpha : A \to (\mathbb{Z}/n)^2$ et $\bar{I}$ l'ensemble des couples (α, β) formés de $\bar{\alpha} : B \to (\mathbb{Z}/n)^2$ et de $\beta : \mu \to \mathbb{Z}/n$ tels que le diagramme suivant soit commutatif

(6.2.1)
$$\begin{array}{ccc} \overset{2}{\Lambda} B & \xleftarrow{\overset{2}{\Lambda}\alpha} & \overset{2}{\Lambda}(\mathbb{Z}/n)^2 \\ \downarrow{\scriptstyle \beta_1} & & \downarrow{\scriptstyle s} \\ \mu & \xrightarrow{\beta} & \mathbb{Z}/n \end{array} .$$

On définit $c : I \to \overline{I}$ par $\alpha \to (\alpha|B, \overset{2}{\wedge} \alpha \circ \beta_o^{-1})$. Le groupe $GL(2, \mathbb{Z}/n)$ agit sur I et $\overline{I}$ à gauche par $g.\alpha = g \circ \alpha$ et $g.(\alpha, \beta) = (g\alpha, \det(g).\beta)$. Soit U le sous-groupe de $Aut(A)$ qui agit trivialement sur A' et A/A' . Il agit à droite sur I et $\overline{I}$ par $\alpha.u = \alpha \circ u$ et $(\overline{\alpha}, \beta)u = (\overline{\alpha} \circ (u|B), \beta)$. Ces actions sont compatibles à c .

Lemme 6.2.2. L'application c est surjective.

La vérification est laissée au lecteur.

Les sous-groupes U' de U et les sous-groupes B' de A contenant A' se correspondent bijectivement par

$U' \mapsto$ sous-groupe $A^{U'}$ des invariants de U'

$B' \mapsto$ sous-groupe de $U(B')$ agissant trivialement sur B' .

On a $\overline{I} = I/U(B)$.

Soit $\overline{a} \in H \backslash \overline{I}$, image de $\alpha \in I$. L'ensemble des $\alpha' \in I$ d'image $\overline{a}$ est $H\alpha U(B)$. Nous dirons que B est adéquat si $U(B)$ est le sous-groupe de U qui stabilise l'image a de α dans $H \backslash I$

$$\begin{array}{ccc} I & \longrightarrow & \overline{I} = I/U(B) \\ \downarrow & & \downarrow \\ H\backslash I & \longrightarrow & H \backslash I/U(B) \end{array}$$

Ceci signifie que

(6.2 3) a est le seul élément de $H \backslash I$ d'image $\overline{a}$

(6.2.4) tout $u \in U$ tel que $\overline{a}u = \overline{a}$ est dans $U(B)$.

Notons ${}_H J_B$ l'ensemble des $a \in H \backslash \overline{I}$ pour lesquels B est adéquat. Il résulte de la discussion précédente que

Lemme 6.2.5 On a $H \backslash I \xrightarrow{\sim} \coprod_{A' \subset B' \subset A} {}_H J_{B'}$ (somme sur B')

6.3. Soient donnés seulement un groupe B , un sous-groupe A' , avec (A', B)

isomorphe à $(\mathbb{Z}/n \times \{0\}, \mathbb{Z}/n\mathbb{Z} \times m\mathbb{Z}/n\mathbb{Z})$ pour $m|n$ convenable, μ isomorphe à $\mathbb{Z}/n$ et $\beta_1 : \overset{2}{\wedge} B \hookrightarrow \mu$. Notons encore $\overline{I}$ l'ensemble des couples $(\bar{\alpha}, \beta)$ formés de $\bar{\alpha} : B \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^2$ et de $\beta : \mu \xrightarrow{\sim} \mathbb{Z}/n$ tels que le diagramme 6.2.1 soit commutatif

Le groupe $GL(2, \mathbb{Z}/n)$ agit à gauche sur $\overline{I}$ par $g.(\alpha, \beta) = (g \circ \alpha, \det(g).\beta)$ et le groupe $\overline{U}$ des automorphismes de B induisant l'identité sur A' et B/A' agit à droite par $(\alpha, \beta)u = (\alpha \circ u, \beta)$. Nous noterons ${}_H J_B$ l'ensemble des $a \in H \backslash \overline{I}$ tels que

a) si $\tilde{a} \in \overline{I}$ est d'image $\bar{a}$, et que $g\tilde{a} = \tilde{a}'$, on a $g \in H$;

b) tout $u \in \overline{U}$ tel que $\tilde{a}u = \tilde{a}$ est l'identité.

Cette notation coincide avec celle de 3.11 lorsque cette dernière a un sens.

6.4. Soient S un schéma sur lequel n est inversible, et C une courbe elliptique généralisée sur S . On suppose que les fibres géométriques de C sont lisses ou des polygones de Néron à m côtés, avec $m|n$. On se propose de définir un faisceau étale F sur S , de formation compatible à tout changement de base, intuivement décrit par les deux propriétés suivantes.

a) Si C est lisse sur S , $F(S)$ est l'ensemble de structures de niveau H de C sur S .

b) Supposons S spectre d'un corps algébriquement clos, et que C soit un polygone de Néron à m côtés $(m|n)$. Appliquons 6.3 pour $B = C_n^{reg}$, $A' = C_n^o$, $\mu = \mu_n$ et $\beta_1 = e_n$ (cf. 6.1). On veut avoir $F(S) = {}_H J_B$.

6.5. Soit $F_1(S)$ l'ensemble des systèmes $(B, \bar{\alpha}, \beta)$ consistant en

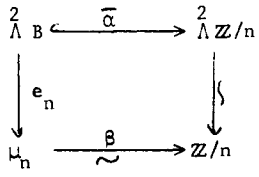
a) un sous-schéma en groupes fini étale $B \subset C_n$;

b) $\bar{\alpha} : B \hookrightarrow (\mathbb{Z}/n)^2$ et $\beta : \mu_n \xrightarrow{\sim} \mathbb{Z}/n$

tels que

c) localement sur S , B contient un sous-groupe isomorphe à $\mathbb{Z}/n$;

d) le diagramme



est commutatif;

e) pour tout point géométrique $\bar{s}$ de S, si $C_{\bar{s}}$ est singulier, $(\bar{\alpha},\beta)$ mod H est du type décrit en 6.4. Dans tous les cas, on demande que si $g \in GL(2,\mathbb{Z}/n)$ est tel que $(g\bar{\alpha}_{\bar{s}},\det(g).\beta_{\bar{s}}) = (\bar{\alpha}_{\bar{s}},\beta_{\bar{s}})$, on a $g \in H$.

Si C/S est lisse, un système $(B,\bar{\alpha},\beta)$ définit une et une seule H-structure sur C : celle localement représentée par des $\alpha : C_n \xrightarrow{\sim} (\mathbb{Z}/n)^2$ qui prolongent $\bar{\alpha}$ et de déterminant β (l'existence locale de α résulte de 6.2.1, l'unicité mod H de la condition e)).

On dira que a et b dans $F_1(S)$ sont équivalents si :

1) Soit U l'ouvert de S au-dessus duquel C est lisse; a et b doivent définir la même structure de niveau H sur C_U/U.

2) Soit $\bar{s}$ un point géométrique de S tel que $C_{\bar{s}}$ soit singulier. $a_{\bar{s}}$ et $b_{\bar{s}}$ doivent être conjugués sous H. Cette condition implique que a et b sont conjugués sous H dans un voisinage étale V de $\bar{s}$, donc que 1) est vérifié dans $U \times_S V$.

Le <u>faisceau</u> F <u>des structures de niveau</u> H sur C/S est le faisceau engendré par le préfaisceau F_o quotient de F_1 par la relation d'équivalence précédente.

On a fait ce qu'il fallait pour que F soit de formation compatible à tout changement de base, admette les valeurs 6.4 et soit représenté par un S-schéma S' étale sur S.

<u>Définition</u> 6.6. (i) <u>Une structure de niveau</u> H <u>sur une courbe elliptique généralisée</u> C/S comme en 6.4 est un élément de $F(S)$.

(ii) Le champ algébrique $\mathcal{M}'_H[1/n]$ sur $\mathbb{Z}[1/n]$ est le champ algébrique qui classifie les courbes elliptiques généralisées C/S , (n inversible sur S) à fibres géométriques de C/S lisse ou des polygones de Néron à $m|n$ côtés, munies d'une structure de niveau H .

Par oubli de la structure de niveau H , on définit un morphisme étale $\mathcal{M}'_H[1/n] \to \mathcal{M}_*$; $\mathcal{M}'_H[1/n]$ est donc lisse sur $\mathbb{Z}[1/n]$, et $\mathcal{M}'^{\infty}_H[1/n]$ étale sur $\mathbb{Z}[1/n]$.

Par contraction (1.3 pour $n = 1$) et oubli de la structure de niveau, on définit $c : \mathcal{M}'_H[1/n] \to \mathcal{M}_1$.

Théorème 6.7 : (i) $\mathcal{M}'_H[1/n]$ est propre et lisse sur $\mathbb{Z}[1/n]$; l'image $\mathcal{M}'^{\infty}_H[1/n]$ du sous-schéma de non lissité de la courbe universelle est fini étale sur $\mathbb{Z}[1/n]$.

(ii) Le morphisme c est fini et représentable. Le champ $\mathcal{M}'_H[1/n]$ coincide donc (cf. 3.5) avec $\mathcal{M}_H[1/n]$.

Il reste à prouver que $\mathcal{M}'_H[1/n]$ est propre sur $\mathbb{Z}[1/n]$, et que c est représentable, i.e. que, pour tout objet C du champ $\mathcal{M}'_H[1/n]$ sur k algébriquement clos,

$$\mathrm{Aut}(C) \to \mathrm{Aut}(c(C)) \tag{6.7}$$

est injectif (cf 3.5).

Le propreté résultera du critère valuatif de propreté et de 6.2.5 . Soient S un trait complet à corps résiduel algébriquement clos, C_η une courbe elliptique sur le point générique η de S , et a une structure de niveau H sur C_η . On peut supposer que le modèle minimal C' de C_η est lisse ou un polygone de Néron à k côtés, avec $n|k$. Si C' est lisse, la structure de niveau H de C_η se prolonge de façon unique à C' , et on pose $C = C'$. Sinon, soit C'' la courbe déduite de C' par contraction, comme en 1.3 (C''_s a n côtés). Avec les notations de 6.1, soit $U(B')$ le plus grand sous-groupe de U qui fixe a . B' correspond à un sous-schéma en groupes fini et étale de C''_n , d'ordre $n \cdot m$, et on note C la courbe déduite de C'' par 1.3 (avec n de loc. cit. $= m$) . a se prolonge de façon unique en une structure de niveau H sur C . A l'aide de 6.2.5 et comme en 1.6 , on voit que

(C , prolongement de a) est l'unique prolongement de $(C_\eta$, a) sur S .

Prouvons (6.7) injectif. Pour C lisse, c'est clair. Sinon, le noyau de (6.7.1) est l'ensemble A des automorphismes de C , agissant trivialement sur $Pic^o(C)$, et respectant la structure de niveau. La condition e) dans la définition 6.5. des structures de niveau assure que $A = \{1\}$.

V. Réduction modulo p .

Dans ce chapitre, nous étudions la réduction modulo p des champs $\mathcal{M}_K$, pour $K = \Gamma_o(p)$, $\Gamma_{oo}(p)$ et $\Gamma(p^k)$. La comparaison des résultats obtenus pour $\Gamma_o(p)$ et $\Gamma_{oo}(p)$ nous permet de montrer que, conformément à une conjecture de Shimura, certains schémas abéliens étudiés par Shimura et Casselman [5] ont bonne réduction sur l'anneau des entiers d'extensions cyclotomiques convenables de $\mathbb{Q}$.

1. Etude de $\mathcal{M}_{\Gamma_o(p)}$.

Nous nous proposons dans ce § de donner une interprétation modulaire du champ $\mathcal{M}_{\Gamma_o(p)}$ lorsque p est premier. Quelques résultats préliminaires reservirons aux paragraphes suivants.

1.1. Soit $\mathcal{C}_n$ le champ classifiant les courbes elliptiques généralisées à fibres géométriques irréductibles C/S, munies d'un sous-schéma en groupes A localement isomorphe à μ_n (pour la topologie étale), i.e. fini plat localement libre de rang n de dual de Cartier étale.

Proposition 1.2. *Le morphisme "oubli de A" : $\mathcal{C}_n \to \mathcal{M}_1$ est étale ; en particulier, $\mathcal{C}_n$ est un champ algébrique lisse sur $\mathbb{Z}$.*

Soit C/S classifié par $\mathcal{M}_1$. Il faut vérifier que le foncteur $F : (Sch/S) \to (Ens)$, qui à T/S associe l'ensemble des sous-groupes A de $(C_T)_n$ localement isomorphes à μ_n, est représentable par un schéma M étale sur S. La représentabilité résulte de la théorie du schéma de Hilbert; M est étale car formellement étale (SGA 3 IX 3.6).

1.3. Soit $\mathcal{B}_n$ le champ classifiant les courbes elliptiques généralisées C/S, à fibres géométriques lisses ou des n-gones, munies d'un sous-schéma en groupes B localement isomorphe à $\mathbb{Z}/n$ (pour la topologie étale), qui rencontre chaque composante irréductible de chaque fibre géométrique.

Soit (C,B) comme plus haut. Le schéma en groupes B agit librement sur C

et C/B est à fibres géométriques irréductibles. Dans la suite exacte

$$0 \to B \to C_n \to A \to 0 \quad ,$$

les termes extrêmes sont en dualité de Cartier. Le couple $(C/B, C_n/B)$ est donc classifié par $\mathcal{G}_n$ et ceci définit

(1 3.1) $$w : \mathcal{B}_n \to \mathcal{G}_n$$

Proposition 1.4. *Le morphisme 1.3.1 est un isomorphisme. En particulier, $\mathcal{B}_n$ est un champ algébrique lisse sur $\mathbb{Z}$.*

Preuve : Notons encore w le morphisme de $\mathcal{G}_n^o$ dans $\mathcal{B}_n^o$

$$w : (C,A) \mapsto (C/A, C_n/A) \quad .$$

Une construction identique à celle de IV.4.4. montre que ce morphisme est un inverse de la restriction $w : \mathcal{B}_n^o \to \mathcal{G}_n^o$ de w à $\mathcal{B}_n^o$.

Soit (C,A) sur S , classifié par $\mathcal{G}_n$. Il faut prouver qu'il existe $(\tilde{C},\tilde{A})$ sur S , classifié par $\mathcal{B}_n$, un isomorphisme $\beta : w(\tilde{C},\tilde{A}) \xrightarrow{\sim} (C,A)$, et que $(\tilde{C},\tilde{A},\beta)$ est unique à isomorphisme unique près. Par abus de notation, on note encore β le morphisme composé $\tilde{C} \to \tilde{C}/\tilde{A} \xrightarrow{\beta}_{\sim} C$. La courbe à section marquée $(\tilde{C},e)$ sera nécessairement un revêtement étale de degré n de (C,e) , muni de sa structure de courbe elliptique généralisée.

Rappelons le lemme suivant, qui résulte de SGA 4 XII.5.9 bis.

Lemme 1.5. *Soit $f : X \to S$ un morphisme propre à fibres géométriques connexes et e une section de f . Si $p : (Y,e) \to (X,e)$ est un revêtement fini étale à section marquée de (X,e) et que Y/S est à fibres géométriques connexes le triple (Y,p,e) n'a pas d'automorphisme non trivial. Le foncteur F sur (Sch/S) des classes d'isomorphie des triples (Y,p,e) comme plus haut est représentable par un faisceau étale.*

Appliquons ce lemme à C/S . Soit $\mathcal{F}$ le champ des $(\tilde{C},\tilde{A},\beta)$ du type voulu. Le lemme montre que les objets de $\mathcal{F}$ n'ont pas d'automorphisme non trivial, et que le

foncteur $[\mathfrak{F}]$ des classes d'isomorphie d'objets de $\mathfrak{F}$ est le sous-foncteur de F formé des $(\tilde{C},p;e)$ tels que $p^{-1}(e)$ soit localement isomorphe à $\underline{\mathbb{Z}/n}$ et que A soit l'image de $\tilde{C}_n$. Ces conditions sont ouvertes (car A est de type multiplicatif), donc $[\mathfrak{F}]$ est représenté par T étale sur S.

Là où C est lisse, on sait que $T \xrightarrow{\sim} S$. Par ailleurs, un 1-gone sur k algébriquement clos admet un unique revêtement étale par un n-gone. Toutes les fibres géométriques de T/S sont donc réduites à un point, et $T \xrightarrow{\sim} S$. Ceci prouve 1.4.

Soit p un nombre premier.

Théorème 1.6. $\mathfrak{M}_{\Gamma_0(p)}$ est le champ algébrique classifiant les courbes elliptiques généralisées C/S, munies d'un sous-schéma en groupes A localement libre de rang p, qui rencontre chaque composante irréductible de chaque fibre géométrique de C/S.

Preuve : Rappelons [22] qu'un schéma en groupes (commutatifs) localement libre de rang p est tué par p. Pour A comme plus haut, on a donc $A \subset C_p$.

Notons provisoirement $'\mathfrak{M}_{\Gamma_0(p)}$ le champ qui à chaque schéma S associe la catégorie ayant pour objets les (C,A) comme en 1.6 et pour morphismes les isomorphismes. En IV.4.3, nous avons construit un isomorphisme entre $\mathfrak{M}^0_{\Gamma_0(p)}[1/p]$ et $'\mathfrak{M}^0_{\Gamma_0(p)}[1/p]$. L'isomorphisme 1.6 prolongera cet isomorphisme; raisonnant comme en IV.3.5, on trouve que 1.6 résulte de la conjonction des assertions suivantes

A. $'\mathfrak{M}_{\Gamma_0(p)}$ est un champ algébrique.

B. $'\mathfrak{M}_{\Gamma_0(p)}$ est propre sur $\mathrm{Spec}(\mathbb{Z})$.

C. Le morphisme $c : '\mathfrak{M}_{\Gamma_0(p)} \to \mathfrak{M}_1 : (C,A) \mapsto c(C)$ défini par IV.14. est fini et représentable.

D. $'\mathfrak{M}_{\Gamma_0(p)}$ est normal.

E. $'\mathfrak{M}_{\Gamma_0(p)}[1/p]$ est dense dans $'\mathfrak{M}_{\Gamma_0(p)}$.

(1) Points à l'infini de $'\mathfrak{M}_{\Gamma_0(p)}$.

Soit C le polygone de Néron à un côté sur Spec($\mathbb{Z}$) . On a $C^{reg} \simeq \mathbb{G}_m$, $C_p \simeq \mu_p$ et (C,C_p) est une section e_1 de $'\mathfrak{M}_{\Gamma_0(p)}$ sur $\mathbb{Z}$.

Soit C le p-gone sur Spec($\mathbb{Z}$) . On a $C^{reg} \simeq G_m \times \mathbb{Z}/p$, $C_p \simeq \mu_p \times \mathbb{Z}/p$ et $(C,e \times \mathbb{Z}/p)$ est une section e_2 de $'\mathfrak{M}_{\Gamma_0(p)}$ sur $\mathbb{Z}$.

Soit k un corps algébriquement clos. On vérifie que les seuls objets (C,A) de $'\mathfrak{M}_{\Gamma_0(p)}(k)$, avec C singulier, sont $e_1(k)$ et $e_2(k)$.

(2) Preuve de A (représentabilité de $'\mathfrak{M}_{\Gamma_0(p)}$) .

Soient $\mathfrak{U}_1$ et $\mathfrak{U}_2$ les deux ouverts suivants de $'\mathfrak{M}_{\Gamma_0(p)}$: $\mathfrak{U}_1$ classifie les courbes (C,A) comme en 1.6, les fibres géométriques de C étant irréductibles, et $\mathfrak{U}_2$ classifie les courbes (C,A) , les fibres géométriques de C étant lisses ou des p-gones.

Lemme 1.7. Le morphisme "oubli" : $\varphi : \mathfrak{U}_1 \to \mathfrak{M}_1$ est représentable.

Preuve. Il faut voir que pour C/S une courbe elliptique généralisée à fibres géométriques irréductibles sur S , le foncteur suivant $F : (Sch/S) \to (Ens)$ est représentable. A T/S , F associe l'ensemble des sous-schémas en groupes finis localement libres de rang p de C_T^{reg} . La représentabilité de F résulte de la théorie des schémas de Hilbert.

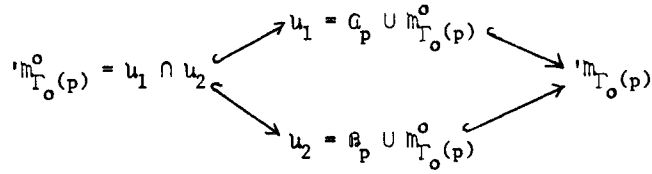
D'après 1.7 et IV.2., $\mathfrak{U}_1$ est un champ algébrique. Nous verrons ci-dessous que $\mathfrak{U}_1$ et $\mathfrak{U}_2$ sont isomorphes. Le champ $\mathfrak{U}_2$ est donc algébrique, ainsi que $'\mathfrak{M}_{\Gamma_0(p)}$, réunion de $\mathfrak{U}_1$ et $\mathfrak{U}_2$ d'après (1) .

1.8. Soit (C,A) classifié par $\mathfrak{U}_2$. D'après II.1.20, C_p est localement libre de rang p^2 . On vérifie fibre par fibre que A agit librement sur C , et ceci permet de définir

(1.8.1) $$w : \mathfrak{U}_2 \to \mathfrak{U}_1 : (C,A) \mapsto (C/A,\ C_p/A_p) \quad .$$

Lemme 1.8.2. Le morphisme (1.8.1) est un isomorphisme .

Avec les notations 1.1 et 1.3, on a



La construction IV.4.4. montre encore que w induit une involution de $'\mathfrak{M}^{o}_{\Gamma_o}(p)$. En 1.4, on a vu que w induit un isomorphisme $\mathcal{C}_p \to \mathcal{B}_p$, et 1.8.2 en résulte.

Ceci achève la démonstration de (A) . La démonstration nous a fourni la construction suivante.

Construction 1.9. Par recollement de $w : U_2 \to U_1$ et de $w^{-1} : U_1 \to U_2$, on obtient une involution $w : '\mathfrak{M}_{\Gamma_o}(p) \to '\mathfrak{M}_{\Gamma_o}(p)$, qui prolonge l'involution (IV.4.4) .

La réunion de $\mathcal{C}_p$ et $\mathcal{B}_p$ est l'ouvert de $'\mathfrak{M}_{\Gamma_o}(p)$ correspondant aux courbes non supersingulières de caractéristique p . Les propositions 1.2 et 1.4 fournissent donc :

Proposition 1.10. $'\mathfrak{M}_{\Gamma_o}(p)$ est lisse sur $\mathrm{Spec}(\mathbb{Z})$ en dehors des points supersinguliers de caractéristique p .

(3) Preuve de (B) (propreté de $'\mathfrak{M}_{\Gamma_o}(p)$) .

D'après (1.10), $'\mathfrak{M}^{o}_{\Gamma_o}(p)$ est dense dans $'\mathfrak{M}_{\Gamma_o}(p)$. Le critère valuatif de propreté nous ramène alors à démontrer le lemme suivant.

Lemme 1.11. Soit (S,η,s) un trait complet à corps résiduel algébriquement clos. Soit (C,A) un objet de $'\mathfrak{M}^{o}_{\Gamma_o}(p)(\eta)$. Il existe une extension finie $k(\eta')$ de $k(\eta)$ telle que, notant S' le normalisé de S dans $k(\eta')$, l'image (C',A') de (C,A) dans $'\mathfrak{M}^{o}_{\Gamma_o}(p)(\eta')$ provienne par changement de base d'un objet $(\overline{C},\overline{A})$ de $'\mathfrak{M}_{\Gamma_o}(p)(S')$, unique à isomorphisme unique près.

Preuve : Quitte à faire une extension préalable de $k(\eta)$, on peut supposer que C a réduction semi-stable et que la fibre spéciale de son modèle minimal $\widetilde{C}$ soit lisse ou un m-gone, avec $p|m$ (IV.1.6). Le groupe $\widetilde{C}_p$ est alors fini sur S (II.1.20) et l'adhérence schématique de A est un sous-schéma en groupes fini localement libre de rang p de $\widetilde{C}$. On obtient $(\overline{C},\overline{A})$ en contractant les composantes de $\widetilde{C}_s$ qui ne rencontrent pas A (IV.1.3).

L'unicité se démontre comme (IV.1.6 (iv)) : Si $(\overline{C}_1,\overline{A}_1)$ a pour fibre générale C , on obtient le modèle minimal $\widetilde{C}$ de C en éclatant successivement les singularités, comme en (IV.1.6 (iv)). L'image réciproque de $\overline{A}_1$ est l'adhérence schématique $\widetilde{A}$ de A et il est clair que C est obtenu en contractant les composantes irréductibles de $\widetilde{C}_s$ dont l'intersection avec $\widetilde{A}$ est vide, d'où l'unicité.

(4) Preuve de C (c fini représentable) .

Pour vérifier que les fibres géométriques de c sont finies, nous distinguerons trois cas.

a) Fibres à l'infini : sur k algébriquement clos, il n'y a qu'un nombre fini (deux) de classes d'isomorphie de couples (C,A) classifiés par $'\mathfrak{M}^{o}_{\Gamma_o}(p)$, avec C singulier.

b) Fibres à distance finie : Soient C une courbe elliptique sur k et T la fibre de c en le point géométrique $\mathrm{Spec}(k) \to \mathfrak{M}^{o}_{1}$ défini par C . T représente le foncteur des sous-schémas en groupes de rang p de C_p . Distinguons les cas $C_p \simeq \mathbb{Z}/p \times \mu_p$ et $\mathrm{car}(k) = p$, $C_p \simeq \alpha_{p^2}$.

b1) On a une suite exacte $0 \to \mu_p \to C_p \to \mathbb{Z}/p \to 0$ (1) .

Pour tout schéma S , et $A \subset C_S$ localement libre de rang p , on a alors $S = S' \amalg S''$, avec $A \xrightarrow{\sim} \mathbb{Z}/p$ sur S'' et $A \subset \mu_p$, donc $A = \mu_p$ sur S' . On a donc $T = T' \cup T''$; T' est réduit, et réduit au point défini par $\mu_p \subset C_p$. T'' représente le foncteur des trivialisations $\mathbb{Z}/p \to C_p$ de la suite exacte (1) . C'est un torseur sous μ_p . Le schéma T a donc $p+1$ (resp.2) points géométriques si $\mathrm{car}(k) \neq p$ (resp. $= p$) .

b2) $C_p \simeq \alpha_{p^2}$. Tout sous-groupe de α_{p^2} est infinitésimal. Si d'ordre p , il est égal au noyau de Frobenius α_p , et T n'a qu'un point géométrique.

Puisque $'\mathbb{M}_{\Gamma_0(p)}$ est propre, c , propre à fibres finies, est fini. Pour prouver c représentable, on procède comme en IV.3.5 : on vérifie sur que pour (C,A) singulier, $\mathrm{Aut}(C,A) = \{\pm 1\}$, de sorte que

$$\mathrm{Aut}(C,A) \hookrightarrow \mathrm{Aut}(c(C)) \quad .$$

(5) Le point clef de la démonstration est le lemme suivant.

Lemme 1.12. *Le morphisme* $c : \mathbb{M}^o_{\Gamma_0(p)} \to \mathbb{M}^o$ *est fini et plat.*

Preuve : Nous prouverons 1.12 à l'aide du critère suivant, applicable car $\mathbb{M}^o_1$ est réduit.

Lemme 1.13. *Soit* $f : X \to S$ *un morphisme fini de schémas noethériens, avec* S *réduit. Si le rang des fibres géométriques de* f *est constant, alors* f *est plat.*

On peut supposer que S est le spectre d'un anneau local A , et que X est le spectre d'une A-algèbre finie B . Soient m l'idéal maximal de A et $\bar{e}_1 \ldots \bar{e}_n$ une base du A/m-espace vectoriel B/mB . Relevons les $\bar{e}_i$ en des éléments $e_i \in B$. D'après le lemme de Nakayama, les e_i engendrent le A-module B . Si $\Sigma \lambda_i e_i = 0$, avec $\lambda_i \in A$, il résulte de l'hypothèse que les λ_i sont nuls modulo tout idéal premier, donc nuls puisque A est réduit; le A-module B est donc libre de base les e_i .

Vérifions que le morphisme 1.12 vérifie l'hypothèse de 1.13.

Soit donc C une courbe elliptique sur un corps algébriquement clos k . La fibre T de c en le point géométrique $\mathrm{Spec}(k) \to \mathbb{M}^o$ défini par C représente le foncteur des sous-schémas en groupes de rang p de C_p . Prouvons qu'il est de rang $p+1$.

Si $C_p \simeq \mu_p \times \mathbb{Z}/p$, on a vu en (4) que T est isomorphe à $\mathrm{Spec}(k) \amalg \mu_p$,

donc de rang $p+1$

Il reste à traiter le cas où k est de caractéristique p et que $C_p \simeq \alpha_{p^2}$. Dans ce cas, T représente le foncteur des sous-schémas localement libre de rang p A de $\mathbb{G}_a$, contenus dans α_{p^2} .

Un sous-schéma localement libre de rang p A de $\mathbb{G}_a$, sur une base quelconque, est défini par une équation

$$(*) \qquad X^p + \sum_0^{p-1} a_i X^i = 0 \quad .$$

Pour que A soit stable par l'homothétie $X \mapsto nX$ $(n \in (\mathbb{Z}/p)^*)$, il faut et il suffit que (*) soit identique à l'équation

$$X^p + \sum_0^{p-i} n^{p-i} a_i X^i \quad .$$

En particulier, si A est un sous-schéma en groupes de $\mathbb{G}_a$, son équation se réduit à

$$X^p - a X = 0 \quad .$$

Pour que A soit sous-schéma de α_{p^2} , il faut et il suffit que le premier membre de cette équation divise X^{p^2} . Puisque

$$X^{p^2} = (X^p - aX) \cdot \left(\sum_{i=0}^{p} a^i X^{p^2-i(p-1)-p} \right) + a^{p+1} X \quad ,$$

tel est le cas si et seulement si $a^{p+1} = 0$. On a

$$T \simeq \mathrm{Spec}(k[a]/(a^{p+1})) \quad ,$$

et ceci achève la démonstration de 1.12.

Puisque c est fini et plat et $\mathfrak{M}^c$ régulier, $'\mathfrak{M}^o_{\Gamma_o(p)}$ est de Cohen-Macaulay (EGA IV.15 4.2) , purement de dimension relative un sur $\mathrm{Spec}(\mathbb{Z})$. A l'infini, $\mathfrak{M}_{\Gamma_o(p)}$ est même lisse (1.10); $'\mathfrak{M}_{\Gamma_o(p)}$ tout entier est donc de Cohen-Macaulay et, d'après 1.10 encore, lisse sur $\mathrm{Spec}(\mathbb{Z})$ en dehors d'un ensemble fini (de codimension 2). Dès lors, (D) résulte du critère de normalité de Serre (EGA IV. 5.8.6).

1.14. Variantes : Soit n un entier premier à p, $H \subset GL(2, \mathbb{Z}/n)$ et K l'image réciproque de H dans $GL(2, \hat{\mathbb{Z}})$. Le théorème 1.6 se généralise aux $\mathfrak{M}_{K \cap \Gamma_o(p)}[1/n]$:

(1.14.1) $\mathfrak{M}_{\Gamma(n) \cap \Gamma_o(p)}[1/n]$ classifie les courbes elliptiques généralisées C/S, de fibres géométriques lisses, des n-gones ou des np-gones, munies d'un isomorphisme $\alpha : C_n \xrightarrow{\sim} (\mathbb{Z}/n)^2$ et d'un sous-groupe localement libre de rang p H de C tel que $C_n.H$ rencontre chaque composante géométrique de chaque fibre géométrique.

(.14.2) Pour n sans facteur carré, $\mathfrak{M}_{\Gamma_o(n)}$ classifie les courbes elliptiques généralisées C/S munies d'un sous-groupe localement libre de rang n H de C, qui rencontre chaque composante géométrique de chaque fibre géométrique.

1.15. Soit S un schéma de caractéristique p et E une courbe elliptique sur S. A E, on associe les deux objets suivants de $\mathfrak{M}^o_{\Gamma_o(p)}(S)$.

$$\Phi_1(E) : (E, \mathrm{Ker}(F : E \to E^{(p)}))$$

$$\Phi_2(E) = w\Phi_1(E) : (E^{(p)}, \mathrm{Ker}(V : E^{(p)} \to E))$$

Dans ces formules, F désigne le morphisme de Frobenius et V son transposé, la Verschiebung : $FV = VF = p$. Ces constructions définissent un diagramme

$$\begin{array}{ccccc} \mathfrak{M}^o_1 \otimes \mathbb{F}_p & & & & \mathfrak{M}^o_1 \otimes \mathbb{F}_p \\ & \searrow^{\Phi_1} & & \swarrow^{w\Phi_1} & \\ & & \mathfrak{M}^o_{\Gamma_o(p)} \otimes \mathbb{F}_p & & \\ & \swarrow^{c} & & \searrow^{cw} & \\ \mathfrak{M}^o_1 \otimes \mathbb{F}_p & & & & \mathfrak{M}^o_1 \otimes \mathbb{F}_p \end{array}$$

Les composés $c\Phi_1 : E \mapsto (E, \mathrm{Ker}\ F) \mapsto E$ et $cww\Phi_1$ sont l'identité. Les composés $cw\Phi_1 : E \mapsto (E^{(p)}, \mathrm{Ker}\ V) \mapsto E^{(p)}$ sont l'endomorphisme de Frobenius de $\mathfrak{M}^o_1 \otimes \mathbb{F}_p$.

Théorème 1.16 (i) Les applications Φ_1 et $\Phi_2 = w\Phi_1$ sont des plongements fermés. Leurs images sont les deux composantes irréductibles de $\mathcal{M}^o_{\Gamma_o(p)} \otimes \mathbb{F}_p$.

(ii) Ces composantes irréductibles se coupent transversalement en les points supersinguliers. Le champ $\mathcal{M}_{\Gamma_o(p)} \otimes \mathbb{F}_p$, qui est réduit, n'a donc pour seules singularités que des points doubles ordinaires .

(iii) $\mathcal{M}_{\Gamma_o(p)}$ est régulier.

Indiquons par un exposant ^{h} le champ obtenu en ôtant les points supersinguliers de caractéristique p On vérifie que Φ_1 et $w\Phi_1$ définissent un isomorphisme

$$\Phi_1 \amalg w\Phi_1 : \mathcal{M}_1^{oh} \otimes \mathbb{F}_p \amalg \mathcal{M}_1^{oh} \otimes \mathbb{F}_p \xrightarrow{\sim} \mathcal{M}^{oh}_{\Gamma_o(p)} \otimes \mathbb{F}_p \ .$$

L'isomorphisme réciproque est défini par c et cw , restreints aux images de Φ_1 et $w\Phi_1$.

Que Φ_1 (resp. $w\Phi_1$) soit un plongement fermé résulte de l'existence d'une rétraction (car ce sont des morphismes représentables). On sait (IV.5.6) que $\mathcal{M}_1 \otimes \mathbb{F}_p$ est géométriquement irréductible, et ceci prouve (i).

$\mathcal{M}_{\Gamma_o(p)}$ est réduit car de Cohen-Macaulay et génériquement réduit (I.7.3.). Les points supersinguliers sont dans l'image tant de Φ_1 que de Φ_2 car, pour E une courbe elliptique supersingulière sur k algébriquement clos, le seul sous-groupe de rang p est $\mathrm{Ker}(F) = \mathrm{Ker}(V : E \to E^{(1/p)})$. Les deux composantes irréductibles de $\mathcal{M}^o_{\Gamma_o(p)}$ mod p se coupent donc en ces points. L'intersection est transversale, car les vecteurs tangents aux deux branches sont linéairement indépendants : l'un est annulé par dc et non par d(wc) , l'autre par d(wc) et non par dc . Ceci prouve (ii). Nous prouverons (iii) en 1.19.

Variante 1.17. Soit $n \geq 3$, et considérons $\mathcal{M}^o_{\Gamma(n) \cap \Gamma_o(p)}$. Ce champ, ainsi que $\mathcal{M}^o_{\Gamma(n)}$, est un schéma : les objets classifiés n'ont pas d'automorphismes (cf. IV.2.7). D'après 1.14, ces schémas représentent les foncteurs de classes d'isomorphie d'objets du type suivant

$$\mathcal{M}^{o}_{\Gamma(n)} : (E,\alpha_n) : \alpha_n : E_n \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^2 \quad ;$$

$$\mathcal{M}_{\Gamma(n)\cap\Gamma_o(p)} : (E,\alpha_n,H) : \alpha_n : E_n \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^2 \ ; \ H \subset E \text{ de rang } p \ ,$$

ou plus symétriquement (cf. IV.4.5) ; on pose $F = E/H$)

$$(E \xrightarrow{h} F,\ \alpha_n) : h \text{ p-isogénie et } \alpha_n : E_n \xrightarrow{\sim} F_n \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^2 \ .$$

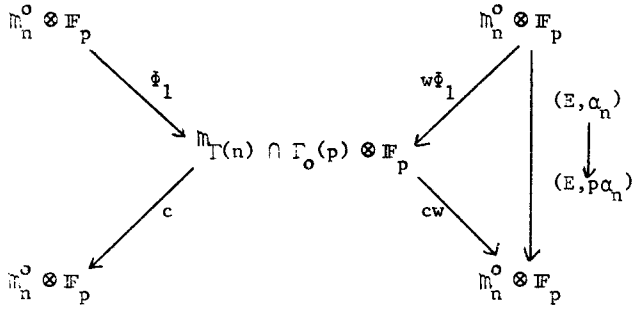
Après réduction mod p , on dispose d'un diagramme analogue à (1.15.1). En voici les flèches (exprimées comme morphismes de foncteurs)

$$\Phi_1 : \mathcal{M}^{o}_{\Gamma(n)} \otimes \mathbb{F}_p \to \mathcal{M}^{o}_{\Gamma(n)\cap\Gamma_o(p)} \otimes \mathbb{F}_p : (E,\alpha_n) \longmapsto (E,\alpha_n, \operatorname{Ker} F)$$

$$w : \mathcal{M}^{o}_{\Gamma(n)\cap\Gamma_o(p)} \xrightarrow{\sim} \mathcal{M}^{o}_{\Gamma(n)\cap\Gamma_o(p)} : (E,\alpha_n,H) \longmapsto (E/H,\alpha_n,E_p/H)$$

$$c : \mathcal{M}^{o}_{\Gamma(n)\cap\Gamma_o(p)} \longrightarrow \mathcal{M}^{o}_{\Gamma(n)} : (E,\alpha_n,H) \longmapsto (E,\alpha_n) \ .$$

On prendra garde que l'isomorphisme $w^2(E,H) \simeq (E,H)$ défini en IV.4.4 induit un isomorphisme $w^2(E,\alpha_n,H) \simeq (E,p\alpha_n,H)$. Le composé $cw\Phi_1 : (E,\alpha_n) \mapsto (E^{(p)},\alpha_n)$ est le Frobenius.



(diagonales composées : Frobenius) .

Sur k algébriquement clos de caractéristique p , la condition

$$\Phi_1((E,\alpha_n)) = w\Phi_1(F,\beta_n)$$

signifie que F est supersingulier, que $E = F^{(p)}$ et que le diagramme

$$\begin{array}{ccc} E_n = F_n^{(p)} & \xleftarrow{\sim} & F_n \\ \downarrow{\scriptstyle \alpha_n} & & \downarrow{\scriptstyle \beta_n} \\ (\mathbb{Z}/n\mathbb{Z})^2 & = & (\mathbb{Z}/n\mathbb{Z})^2 \end{array}$$

est commutatif, i.e. que $(E,\alpha_n) = (F,\beta_n)^{(p)}$. Les points (i) et (ii) de 1.16 admettent donc la variante suivante.

Variante 1.18. Le schéma $\mathcal{M}^o_{\Gamma(n)\cap\Gamma_o(p)} \otimes_{\mathbb{Z}} \overline{\mathbb{F}}_p$ peut s'obtenir en recollant deux copies de $\mathcal{M}^o_{\Gamma(n)} \otimes \overline{\mathbb{F}}_p$ selon les points supersinguliers : on identifie le point supersingulier x de la 2ème copie au point $x^{(p)}$ de la première copie.

1.19. Prouvons que $\mathcal{M}_{\Gamma_o(p)}$ est régulier. En dehors des points supersinguliers, cela résulte de 1.10. Puisqu'en un point supersingulier $\mathcal{M}_{\Gamma_o(p)} \to \mathrm{Spec}(\mathbb{Z})$ présente une singularité quadratique ordinaire, (I.5.2) montre qu'il existe $k \in \mathbb{N}$ tel que le complété de l'anneau strictement local de $\mathcal{M}_{\Gamma_o(p)}$ en un tel point soit isomorphe à $W(\overline{\mathbb{F}}_p)[[X,Y]]/(X.Y - p^k)$ (W = vecteurs de Witt). Si $k = 1$, cet anneau local complet est régulier. Sinon, son spectre admet la section $X = Y = 0$ au-dessus de $W(\mathbb{F}_p)/(p^k)$ $(k > 1)$, et il existe sur $W(\overline{\mathbb{F}}_p)/(p^k)$ une courbe elliptique E , munie d'un sous-groupe localement libre de rang p H , avec E supersingulière en réduction modulo p (donc $H \otimes \overline{\mathbb{F}}_p \simeq \alpha_p$) . Ceci est absurde, car d'après [22] α_p n'admet aucun relèvement sur $W(\overline{\mathbb{F}}_p)/(p^k)$ $(k > 1)$.

1.20. Variantes. Pour $H \subset GL(2, \mathbb{Z}/n)$ d'image réciproque K dans $GL(2, \hat{\mathbb{Z}})$, et $(n,p) = 1$, $\mathcal{M}_{K\cap\Gamma_o(p)}[1/n]$ est régulier. Par exemple, si $n \geq 3$, le schéma $\mathcal{M}_{\Gamma(n)\cap\Gamma_o(p)}[1/n]$ est régulier; pour n sans facteur carré, $\mathcal{M}_{\Gamma_o(n)}$ est régulier.

2. Etude de $\mathcal{M}_{\Gamma_{oo}(p)}$.

2.1. En IV.4, nous avons donné une interprétation modulaire de $\mathcal{M}_{\Gamma_{oo}(p)}[1/p]$: notant (C,A) la courbe elliptique généralisée universelle sur $\mathcal{M}_{\Gamma_o(p)}$, et son image réciproque sur $\mathcal{M}_{\Gamma_o(p)}[\zeta_p, 1/p]$, on a

$$\mathcal{M}_{\Gamma'_{oo}(p)}[1/p] = \underline{\mathrm{Isom}}_{\mathcal{M}_{\Gamma_o(p)}[\zeta_p,\frac{1}{p}]}(\mathbb{Z}/p, A) \quad .$$

Par définition, $\mathcal{M}_{\Gamma'_{oo}(p)}$ est le normalisé de $\mathcal{M}_{\Gamma_o(p)}[\zeta_p]$ dans ce champ $\underline{\mathrm{Isom}}_{\mathcal{M}_0(p)[\zeta_p,1/p]}(\mathbb{Z}/p, A)$. On en déduit facilement la description ci-dessous du champ $\mathcal{M}^h_{\Gamma'_{oo}(p)}$ déduit de $\mathcal{M}_{\Gamma'_{oo}(p)}$ en ôtant les points supersinguliers de caractéristique p .

2.2. Soit $\mathcal{C}'_p \subset \mathcal{M}_{\Gamma_o(p)}$ l'ouvert classifiant les (C,A) avec A localement isomorphe à μ_p (pour la topologie étale), et $\mathcal{B}'_p \subset \mathcal{M}_{\Gamma_o(p)}$ l'ouvert classifiant les (C,A) avec A localement isomorphe à $\mathbb{Z}/p$. Posons

$$\mathcal{U} = \underline{\mathrm{Isom}}_{\mathcal{C}'_p}(\mu_p, A)$$

$$\mathcal{V} = \underline{\mathrm{Isom}}_{\mathcal{B}'_p}(\mathbb{Z}/p, A) \quad ;$$

$\mathcal{U}$ et $\mathcal{V}$ sont finis étales sur $\mathcal{C}'_p$ et $\mathcal{B}'_p$ respectivement. Au-dessus de $\mathbb{Z}[\zeta_p, \frac{1}{p}]$, $\mathbb{Z}/p$ et μ_p sont canoniquement isomorphes, d'où un isomorphisme $\mathcal{U}[\zeta_p, 1/p] \simeq \mathcal{V}[\zeta_p, 1/p]$.

<u>Proposition</u> 2.3. $\mathcal{M}^h_{\Gamma'_{oo}(p)}$ <u>s'obtient en recollant</u> $\mathcal{U}[\zeta_p]$ <u>et</u> $\mathcal{V}[\zeta_p]$ <u>selon l'ouvert commun</u> $\mathcal{U}[\zeta_p,1/p]$. <u>En particulier</u>, $\mathcal{M}^h_{\Gamma'_{oo}(p)}$ <u>est lisse sur</u> $\mathbb{Z}[\zeta_p]$.

Pour étudier $\mathcal{M}_{\Gamma'_{oo}(p)}$ au voisinage des points supersinguliers, nous ferons usage des résultats de [22] rappelés ci-dessous.

2.4. Le foncteur F qui à un schéma S associe l'ensemble des isomorphismes $\chi : \mathbb{F}_p^* \xrightarrow{\sim} \mu_{p-1}$ vérifiant (2.4.1) ci-dessous est représentable par un schéma $\mathrm{Spec}(\Lambda_p)$.

(2.4.1) En tout point s de caractéristique p de S , l'isomorphisme induit par $\chi : \mathbb{F}_p^* \xrightarrow{\sim} \mu_{p-1}(k(s)) \simeq \mathbb{F}_p^*$ est l'identité.

$\mathrm{Spec}(\Lambda_p)$ est isomorphe à l'ouvert de $\mathrm{Spec}(\mathbb{Z}[\zeta_{p-1}])$ obtenu en enlevant les places divisant $p-1$ et toutes les places au-dessus de p sauf une. $\mathrm{Spec}(\Lambda_p)$

est étale sur $\mathrm{Spec}(\mathbb{Z})$ et $\mathbb{F}_p \xrightarrow{\sim} \Lambda_p \otimes \mathbb{F}_p$.

Soient S muni de χ vérifiant (2.4.1) (S est un Λ_p-schéma) et A un schéma en groupes localement libre de rang p sur S . Soit L le sous-module de l'algèbre affine $G(A)$ de A (un faisceau de $\mathcal{O}_S$-algèbres) formé des f tels que

$$f(ix) = \chi(i)\, f(x) \qquad (i \in \mathbb{F}_p^*) \ .$$

D'après [22], L est un module inversible sur S , et il existe une unique section a de $L^{\otimes(1-p)}$ tel que pour f comme plus haut

$$f^p = \langle a, f^{p-1} \rangle . f \qquad \text{dans} \quad L \subset G(A) \ .$$

Soit A^* le dual de Cartier de A et L^* défini par A^* . La dualité e entre $G(A)$ et $G(A^*)$ met L et L^* en dualité. Soit $b \in (L^*)^{\otimes 1-p}$ l'analogue pour A^* de a ci-dessus. Alors,

$$a.b = w(\chi)$$

pour un certain nombre $w(\chi) \in \Lambda_p$, avec $(w(\chi)) = (p)$ dans Λ_p .

Le foncteur (pour les isomorphismes) (A : schéma en groupes localement libre de rang p) $\longmapsto$ ((L,a,b) : L inversible, $a \in L^{\otimes(1-p)}$, $b \in L^{\otimes(p-1)}$, $a.b = w(\chi)$) est une équivalence de catégories.

L'ensemble des sections de A sur S s'identifie à l'ensemble des sections s de L^* sur S telles que $s^{\otimes p} = as$. Pour que s définisse un isomorphisme entre A et $\mathbb{Z}/p$, il faut et il suffit que s soit une section inversible de L .

Exemples : On a

(2.4.2) $\qquad \mathbb{Z}/p \mapsto (\mathcal{O}_S, 1, w(\chi))$

(2.4.3) $\qquad \mu_p \mapsto (\mathcal{O}_S, w(\chi), 1)$

(2.4.4) $\qquad \alpha_p \mapsto (\mathcal{O}_S, 0, 0)$.

2.5. Soit donné sur S un isomorphisme $\zeta : \mathbb{Z}/p \xrightarrow{\sim} \mu_p$ (S est un $\Lambda_p[\zeta_p, 1/p]$-schéma). L'isomorphisme ζ définit $\zeta^* : G(\mu_p) \to G(\mathbb{Z}/p)$ et, via (2.4.2) (2.4.3), induit $\zeta^* : \mathcal{O}_S = L(\mu_p) \longrightarrow L(\mathbb{Z}/p) = \mathcal{O}_S$: la multiplication par un nombre $w(\chi,\zeta) \in \Lambda_p[\zeta_p]$. On a

$$w(\chi,\zeta)^{p-1} = w(\chi) \quad .$$

Un isomorphisme $s : \mathbb{Z}/p \xrightarrow{\sim} A$ définit par dualité $s^* : A^* \xrightarrow{\sim} \mu_p \simeq \mathbb{Z}/p$ d'inverse t. Les sections $s(1)$ et $t(1)$ s'identifient à des sections x et y de L^* et L avec

$$x^{p-1} = a \qquad y^{p-1} = b$$

$$xy = w(\chi,\zeta) \quad .$$

2.6. Soit ${}'\mathfrak{M}_{\Gamma'_{oo}(p)} \otimes \Lambda_p$ le $\Lambda_p[\zeta_p]$-champ algébrique sur $\mathfrak{M}_{\Gamma_o(p)} \otimes \Lambda_p[\zeta_p]$ suivant : un objet (C,A,x,y) de ${}'\mathfrak{M}_{\Gamma_{oo}(p)} \otimes \Lambda_p$ sur un $\Lambda_p[\zeta_p]$ schéma S consiste en

a) un objet (C,A) de $\mathfrak{M}_{\Gamma_o(p)}$. Soit (L,a,b) déduit de A.

b) des sections x de L^* et y de L telles que $x^{p-1} = a, y^{p-1} = b$ et que $xy = w(x,\zeta)$.

Les constructions 2.5 et IV.4.8 définissent un isomorphisme

$$\mathfrak{M}_{\Gamma'_{oo}(p)} \otimes \Lambda_p[1/p] \simeq {}'\mathfrak{M}_{\Gamma'_{oo}(p)} \otimes \Lambda_p[1/p] \quad . \tag{2.6.1}$$

Théorème 2.7. L'isomorphisme 2.6.1 se prolonge en un isomorphisme

$$\mathfrak{M}_{\Gamma'_{oo}(p)} \otimes \Lambda_p \simeq {}'\mathfrak{M}_{\Gamma'_{oo}(p)} \otimes \Lambda_p \quad .$$

Montrons tout d'abord que l'isomorphisme (2.6.1) se prolonge en dehors des points supersinguliers (on interprète le membre de gauche par 2.3). Au-dessus de l'ouvert $\mathcal{B}'_p$ de $\mathfrak{M}_{\Gamma_o(p)}$ (A étale), a est inversible; se donner x tel que $x^{p-1} = a$ revient à se donner un isomorphisme de $\mathbb{Z}/p$ avec A, et (x,ζ) détermine y uniquement. Dualement, au-dessus de $\mathcal{C}'_p$ (A^* étale), b est inversible. Se donner y tel que $y^{p-1} = b$ revient à se donner un isomorphisme de μ_p avec A, et (y,ζ)

détermine x uniquement. Là où p est inversible, ces deux constructions sont compatibles, via l'isomorphisme $\zeta : \mathbb{Z}/p \xrightarrow{\sim} \mu_p$.

Le champ $'\mathcal{M}_{\Gamma'_{oo}}(p) \otimes \Lambda_p$ est fini représentable sur $\mathcal{M}_{\Gamma_o}(p) \otimes \Lambda_p$. Il nous suffit donc de prouver que $'\mathcal{M}_{\Gamma'_{oo}}(p) \otimes \Lambda_p$ est normal en les points supersinguliers. Le lemme suivant montre que $'\mathcal{M}_{\Gamma'_{oo}}(p) \otimes \Lambda_p$ est même régulier en ces points.

Lemme 2.8. Soit $\bar{s}$ un point géométrique supersingulier de caractéristique p de $\mathcal{M}_{\Gamma_o}(p)$. Soit $\hat{S}$ le complété de l'hensélisé strict de $\mathcal{M}_{\Gamma_o}(p)$ en $\bar{s}$, muni de son unique structure de Λ_p-algèbre. Soient (C,A) sur $\hat{S}$ défini par $\hat{S} \to \mathcal{M}_{\Gamma_o}(p)$ et (L,a,b) défini par A .

(i) $\hat{S} \simeq W(\bar{\mathbb{F}}_p)[[u,v]]/(uv-w(\chi))$ avec $(L,a,b) \simeq (\mathcal{G},u,v)$.

(ii) Le normalisé $'\mathcal{M}_{\Gamma_{oo}}(p) \otimes_{\mathcal{M}_{\Gamma_o}(p)} \hat{S}$ de $\hat{S}$ dans $\mathrm{Isom}_{\hat{S}[\zeta_p,1/p]}(\mathbb{Z}/p,A)$ est $\hat{S}$-isomorphe à

$$W(\bar{\mathbb{F}}_p)[[\zeta_p,x,y]]/(xy-w(\chi,\zeta)) \simeq W(\bar{\mathbb{F}}_p)[[x,y]]/(x^{p-1}\, y^{p-1} - w(\chi))$$

avec $x^{p-1} = u$ et $y^{p-1} = v$.

On sait que $\hat{S} \simeq W(\mathbb{F}_p)[[u,v]]/(uv - p)$ (1.16), que $ab = w(\chi) = p.\text{unité}$ (cf.2.5) et que a et b s'annulent aux points supersinguliers (2.4.4). (i) et (ii) en résultent.

Remarque 2.9. Il résulte de 2.4, 2.4.4 et 2.8 (ii) que $\hat{S}$, muni de A , est un schéma formel versel de modules pour les déformations de α_p

Variante 2.10. Voici comment modifier 2.6 pour obtenir une description modulaire de $\mathcal{M}_{\Gamma'_{oo}}(p)$: c'est le champ algébrique sur $\mathbb{Z}[\zeta_p]$ dont les sections sur un $\mathbb{Z}[\zeta_p]$-schéma S classifient les objets (C,H) de $\mathcal{M}_{\Gamma_o}(p)$ sur S , munis de

a) un morphisme $\mathbb{Z}/p \xrightarrow{\sim} H$ au-dessus de $S[1/p]$;

b) au-dessus de $S \otimes \Lambda_p$, où H définit (L,a,b) , des sections x de L^* et y de L telles que $x^{p-1} = a$, $y^{p-1} = b$, $xy = w(\chi,\zeta)$.

On exige que ces deux données soient compatibles, via le dictionnaire 2.4, sur $S \otimes \Lambda_p[1/p]$.

2.11. Avec les notations de 2.2 et de 1.1 et 1.3, $\mathcal{U} \otimes \mathbb{F}_p$ et $\mathcal{V} \otimes \mathbb{F}_p$ sont des revêtements étales de $\mathcal{G}_p \otimes \mathbb{F}_p$ et $\mathcal{B}_p \otimes \mathbb{F}_p$ respectivement. Les morphismes Φ_1 et $w\Phi_1$ (cf. 1.15) identifient $\mathcal{G}_p \otimes \mathbb{F}_p$ et $\mathcal{B}_p \otimes \mathbb{F}_p$ à des ouverts de $\mathcal{M}_1 \otimes \mathbb{F}_p$; via cette identification, le théorème de structure local 2.8, montre que les revêtements $\mathcal{U} \otimes \mathbb{F}_p$ et $\mathcal{V} \otimes \mathbb{F}_p$ de $\mathcal{M}_1^h \otimes \mathbb{F}_p$ se ramifient complètement en les points supersinguliers de $\mathcal{M}_1 \otimes \mathbb{F}_p$. En particulier, $\mathcal{U} \otimes \mathbb{F}_p$ et $\mathcal{V} \otimes \mathbb{F}_p$ sont géométriquement irréductibles et $\mathcal{M}_{\Gamma'_{oo}(p)} \otimes \mathbb{F}_p$ a deux composantes irréductibles, images réciproques des composantes irréductibles de $\mathcal{M}_{\Gamma_o(p)} \otimes \mathbb{F}_p$. La démonstration de 2.7 fournit le résultat suivant.

Théorème 2.12 (i) Les deux composantes irréductibles de $\mathcal{M}_{\Gamma'_{oo}(p)} \otimes \mathbb{F}_p$ sont lisses et se coupent transversalement en les points supersinguliers.

(ii) $\mathcal{M}_{\Gamma'_{oo}(p)}$ est un schéma régulier ; $\mathcal{M}_{\Gamma'_{oo}(p)} \to \mathrm{Spec}(\mathbb{Z}[\zeta_p])$ ne présente que des singularités quadratiques.

(iii) $\mathcal{M}_{\Gamma'_{oo}(p)} \to \mathcal{M}_{\Gamma_o(p)}$ induit une bijection (une équivalence de catégorie) sur les points géométriques supersinguliers de caractéristique p .

2.13. Soit n un entier ≥ 3 et premier à p . Comme en 1.17, on peut rendre 2.12 plus concret en passant au schéma $\mathcal{M}_{\Gamma(n) \cap \Gamma'_{oo}(p)}$. Soit $\mathcal{J}_n^h$ le revêtement étale $\underline{\mathrm{Isom}}(\mu_p, (\mathcal{C}_p)^o)$ de $\mathcal{M}^h_{\Gamma(n)} \otimes \mathbb{F}_p$. Il se prolonge en un revêtement $\mathcal{J}_n$ de $\mathcal{M}_{\Gamma(n)} \otimes \mathbb{F}_p$, complètement ramifié en les points supersinguliers, et $\mathcal{M}_{\Gamma(n) \cap \Gamma'_{oo}(p)} \otimes_{\mathbb{Z}[\zeta_p]} \overline{\mathbb{F}}_p$ s'obtient en recollant deux copies de $\mathcal{J}_{n,p} \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p$ selon les points supersinguliers, en identifiant x de la 2^e copie à $x^{(p)}$ de la première (comme en 1.17). En particulier, le morphisme $\mathcal{M}_{\Gamma(n) \cap \Gamma'_{oo}(p)} \otimes_{\mathbb{Z}[\zeta_p]} \overline{\mathbb{F}}_p \to \mathcal{M}_{\Gamma(n) \cap \Gamma_o(p)} \otimes_{\mathbb{Z}} \overline{\mathbb{F}}_p$ induit une bijection sur les ensembles de composantes irréductibles, et $\mathcal{M}_{\Gamma(n) \cap \Gamma'_{oo}(p)} \otimes \overline{\mathbb{F}}_p \to \mathcal{M}_{\Gamma(n)} \otimes \overline{\mathbb{F}}_p$ induit une bijection sur l'ensemble des points supersinguliers.

Puisque $\mathcal{M}^o_{\Gamma(n) \cap \Gamma'_{oo}(p)}[1/n]$ est fini étale sur $\mathcal{M}^o_{\Gamma'_{oo}(p)}[1/n]$, les

propriétés locales sont les mêmes.

2.14. Soient H un sous-groupe de $(\mathbb{Z}/p)^*$, et d son indice. Nous noterons $\Gamma_{oo}(H)$ et $\Gamma'_{oo}(H)$ les sous-groupe de $GL(2,\hat{\mathbb{Z}})$ images réciproques des sous-groupes suivants de $GL(2,\mathbb{Z}/p)$:

$$\Gamma_{oo}(H) : \begin{pmatrix} H & \mathbb{Z}/p \\ 0 & \mathbb{Z}/p^* \end{pmatrix} \qquad \Gamma'_{oo}(H) : \begin{pmatrix} H & \mathbb{Z}/p \\ 0 & H \end{pmatrix} .$$

Pour $H = \{e\}$ (resp. $H = \mathbb{Z}/p^*$), on a $\Gamma_{oo}(H) = \Gamma_{oo}(p)$ et $\Gamma'_{oo}(H) = \Gamma'_{oo}(p)$ (resp. $\Gamma_{oo}(H) = \Gamma'_{oo}(H) = \Gamma_o(p)$).

Nous noterons $\mathbb{Z}[\zeta_p]^H$ l'anneau des invariants de H agissant sur $\mathbb{Z}[\zeta_p]$ par $i \in H \subset (\mathbb{Z}/p)^* \longmapsto (\zeta_p \mapsto \zeta_p^i)$. On vérifie comme en IV 4, que $\mathfrak{M}_{\Gamma_{oo}(H)}[1/p]$ et $\mathfrak{M}_{\Gamma'_{oo}(H)}[1/p]$ admettent les descriptions suivantes. Si (C,A) est la courbe universelle sur $\mathfrak{M}_{\Gamma_o(p)}$:

(2.14.1) $\mathfrak{M}_{\Gamma_{oo}(H)}[1/p] \simeq \underline{\mathrm{Isom}}_{\mathfrak{M}_{\Gamma_o(p)}[1/p]}(\mathbb{Z}/p, A)/H$ (cf. IV 4.14)

(2.14.2) $\mathfrak{M}_{\Gamma'_{oo}(H)}[1/p] \simeq \mathfrak{M}_{\Gamma_{oo}(H)}[1/p] \otimes \mathbb{Z}[\zeta_p]^H$ (cf. IV 4.15)

La formule (2.14.1) signifie que si S est un schéma sur lequel p est inversible, un objet de $\mathfrak{M}_{\Gamma_{oo}(H)}$ sur S s'identifie à un objet (C,A) de $\mathfrak{M}_{\Gamma_o(p)}$ sur S, muni d'une section globale du faisceau quotient $\underline{\mathrm{Isom}}_S(\mathbb{Z}/p, A)/H$.

2.15. Soit A un groupe localement libre de rang p sur un schéma S sur Λ_p, et soient (L,a,b) définis par A. Ainsi qu'on l'a vu en 2.4, se donner un isomorphisme entre $\mathbb{Z}/p$ et A revient à se donner x inversible tel que $x^{p-1} = a$. Multiplier l'isomorphisme par $i \in (\mathbb{Z}/p)^*$ revient à multiplier x par $\chi(i)$. L'application $x \mapsto x^{(p-1)/d}$ induit donc un isomorphisme de $\underline{\mathrm{Isom}}(\mathbb{Z}/p, A)/H$ avec le faisceau des sections inversibles u de $L^{\otimes(p-1)/d}$ telles que $u^d = a$.

On vérifie que

$$w(\chi,\zeta)^{(p-1)/d} \in \Lambda_p[\zeta_p]^H \quad .$$

2.16. Soit ${}'\mathcal{M}_{\Gamma'_{oo}(H)} \otimes \Lambda_p$ le $\Lambda_p[\zeta_p]^H$ - champ algébrique suivant : un objet de ${}'\mathcal{M}_{\Gamma'_{oo}(H)} \otimes \Lambda_p$ sur un $\Lambda_p[\zeta_p]^H$ - schéma S est un objet (C,A) de $\mathcal{M}_{\Gamma_o(p)}$ sur S, A définissant (L,a,b), suivi de sections u de $L^{\otimes \frac{(1-p)}{d}}$ et v de $L^{\otimes \frac{(p-1)}{d}}$, telles que

$$u^d = a \quad , \quad v^d = b \quad , \quad uv = w(\chi,\zeta)^{\frac{p-1}{d}} \quad .$$

Les constructions 2.14 et 1.15 définissent un isomorphisme

$$(2.16.1) \qquad {}'\mathcal{M}_{\Gamma'_{oo}(H)} \otimes \Lambda_p[1/p] \simeq \mathcal{M}_{\Gamma'_{oo}(H)} \otimes \Lambda_p[1/p] \quad .$$

2.17. Comme en 2.10, on peut modifier cette définition pour obtenir un champ ${}'\mathcal{M}_{\Gamma'_{oo}(H)}$ sur $\mathbb{Z}[\zeta_p]^H$: un objet de ${}'\mathcal{M}_{\Gamma'_{oo}(H)}$ sur un $\mathbb{Z}[\zeta_p]^H$ - schéma S est un objet (C,A) de $\mathcal{M}_{\Gamma_o(H)}$ sur S, muni de

a) u_1, section globale de $\mathrm{Isom}_{S[1/p]}(\mathbb{Z}/p,A)/H$;

b) au-dessus de $S \otimes \Lambda_p$, où A définit (L,a,b), des sections u et v de $L^{\otimes \frac{(1-p)}{d}}$ et $L^{\otimes \frac{(p-1)}{d}}$ avec $u^d = a$, $v^d = b$, $uv = w(\chi,\zeta)^{\frac{p-1}{d}}$.

On exige que ces données soient compatibles, via (2.16.1), sur $S \otimes \Lambda_p[1/p]$.

La démonstration de 2.7 et 2.12 fournit les résultats suivants.

Théorème 2.18. (i) On a $\mathcal{M}_{\Gamma'_{oo}(H)} \simeq \mathcal{M}_{\Gamma'_{oo}(H)}$.

(ii) Le champ $\mathcal{M}_{\Gamma'_{oo}(H)} \otimes_{\mathbb{Z}[\zeta_p]^H} \overline{\mathbb{F}}_p$ a deux composantes irréductibles. Elles sont lisses et se coupent transversalement en les points supersinguliers.

(iii) $\mathcal{M}_{\Gamma'_{oo}(H)}$ est un schéma régulier; $\mathcal{M}_{\Gamma'_{oo}(H)} \to \mathrm{Spec}(\mathbb{Z}[\zeta_p]^H)$ ne présente que des singularités quadratiques.

(iv) $\mathcal{M}_{\Gamma'_{oo}(H)} \to \mathcal{M}_{\Gamma_o(p)}$ induit une bijection (équivalence de catégories) sur les points géométriques supersinguliers de caractéristique p .

2.19. Soit n un entier premier à p et ≥ 3. Le théorème 2.18 se généralise aux schémas $\mathfrak{M}_{\Gamma(n)\cap\Gamma'_{oo}(H)}[1/n]$.

(i) $\mathfrak{M}_{\Gamma(n)\cap\Gamma'_{oo}(H)}[1/n]$ est régulier.

(ii) $\mathfrak{M}_{\Gamma(n)\cap\Gamma'_{oo}(H)}[1/n] \to \mathrm{Spec}(\mathbb{Z}[\zeta_p, \frac{1}{p}]^H)$ est lisse en dehors des points supersinguliers de caractéristique p, où on a des points quadratiques ordinaires.

(iii) $\mathfrak{M}_{\Gamma(n)\cap\Gamma'_{oo}(H)} \otimes_{\mathbb{Z}[\zeta_p]^H} \overline{\mathbb{F}}_p \to \mathfrak{M}_{\Gamma(n)} \otimes_{\mathbb{Z}} \overline{\mathbb{F}}_p$ induit une bijection sur les points supersinguliers.

(iv) $\mathfrak{M}_{\Gamma(n)\cap\Gamma'_{oo}(H)} \otimes_{\mathbb{Z}[\zeta_p]^H} \overline{\mathbb{F}}_p \to \mathfrak{M}_{\Gamma(n)\cap\Gamma_o(p)} \otimes_{\mathbb{Z}} \overline{\mathbb{F}}_p$ induit une bijection sur les ensembles de composantes irréductibles.

(v) $\mathfrak{M}_{\Gamma(n)\cap\Gamma'_{oo}(H)} \otimes_{\mathbb{Z}[\zeta_p]^H} \overline{\mathbb{F}}_p$ s'obtient en recollant deux copies de $\mathcal{S}_n/H$ selon les points supersinguliers (cf. 2.13).

3. Un théorème de bonne réduction.

3.1. Soient p un nombre premier, $H \subset (\mathbb{Z}/p)^*$, $\Gamma'_{oo}(H)$ le groupe 2.14, $\mathbb{Z}[\zeta_p]^H$ comme en 2.14 et n un entier premier à p. On suppose $n \geq 3$, de sorte que $\mathfrak{M}_{\Gamma(n)\cap\Gamma'_{oo}(H)} \otimes \mathbb{Q} = M_{\Gamma(n)\cap\Gamma'_{oo}(H)} \otimes \mathbb{Q}$ est un schéma. C'est un schéma sur $\mathbb{Q}[\zeta_n, \zeta_p]^H$.

Dans ce §, nous noterons $J(n,H)$ la variété abélienne sur $\mathbb{Q}[\zeta_n,\zeta_p]^H$ composante neutre du schéma de Picard de $M_{\Gamma(n)\cap\Gamma'_{oo}(H)} \otimes \mathbb{Q}$

$$J(n,H) = \mathrm{Pic}^o(M_{\Gamma(n)\cap\Gamma'_{oo}(H)} \otimes \mathbb{Q} \,/\, \mathbb{Q}[\zeta_n,\zeta_p]^H) .$$

Pour $H = (\mathbb{Z}/p)^*$, on a $\Gamma'_{oo}(H) = \Gamma_o(p)$ et l'application $\mathfrak{M}_{\Gamma'_{oo}(H)} \to \mathfrak{M}_{\Gamma_o(p)}$ induit un morphisme

$$J(n,(\mathbb{Z}/p)^*) \otimes_{\mathbb{Q}[\zeta_n]} \mathbb{Q}[\zeta_n,\zeta_p]^H \longrightarrow J(n,H) \tag{3.1.1}$$

de noyau fini.

Théorème 3.2. La variété abélienne $I(n,H)$ sur $\mathbb{Q}[\zeta_n,\zeta_p]^H$ conoyau de (3.1.1) a bonne réduction en les places divisant p .

Soient v un point de caractéristique p de $\mathbb{Z}[\zeta_n,\zeta_p]^H$, et $\overline{k(v)}$ une clôture algébrique du corps résiduel. Soit ν le nombre de points supersinguliers de $M_{\Gamma(n)} \otimes_{\mathbb{Z}[\zeta]} \overline{k(v)}$. On sait que $M_{\Gamma(n)} \otimes_{\mathbb{Z}[\zeta]} \overline{k(v)}$ est irréductible; il en résulte que le schéma connexe $M_{\Gamma(n) \cap \Gamma(H)} \otimes_{\mathbb{Z}[\zeta_n,\zeta_p]^H} \overline{k(v)}$ a 2 composantes irréductibles, se coupant transversalement en ν points (cf. 1.18) et la variété abélienne sur $\overline{k(v)}$

$$\mathrm{Pic}^0(M_{\Gamma(n) \cap \Gamma(H)} \otimes_{\mathbb{Z}[\zeta_n,\zeta_p]^H} \overline{k(v)}/\overline{k(v)})$$

est extension d'un schéma abélien par un tore de dimension $\nu - 1$ (cf. I. 3.7). En particulier :

Proposition 3.3. La variété abélienne $J(n,H)$ sur $\mathbb{Q}[\zeta_n,\zeta_p]^H$ a réduction semi-stable en les places divisant p .

Si $0 \to A \to B \to C \to 0$ est une suite exacte à isogénies près de variétés abéliennes sur le corps des fractions d'un anneau de valuation discrète, et que α_{ab} , α_m, α_{add} désignent le rang abélien, multiplicatif et unipotent de la fibre spéciale du modèle de Néron, on sait que

$$\alpha_{ab}(A) - \alpha_{ab}(B) + \alpha_{ab}(C) = 0$$

et de même pour α_m et α_{add} . De plus, si $\alpha_{add} = 0$, α_{ab} et α_m sont invariants par extension des scalaires (cas semi-stable). $\alpha_{add} = \alpha_m = 0$ équivaut à bonne rédaction. On a $\alpha_{add}(J(n,H)) = 0$ et $\alpha_m(J(n,H)) = \nu-1$, indépendant de H ; le théorème en résulte.

Variante 3.4. Il résulte de 2.14.2 que

$$J(n,H) = \mathrm{Pic}^0(M_{\Gamma(n) \cap \Gamma_{oo}(H)} \otimes \mathbb{Q} / \mathbb{Q}(\zeta_n)) \otimes_{\mathbb{Q}(\zeta_n)} \mathbb{Q}(\zeta_n,\zeta_p)^H \ .$$

Soit $I_1(n,H)$ la variété abélienne sur $\mathbb{Q}(\zeta_n)$ conoyau du morphisme de

noyau fini défini par $\mathbb{m}_{\Gamma_{oo}}(H) \to \mathbb{m}_{\Gamma_o}(p)$:

$$\mathrm{Pic}^o(M_{\Gamma(n)\cap\Gamma_o(p)} \otimes \mathbb{Q}/\mathbb{Q}(\zeta_n)) \to \mathrm{Pic}^o(M_{\Gamma(n)\cap\Gamma_{oo}(H)} \otimes \mathbb{Q}/\mathbb{Q}(\zeta_n)) \to I_1(n,H) \to 0 \quad .$$

On a $I(n,H) = I_1(n,H) \otimes_{\mathbb{Q}(\zeta_n)} \mathbb{Q}(\zeta_n,\zeta_p)^H$, et 3.2 peut donc encore se formuler en disant que, après extension des scalaires de $\mathbb{Q}(\zeta_n)$ à $\mathbb{Q}(\zeta_n,\zeta_p)^H$, $I_1(n,H)$ acquiert une bonne réduction en les places divisant p .

Variante 3.5. La variété abélienne sur $\mathbb{Q}(\zeta_p)^H)$

$$RJ(n,H) = {}_{\mathrm{dfn}}\ \mathrm{Pic}^o(M_{\Gamma(n)\cap\Gamma'_{oo}(H)} \,/\, \mathbb{Q}(\zeta_p)^H)$$

se déduit de $J(n,H)$ par restriction des scalaires à la Weil de $\mathbb{Q}(\zeta_n,\zeta_p)^H$ à $\mathbb{Q}(\zeta_p)^H$. Le conoyau $RI(n,H)$ de

$$\mathrm{Pic}^o(M_{\Gamma(n)\cap\Gamma_o(p)} \,/\, \mathbb{Q}) \otimes \mathbb{Q}(\zeta_p)^H \to \mathrm{Pic}^o(M_{\Gamma(n)\cap\Gamma'_{oo}(p)} \,/\, \mathbb{Q}(\zeta_p)^H)$$

se déduit de même de $I(n,H)$ par restriction des scalaires à la Weil. Puisque $\mathbb{Q}(\zeta_n)$ est non ramifié en p , $RI(n,H)$ a encore bonne réduction sur $\mathbb{Q}(\zeta_p)^H$ en les places divisant p .

Variante 3.6. Soit K un sous-groupe de $GL(2,\hat{\mathbb{Z}})$ contenant $\Gamma(n)$, et soit $RI_1(K,H)$ la variété abélienne sur $\mathbb{Q}$ conoyau de

$$\mathrm{Pic}^o(M_{K\cap\Gamma_o(p)}) \longrightarrow \mathrm{Pic}^o(M_{K\cap\Gamma_{oo}(H)}) \quad .$$

On a $RI_1(K,H) \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_p)^H \longleftrightarrow RI(n,H)$ (à isogénie près); la variété abélienne $RI_1(K,H)$ acquiert donc bonne réduction en les places divisant p sur $\mathbb{Q}(\zeta_p)^H$.

Exemples 3.7. (i) La variété abélienne sur $\mathbb{Q}$

$$\mathrm{coker}(\mathrm{Pic}^o(M_{\Gamma_o(p)}) \to \mathrm{Pic}^o(M_{\Gamma_{oo}(p)}))$$

a bonne réduction sur $\mathbb{Q}(\zeta_p)$. Soit H le sous-groupe $\{\pm 1\}$ de $(\mathbb{Z}/p)^*$. On a $M_{\Gamma_{oo}(p)} = M_{\Gamma_{oo}(H)}$. La variante abélienne ci-dessus acquiert donc bonne réduction déjà le plus grand sous-corps totalement réel de $\mathbb{Q}(\zeta_p)$.

(ii) Soit p un nombre premier de la forme $4n + 1$, et soit $H \subset (\mathbb{Z}/p)^*$ le sous-groupe des carrés. La variété abélienne sur $\mathbb{Q}$

$$\operatorname{coker}(\mathrm{Pic}^0(M_{\Gamma_0(p)}) \to \mathrm{Pic}^0(M_{\Gamma_{00}(H)})$$

acquiert partout bonne réduction sur le corps quadratique réel $\mathbb{Q}(\sqrt{p})$.

(iii) Soient n un entier sans facteurs carrés, H un sous-groupe de $(\mathbb{Z}/n)^*$ et $\Gamma_{00}(H)$ le sous-groupe de $GL(2, \hat{\mathbb{Z}})$ image réciproque de

$$\begin{pmatrix} H & \mathbb{Z}/n \\ 0 & (\mathbb{Z}/n)^* \end{pmatrix} \subset GL(2, \mathbb{Z}/n) .$$

Si $n = pm$, on a $\mathbb{Z}/n^* \simeq (\mathbb{Z}/p)^* \times (\mathbb{Z}/m)^*$. Nous poserons $H_p = (\mathbb{Z}/p)^* \cap H$ et nous noterons $H.(\mathbb{Z}/p)^*$ le sous-groupe de $(\mathbb{Z}/n)^*$ engendré par H et $(\mathbb{Z}/p)^*$. La variété abélienne sur $\mathbb{Q}$

$$\operatorname{coker}\Big(\sum_{p|n} \mathrm{Pic}^0(M_{\Gamma_{00}(H.(\mathbb{Z}/p)^*)}) \longrightarrow \mathrm{Pic}^0(M_{\Gamma_{00}(H)})\Big)$$

acquiert bonne réduction sur $\mathbb{Q}(\zeta_n)^H$.

Preuve : Soit p un nombre premier divisant n : $n = mp$ avec $(m,p) = 1$. Prouvons que la variété abélienne A considérée a bonne réduction en les places de $\mathbb{Q}(\zeta_n)^H$ divisant p. Puisque $\mathbb{Q}(\zeta_n)^{H_p}$ est non ramifié sur $\mathbb{Q}(\zeta_n)^H$ en les places divisant p, il suffit de prouver que A a bonne réduction en les places divisant p de $\mathbb{Q}(\zeta_n)^{H_p}$. D'après 3.6,

$$B = \operatorname{coker}(\mathrm{Pic}^0(M_{\Gamma_0(p) \cap \Gamma_{00}(m)}) \longrightarrow \mathrm{Pic}^0(M_{\Gamma_{00}(H_p)}))$$

a bonne réduction en ces places. La variété abélienne

$$C = \operatorname{coker}(\mathrm{Pic}^0(M_{\Gamma_{00}(H.(\mathbb{Z}/p)^*)}) \longrightarrow \mathrm{Pic}^0(M_{\Gamma_{00}(H)}))$$

est isogène à celle déduite de B par passage aux invariants sous H (noter que $\Gamma_{00}(H).(\Gamma_0(p) \cap \Gamma_{00}(m)) = \Gamma_{00}(H.(\mathbb{Z}/p)^*)$). La variété abélienne A est quotient de

C donc a aussi bonne réduction.

(iv) Puisque $M_{\Gamma_{oo}(H)} = M_{\pm\Gamma_{oo}(H)}$, on ne restreint pas la généralité en supposant que $-1 \in H$. En particulier, dans (iii), on peut remplacer $Q(\zeta_p)^H$ par son sous-corps totalement réel.

Remarque 3.8. Les variétés abéliennes 3.7 (ii) sont celles étudiées par Casselman dans [5] .

4. Etude de $\mathfrak{M}_n$

4.1. Soient C une courbe elliptique généralisée sur un schéma S et n un entier. On suppose

a) les fibres géométriques de C sont lisses ou des m-gones , avec $n|m$;

b) elles ne sont jamais supersingulières de caractéristique $p|n$.

Les conditions a) et b) assurent que, localement pour la topologie étale, C_n est extension de $\mathbb{Z}/n$ par μ_n . Le e_n-pairing définit un isomorphisme de faisceaux fppf

$$e_n : \overset{2}{\Lambda} C_n \xrightarrow{\sim} \mu_n \quad .$$

Soit R un schéma en groupes sur S , localement isomorphe à une extension de $\mathbb{Z}/n$ par μ_n , et muni d'un isomorphisme de faisceaux fppf $i : \overset{2}{\Lambda} R \xrightarrow{\sim} \mu_n$. Un isomorphisme $\alpha : C_n \xrightarrow{\sim} R$ sera dit de déterminant un si le diagramme

$$\begin{array}{ccc} \overset{2}{\Lambda} C_n & \xrightarrow{\overset{2}{\Lambda}\alpha} & \overset{2}{\Lambda} R \\ \downarrow{\scriptstyle e_n} & & \downarrow{\scriptstyle i} \\ \mu_n & = & \mu_n \end{array}$$

est commutatif.

4.2. Nous utiliserons 4.1 dans les 3 cas suivants :

a) S est un schéma sur $\mathbb{Z}[\zeta_n, \frac{1}{n}]$, et $R = (\mathbb{Z}/n)^2$.

Dans ce cas, on dispose sur S de l'endomorphisme $\zeta : \mathbb{Z}/n \xrightarrow{\sim} \mu_n$ et i est le composé $\overset{2}{\Lambda}(\mathbb{Z}/n)^2 = \mathbb{Z}/n \xrightarrow{\sim} \mu_n$.

b) $R = \mu_n \times \mathbb{Z}/n$ et i l'isomorphisme évident : si $a \in \mu_n$ et $b \in \mathbb{Z}/n$, $i(a \wedge b) = b.a$ ($= b^a$ si la loi de groupe de μ_n est notée multiplicativement).

c) S est un schéma sur $\mathbb{Z}[\zeta_n]$ et $A \subset (\mathbb{Z}/n)^2$ un sous-groupe cyclique d'ordre n. Dans ce cas, on note $R(A)$ le S-schéma en groupe obtenu par "push-out" :

$$\begin{array}{ccccc} A & \longrightarrow & (\mathbb{Z}/n)^2 & \longrightarrow & (\mathbb{Z}/n)^2/A \\ \downarrow \zeta & & \downarrow & & \| \\ A \otimes \mu_n & \longrightarrow & R(A) & \longrightarrow & (\mathbb{Z}/n)^2/A \end{array} .$$

On a encore $\overset{2}{\Lambda} R(A) \simeq (A \otimes \mu_n) \otimes (\mathbb{Z}/n)^2/A \simeq (A \otimes (\mathbb{Z}/n)^2/A) \otimes \mu_n \simeq \overset{2}{\Lambda}(\mathbb{Z}/n)^2 \otimes \mu_n \simeq \mathbb{Z}/n \otimes \mu_n \simeq \mu_n$.

4.3. En IV 3.10.1, nous avons défini

$$d : \mathcal{M}_n \longrightarrow \mathrm{Spec}(\mathbb{Z}[\zeta_n]) .$$

En tant que $\mathrm{Spec}(\mathbb{Z}[\zeta_n])$ - champ algébrique, $\mathcal{M}_n[1/n]$ classifie les courbes elliptiques généralisées C sur les $\mathbb{Z}[\zeta_n][\frac{1}{n}]$ schémas S, de fibres géométriques lisses ou des n-gones, munies d'un isomorphisme $\alpha : C_n \xrightarrow{\sim} (\mathbb{Z}/n)^2$ de déterminant un.

4.4. Soit $\mathcal{G}$ le champ qui classifie les courbes elliptiques généralisées C sur les schémas S, de fibres géométriques lisses ou des n-gones, munies d'un isomorphisme $\alpha : C_n \xrightarrow{\sim} \mu_n \times \mathbb{Z}/n$ de déterminant un (4.2 b)). Au-dessus de $\mathbb{Z}[\zeta_n, \frac{1}{n}]$, l'isomorphisme $\zeta : \mathbb{Z}/n \xrightarrow{\sim} \mu_n$ identifie $(\mathbb{Z}/n)^2$ et $(\mu_n \times \mathbb{Z}/n)$, d'où un isomorphisme

$$\zeta : \mathcal{M}_n[1/n] \xrightarrow{\sim} \mathcal{G}[1/n] \otimes \mathbb{Z}[\zeta_n] . \tag{4.4.1}$$

Nous noterons $\mathcal{G}'$ l'ouvert de $\mathcal{G}$ classifiant les (C,α) vérifiant

(4.4.2) Pour tout point géométrique $\bar{s}$ de S, si $C_{\bar{s}}$ est un n-gone, $\alpha((C^0_{\bar{s}})_n) = \mu_n$.

Si (C,α) est un objet de $\mathcal{G}'$ sur S, $(C,\alpha^{-1}(e \times \mathbb{Z}/n))$ est un objet du champ $\mathcal{B}_n$ (1.3), d'où un morphisme

$$\gamma : \mathcal{G}' \to \mathcal{B}_n \quad . \tag{4.4.3}$$

Proposition 4.5. Le morphisme 4.3.3 est étale et séparé. En particulier, $\mathcal{G}'$ est un champ algébrique lisse sur $\mathrm{Spec}(\mathbb{Z})$.

Soit (C,B) un objet de $\mathcal{B}_n$ sur S. Alors, $\mathcal{G}' \times_{\mathcal{B}_n} S$ représente le foncteur $F : (\mathrm{Sch}/S) \to (\mathcal{E}ns)$ suivant : $F(T)$ est l'ensemble des couples (A,u) formés d'un sous-schéma en groupes de C_T, localement isomorphe à μ_n et tel que $A \times B \xrightarrow{\sim} C_n$, et de $u : B \xrightarrow{\sim} \mathbb{Z}/n$.

Pour (A,u) un tel couple, il existe en effet un seul isomorphisme $v : A \xrightarrow{\sim} \mu_n$, tel que

$$\alpha : C_n \xleftarrow{\sim} A \times B \xrightarrow{(v,u)} \mu_n \times \mathbb{Z}/n\mathbb{Z}$$

soit de déterminant un. On laisse au lecteur le soin de vérifier que F est représentable par un S-schéma étale et séparé.

4.6. Soit p un nombre premier divisant n, et posons $n = p^k.m$ avec $(m,p) = 1$. Nous nous proposons d'étudier $\mathcal{M}_n[1/m]$, spécialement en caractéristique p. En recollant les résultats obtenus pour les divers p, on obtient des résultats sur $\mathcal{M}_n$ lui-même.

Nous mettrons en évidence le "p-aspect" d'une structure de niveau n comme suit.

a) Les morphismes de réduction définissent

$$\mathbb{Z}/n \xrightarrow{\sim} \mathbb{Z}/p^k \times \mathbb{Z}/n \quad . \tag{4.6.1}$$

b) Les applications $x \mapsto x^m$ et $x \mapsto x^{p^k}$ définissent

(4.6.2) $$\mu_n \xrightarrow{\sim} \mu_{p^k} \times \mu_m \quad .$$

c) compatibilité : si $d|n$, on identifie $\mathbb{Z}[\zeta_d]$ au sous-anneau $\mathbb{Z}[\zeta_n^{n/d}]$ de $\mathbb{Z}[\zeta_n]$. Avec cette convention, un $\mathbb{Z}[\zeta_n]$ - schéma S est aussi un $\mathbb{Z}[\zeta_{p^k}]$- et un $\mathbb{Z}[\zeta_m]$ - schéma; les morphismes $\zeta : \mathbb{Z}/p^k \to \mu_{p^k}$ et $\zeta : \mathbb{Z}/m \to \mu_m$ sont les composantes, via (4.6.1) (4.6.2) de $\zeta : \mathbb{Z}/n \to \mu_n$.

d) Les applications $x \mapsto x^m$ et $x \mapsto x^{p^k}$ définissent

(4.6.3) $$C_n \xrightarrow{\sim} C_{p^k} \times C_m \quad .$$

Un morphisme $\alpha : C_n \xrightarrow{\sim} (\mathbb{Z}/n)^2$ est de déterminant un si et seulement si ses composantes, via (4.6.2) (4.6.4) : $\alpha' : C_{p^k} \xrightarrow{\sim} (\mathbb{Z}/p^k)^2$ et $\alpha'' : C_m \xrightarrow{\sim} (\mathbb{Z}/m)^2$ le sont.

e) Nous identifierons $\mathcal{M}_n[1/n]$ au champ qui classifie les courbes C sur un $\mathbb{Z}[\zeta_n, \frac{1}{n}]$ - schéma S comme en 4.3, munies de $\alpha' : C_{p^k} \xrightarrow{\sim} (\mathbb{Z}/p^k)^2$ et $\alpha'' : C_m \xrightarrow{\sim} (\mathbb{Z}/m)^2$ de déterminant un.

f) De même, $\mathcal{G}$ classifie les (C,α',α'') : $\alpha' : C_{p^k} \xrightarrow{\sim} \mu_{p^k} \times \mathbb{Z}/p^k$, $\alpha'' : C_m \xrightarrow{\sim} \mu_m \times \mathbb{Z}/m$, $\det(\alpha') = \det(\alpha'') = 1$.

Lemme 4.7. *$\mathcal{G}$ est un champ algébrique lisse sur $\mathbb{Z}$.*

Il suffit de montrer que $\mathcal{G} \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_m, \frac{1}{m}]$ est lisse sur $\mathbb{Z}[\zeta_m, \frac{1}{m}]$. Ce champ est réunion d'ouverts isomorphes à $\mathcal{G}' \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_m, 1/m]$, et on applique 4.5.

4.8. Soit P l'ensemble des sous-groupes cycliques d'ordre p^k de $(\mathbb{Z}/p^k)^2$: $P \simeq \mathbb{P}^1(\mathbb{Z}/p^k)$. Pour $A \in P$, soit $R(A)$ sur $\mathbb{Z}[\zeta_{p^k}]$ comme en 4.2 c).

Nous noterons $\mathcal{C}_A$ le champ sur $\mathbb{Z}[\zeta_n, \frac{1}{m}]$ classifiant les courbes elliptiques généralisées C sur les $\mathbb{Z}[\zeta_n, \frac{1}{m}]$ - schémas S, de fibres géométriques lisses ou des n-gones, munies de

a) $\alpha'' : C_m \xrightarrow{\sim} (\mathbb{Z}/m)^2$, de déterminant un

b) $\alpha' : C_{p^k} \xrightarrow{\sim} R(A)$, de déterminant un.

Puisque $R(A)$ est isomorphe à $\mu_{p^k} \times \mathbb{Z}/p^k$, le champ C_A est isomorphe à $G \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_n, \frac{1}{m}]$, donc est un champ algébrique lisse sur $\mathbb{Z}[\zeta_n, \frac{1}{m}]$.

Pour p inversible, $\zeta : (\mathbb{Z}/p^k)^2 \xrightarrow{\sim} R(A)$ est un isomorphisme, d'où un isomorphisme de champs sur $\mathbb{Z}[\zeta_n, \frac{1}{n}]$

$$\mathcal{M}_n[1/n] \simeq C_A[1/p] \quad . \tag{4.8.1}$$

4.9. Soit $\mathcal{M}_1^h$ le complément dans $\mathcal{M}_1$ de l'ensemble fini des points correspondant aux courbes elliptiques supersingulières de caractéristique divisant n . On définit $c : C_A \to \mathcal{M}_1^h$ en associant à (C,α',α'') sur S la courbe $c(C)$ (IV 1.4).

Lemme 4.10. Le morphisme $c : C_A \to \mathcal{M}_1^h$ est représentable et quasi-fini.

La vérification est laissée au lecteur.

4.11. Soit $C[1/m]$ le champ obtenu en recollant les champs C_A $(A \in P)$ selon leur ouvert commun $C_A[1/p]$ (4.8.1). Soit C obtenu en recollant les $C[1/m]$ selon leur ouvert commun $C[1/m,1/p] \simeq \mathcal{M}_n[1/n]$. Le champ C est lisse sur $Z[\zeta_n]$, on a

$$C[1/n] \simeq \mathcal{M}_n[1/n] \tag{4.11.1}$$

et les morphismes 4.9 se recollent en un morphisme

$$c : C \to \mathcal{M}_1^h \quad . \tag{4.11.2}$$

Lemme 4.11.3. Le morphisme représentable (4.11.2) est fini et séparé.

Preuve : Il suffit de montrer que, pour chaque $p|n$, c induit un morphisme propre (en particulier séparé)

$$c : C[1/m] \to \mathcal{M}_1^h[1/m] \quad .$$

Utilisons le critère valuatif ([8]). Soient donc (S,η,s) un trait complet à

corps résiduel algébriquement clos, $u : S \to \mathcal{M}_1^h[1/m]$ et $v_\eta : \eta \to C$ tel que $cv_\eta = u_\eta$.

Il faut montrer que, après passage au normalisé de S dans une extension finie de $k(\eta)$, u admet un relèvement $v : S \to C$ qui prolonge v_η , et que v est unique à isomorphisme unique près. Puisque $\mathcal{M}_n^o[\frac{1}{n}]$ est dense dans C , on peut supposer que v_η envoye η dans $\mathcal{M}_n^o[\frac{1}{n}]$. Puisque $C[\frac{1}{p}] \simeq \mathcal{M}_n[\frac{1}{n}]$ est fini sur $\mathcal{M}_1[\frac{1}{n}]$ (cf. IV.2.5.), on peut se limiter au cas où s est de caractéristique p .

Soit $(C_\eta, \alpha'_\eta, \alpha''_\eta)$ la courbe elliptique avec structure de niveau n sur η qui définit v_η . Une extension finie préliminaire de $k(\eta)$ nous permet de supposer que C_η se prolonge en une courbe elliptique généralisée C sur S , de fibre spéciale lisse ou un n-gone. Cette courbe est unique (IV 1.6). C_m est fini étale sur S , de sorte que α''_η se prolonge, de façon unique, en $\alpha'' : C_m \xrightarrow{\sim} (\mathbb{Z}/m)^2$.

Par hypothèse, la fibre spéciale C_s n'est pas supersingulière. Le sous-groupe multiplicatif $(C_s)^o_{p^k}$ de $(C_s)_{p^k}$ se relève de façon unique en un sous-groupe de C_{p^k} , qui devient une extension

$$0 \to A \to C_{p^k} \to B \to 0$$

avec $A \simeq \mu_n$ et $B \simeq \mathbb{Z}/n$. Soit $A = \alpha'(A_\eta) \in P$. L'isomorphisme α'_η se prolonge en $\alpha' : C_{p^k} \xrightarrow{\sim} R(A)$, v_η se prolonge en $v : S \to C_A$, défini par (C, α', α'') , et ne se prolonge en aucun $v : S \to C_A$, pour $A \neq A'$. Ceci prouve 4.11.3.

Notons $\mathcal{M}_n^h$ le normalisé de $\mathcal{M}_1^h$ dans $\mathcal{M}_n[1/n]$, i.e. le complément dans $\mathcal{M}_n$ des points dont l'image dans $\mathcal{M}_1$ est supersingulière de caractéristique divisant n . De la lissité des C_A (4.8) et de 4.11 on tire les résultats suivants.

Théorème 4.12. *On a* $C \simeq \mathcal{M}_n^h$.

Corollaire 4.13. $\mathcal{M}_n^h$ *est lisse sur* $\mathbb{Z}[\zeta_n]$.

4.14. Etudions G en caractéristique p . Si C/S est une courbe elliptique sur

S , avec p nilpotent sur S , de fibres géométriques lisses non supersingulières ou des n-gones, alors $(C_{p^k})^0$ est localement isomorphe à μ_{p^k} (pour la topologie étale), et se donner un isomorphisme $\alpha' : C_{p^k} \xrightarrow{\sim} \mu_{p^k} \times \mathbb{Z}/p^k$ revient à se donner un isomorphisme d'extensions

$$\begin{array}{ccccccccc} 0 & \to & (C_{p^k})^0 & \to & C_{p^k} & \longrightarrow & C_{p^k}/(C_{p^k})^0 & \to & 0 \\ & & \downarrow \wr\, \alpha_1' & & \downarrow \wr\, \alpha' & & \downarrow \wr\, \alpha_2' & & \\ 0 & \to & \mu_{p^k} & \to & \mu_{p^k} \times \mathbb{Z}/p^k & \to & \mathbb{Z}/p^k & \longrightarrow & 0 \end{array} \qquad (4.14.1)$$

Ceci revient à se donner

a) une trivialisation τ de l'extension en première ligne de 4.14.1.

b) des isomorphismes $\alpha_1' : C^0_{p^k} \xrightarrow{\sim} \mu_{p^k}$ et $\alpha_2' : C_{p^k}/C^0_{p^k} \xrightarrow{\sim} \mathbb{Z}/p^k$.

Se donner τ revient à se donner le sous-groupe étale $\alpha^{-1}(\mathbb{Z}/p^k)$ de C_{p^k}, de sorte que $(C,\alpha) \mapsto (C,\tau)$ correspond au morphisme $\mathcal{G} \to \mathcal{B}_{p^k}$ déja considéré. Par ailleurs, si $\det(\alpha') = 1$, α_2' est uniquement déterminé par α_1' .

4.15. Soit $\mathcal{I}_k^h \otimes \mathbb{Z}/p^N$ le champ algébrique sur $\mathbb{Z}/p^N$ classifiant les courbes elliptiques généralisées à fibres irréductibles C/S , avec $p^N = 0$ sur S , munies d'un isomorphisme $\alpha_1' : C^0_{p^k} \xrightarrow{\sim} \mu_{p^k}$. La discussion 4.14 montre que le champ $\mathcal{G} = \mathcal{G}(p^k)$ est en réduction mod p^N , un produit fibré

$$\begin{array}{ccc} \mathcal{G}(p^k) \otimes \mathbb{Z}/p^N & \xrightarrow{(C,\alpha) \mapsto (C,\alpha^{-1}(\mathbb{Z}/p^k))} & \mathcal{B}_{p^k} \otimes \mathbb{Z}/p^N \\ \Big\downarrow (c,\alpha) \\ \Big\downarrow (c(C),\alpha_1') & & \Big\downarrow (C,B) \\ & & \Big\downarrow (c(C)) \\ \mathcal{I}_k^h \otimes \mathbb{Z}/p^N & \xrightarrow{\text{oubli}} & \mathcal{M}_1^h \otimes \mathbb{Z}/p^N \end{array} \qquad (4.15.1)$$

La vérification du lemme suivant est laissée au lecteur.

Lemme 4.16. (i) Soit C la courbe universelle sur $\mathcal{M}_1^h$, de sorte que $\mathcal{I}_k \otimes \mathbb{Z}/p^N = \underline{\mathrm{Isom}}_{\mathcal{M}_1} \otimes \mathbb{Z}/p^N (\mu_{p^k}, C^0_{p^k})$. La flèche verticale droite de (4.15.1) fait de $\mathcal{B}^0_{p^k} \otimes \mathbb{Z}/p^N$ un espace principal homogène sous $C^0_{p^k}$; la flèche verticale gauche

fait de $\mathcal{C}^o \otimes \mathbb{Z}/p^N$ un espace principal homogène sous μ_{p^k} .

(ii) En particulier, pour $N = 1$, ces flèches identifient $\mathcal{J}_k^h \otimes \mathbb{F}_p$ à $(\mathcal{C} \otimes \mathbb{F}_p)^{(p^k)}$ et $\mathcal{M}_1^h \otimes \mathbb{F}_p$ à $(\mathcal{B}_n \otimes \mathbb{F}_p)^{(p^k)}$ (la flèche devenant un morphisme de Frobenius itéré) (un morphisme bijectif radiciel entre schémas lisses de dimension un est toujours un Frobenius itéré).

(iii) Les flèches horizontales de (4.15.1) sont étales, et font de $(\mathcal{J}_n^h \otimes \mathbb{Z}/p^N)$ (resp. $\mathcal{C} \otimes \mathbb{Z}/p^N$) un espace principal homogène de groupe $(\mathbb{Z}/p^k)^*$ sur $(\mathcal{M}_1^h \otimes \mathbb{Z}/p^N)$ (resp. $\mathcal{B}_n \otimes \mathbb{Z}/p^N$) , le groupe $(\mathbb{Z}/p^k)^*$ agissant par $(i,(C,\alpha_1)) \longmapsto (C,i\alpha_1)$.

Soit $\mathcal{J}_k \otimes \mathbb{Z}/p$ le normalisé de $\mathcal{M}_1 \otimes \mathbb{Z}/p$ dans $\mathcal{J}_k^h$. Nous ferons usage du théorème suivant de Igusa [35] (voir Katz [13] 4.3 (bis)).

Théorème 4.17 (Igusa). Le revêtement $\mathcal{J}_k \otimes \mathbb{Z}/p \to \mathcal{M}_1 \otimes \mathbb{Z}/p$ est complètement ramifié en les points supersinguliers.

4.18. Pour n général, $\mathcal{C}^o = \mathcal{C}^o(n)$ est un produit fibré

$$\mathcal{C}^o = \mathcal{C}^o(m) \times_{\mathcal{M}_1} \mathcal{C}^o(p^k) \quad . \tag{4.18.1}$$

(Cela reste d'ailleurs vrai à l'infini). De l'irréductibilité des fibres géométriques de $\mathcal{M}_m[1/m]/\mathbb{Z}[\zeta_m,\frac{1}{m}]$ et de 4.4.1, 4.18.1, 4.15.1, 4.16 (ii) et 4.17, on déduit que $\mathcal{C}^o \otimes_{\mathbb{Z}[\zeta_m]} \overline{\mathbb{F}}_p$ est irréductible, et le corollaire suivant.

Théorème 4.19. Via 4.12, les composantes irréductibles de $\mathcal{M}_n^h \otimes_{\mathbb{Z}[\zeta_n]} \overline{\mathbb{F}}_p$ s'identifient aux $\mathcal{C}_A \otimes_{\mathbb{Z}[\zeta_n]} \mathbb{F}_p$, $A \in P$.

4.20. D'après 4.17 et 4.19, les composantes irréductibles de $\mathcal{M}_n \otimes_{\mathbb{Z}[\zeta_n]} \overline{\mathbb{F}}_p$ sont indexées par $P = \mathbb{P}^1(\mathbb{Z}/p^k)$, ne se coupent qu'en les points supersinguliers, et sont unibranches. Le théorème suivant affirme que toutes les composantes irréductibles se coupent en chaque point supersingulier.

Théorème 4.20. Le morphisme $\mathcal{M}_1 \to \mathcal{M}_m$ est complètement ramifié en les points supersinguliers de caractéristique p .

Preuve : D'après 4.6, la validité de 4.20 ne dépend que de p^k , non de m ; on peut donc supposer $m \geq 3$, pour n'avoir affaire qu'à des schémas.

Soit E_o une courbe elliptique supersingulière sur $\overline{\mathbb{F}}_p$, et $E/\hat{S}$ le schéma formel de modules de E_o au-dessus de $W(\overline{\mathbb{F}}_p)$. On a $S \simeq W(\mathbb{F}_p)[[t]]$; c'est le complété de l'hensélisé strict de $\mathbb{m}_1$ au point géométrique donné.

Soit $\hat{T}$ le normalisé de $\hat{S}$ dans le $\hat{S}[1/p]$-schéma $\underline{\mathrm{Isom}}_{\hat{S}}(E_{p^k}, (\mathbb{Z}/p^k)^2)$. Puisque complétions et normalisations commutent,

$$\hat{T} = \mathbb{m}_{p^k} \times_{\mathbb{m}_1} \hat{S} \quad .$$

D'après 4.17, les composantes irréductibles de $\hat{T} \otimes \overline{\mathbb{F}}_p$ sont naturellement indexées par $P = \mathbb{P}^1(\mathbb{Z}/p^k)$. Les composantes connexes de $\hat{T}$ définissent une partition $\mathcal{P}$ de P . 4.20 signifie que $\hat{T}$ est toujours connexe, i.e. $\mathcal{P}$ trivial.

Lemme 4.21. La partition $\mathcal{P}$ est indépendante de E_o .

Preuve : Soient E_o et E'_o deux courbes elliptiques supersingulières sur $\overline{\mathbb{F}}_p$, $\hat{S}$ et $\hat{S}'$ leurs schémas formels de module sur $W(\overline{\mathbb{F}}_p)$, E et E' leurs déformations universelles sur $\hat{S}$ et $\hat{S}'$ et $\hat{T}$, $\hat{T}'$ comme en 4.20.

On sait qu'il existe une isogénie $\varphi_o : E_o \to E'_o$ de noyau K_o premier à p . Soit N un entier premier à p tel que $K_o \subset E_{oN}$. Puisque E_{oN} est étale, les déformations infinitésimales de E_o s'identifient aux déformations infinitésimales du couple $(E_o, K_o \subset E_{oN})$, et il existe un et un seul isomorphisme $\varphi_S : \hat{S} \to \hat{S}'$ donnant lieu à un diagramme commutatif

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & E' \\ \downarrow & & \downarrow \\ \hat{S} & \xrightarrow{\varphi_S} & \hat{S}' \end{array}$$

où φ prolonge φ_o . L'isogénie φ induit un isomorphisme de E_{p^k} avec E'_{p^k} , d'où un isomorphisme $\varphi_T : \hat{T} \to \hat{T}'$ au-dessus de φ_S .

La bijection de l'ensemble $I(\hat{T} \otimes \overline{\mathbb{F}}_p)$ des composantes irréductibles de $\hat{T} \otimes \overline{\mathbb{F}}_p$ avec P peut se décrire ainsi : sur $\hat{T}$, on dispose d'un morphisme $u : (\mathbb{Z}/p^k)^2 \longrightarrow E_{p^k}$, qui est un isomorphisme sur $\hat{T}[1/p]$. L'élément de P associé à une composante de $\hat{T} \otimes \overline{\mathbb{F}}_p$ est le noyau de u au point générique de cette composante. Cette description montre que le diagramme

$$\begin{array}{ccc} I(\hat{T} \otimes \overline{\mathbb{F}}_p) & \xrightarrow{\varphi_T} & I(\hat{T}' \otimes \overline{\mathbb{F}}_p) \\ \| & & \| \\ P & = & P \end{array}$$

est commutatif. Le lemme en résulte.

Prouvons 4.20. Si $\mathcal{P}$ est non trivial et que $X \in \mathcal{P}$, la réunion des adhérences $(C_A \otimes \overline{\mathbb{F}}_p)^-$ pour $A \in X$ est une composante connexe de $\mathfrak{M}_n \otimes \overline{\mathbb{F}}_p$, qui est donc disconnexe. Ceci contredit (IV 5.5).

VI. Schémas grossiers de modules.

Dans ce chapitre nous étudions les schémas grossiers de modules, en particulier la relation entre $\mathcal{M}_H$ et M_H. Quelques résultats classiques sont démontrés par "pure thought". Le résultat du § 5 est précisé au chapitre suivant.

1. L'invariant modulaire.

Théorème 1.1. *L'espace grossier M_1 et $\mathcal{M}_1$ est isomorphe à $\mathbb{P}^1_{\mathbb{Z}}$.*

Les caractéristiques 2 et 3 rendent la vérification directe de 1.1 quelque peu pénible. Nous allons déduire 1.1. de son corollaire

(1.1.1) $$M_{1\mathbb{C}} \simeq \mathbb{P}^1_{\mathbb{C}} .$$

a) *M_1 est propre et plat sur $\mathrm{Spec}(\mathbb{Z})$, normal et donc de Cohen-Macaulay (I.7.2) et les fibres géométriques de M_1 sur $\mathrm{Spec}(\mathbb{Z})$ sont irréductibles.*

On sait déjà que M_1 est propre, plat, normal, à fibres géométriques unibranches (IV. 3.10). D'après 1.1.1. (ou IV 5.4), la fibre générique géométrique de M_1 est connexe. Toutes les fibres géométriques de M_1 sont donc connexes (Zariski) et, étant unibranches, sont irréductibles.

b) *Les fibres géométriques de M_1 sur $\mathrm{Spec}(\mathbb{Z})$ sont réduites.*

Soit $\mathcal{U}$ le sous-champ ouvert de $\mathcal{M}_1$ correspondant aux courbes généralisées n'ayant pas d'autres automorphismes que Id et $x \mapsto -x$. C'est un ouvert car, pour C/S une courbe classifiée par $\mathcal{M}_1$, $\mathrm{Aut}_S(C)$ est fini et non ramifié sur S (résulte de ce que $\mathcal{M}_1$ est séparé).

L'application $\mathcal{U} \to M_1$ est étale, son image A est donc lisse sur $\mathbb{Z}$. On vérifie que $\mathcal{U} \supset \mathcal{M}_1^{\infty}$. Les fibres de A sont donc non vides; d'après a), elles sont denses dans les fibres de M_1. Les $(M_1)_{\overline{s}}$ sont donc génériquement réduits; étant de Cohen-Macaulay, ils sont même réduits.

c) Fin de la démonstration.

Par invariance du genre arithmétique par spécialisation, et (1.1.1) on trouve que les fibres géométriques de M_1 sont intègres et de genre arithmétique 0. Elles sont donc isomorphes à la droite projective. En particulier, M_1 est propre et lisse sur $\mathbb{Z}$.

Le polygone de Néron à un côté sur $\mathrm{Spec}(\mathbb{Z})$ définit une section de M_1, d'image M_1^∞. On vérifie fibre géométrique par fibre géométrique que $H^1(M_1, \mathcal{O}(M_1^\infty)) = 0$, puis que $H^0(M_1, \mathcal{O}(M_1^\infty))$ est localement libre de rang 2 sur $\mathbb{Z}$, de formation compatible au passage aux fibres géométriques. Puisque $\mathbb{Z}$ est principal, $H^0(M_1, \mathcal{O}(M_1^\infty))$ est libre, et admet une base $\{1, j\}$. On vérifie fibre géométrique par fibre géométrique que $\mathcal{O}(M_1^\infty)$ est très ample, et que j définit un isomorphisme $M_1 \xrightarrow{\sim} \mathbb{P}^1_{\mathbb{Z}}$.

Preuve de (1.1.1) Voici deux démonstration classiques de (1.1.1).

(1) On vérifie que $M_1^0(\mathbb{C})$ est le quotient du demi-plan de Poincaré par $SL(2, \mathbb{Z})$ (IV 5.4). On trace un domaine fondamental, et on trouve que $M_1^0(\mathbb{C})$ est homéomorphe à $\mathbb{R}^2$. L'espace $M_1(\mathbb{C})$, qui s'en déduit par adjonction d'un point, est donc une sphère.

(2) Sur $\mathbb{C}$, le schéma de modules classifiant les courbes elliptiques généralisées intègres munies d'une forme différentielle invariante est

$$\mathrm{Spec}(\mathbb{C}[g_2, g_3]) - (\text{le point } g_2 = g_3 = 0) ,$$

avec pour courbe universelle, en coordonnées non homogènes

$$\begin{cases} Y^2 = 4X^3 - g_2 X - g_3 \\ \omega = \dfrac{dX}{Y} \end{cases} \qquad ([33]\ 2.5)$$

M_1 est le quotient de ce schéma par $\mathbb{G}_m$ agissant par

$$\lambda.(g_2, g_3) = (\lambda^4 g_2, \lambda^6 g_3) ,$$

et on l'identifie facilement à $\mathbb{P}^1$.

L'irréductibilité des fibres de M_1 sur $\mathbb{Z}$ a le corollaire suivant.

Corollaire 1.2. Soit k un corps algébriquement clos de caractéristique p. Il n'y a qu'un nombre fini de classes d'isomorphie de courbes elliptiques supersingulières sur k.

L'ensemble des points de $(M_1)_k$ correspondant à des courbes elliptiques généralisées E pour lesquelles le noyau de Frobenius est de type multiplicatif est ouvert et contient le point à l'infini. Son complément, qui correspond aux courbes supersingulières, est donc fini.

1.3. La fonction j introduite en 1.1 c) n'est pas uniquement déterminée; l'arbitraire est $j \mapsto \pm j + n$ $(n \in \mathbb{Z})$. Un choix de j, rappelé ci-dessous, est classique.

Soit C/S une courbe elliptique généralisée à fibres irréductibles sur S. On explique dans le formulaire de Tate [33] comment associer à C/S une section j de $\mathbb{P}^1$ sur S, avec $j = \infty$ là où C est singulière. Par la propriété universelle de M_1, ce morphisme $j : \mathfrak{M}_1 \to \mathbb{P}^1$ se factorise par $j : M_1 \to \mathbb{P}^1$. On vérifie facilement que $j : M_1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ est bijectif [33]. Le morphisme j est dominant, plat (I 7.1.), de degré un, donc un isomorphisme. En particulier, sur tout corps algébriquement clos k, $j(C_1) = j(C_2)$ si et seulement si C_1 est isomorphe à C_2. Ce fait est prouvé par force brutale dans [33].

On appelle j l'invariant modulaire.

1.4. Soit C une courbe elliptique généralisée irréductible sur k algébriquement clos On prouve dans [33] que $\mathrm{Aut}(C) = \{\pm 1\}$ si et seulement si $j(C) \neq 0, 2^6.3^3$. Au dessus de l'ouvert de $\mathfrak{M}_1$ où $j \neq 0$, $2^6.3^3$, $\underline{\mathrm{Aut}}(C)$ (C courbe universelle) est donc localement constant. Dès lors :

Lemme 1.5. $\mathfrak{M}_1 \to M_1$ est étale en dehors des sections $j = 0, 2^6 3^3$ de M_1.

Par contre, $\mathfrak{M}_1$ est ramifié sur M_1 le long de ces sections. A cause de cette ramification, il ne peut pas y avoir de section $M_1 \to \mathfrak{M}_1$, i.e. il n'y a pas de

courbe elliptique généralisée sur $\mathbb{P}^1$ d'invariant modulaire j. Toutefois, Tate a montré que sur $\mathbb{P}^1_{\mathbb{Z}}$, moins les deux sections 0 et $2^6 3^3$, i.e. sur

$$S = \mathrm{Spec}\, \mathbb{Z}[\tfrac{1}{j}]\ (2^6 3^3 \tfrac{1}{j} - 1)^{-1} ,$$

il existe deux courbes d'invariant j. Posons $k = j - 2^6 3^3$, de sorte que $1/j$ et $1/k$ sont des sections de $\mathcal{O}_S$, et j/k une section inversible.

Proposition 1.6 (Tate). Les courbes

$$y^2 + xy = x^3 - \frac{2^2 3^2}{k} x - \frac{1}{k} \tag{1.6.1}$$

$$y^2 + xy = x^3 + \frac{2^2 3^2}{j} x - \frac{j - 2^7 3^2}{j^2} \tag{1.6.2}$$

ont pour invariant modulaire j.

Pour (1.6.1), $c_4 = j/k$, $c_6 = -j/k$ et $\Delta = j^2/k^3$.

Pour (1.6.2), $c_4 = k/j$, $c_6 = -k^2/j^2$ et $\Delta = k^3/j^4$.

Notons C_o la courbe (1.6.1). Si C est une courbe sur un ouvert U de S, d'invariant j, $\underline{\mathrm{Isom}}(C, C_o)$ est un $\mathbb{Z}/2$-torseur $\tau(C)$, et C se déduit de C_o par "torsion" par $\tau(C)$. Les courbes C sont donc classifiées par $H^1(U, \mathbb{Z}/2)$ (H^1 étale). Par exemple, (1.6.2) correspond au revêtement double de S normalisé de $S[(j/k)^{1/2}]$. En calculant ce H^1, Tate a montré que (1.6.1) et (1.6.2) sont les seules courbes elliptiques d'invariant j sur $\mathbb{P}^1_{\mathbb{Z}}$ moins les 3 sections $0, 2^6.3^3$ et ∞.

Proposition 1.7. Soient k un corps, et $j \in k$. Il existe une courbe elliptique sur k d'invariant modulaire j.

Le cas où $j \neq 0, 2^6 3^3$ résulte de 1.6. Pour k de caractéristique p, et $j = 0$ ou $2^6 3^3$, on peut prendre l'équation non homogène suivante.

$$p \neq 3\ ,\ j = 0 \qquad y^2 + y = x^3 - 1$$

$$p \neq 2\ ,\ j = 2^6.3^3 \qquad y^2 = x^3 - x\ .$$

1.8. Soit C la courbe elliptique universelle sur $\mathcal{M}_1^o$ et γ le morphisme $\underline{\mathrm{Aut}}(C) \to \underline{\mathrm{Aut}}(\mathrm{Lie}(C)) \simeq \mathbb{G}_m$. Nous extrayons de [33] le résultat suivant sur $\underline{\mathrm{Aut}}(C)$.

Lemme 1.9. *Au-dessus du sous-champ de $\mathcal{M}_1^o[\frac{1}{6}]$ d'équation $c_4 = 0$ (resp. $c_6 = 0$) (i.e. $\sqrt[3]{j} = 0$, resp. $\sqrt[2]{j-1728} = 0$) , γ est un isomorphisme $\underline{\mathrm{Aut}}(C) \xrightarrow{\sim} \mu_6$ (resp. $\underline{\mathrm{Aut}}(C) \xrightarrow{\sim} \mu_4$) .*

2. Automorphismes des courbes elliptiques. Critère pour que $\mathcal{M}_H^o = M_H^o$.

2.1. Pour qu'un champ algébrique soit un espace algébrique, il faut et il suffit que ses points géométriques n'aient pas d'automorphisme non trivial. Ainsi, si $H \subset GL(2, \mathbb{Z}/n)$, pour que $\mathcal{M}_H^o[1/n] = M_H^o[1/n]$ (resp. $\mathcal{M}_H[1/n] = M_H[1/n]$), il faut et il suffit qu'une courbe elliptique (resp. généralisée) munie d'une structure de niveau H , sur k algébriquement clos de caractéristique $p \nmid n$, n'ait pas d'automorphisme non trivial.

Par exemple, $\mathcal{M}_n[1/n] = M_n[1/n]$ pour $n \geq 3$ (IV 2.7) .

Dans [32] , les automorphismes des courbes elliptiques sont décrits explicitement, de sorte que le critère précédent est effectif. Les calculs de [33] montrent que les caractéristiques 2 et 3 sont exceptionnelles, les autres étant "pareilles" à la caractéristique 0 . Nous nous proposons de vérifier ce point a priori. Pour ne pas paraître trop ridicules, nous traiterons aussi le cas des variété abéliennes.

Lemme 2.2. *Soient (A,θ) une variété abélienne polarisée sur un corps algébriquement clos k de caractéristique $p > 0$ et φ un automorphisme de (A,θ). On sait que φ est d'ordre fini. Si le degré de θ et l'ordre de φ sont premiers à p , le triple (A,θ,φ) se relève sur l'anneau des vecteurs de Witt $W(k)$.*

On sait qu'il n'y a pas d'obstruction à déformer (A,θ) : le schéma formel des modules de (A,θ) sur $W(k)$ est un schéma

$$M = \mathrm{Spec}(W/k)[[t_1 \ldots t_k]]) \qquad (k = \tfrac{1}{2}\dim(A)(\dim(A)+1)) \ .$$

Interprétons φ comme l'action sur (A,θ) d'un groupe cyclique G, d'ordre premier à p. Par transport de structure, G agit sur M : l'automorphisme φ de (A,θ) se prolonge en un automorphisme de M et de la déformation universelle (A_M,θ_M) de (A,θ) sur M. On vérifie que le schéma formel des modules de (A,θ,φ) est le sous-schéma M^G de M fixe par G. Puisque G est d'ordre premier à p, ce sous-schéma est lisse sur $W(k)$, donc admet des sections sur $W(k)$, et ceci prouve 2.2.

Proposition 2.3. *Soit A une variété abélienne de dimension g sur un corps algébriquement clos. Soit φ un automorphisme d'ordre un nombre premier q et notons $A^\varphi =_{dfn} \mathrm{Ker}(\varphi - id_A)$.*

Il existe un entier k, tel que

$$2.g = \dim(A^\varphi) + k.(q-1) \quad .$$

Preuve : Passant de A à A/A^φ on est réduit au cas où A^φ est fini.

Le polynôme caractéristique de φ agissant sur A est à coefficients entiers, n'a pas 1 pour racine et a pour seules racines des q-ièmes racines d'unité. Il est donc une puissance du polynôme cyclotomique qui est de degré $q-1$. La comparaison des degrés donne le lemme.

Corollaire 2.4. *Soit A une variété abélienne de dimension g sur un corps algébriquement clos. Soit φ un automorphisme d'ordre fini de A. Tous les facteurs premiers de l'ordre de φ sont plus petits que $2g + 1$.*

Preuve : Cela suit de 2.4.

Corollaire 2.5. *Soit (A,θ) une variété abélienne polarisée de dimension g sur un corps algébriquement clos k de caractéristique p, telle que le degré de la polarisation soit premier à p. On suppose que $p > 2g + 1$. Si φ est un automorphisme de (A,θ), (A,θ,φ) se relève en caractéristique 0 (sur $W(k)$).*

Preuve : Résulte de 2.2 et 2.4.

2.6. Une courbe elliptique admet une polarisation principale canonique. D'après 2.6, si φ est un automorphisme d'une courbe elliptique E sur un corps algébriquement clos k de caractéristique $p > 3$, (E,φ) se relève en caractéristique 0 (sur $W(k)$).

Théorème 2.7. Pour que $\mathcal{M}_H^0[1/6n]$ soit un espace algébrique, il faut et il suffit que l'image réciproque Γ de H dans $SL(2,\mathbb{Z})$ n'ait pas d'élément d'ordre fini $\neq 1$.

Soit $(E,\bar{\alpha})$ une courbe elliptique munie d'une structure de niveau H sur k algébriquement clos de caractéristique $p = 0$ ou $p > 3$, $p \nmid n$. Il faut montrer que tout automorphisme φ de $(E,\bar{\alpha})$ est trivial. Puisque d'après 2.6 (E,φ), donc $(E,\bar{\alpha},\varphi)$, se relève en caractéristique 0, il suffit de traiter le cas où $p = 0$.

$\bar{\alpha}$ définit une inclusion (IV.3.20) $\mathbb{Q}[\zeta_n]^{\det H} \subset k$. On se ramène à supposer k de degré de transcendance absolu fini, auquel cas il existe $k \hookrightarrow \mathbb{C}$ induisant l'inclusion identique de $\mathbb{Q}[\zeta_n]$ dans $\mathbb{C}$. Ceci nous ramène au cas où $k = \mathbb{C}$ et où $\bar{\alpha}$ est défini par $\alpha : E_n \xrightarrow{\sim} (\mathbb{Z}/n)^2$ de déterminant un.

Si $\beta : \mathbb{Z}^2 \longrightarrow H_1(E(\mathbb{C}),\mathbb{Z})$ relève l'inverse de α (via IV 5.2.1), on vérifie que $\mathrm{Aut}(E,\bar{\alpha})$ est le stabilisateur de $z(\beta)$ (IV 5.1) dans Γ. Si $\mathrm{Aut}(E,\bar{\alpha}) \neq \{e\}$, Γ a donc des éléments d'ordre fini.

Réciproquement, tout élément d'ordre fini φ de Γ a un point fixe dans X, auquel correspond $(E,\bar{\alpha},\varphi)$ sur $\mathbb{C}$.

3. Points rationnels des schémas grossiers.

3.1. Soit $H \subset GL(2,\mathbb{Z}/n)$. Une courbe elliptique E munie d'une structure de niveau H α, sur un corps k, définit un point de $M_H^0(k)$. Réciproquement, si $x \in M_H^0[1/n](k)$, on sait seulement que sur la clôture séparable $\bar{k}$ de k il existe (E,α) définissant x. La classe d'isomorphie de (E,α) est invariante par $\mathrm{Gal}(\bar{k}/k)$.

Si (E,α) provient de (E_o,α_o) sur k, l'ensemble des k-classes d'isomorphie de courbes (E_1,α_1) définissant x est canoniquement $H^1(Gal(\bar{k}/k),\underline{Aut}(E_o,\alpha_o)(\bar{k}))$. L'obstruction à l'existence d'un (E_o,α_o) est dans un H^2 (au sens de Giraud). Dans le cas particulier où $Aut(E,\alpha)$ est commutatif, $Gal(\bar{k}/k)$ agit sur $Aut(E,\alpha)$ et l'obstruction est dans $H^2(Gal(\bar{k}/k),Aut(E,\alpha))$.

Proposition 3.2. Soient k un corps de caractéristique p et $H \subset GL(2,\mathbb{Z}/n)$. On suppose que $p\nmid n$. Tout point $x \in M_H^o(k)$ est défini par une courbe elliptique E sur k, munie d'une structure de niveau H.

Preuve (d'après J-P. Serre et J.S. Milne). Soient $\bar{k}$ une clôture séparable de k et (E,α) sur $\bar{k}$ qui définisse l'image de x dans $M_H^o(\bar{k})$. Si $H = GL(2,\mathbb{Z}/n)$ (ce qui revient à supposer que $n = 1$), 3.2 se réduit à 1.7. Dans le langage 3.1, une certaine obstruction $\epsilon(E)$ est donc nulle. Si $Aut(E,\alpha)$ est trivial, 3.2 est clair. Si $Aut(E)$ est réduit à ± 1 et que $Aut(E,\alpha)$ est non trivial, on a $Aut(E,\alpha) \xrightarrow{\sim} Aut(E)$; les obstructions $\epsilon(E,\alpha)$ et $\epsilon(E)$ à définir (E,α) ou E sur k sont donc égales, et nulles. Pour achever la démonstration, il nous suffira de traiter les deux cas suivants.

Cas 1 $p \neq 2,3$. D'après 1.9, on a alors $Aut(E) = \mu_2,\mu_4$ ou μ_6. Le groupe $Aut(E,\alpha)$ des automorphismes de (E,α) est un sous-groupe de $Aut(E)$. La proposition 3.2 affirme que la classe d'obstruction $\epsilon(E,\alpha) \in H^2(Gal(k/k), Aut(E,\alpha))$ est nulle. On sait par 1.7 que son image $\epsilon(E)$ dans $H^2(Gal(\bar{k}/k), Aut(E))$ est nulle, et on applique le lemme suivant.

Lemme 3.3. Soit n premier à p.

(i) les sous-groupes de μ_n sont les μ_m, $m|n$.

(ii) l'application $H^2(Gal(\bar{k}/k), \mu_m) \to Gal(\bar{k}/k, \mu_n)$ est injective

Preuve : Nous laissons la preuve de (i) au lecteur. Soit la suite exacte longue de cohomologie associée à la suite exacte courte

$$0 \to \mu_m \to \mu_n \xrightarrow{x \mapsto x^m} \mu_{n/m} \to 0 \quad : \quad H^1(\mu_n) \xrightarrow{①} H^1(\mu_{n/m}) \xrightarrow{j} H^2(\mu_m) \xrightarrow{②} H^2(\mu_n) \quad .$$

Pour prouver ② injectif, il suffit de prouver ① surjectif. D'après le théorème 90 de Hilbert $H^1(\mu_n) = k^*/k^{*n}$; ① est le passage au quotient

$$k^*/k^{*m/n} \longrightarrow k^*/k^{*m/n} \quad ,$$

et 3.3 en résulte.

Cas 2 $p \neq 0$, $\mathrm{Aut}(E)$ n'est pas réduit à ± 1 .

Dans ce cas, x provient par extension des scalaires d'un point de M_H^0 à valeurs dans un corps fini (on a $j = 0$ ou $2^6.3^3$ et le corps de définition de x est algébrique sur celui engendré par $j(x)$). On peut donc supposer k fini. Puisque $\mathrm{Gal}(\bar{k}/k) = \hat{\mathbb{Z}}$ et que $\mathrm{Aut}(E,\alpha)$ est fini, le H^2 de Giraud où vit l'obstruction est nul, et 3.2 en résulte. Autrement dit : soit $x \in M_H^0(\mathbb{F}_q)$; il existe une extension finie $\mathbb{F}_{q^n}$ de $\mathbb{F}_q$ et (E,α) sur $\mathbb{F}_{q^n}$ qui définisse x . La courbe (E,α) est géométriquement isomorphe à ses conjuguées sous $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. Quitte à remplacer $\mathbb{F}_{q^n}$ par une extension, on peut donc supposer qu'il existe un isomorphisme $\varphi' : (E,\alpha)^{(q)} \xrightarrow{\sim} (E,\alpha)$. Cet isomorphisme définit une donnée de descente de $\mathbb{F}_{q^n}$ à $\mathbb{F}_q$ si et seulement si la puissance $n^{\text{ième}}$ de $\varphi : E \xrightarrow{Fr} E^{(q)} \xrightarrow{\varphi'} E$ est l'endomorphisme de Frobenius F de $E/\mathbb{F}_{q^n}$. En général, on a $\varphi^n = F\beta$, avec β d'ordre fini m. On a $\varphi^{nm} = F^m$, et après extension des scalaires à $\mathbb{F}_{q^{nm}}$, φ' définit une donnée de descente de $\mathbb{F}_{q^{nm}}$ à $\mathbb{F}_q$ pour (E,α). La courbe descendue résoud le problème posé.

4. Remarques numériques

Nous nous proposons de traduire dans le langage des champs algébriques les formules classiques donnant le genre des courbes modulaires. Pour ce faire, il nous faut au préalable définir la caractéristique d'Euler-Poincaré $\chi(\mathcal{C})$ d'un champ algébrique de présentation finie sur $\mathbb{C}$. Cette notion est liée à celle de caractéristique d'Euler-Poincaré virtuelle d'un groupe discret introduite par Wall.

4.1. a) Soit $\mathcal{X}_i)$ une partition finie de $\mathcal{C}$ en sous-champs localement fermés et séparés telle que, au-dessus de $\mathcal{X}_i$ le schéma en groupes des automorphismes des objets classifiés par $\mathcal{C}$ soit localement constant de rang u_i . En d'autres termes, pour tout point géométrique $x \to \mathcal{X}_i$, on veut que $|\mathrm{Aut}(x)| = u_i$. Une telle décomposition existe.

b) Soient F_i le schéma grossier de modules de $\mathcal{X}_i$ et $\chi(F_i)$ la caractéristique d'Euler-Poincaré de l'espace topologique $F_i(C)$. On pose

$$\chi(\mathcal{C}) \underset{\text{dfn}}{=} \sum \frac{1}{u_i} \chi(F_i(\mathbb{C})) \quad .$$

On vérifie que cette définition est indépendante de la décomposition $(\mathcal{X}_i)$. Elle coïncide avec la définition usuelle quand $\mathcal{C}$ "est" un schéma.

DeRa-134

La caractéristique d'Euler-Poincaré jouit des propriétés suivantes :

α) additivité : si $\mathcal{F}$ est un fermé de $\mathcal{C}$, d'ouvert complémentaire $\mathcal{U}$,

$$\chi(\mathcal{C}) = \chi(\mathcal{U}) + \chi(\mathcal{F}) \quad ;$$

si $\mathcal{U}$ et $\mathcal{V}$ sont deux ouverts,

$$\chi(\mathcal{U} \cup \mathcal{V}) + \chi(\mathcal{U} \cap \mathcal{V}) = \chi(\mathcal{U}) + \chi(\mathcal{V}) \quad .$$

β) multiplicativité : si $f : \mathcal{C} \to \mathcal{S}$ est un morphisme, et que les fibres géométriques $\mathcal{C}_s$ de f ont une caractéristique d'Euler-Poincaré constante, on a

$$\chi(\mathcal{C}) = \chi(\mathcal{S}).\chi(\mathcal{C}_s) \quad .$$

γ) caractère algébrique : la définition donnée s'étend aisément et permet de définir $\chi(\mathcal{C})$ pour $\mathcal{C}$ un champ algébrique de présentation finie sur un corps algébriquement clos k de caractéristique zéro.

δ) Soit $f : \mathcal{C} \to \mathcal{S}$ un morphisme fini et plat (i.e. plat, propre, à fibres finies), et s un point géométrique de $\mathcal{S}$. Pour x un point géométrique de $\mathcal{C}_s$, soit $\tilde{A}_x$ l'anneau local de $\mathcal{C}_s$ en x. C'est un anneau artinien. On pose

$$\deg_s(f) = \sum_x \frac{1}{|\mathrm{Aut}(x)|} \dim_{k(s)}(A_x) \quad . \tag{4.1.1}$$

Ce nombre est localement constant en s. S'il est constant, on le note $\deg(f)$. Si f est fini étale, on a $\chi(\mathcal{C}_s) = \deg_s(f)$ et β) fournit

$$\chi(\mathcal{C}) = \deg(f)\ \chi(\mathcal{S}) \quad . \tag{4.1.2}$$

En termes plus concrets, un point géométrique fermé s de $\mathcal{S}$ n'est autre qu'un objet de $\mathcal{S}$ sur $\mathbb{C}$, et un point géométrique de $\mathcal{C}_s$ est un objet x de $\mathcal{C}$ muni d'un isomorphisme $\alpha : f(x) \xleftrightarrow{\sim} s$. On a

$$\chi(\mathcal{C}_s) = \sum \frac{1}{\mathrm{Aut}(x,\alpha)} \quad . \tag{4.1.3}$$

4.2. Appliquons la définition 4.1 à $\mathcal{M}_1^o \otimes \mathbb{C}$.

Nous séparons les fermés "$c_4 = 0$" (6 automorphismes), "$c_6 = 0$" (4 auto-

morphismes), et l'ouvert complémentaire (2 automorphismes) de schéma grossier la droite affine moins les points $j = 0$, $j = 1728$. On trouve

$$\chi(\mathcal{M}_1^o \otimes \mathbb{C}) = \frac{1}{6} + \frac{1}{4} + \frac{-1}{2} = -\frac{1}{12} \quad , \tag{4.2.1}$$

plus sympathique sous la forme

$$\chi(\mathcal{M}_1^o \otimes \mathbb{C}) = \zeta(-1) \quad . \tag{4.2.2}$$

Pour $H \subset GL(2, \mathbb{Z}/n)$, on déduit de 4.1.5 que

$$\chi(\mathcal{M}_H^o \otimes \mathbb{C}) = [GL(2, \mathbb{Z}/n) : H] \cdot \frac{-1}{12} \quad . \tag{4.2.3}$$

Pour passer de là à la formule classique donnant $\chi(M_H \otimes \mathbb{C})$, il faut tenir compte des pointes et des automorphismes. Traitons le cas de $M_n \otimes \mathbb{C}$ $(n \geq 3)$. Soit $\pm U$ le groupe des matrices $\pm \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$ $(u \in \mathbb{Z}/n\mathbb{Z})$. Il y a $[GL(2, \mathbb{Z}/n) : \pm U]$ pointes (5.1) et les objets de $\mathcal{M}_n \otimes \mathbb{C}$ n'ont pas d'automorphisme non trivial (IV 2.7). On a donc

$$\chi(M_n(\mathbb{C})) = |GL(2, \mathbb{Z}/n)| \cdot \frac{-1}{12} + [GL(2, \mathbb{Z}/n) : \pm U]$$

$$= \frac{-1}{12} n^4 \cdot \prod_{p|n} (1 - \frac{1}{p^2}) (1 - \frac{1}{p}) + \frac{n^3}{2} \prod_{p|n} (1 - \frac{1}{p^2}) (1 - \frac{1}{p}) \quad .$$

La courbe $M_n(\mathbb{C})$ a $\varphi(n)$ composantes connexes, toutes isomorphes. Leur genre g est donné par

$$2g - 2 = \prod_{p|n} (1 - \frac{1}{p^2}) \cdot (\frac{n^3}{12} - \frac{n^2}{2}) \quad .$$

4.3. Soit C un champ algébrique propre, de Cohen-Macaulay, purement de dimension un, sur un corps algébriquement clos k (par exemple, $\mathcal{M}_1 \otimes \mathbb{C}$). Soit ω un faisceau inversible sur C . Le degré de ω est défini comme suit .

a) On prend une section rationnelle f de ω .

b) Soit x un point géométrique fermé de C . Soit $\tilde{\mathcal{O}}_x$ l'anneau local hensélien de C en x . Si f est régulier en x , on pose $\deg_x(f) = \dim_k \tilde{\mathcal{O}}_x/(f)$. Si f^{-1} l'est, on pose $\deg_x(f) = -\dim_k \tilde{\mathcal{O}}_x/(f^{-1})$

c) On pose

$$\deg(\omega) = \deg(C,\omega) = \sum_x \frac{1}{|\mathrm{Aut}(x)|} \deg_x(f) \quad .$$

Pour k non algébriquement clos, on définit deg en étendant au préalable les scalaires à $\bar{k}$. Ce degré est indépendant du choix de f et coincide avec la notion usuelle quand C "est" un schéma.

Il vérifie

α) <u>additivité en</u> ω : $\deg(\omega \otimes \omega') = \deg(\omega) + \deg(\omega')$.

β) <u>revêtements</u> : Soit $f : C' \to C$ un morphisme fini et plat de degré constant. On a

$$\deg(f^* \omega) = \deg(f).\ \deg(\omega) \quad .$$

γ) <u>spécialisation</u> : Soient S un trait, C un champ algébrique propre et plat, de Cohen-Macaulay, purement de dimension relative un sur S . Soit ω un faisceau inversible sur C . On a

$$\deg(C_\eta, \omega) = \deg(C_s, \omega) \quad .$$

4.4. Calculons le degré sur $\mathcal{M}_1$ de ω , le dual de l'algèbre de Lie de la courbe elliptique universelle. Le discriminant Δ est une section de $\omega^{\otimes 12}$, s'annulant simplement à l'infini. Le point à l'infini ayant deux automorphismes, on trouve

$$\deg(\omega) = \frac{1}{24} \quad . \tag{4.4.1}$$

Partant de (4.4.1), et exploitant (4.2.2), 4.3. β) , on trouve que pour tout $H \subset GL(2, \mathbb{Z}/n)$, on a

$$\chi(\mathcal{M}_H^o \otimes \mathbb{C}) = -2 \deg(\mathcal{M}_H, \omega) \ . \tag{4.4.2}$$

4.5. Voici une démonstration directe de (4.4.2). En tout point s de $\mathcal{M}_1^o$, sur $\mathbb{C}$, correspondant à une courbe elliptique E , la théorie des déformations fournit un isomorphisme entre l'espace tangent à $\mathcal{M}_1^o$ en s et $H^1(E, T_E^1) \simeq H^1(E, \mathcal{O}) \otimes \omega^{\otimes -1} \simeq \omega_s^{\otimes -2}$. Une étude à l'infini montre que l'isomorphisme $\Omega^1_{\mathcal{M}_1^o} \simeq \omega^{\otimes 2}$ correspondant se prolonge

à l'infini en

$$\Omega^1_{\mathcal{M}_1}(\mathcal{M}_1^\infty) \simeq \omega^{\otimes 2} \tag{4.5.1}$$

Vu les propriétés de multiplicativité des deux membres de (4.4.2), il suffit de considérer $\mathcal{M}_n$, pour un entier $n \geq 3$. On a alors affaire à de vrais schémas, de sorte que

$$\chi(M_n \otimes \mathbb{C}) = -\deg(M_n, \Omega^1_{M_n}) \quad .$$

Puisque l'image réciproque d'une forme différentielle à pôles logarithmiques est encore de ce type, (4.5.1) nous fournit un isomorphisme

$$\Omega^1_{\mathcal{M}_H}(\mathcal{M}_H^\infty) \simeq \omega^{\otimes 2} \quad ; \tag{4.5.2}$$

si c est le nombre de points à l'infini de $\mathcal{M}_n$, on a donc

$$\chi(\mathcal{M}_n^o \otimes \mathbb{C}) = \chi(\mathcal{M}_n \otimes \mathbb{C}) - c = -\deg(\Omega^1) - c$$

$$= -\deg(\Omega^1(\infty)) = -\deg(\omega^{\otimes 2}) = -2\deg(\omega) \quad .$$

Dans la fin de ce §, nous définissons l'invariant de Hasse et donnons une démonstration, basée sur des théorèmes de Grothendieck, du théorème de Igusa selon lequel ses zéros sont simples. L'un de nous a appris la jolie formule 4.9.1 à un cours de Serre.

4.6. Définition de l'invariant de Hasse .

Soit $f : E \to S$ une courbe elliptique généralisée sur un schéma S de caractéristique p , $\omega = f_* \omega_{E/S}$ et F le morphisme de Frobenius

$$\begin{array}{ccc} E & \xrightarrow{F} & E^{(p)} \\ & {\scriptstyle f}\searrow \quad \swarrow{\scriptstyle f^{(p)}} & \\ & S & \end{array}$$

On a $f^{(p)}_* \omega_{E^{(p)}/S} = \omega^{(p)} = \omega^{\otimes p}$. L'application trace (ou : "opération de Cartier")

$$Tr_F : F_* \omega_{E/S} \longrightarrow \omega_{E^{(p)}/S}$$

définit un morphisme

(4.6.1) $$Tr_F : \omega \longrightarrow \omega^{\otimes p} ,$$

i.e. une section

(4.6.2) $$h \in \Gamma(S, \omega^{\otimes(p-1)}) .$$

C'est l'invariant de Hasse. En voici une expression duale : la dualité des faisceaux cohérents met en dualité ω et $R^1 f_* \mathcal{O}$, et de même $\omega^{(p)}$ et $R^1 f^{(p)}_* \mathcal{O}$. Le transposé de (4.6.1) est l'image réciproque

(4.6.3) $$F^* : R^1 f^{(p)}_* \mathcal{O} \longrightarrow R^1 f_* \mathcal{O} .$$

Si on identifie $R^1 f_* \mathcal{O}$ et $R^1 f^{(p)} \mathcal{O}$ à $\omega^{\otimes(-1)}$ et $\omega^{\otimes(-p)}$, (4.6.3) devient la multiplication par h (4.6.2).

Sur $\mathcal{M}_1 \otimes \mathbb{F}_p$, on sait que l'invariant de Hasse ne s'annule pas à l'infini, et que ses zéros correspondent aux courbes elliptiques supersingulières (voir Katz [13]).

On sait que sur $\mathcal{M}_1 \otimes \overline{\mathbb{F}}_p$, les zéros de h sont simples. Nous en donnons en 4.8 une démonstration directe, basée sur la théorie de Grothendieck des déformations des schémas abéliens, dont un cas particulier est rappelé ci-dessous.

4.7. Soit A_o une variété abélienne sur un corps k algébriquement clos. Pour toute déformation A de A_o sur les nombres duaux $k[\varepsilon]$ ($\varepsilon^2 = 0$), on définit

$$H_{DR}(A) = \mathbb{H}^1(A, \Omega^*_{A/\mathrm{Spec}(k[\varepsilon])}) .$$

On dispose d'une suite exacte

(4.7.1) $$0 \to H^0(A, \Omega^1_A) \to H_{DR}(A) \to H^1(A, \mathcal{O}) \to 0 .$$

Grothendieck a défini un isomorphisme canonique

(4.7.2) $$H_{DR}(A) \simeq H_{DR}(A_o) \otimes_k k[\varepsilon] \quad ,$$

et a prouvé que

a) Pour tout morphisme $f : A \to B$, le diagramme

$$\begin{array}{ccc} H_{DR}(B_o) \otimes k[\varepsilon] & \xrightarrow{f_o \otimes k[\varepsilon]} & H_{DR}(A_o) \otimes k[\varepsilon] \\ \| & & \| \\ H_{DR}(B) & \xrightarrow{f^*} & H_{DR}(A) \end{array}$$

est commutatif .

b) L'application qui à chaque classe d'isomorphie de déformations A associe la filtration (4.7.1) de $H_{DR}(A_o) \otimes k[\varepsilon]$, assujettie à relever la filtration (4.7.1) de $H_{DR}(A_o)$, est bijective.

4.8. Soit E_o une courbe elliptique supersingulière sur k , E une déformation non triviale de E_o sur $k[\varepsilon]$, et prouvons que $h \neq 0$ (i.e. que h est un multiple non nul de ε). Puisque $E^{(p)}$ est la déformation triviale de $E_o^{(p)}$, on dispose d'un diagramme commutatif

$$\begin{array}{ccccccc} 0 \longrightarrow & H^0(E_o^{(p)},\Omega^1) \otimes k[\varepsilon] & \longrightarrow & H_{DR}(E_o^{(p)}) \otimes k[\varepsilon] & \longrightarrow & H^1(E_o^{(p)},\mathcal{O}) \otimes k[\varepsilon] & \\ & \downarrow 0 & & \downarrow F^* \otimes k[\varepsilon] & & \downarrow h & \\ 0 \longrightarrow & H^0(E,\Omega^1) & \longrightarrow & H_{DR}(E) \otimes k[\varepsilon] & \longrightarrow & H^1(E,\mathcal{O}) & \longrightarrow 0 \end{array} \quad .$$

On sait que le noyau de F^* est exactement $H^0(E_o^{(p)},\Omega^1) \subset H_{DR}(E_o^{(p)})$, et $h \neq 0$ résulte formellement de ce que la $2^{\text{ème}}$ ligne n'est pas de la forme $\Sigma \otimes k[\varepsilon]$.

4.9. Si on applique la définition 4.3. à la section h du faisceau inversible $\omega^{\otimes(p-1)}$ sur $\mathcal{M}_1 \otimes \overline{\mathbb{F}}_p$ on trouve le résultat suivant : si I est l'ensemble des classes d'isomorphie de courbes elliptiques supersingulières sur $\overline{\mathbb{F}}_p$, on a

$$(p-1).\deg(\omega) = \sum_i \frac{1}{|\mathrm{Aut}(E_i)|}$$

D'après 4.3 α) et (4.4.1), on a donc

(4.9.1) $$\sum_{E \text{ supersingulier}} \frac{1}{|\mathrm{Aut}(E)|} = \frac{p-1}{24} \quad .$$

Par exemple, si $p = 2$ (resp. 3), seule la courbe elliptique d'invariant modulaire 0 est supersingulière. Elle a 24 (resp. 12) automorphismes. De même, si $n \geq 3$ et si $(p,n) = 1$, il y a sur $M_n^o \otimes \overline{\mathbb{F}}_p$ exactement $\frac{1-p}{2}\chi(M_n^o(\mathbb{C}))$ points supersinguliers.

5. L'action de Galois sur les pointes.

5.1. L'ensemble $M_n^\infty(\mathbb{C})$ est l'ensemble des classes d'isomorphie, sur $\mathbb{C}$, de courbes elliptiques généralisées singulières à n côtés, munies d'une structure de niveau n.

Soit $(C,+)$ le n-gone standard sur $\mathbb{C}$, muni de sa structure de courbe elliptique généralisée II.1.9. On a canoniquement

$$C_n = \mu_n \times \mathbb{Z}/n \quad .$$

Le groupe des automorphismes de $(C,+)$ a été calculé en II 1.10. Son image dans $GL(\mu_n \times \mathbb{Z}/n)$ est le groupe $\pm U$ des matrices

$$\pm \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \qquad (u \in \mathrm{Hom}(\mathbb{Z}/n, \mu_n)) \quad .$$

L'ensemble des structures de niveau n sur $(C,+)$ est $\mathrm{Isom}(C_n, (\mathbb{Z}/n)^2)$. On a donc canoniquement

$$M_n^\infty(\mathbb{C}) = \mathrm{Isom}(\mu_n \times \mathbb{Z}/n, (\mathbb{Z}/n)^2) / \pm U \quad .$$

Cette bijection est compatible à l'action de $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ sur les deux membres.

5.2. Pour $H \subset GL(2, \mathbb{Z}/n)$, on a $M_H = M_n/H$. Dès lors,

$$M_H^\infty(\mathbb{C}) = H\backslash \mathrm{Isom}(\mu_n \times \mathbb{Z}/n, (\mathbb{Z}/n)^2)/\pm U \quad .$$

Puisque $M_H^\infty[1/n]$ est fini étale sur $\mathbb{Z}[1/n]$, cet isomorphisme d'ensembles galoisiens se prolonge en un isomorphisme de schémas :

Construction 5.3. $M_H^{\infty}[1/n] = H\backslash\underline{\mathrm{Isom}}_{\mathbb{Z}[1/n]}(\mu_n \times \mathbb{Z}/n, (\mathbb{Z}/n)^2) / \pm U$.

6. Etude de $M_{\Gamma_o(n)}$.

6.1. En IV.4.5, nous avons décrit $\mathfrak{M}^o_{\Gamma_o(n)}[1/n]$ comme le champ sur $\mathbb{Z}[1/n]$ classifiant les isogénies $E \to F$ à noyau cyclique de degré n . Ceci met en évidence deux applications $\mathfrak{M}^o_{\Gamma_o(n)}[1/n] \longrightarrow \mathfrak{M}^o_1[1/n]$, définies par E et F respectivement, et échangées par une involution w (IV.4.4). D'après IV.3.19, les applications induites sur les schémas grossiers se prolongent en

(6.1.1) $$c \text{ et } cw : M_{\Gamma_o(n)} \longrightarrow M_1 \quad .$$

6.2. L'application finie $(c,cw) : M_{\Gamma_o(n)} \longrightarrow M_1 \times M_1$ a pour image un diviseur, invariant par permutation des coordonnées. Puisque l'application $M_{\Gamma_o(n)} \longrightarrow M_1$ est de degré le nombre $P(n)$ de points de la droite projective sur $\mathbb{Z}/n$, et est génériquement injective, ce diviseur est de bidegré $(P(n), P(n))$. Les applications c et cw transforment points à l'infini en points à l'infini. Puisque $M_1^o = \mathrm{Spec}(\mathbb{Z}[j])$ et que $\mathbb{Z}[j,j']$ est factoriel, le diviseur image de

(6.2.1) $$(c,cw) : M^o_{\Gamma_o(n)} \longrightarrow M_1^o \times M_1^o$$

et défini par une équation $\Phi_n \in \mathbb{Z}[j,j']$, l'<u>équation modulaire</u>. On a $\Phi_n(X,Y) = \sum_{a,b \le P(n)} c_{ab} X^a Y^b$, et les seuls c_{ab} non nuls et tels que $a = P(n)$ ou $b = P(n)$ sont obtenus pour $(a,b) = (P(n),0)$ ou $(0,P(n))$; ils valent ± 1 .

6.3. L'invariance par symétrie montre que $\Phi_n(X,Y) = \pm \Phi_n(Y,X)$. Il est classique, et résulte d'une étude à l'infini, pour $n \neq 1$, que le signe correct est $+$.

(6.3.1) $$\Phi_n(X,Y) = \Phi_n(Y,X) \qquad (n > 1) \quad .$$

On peut donc normaliser le signe de Φ_n pour avoir

(6.3.2) $$\Phi_n(X,Y) = X^{P(n)} + Y^{P(n)} + \sum_{a,b<P(n)} c_{ab} X^a Y^b$$

$$c_{ab} = c_{ba} \in \mathbb{Z} \quad .$$

6.4. On prendra garde que l'application (6.2.1) n'est pas nécessairement injective. Sur k algébriquement clos avec n inversible dans k, il peut en effet exister deux n-isogénies à noyau cyclique

(6.4.1) $$\varphi_1 : E_1 \longrightarrow F_1$$
$$\varphi_2 : E_2 \longrightarrow F_2$$

non isomorphes, mais telles qu'il existe des isomorphismes $e : E_1 \xrightarrow{\sim} E_2$ et $f : F_1 \longrightarrow F_2$. L'endomorphisme $g = e^{-1} \varphi_2^* f \varphi_1$ de E_1 est alors de degré n^2, mais son noyau n'est pas le noyau de la multiplication par n. La courbe E_1 est donc à multiplication complexe.

Réciproquement, si g est un endomorphisme de degré n^2 d'une courbe elliptique E, que $\mathrm{Ker}(g) \neq E_n$, et que $A \subset \mathrm{Ker}(g)$ est cyclique d'ordre n, on obtient une paire (6.4.1) en prenant

$$E \longrightarrow E/A \quad , \quad \text{et le transposé de}$$

$$E/\mathrm{Ker}(g) \longleftarrow E/A \quad .$$

La discussion précédente montre toutefois que (6.2.1) est génériquement radiciel; on montre facilement qu'il existe même un ouvert U de $M^o_{\Gamma_o(n)}$, dense dans les fibres de caractéristique $p \nmid n$, tel que la restriction de (6.2.1) à U soit un plongement.

Le résultat suivant en résulte.

Proposition 6.5. *$M^o_{\Gamma_o(n)}$ est le spectre du normalisé de $\mathbb{Z}[j,j']/(\Phi_n(j,j'))$.*

Si k est un corps de caractéristique p et que $p \nmid n$, il résulte de 3.2 que tout point $x \in M^o_{\Gamma_o(n)}(k)$ est défini par une n-isogénie à noyau cyclique

$E \longrightarrow F$ définie sur k . Il n'en résulte pas que si j,j' sont dans k et que $\Phi_n(j,j') = 0$, il existe une telle n-isogénie avec $j(E) = j$, $j(F) = j'$.

Si n est un nombre premier p , la décomposition V.1.16 de $\mathfrak{m}_{\Gamma_0(p)}$ mod p se traduit comme suit au niveau des schémas grossiers.

Théorème 6.6. (H. Weber-Lehrbuch der Algebra III, p.244 eq. (32)).

$$\Phi_p(j,j') \equiv (j-j'^p)\,(j^p-j') \mod p .$$

Par une étude à l'infini, on démontre plus généralement que si $(n,p) = 1$, on a

$$\Phi_{np}(j,j') \equiv \Phi_n(j^p,j')\,\Phi_n(j,j'^p) \quad (p) \tag{6.6.1}$$

$$\Phi_{np^2}(j,j') \equiv \Phi_n(j'^2,j')\,\Phi_n(j,j')^{p-1}\,\Phi_n(j,j'^{p^2}) \quad (p) \tag{6.6.2}$$

$$\Phi_{np^k}(j,j') \equiv \prod_{\substack{\ell+m=k \\ K=\inf(\ell,m)}} \Phi_n(j^{p^{\ell-K}},j'^{p^{m-K}})^{\varphi(p^K)} \quad (p) \tag{6.6.3}$$

Si $p^2 \mid n$, on tire de 6.6.3 que

$$\Phi_{np}(j,j')\,\Phi_{n/p}(j^p,j'^p) \equiv \Phi_n(j^p,j')\,\Phi_n(j,j'^p) \quad (p) . \tag{6.6.4}$$

Proposition 6.7. Soient $H \subset GL(2,\mathbb{Z}/n)$ et K l'image inverse de H dans $GL(2,\hat{\mathbb{Z}})$. Le schéma $M_K[1/n]$ est lisse sur $\mathbb{Z}[1/n]$.

Au-dessus du complément des sections $0, 2^6.3^3$ et ∞ de $M_1, M_K[1/n] \to M_1[1/n]$ est fini étale. En effet, sur cet ouvert $\mathfrak{m}_K[1/n]$ (resp. $\mathfrak{m}_1[1/n]$) est étale sur $M_K[1/n]$ (resp. $M_1[1/n]$) , et $\mathfrak{m}_K^o[1/n]$ est étale sur $\mathfrak{m}_1^o[1/n]$.

Il résulte donc du lemme d'Abhyankar que $M_K[1/n]$ est lisse sur $\mathbb{Z}[1/n]$ en dehors des points de caractéristique 2 ou 3 d'invariant modulaire 0 .

Caractéristique 2. Soit E la courbe elliptique d'invariant 0 sur $\overline{\mathbb{F}}_2$, correspondant à $x : \mathrm{Spec}(\overline{\mathbb{F}}_2) \to \mathfrak{m}_1$. Soit $W(\overline{\mathbb{F}}_2)[[t]]$ le complété de l'hensélisé strict

de $\mathfrak{m}_1$ en x . Le groupe $A = \mathrm{Aut}(E)$ agit sur $W(\overline{\mathbb{F}}_2)[[t]]$ et, vu I.8, il faut prouver que pour tout sous-groupe B de A , l'algèbre $W(\overline{\mathbb{F}}_2)[[t]]^B$ est formellement lisse sur $W(\overline{\mathbb{F}}_2)$. Le groupe A s'injecte dans $GL(2,E_3)$ (IV.2.7). En fait, $A = SL(2,E_3)$. Il en résulte que si l'une des algèbres $W(\overline{\mathbb{F}}_2)[[t]]^B$ n'était pas formellement lisse, déjà l'un des schémas M_H ($H \subset GL(2,\mathbb{Z}/3)$) ne serait pas lisse sur $\mathbb{Z}$.

On sait que la courbe $M_3/\mathbb{Z}[\zeta_3]$ est de genre 0 . Il en résulte que pour $H \subset GL(2,\mathbb{Z}/3)$, $M_H = M_3/H$ sur $\mathbb{Z}[\zeta_3]^H$ est de genre 0 . On sait aussi que les fibres géométriques de $M_H[1/3]$ sont génériquement lisses, irréductibles et réduites (car de Cohen-Macaulay, M_H étant normal). Etant de genre arithmétique 0 , elles sont lisses.

Caractéristique 3 : On procède de même, en utilisant que $\mathrm{Aut}(E)$ s'injecte dans $GL(2,E_4)$ et que $M_4/\mathbb{Z}[\zeta_4]$ est de genre 0 .

6.8. Soient n,H,K comme en 6.7 et p un nombre premier premier à n . Nous allons utiliser (V.1) pour étudier $M_{K\cap\Gamma_0(p)}$ en caractéristique p , la structure des singularités de $M_{K\cap\Gamma_0(p)}[1/n]$ et leur résolution minimale. Rappelons que le champ $\mathfrak{M}^o_{K\cap\Gamma_0(p)}[1/n]$ correspondant classifie les courbes elliptiques E munies d'une structure de niveau H et d'un sous-groupe localement libre de rang p A . Il est régulier, et $\mathfrak{M}^o_{K\cap\Gamma_0(p)} \otimes \overline{\mathbb{F}}_p$ est réunion de deux copies de $\mathfrak{M}^o_K \otimes \overline{\mathbb{F}}_p$ se coupant transversalement aux points supersinguliers.

Théorème 6.9. (i) $M_{K\cap\Gamma_0(p)}[1/n]$ est lisse sur $\mathbb{Z}[1/n]$ en dehors des points supersinguliers de caractéristique p .

(ii) $M_{K\cap\Gamma_0(p)} \otimes \overline{\mathbb{F}}_p$ est réunion de deux copies de $M_K \otimes \overline{\mathbb{F}}_p$ se coupant transversalement aux points supersinguliers. On recolle le point supersingulier x de la 2^e copie au point $x^{(p)}$ de la 1^{ere} .

(iii) Si x est un point supersingulier de $M_K \otimes \overline{\mathbb{F}}_p$ défini par (E,α) , et que

$$k = \tfrac{1}{2}\,|\,\mathrm{Aut}(E,\alpha)\,| \qquad \text{si } -1 \in \mathrm{Aut}(E,\alpha)$$

$$k = \quad |\,\mathrm{Aut}(E,\alpha)\,| \qquad \text{si } -1 \notin \mathrm{Aut}(E,\alpha)$$

alors, au point correspondant de $M_{K\cap\Gamma_o(p)} \otimes \mathbb{F}_p$, le schéma $M_{K\cap\Gamma_o(p)} \otimes W(\overline{\mathbb{F}}_p)$ présente une singularité de type A_{k-1} , formellement isomorphe à

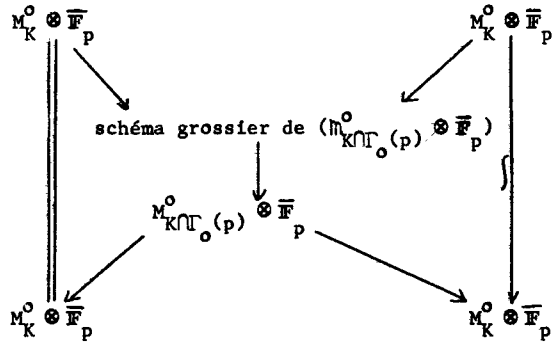
$$W(\overline{\mathbb{F}}_p)[[X,Y]] / (X.Y - p^k) \quad . \tag{6.9.1}$$

Preuve : Au voisinage de l'infini, l'application

$$\mathfrak{M}_{\Gamma_o(p)} \to M_{\Gamma_o(p)}$$

est étale, et $M_{\Gamma_o(p)}$ est lisse sur $\mathbb{Z}$. D'après le lemme d'Abhyankar, $M_{K\cap\Gamma_o(p)}$ est modérément ramifié sur $M_{\Gamma_o(p)}$ le long de l'infini, donc lisse au voisinage de l'infini. Etudions maintenant les points à distance finie.

Par passage aux schémas grossiers de modules, on tire de (V.1.15) et de 6.1.1 un diagramme



(diagonales composées = Frobenius)

On sait que $\mathfrak{M}^o_{K\cap\Gamma_o(p)} \otimes \overline{\mathbb{F}}_p$ est réduit (V.1.16) . Son schéma grossier de modules l'est donc également. Puisque $M^o_{K\cap\Gamma_o(p)}$ est normal, $M^o_{K\cap\Gamma_o(p)} \otimes \overline{\mathbb{F}}_p$ est de Cohen-Macaulay. Etant génériquement réduit, ce schéma est réduit. On peut maintenant raisonner comme en V.1.16 pour prouver (i),(ii) . Les mêmes arguments s'appliquent au schéma grossier de $\mathfrak{M}^o_{K\cap\Gamma_o(p)} \otimes \overline{\mathbb{F}}_p$, et on trouve le corollaire suivant.

Corollaire 6.10. $M_{K\cap\Gamma_o(p)} \otimes \mathbb{F}_p$ est le schéma grossier de modules de $\mathfrak{M}_{K\cap\Gamma_o(p)} \otimes \mathbb{F}_p$.

Prouvons 6.9 (iii). Soient (E,α) et x comme indiqué. Soit A' le groupe des automorphismes de (E,α) et

$$A = A' \text{ si } -1 \notin A'$$

$$A = A'/\{\pm 1\} \text{ si } -1 \in A' \ .$$

Le groupe A est d'ordre k. D'après I.8, le complété de l'hensélisé strict de $M_{K\cap\Gamma_o(p)}$ en x est de la forme

$$\mathrm{Spec}(W(\overline{\mathbb{F}}_p)[[X,Y]]/(XY-p))/A \ ,$$

où le groupe A agit effectivement (I.8 et 1.4). En réduction mod p, le groupe A respecte chaque branche, et agit effectivement sur chacune. On sait aussi, d'après I.5.2 et (ii), que le quotient étudié est de la forme

$$\mathrm{Spec}(W(\overline{\mathbb{F}}_p)[[X',Y']] \ / \ (X'Y'-p^{k'})) \ ,$$

et il nous faut prouver que $k = k'$.

D'après 6.10, on a

$$\mathrm{Spec}(\overline{\mathbb{F}}_p[[X,Y]]/(X.Y))/A = \mathrm{Spec}(\overline{\mathbb{F}}_p[[X',Y']]/(X'Y')) \ ,$$

donc, par restriction à une branche,

$$\mathrm{Spec}(\overline{\mathbb{F}}_p[[X,Y]]/(Y))/A = \mathrm{Spec}(\overline{\mathbb{F}}_p[[X'Y']]/(Y')) \ .$$

Puisque A est d'ordre k, il en résulte que

$$X^k = \text{unité. } X' \ (\mathrm{mod}(p,Y)) \ .$$

Dans le spectre de l'anneau régulier $W(\overline{\mathbb{F}}_p)[[X,Y]]/(XY-p)$, les diviseurs de X et X' ont même support. La formule précédente impose alors que $\mathrm{div}(X') = k\,\mathrm{div}(X)$, i.e. $X^k = \text{unité. } X'$. Le même argument s'applique à Y' ; on a donc

$$X'Y' = \text{unité.} p^k$$

et que $k = k'$ en résulte.

L'invariance par spécialisation de la caractéristique d'Euler-Poincaré de © et 6.9 (ii) fournissent, pour Euler-Poincaré topologique :

Corollaire 6.11. Soient s le nombre de points supersinguliers sur $M_K \otimes \overline{\mathbb{F}}_p$. On a

$$\chi\left(M_{K\cap\Gamma_o(p)}\right) = 2\chi(M_K)-2s \quad . \tag{6.11.1}$$

Si on considère $M_{K\cap\Gamma_o(p)}$ comme une courbe géométriquement irréductible sur $R = \mathbb{Z}[\zeta_n]^H$ et que $s_o = s/[R:\mathbb{Z}]$ désigne le nombre de points supersinguliers de $M_K \otimes_R \overline{\mathbb{F}}_p$, 6.11 se récrit en terme du genre :

$$g\left(M_{K\cap\Gamma_o(p)} \otimes_R \mathbb{C}\right) = 2g(M_K) + (s_o-1) \quad . \tag{6.11.2}$$

Corollaire 6.12. $M_{K\cap\Gamma_o(p)} \otimes_R \mathbb{C}$ est une courbe elliptique si et seulement si $M_K \otimes_R \mathbb{C}$ est de genre 0 et que $s_o = 2$.

Rappel 6.13. Résolvant la singularité (6.9.1) par éclatements, on obtient une chaîne de (k-1) droites projectives de self intersection -2 . Le lieu d'équation $p = 0$ de la résolution est réduit. Ceci permet de calculer la résolution minimale de $M_{K\cap\Gamma_o(p)}$.

Le lemme suivant, tiré de [20], sera prouvé en VII.2.7.

Lemme 6.14. Soit E une courbe elliptique sur le corps des fractions d'un anneau de valuation discrète V . Si le modèle minimal de Néron de E a pour fibre spéciale un polygone de Néron à k côtés, alors $v(j(E)) = -k$.

Lorsque $M_{K\cap\Gamma_o(p)}$ est elliptique, on déduit de 6.11 le corollaire suivant.

Corollaire 6.15. Si $M_{K\cap\Gamma_o(p)} \otimes_R \mathbb{C}$ est elliptique, d'invariant modulaire j , le pôle de $j \in R$ en un idéal premier π de R divisant p est donné par la formule suivante :

$$-v_\pi(j) = 2 + \sum_{(E,\alpha)} \left(\left|\mathrm{Aut}(E,\alpha)/\{\pm 1\}\right|-1\right) ,$$

la somme étant étendue à l'ensemble (à deux éléments) des classes d'isomorphie de

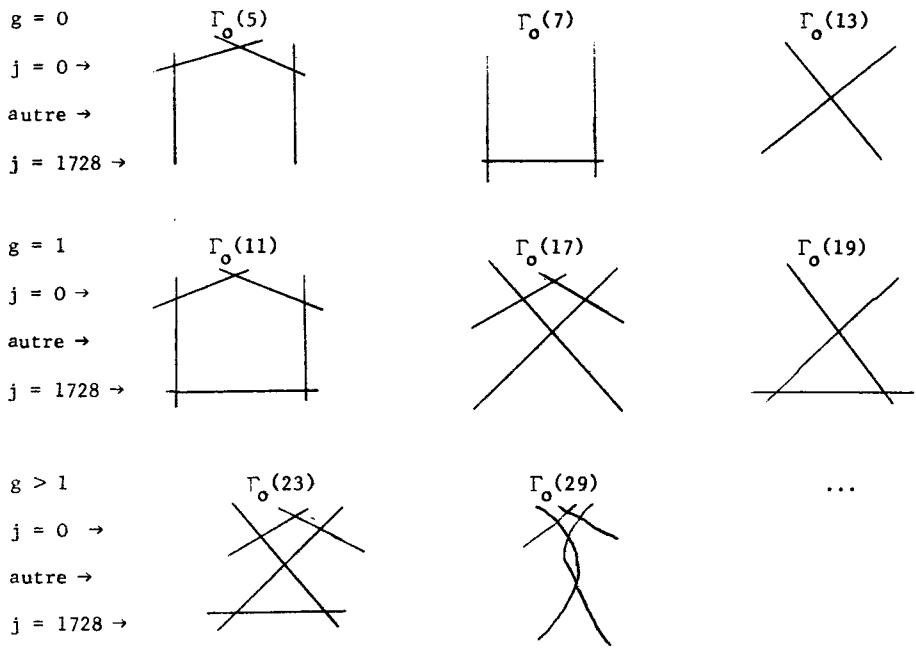
courbes elliptiques supersingulières E , munie d'une structure de niveau H de déterminant un, sur une clôture algébrique $\overline{\mathbb{F}}_p$ de $R/(\pi)$.

6.16. Exemple. Traitons le cas de $M_{\Gamma_o(p)}$, p premier , $p \neq 2,3$. $M_{\Gamma_o(p)} \otimes \overline{\mathbb{F}}_p$ s'obtient en recollant 2 exemplaires de $M_1 \otimes \overline{\mathbb{F}}_p = \mathbb{P}^1_{\overline{\mathbb{F}}_p}$ en les points supersinguliers. Pour obtenir la fibre spéciale de la résolution minimale, il faut remplacer le point $j = 0$ (resp. $j = 1728$), si supersingulier, par une chaine de 2 (resp. 1) droites projectives. Rappelons que

$$j = 0 \text{ supersingulier} \Leftrightarrow p \equiv -1 \pmod 6$$

$$j = 1728 \text{ supersingulier} \Leftrightarrow p \equiv -1 \pmod 4 .$$

Dès lors, sur la clôture algébrique de $\mathbb{F}_p$, la fibre spéciale de la résolution minimale de $M_{\Gamma_o(p)}$ est le diagramme suivant de copies de $\mathbb{P}^1$ se coupant transversalement :



La formule 6.15 dit que l'invariant modulaire de la courbe de genre un $M_{\Gamma_o(p)}$, $p = 11,17,19$ a pour dénominateur respectivement 11^5 , 17^4 , 19^3 .

VII. La courbe de Tate.

Au § 1 de ce chapitre, nous utilisons une méthode due à Raynaud pour construire la courbe de Tate $\mathbb{G}_m/q^{\mathbb{Z}}$ sur $\mathbb{Z}[[q]]$. Ceci nous permet de donner une description explicite du complété formel de $\mathfrak{M}_H$ le long de l'infini (§2). Aux §3 et 4, nous en déduisons des théorèmes d'intégralité sur les coefficients du développement en série de Fourier des formes modulaires.

1. Construction de la courbe de Tate sur $\mathbb{Z}[[q]]$.

1.1. Soient S un schéma et $t \in \Gamma(S,\mathcal{O}_S)$. Nous nous proposons de construire sur S un schéma $\overline{\mathcal{C}}_m^t$, isomorphe à $\mathbb{G}_m$ au-dessus de $S[t^{-1}]$, non quasi-compact si t n'est pas inversible, et dont des courbes elliptiques généralisées se déduiront par passage au quotient si t est nilpotent.

a) Soient $(x_i)_{i \in \mathbb{Z}}$ des indéterminées. $\overline{\mathcal{C}}_m^t$ est réunion des cartes locales $(U_j)_{j \in \frac{1}{2}+\mathbb{Z}}$ suivantes :

$$U_j = S[x_{j-\frac{1}{2}}, y_{j+\frac{1}{2}}] \,/\, (x_{j-\frac{1}{2}}.y_{j+\frac{1}{2}} - t) \tag{1.1.1}$$

b) On recolle $U_{i-\frac{1}{2}}$ et $U_{i+\frac{1}{2}}$ de sorte que

$$U_{i-\frac{1}{2}} \cap U_{i+\frac{1}{2}} \subset U_{i+\frac{1}{2}} \text{ soit } U_{i+\frac{1}{2}}[1/x_i] \simeq S[x_i, x_i^{-1}] \qquad (y_{i+1} = t.x_i^{-1}) \tag{1.1.2}$$

$$U_{i-\frac{1}{2}} \cap U_{i+\frac{1}{2}} \subset U_{i-\frac{1}{2}} \text{ soit } U_{i-\frac{1}{2}}[1/y_i] \simeq S[y_i, y_i^{-1}] \qquad (x_{i-1} = t.y_i^{-1}) \tag{1.1.3}$$

ces ouverts étant identifiés par

$$x_i.y_i = 1 \ . \tag{1.1.4}$$

c) On ne fait d'autre recollement que ceux imposés par b). Explicitement :

(1.1.5) si $|j-j'| \geq 2$, $U_j \cap U_{j'}$ est au-dessus de $S[1/t]$. ;

(1.1.6) au-dessus de $S[1/t]$, les U_j sont tous identifiés, par

$$x_i = t^{-i} x_o$$

$$y_i = t^{-i} y_o \quad .$$

1.2 Exemples : a) si t est inversible,

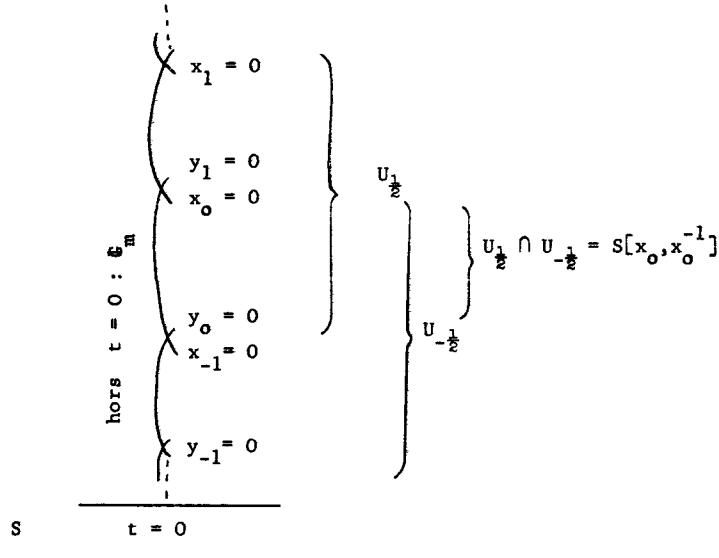
$$\overline{\mathcal{C}}_m^t = U_o = S[x_o, x_o^{-1}] \simeq \mathbb{G}_m \quad ;$$

b) si $t = 0$, $\overline{\mathcal{C}}_m^t$ se déduit par recollement de la somme d'une famille de copies de $\mathbb{P}^1$ indexée par $\mathbb{Z}$: on recolle la $i^{\text{ème}}$ copie à la $(i+1)^{\text{ième}}$ en identifiant la section 0 de la $i^{\text{ième}}$ à la section ∞ de la $(i+1)^{\text{ième}}$;

$$U_j = ((j-\tfrac{1}{2})^{\text{ième}} \text{ copie - section } \infty) \cup ((j+\tfrac{1}{2})^{\text{ième}} \text{ copie - section } 0)$$

$$x_{j-\frac{1}{2}} = \text{coordonnée } x \cup 0$$

$$y_{j+\frac{1}{2}} = 0 \cup (\text{coordonnée } x)^{-1} \quad .$$



c) soit $T_i = U_{i-\frac{1}{2}} \cap U_{i+\frac{1}{2}} = S[x_i, x_i^{-1}]$ et soit $\mathcal{C}_m^t$ la réunion des T_i . C'est le lieu lisse de $\overline{\mathcal{C}}_m^t$. Si $S = \mathrm{Spec}(V)$ est un trait et t une uniformisante de V , $\mathcal{C}_m^t$ est le modèle de Néron de $\mathbb{G}_m$ construit par Raynaud.

Les applications

$$\overline{\mathcal{G}}_m^t(S) \longleftarrow \mathcal{G}_m^t(S) \longrightarrow \mathcal{G}_m^t(K) = \mathbb{G}_m(K) = K^*$$

sont bijectives (K corps des fractions de V). A $t^i u \in K^*$ ($u \in V^*$) correspond la section $x_i = u$ de T_i . Cet exemple motive les définitions qui suivent.

d) Abus de notation : pour a inversible sur S et $k \in \mathbb{Z}$, on notera parfois $a\,t^k$ la section de T^k telle que $x_k(at^k) = a$.

1.3. On définit dans $\mathcal{G}_m^t$ une structure de schéma en groupes abéliens

$$: \mathcal{G}_m^t \times \mathcal{G}_m^t \longrightarrow \mathcal{G}_m^t \quad ; \quad T_i \times T_j \longrightarrow T_{i+j}$$

par

$$x_{i+j}(a.b) = x_i(a)x_j(b) \quad .$$

L'intersection $T_i \cap T_{i'}$ de deux cartes distinctes est l'image inverse de $S[1/t]$; au-dessus de $S[1/t]$, $\mathcal{G}_m^t = \mathbb{G}_m$ et les applications précédentes sont la multiplication dans $\mathbb{G}_m$. Dans l'exemple 1.2 c), $\cdot$ correspond à la multiplication dans K^* .

L'application $\cdot$ se prolonge en une action

$$\cdot \quad : \mathcal{G}_m^t \times \overline{\mathcal{G}}_m^t \longrightarrow \overline{\mathcal{G}}_m^t \quad ; \quad T_i \times U_j \longrightarrow U_{i+j}$$

par

$$x_{i+j-\frac{1}{2}}(a.b) = x_i(a).x_{j-\frac{1}{2}}(b)$$

$$y_{i+j+\frac{1}{2}}(a.b) = x_i(a)^{-1} y_{j+\frac{1}{2}}(b)$$

L'application $x \to x^{-1}$ se prolonge en une involution

$a \mapsto a^{-1} : \overline{\mathcal{G}}_m^t \to \overline{\mathcal{G}}_m^t : U_j \to U_{-j}$ par

$$x_{-j-\frac{1}{2}}(a^{-1}) = y_{j+\frac{1}{2}}(a)$$

$$y_{-j+\frac{1}{2}}(a^{-1}) = x_{j-\frac{1}{2}}(a) \quad .$$

La composante neutre T_o du schéma en groupes $\mathcal{G}_m^t$ est canoniquement iso-

morphe à $\mathbb{G}_m$ (isomorphisme : x_o) .

1.4. Si $u \in \Gamma(S,\mathcal{O}_S)^*$, et que $m \geq 1$ est un entier, on définit

$$[u] : \bar{\mathcal{C}}_m^t \longrightarrow \bar{\mathcal{C}}_m^{ut^m} \quad ; \quad U_j^{(t)} \longrightarrow U_{i+\frac{1}{2}}^{(ut^m)} \qquad (mi + \tfrac{1}{2} \leq j \leq m(i+1) - \tfrac{1}{2})$$

$$x_i^{(ut^m)} \circ [u] = x_{mi+k}^{(t)} \cdot t^k.u^{-i}$$

$$(0 \leq k < m) \ .$$

$$y_i^{(ut^m)} \circ [u] = y_{mi-k}^{(t)} \cdot t^k.u^{i}$$

Pour $t = 0$, ceci contracte en un point les T_i avec $i \not\equiv 0(m)$. Si $m = 1$, $[u]$ est un isomorphisme de $\bar{\mathcal{C}}_m^t$ avec $\bar{\mathcal{C}}_m^{ut}$. Par exemple, le modèle de Néron 1.2 c) de $\mathbb{G}_m$ est indépendant du choix de l'uniformisante.

1.5. Supposons t nilpotent. On a alors $U_j \cap U_{j'} = \emptyset$ si $|j-j'| \geq 2$. Soit g une section de $\mathcal{C}_m^t$, contenue dans T_k avec $k \neq 0$. Faisons agir $\mathbb{Z}$ sur $\bar{\mathcal{C}}_m^t$ par

$$(i,x) \mapsto g^i.x \ .$$

Proposition-définition 1.6. Avec les notations 1.5, le quotient $\bar{\mathcal{C}}_m^t / \mathbb{Z}$ existe; on le note $\bar{\mathcal{C}}_m^t / g^{\mathbb{Z}}$.

Si $|k| \geq 2$, $\bar{\mathcal{C}}_m^t / g^{\mathbb{Z}}$ est encore défini par les cartes locales U_j de 1.1, avec la donnée de recollement supplémentaire que U_j est identifié à U_{j+k} par g (les cartes $(U_j)_{0<j<|k|}$ suffisent donc à recouvrir $\mathcal{C}_m^t / g^{\mathbb{Z}}$) . Ceci reste vrai pour $|k| = 1$, à cela près que cette fois U_j n'est plus un ouvert de Zariski de $\bar{\mathcal{C}}_m^t / g^{\mathbb{Z}}$, mais est seulement étale sur $\mathcal{C}_m^t / g^{\mathbb{Z}}$. On peut aussi arguer que

$$\bar{\mathcal{C}}_m^t / g^{\mathbb{Z}} = (\bar{\mathcal{C}}_m^t / g^{2\mathbb{Z}}) / (\mathbb{Z}/2\mathbb{Z}) \ .$$

Exemple 1.7. Si $t = 0$, et que g est la section $x_k = 1$ de T_k , $\mathcal{C}_m^o / g^{\mathbb{Z}}$ n'est autre que le polygone de Néron standard à k côtés sur S . Ceci résulte de 1.2 b).

1.8. Sous les hypothèses de 1.6, la loi $\cdot$ passe au quotient et définit

$$: \mathcal{G}_m^t / g^{\mathbb{Z}} \times \overline{\mathcal{G}}_m^t / g^{\mathbb{Z}} \to \overline{\mathcal{G}}_m^t / g^{\mathbb{Z}} \quad .$$

Pour $t = 0$ et g comme en 1.7, c'est la loi $+$ définie en (II.1.9) . Plus généralement, on déduit de 1.4 que si $x_k(g)$ est une puissance $k^{\text{ième}}$, $(\overline{\mathcal{G}}_t^m / g^{\mathbb{Z}}, \cdot)$ est isomorphe au k-gone standard. Puisque $\overline{\mathcal{G}}_m^t / g^{\mathbb{Z}}$ est clairement plat de présentation finie, on obtient le résultat suivant.

Proposition 1.9. Pour t nilpotent et $g \in T_k(S)$, $(\overline{\mathcal{G}}_m^t / g^{\mathbb{Z}}, +)$ est une courbe elliptique généralisée. Ses fibres géométriques sont des k-gones.

1.10. Soient A un anneau noethérien, $t \in A$ et g une section de $T_k \subset \mathcal{G}_m^t$ sur $S = \mathrm{Spec}(A)$. Pour chaque entier N , t est nilpotent dans $A/(t^N)$ et on peut effectuer la construction 1.6 : on définit

$$C_N = \overline{\mathcal{G}}_m^t / g^{\mathbb{Z}} \text{ sur } A/(t^N) \quad .$$

Les C_N définissent un schéma formel $C = \varinjlim C_N$ sur le complété formel de S le long de $\mathrm{Spec}(A/(t))$. Si A est complet pour la topologie t-adique (ou, comme nous dirons, t-complet), la démonstration de III 1.2 montre que la courbe elliptique généralisée formelle C est algébrisable :

a) La courbe projective formelle $\hat{C}$ est algébrisable, d'après le théorème d'existence de Grothendieck.

b) Si $k = 1$, la loi $+$ est entièrement déterminée par la section neutre e (II 2.7), donc est algébrisable.

c) Dans le cas général, une descente fppf nous ramène à supposer que g est de la forme g_o^k . La courbe $\overline{\mathcal{G}}_m^t / g^{\mathbb{Z}}$ est alors un revêtement de $\overline{\mathcal{G}}_m^t / g_o^{\mathbb{Z}}$, et on applique II 1.17.

Pour A t-complet, nous appellerons la courbe elliptique généralisée sur $\mathrm{Spec}(A)$ qui algébrise $\hat{C}$ une courbe de Tate; nous la noterons encore (par abus de notation) $\overline{\mathcal{G}}_m^t / g^{\mathbb{Z}}$.

Proposition 1.11. L'image du sous-schéma de non lissité de la courbe de Tate $\bar{\mathcal{C}}_m^t / g^{\mathbb{Z}}$ sur Spec(A) admet l'équation $t = 0$.

Cette image est la même pour $\mathcal{C}_m^t / g^{\mathbb{Z}}$, pour le schéma formel $\hat{\mathcal{C}}$ et pour $\bar{\mathcal{C}}_m^t$. Son calcul pour $\bar{\mathcal{C}}_m^t$ est laissé au lecteur.

1.12. Pour t nilpotent, les composantes neutres de $\mathcal{C}_m^t$ et $\mathcal{C}_m^t / g^{\mathbb{Z}}$ sont canoniquement isomorphe à $\mathbb{G}_m$, d'où des isomorphismes et morphismes

$$\text{(complété } \hat{\mathbb{G}}_m \text{ de } \mathbb{G}_m \text{ le long de la section neutre)} \xrightarrow{\sim} (\mathcal{C}_m^t / g^{\mathbb{Z}})\hat{}$$

$$\mathrm{Lie}(\mathbb{G}_m) = \mathcal{O} \xrightarrow{\sim} \mathrm{Lie}(\mathcal{C}_m^t / g^{\mathbb{Z}})$$

$$\mu_n \hookrightarrow (\bar{\mathcal{C}}_m^t / g^{\mathbb{Z}})_n \ .$$

Pour A noethérien t-complet, on en déduit des isomorphismes et morphismes

(1.12.1) (groupe formel complété de $\mathbb{G}_m$ le long de e) $\xrightarrow{\sim}$

(groupe formel complété de $\bar{\mathcal{C}}_m^t / g^{\mathbb{Z}}$ le long de e)

(1.12.2) $\mathrm{Lie}(\bar{\mathcal{C}}_m^t / g^{\mathbb{Z}}) \xrightarrow{\sim} \mathcal{O}$

(1.12.3) $\mu_n \hookrightarrow (\mathcal{C}_m^t / g^{\mathbb{Z}})_n$.

En particulier, les courbes de Tate sont munies d'une différentielle invariante canonique (l'image réciproque dans $\mathrm{Lie}(\bar{\mathcal{C}}_m / g^{\mathbb{Z}})$ de la section unité de $\mathcal{O}$), notée dx/x .

1.13. Si t est nilpotent, nous noterons $(g^{\mathbb{Z}})^{1/k}$ le sous-schéma de $\mathcal{C}_m^t$ dont l'intersection avec la carte T_i est défini par l'équation $a^k = g^i$ (égalité dans $\mathcal{C}_m^t$) . Le schéma en groupes

(1.13.1) $$(g^{\mathbb{Z}})^{1/k} / g^{\mathbb{Z}} = (\bar{\mathcal{C}}_m^t / g^{\mathbb{Z}})_k$$

est fini localement libre de rang k^2 . C'est une extension

(1.13.2) $$0 \longrightarrow \mu_k \xrightarrow{(1.12.3)} (\mathcal{C}_m^t / g^{\mathbb{Z}})_k \longrightarrow \mathbb{Z}/k \longrightarrow 0 \quad ;$$

la projection sur $\mathbb{Z}/k$ envoie x sur la classe mod k des entiers i tels que x soit image d'une section de T_i .

Supposons maintenant A noethérien t-complet. Par passage à la limite, (1.13.1) définit un sous-schéma en groupes fini H de $(\bar{\mathcal{Q}}_m^t / g^{\mathbb{Z}})_k$; ces deux groupes, étant localement libre de même rang, sont égaux, et (1.13.2) définit une suite exacte

$$0 \longrightarrow \mu_k \xrightarrow{(1.12.3)} (\bar{\mathcal{Q}}_m^t / g^{\mathbb{Z}})_k \xrightarrow{v} \mathbb{Z}/k \longrightarrow 0 \quad . \tag{1.13.3}$$

Si $x_k(g) = u$, le μ_k-torseur $v^{-1}(1)$ est canoniquement isomorphe au μ_k-torseur des racines $k^{\text{ièmes}}$ de u :

$$v^{-1}(1) \simeq \{\sqrt[k]{x_k(g)}\} \quad . \tag{1.13.4}$$

Construction 1.14. Si A est t-complet, que $t = \tau^m$, et que g est une section de $T_k \subset \mathcal{Q}_m^t$, notons encore g la section de $T_{km} \subset \mathcal{Q}_m^\tau$ telle que $x_{km}^{(\tau)}(g) = x_k^{(t)}(g)$. La courbe généralisée $\bar{\mathcal{Q}}_m^t / g^{\mathbb{Z}}$ est le contracté (IV.1.) de $\bar{\mathcal{Q}}_m^\tau / g^{\mathbb{Z}}$. En particulier, $\bar{\mathcal{Q}}_m^t / g^{\mathbb{Z}}$ et $\mathcal{Q}_m^\tau / g^{\mathbb{Z}}$ coïncident sur $A[t^{-1}]$.

Par passage au quotient et passage à la limite, l'application 1.4 définit un morphisme

$$\bar{\mathcal{Q}}_m^\tau / g^{\mathbb{Z}} \longrightarrow \bar{\mathcal{Q}}_m^t / g^{\mathbb{Z}} \quad .$$

Ce morphisme identifie $\bar{\mathcal{Q}}_m^t / g^{\mathbb{Z}}$ au contracté (IV.1) de $\bar{\mathcal{Q}}_m^\tau / g^{\mathbb{Z}}$.

Pour A t-complet, et si t admet une racine $m^{\text{ième}}$ τ , on a donc sur $A[t^{-1}]$ une suite exacte (1.13.3), avec k remplacé par km , et un isomorphisme (1.13.4). On vérifie que cette suite exacte et cet isomorphisme sont indépendants du choix de τ . Par descente, ils sont donc définis sans hypothèse sur t .

Construction 1.15. Sur $\mathrm{Spec}(A[t^{-1}]$, on a une suite exacte

$$0 \longrightarrow \mu_k \xrightarrow{(1.12.3)} \left(\bar{\mathcal{Q}}_m^t / g^{\mathbb{Z}}\right)_k \xrightarrow{v} \mathbb{Z}/k \longrightarrow 0 \quad .$$

Le μ_k-torseur $v^{-1}(1)$ est canoniquement isomorphe au μ_k-torseur des racines $k^{\text{ièmes}}$ de $g \in \mathbb{G}_m^t(A[t^{-1}]) \simeq A[t^{-1}]^*$.

Soit $\mathbb{Z}[[q^{1/k}]]$ l'anneau des séries formelles en une indéterminée $q^{1/k}$. Comme convenu en 1.2 d), nous noterons q la section g de $T_k \subset \overline{\mathbb{G}}_m^{q^{1/k}}$ pour laquelle $x_k(g) = 1$.

Définition 1.16. La courbe de Tate à k côtés sur $\mathbb{Z}[[q^{1/k}]]$ est la courbe elliptique généralisée $\mathbb{G}_m^{q^{1/k}} / q^{\mathbb{Z}}$.

Pour $k = 1$, on parle simplement de la courbe de Tate sur $\mathbb{Z}[[q]]$. La courbe de Tate à k côtés C sur $\mathbb{Z}[[q^{1/k}]]$ est munie des structures suivantes ((1.12.1) (1.12.2) (1.12.3) (1.13.2) (1.13.4))

(1.16.1) un isomorphisme de groupes formels $C^{\wedge} \simeq \hat{\mathbb{G}}_m$; en particulier

(1.16.2) une différentielle invariante, notée dx/x ;

(1.16.3) des morphismes $\mu_n \hookrightarrow C_n$;

(1.16.4) un isomorphisme $C_k \xrightarrow{\sim} \mu_k \times \mathbb{Z}/k$.

L'isomorphisme (1.16.4) précise (1.13.2); il est défini par (1.16.3) pour $n = k$, et par la section $q^{1/k}$ de $\overline{\mathbb{G}}_m^{q^{1/k}}$, qui définit une section d'ordre k de $\overline{\mathbb{G}}_m^{q^{1/k}} / q^{\mathbb{Z}}$. Il y a deux façons naturelles de définir les e_k-products $(k \geq 1)$. Pour l'une d'elles on a, via l'isomorphisme (1.16.4.) $e_n((a,b),(c,d)) = a\cdot d - b\cdot c$. C'est celle qu'on avait utilisée dans l'introduction, n° 2 .

2. Application : structure à l'infini de $\mathcal{M}_H$

Théorème 2.1 . Le morphisme $\tau : \mathrm{Spec}(\mathbb{Z}[[q]]) \to \mathcal{M}_1$ défini par la courbe de Tate sur $\mathbb{Z}[[q]]$ identifie $\mathbb{Z}[[q]]$ au complété formel de $\mathcal{M}_1$ le long de la section à l'infini f_1 .

Puisque $\mathcal{M}_1$ est lisse sur $\mathbb{Z}$, on sait à priori qu'il existe un isomorphisme du complété formel de $\mathcal{M}_1$ le long de f_1 avec $\mathrm{Spec}(\mathbb{Z}[[t]])$. Il transforme la section f_1 en la section $t = 0$. Le morphisme τ est de la forme $q \to t = f(q)$,

pour une série formelle f (i.e., $\tau^*(t) = f(q)$) . On sait que l'image, dans $\mathcal{M}_1$, du sous-schéma de non lissité de la courbe universelle, est f_1 (IV 2.2). D'après 1.11, l'image, dans $\mathrm{Spec}(\mathbb{Z}[[q]])$, du sous-schéma de non-lissité de la courbe de Tate, admet l'équation $q = 0$. Puisque la formation de cette image commute au changement de base, on a

$$(q) = (f(q)) \quad \text{dans } \mathbb{Z}[[q]] \ ,$$

et ceci implique que τ est un isomorphisme.

Soit $H \subset GL(2, \mathbb{Z}/n)$.

Corollaire 2.2. Le produit fibré

$$\mathrm{Spec}(\mathbb{Z}[[q]]) \times_{\mathcal{M}_1} \mathcal{M}_H$$

est le spectre du normalisé de $\mathbb{Z}[[q]]$ dans l'algèbre affine du schéma fini étale sur $\mathbb{Z}[[q]][\frac{1}{n}, \frac{1}{q}]$

$$\underline{\mathrm{Isom}}((\mathbb{G}_m^q / q^{\mathbb{Z}})_n \ , \ (\mathbb{Z}/n)^2)/H \quad .$$

Preuve : résulte des définitions et de ce que normalisation et complétion commutent.

Puisque le schéma en groupes $(\mathbb{G}_m^q / q^{\mathbb{Z}})_n$ sur $\mathbb{Z}[[q]][1/q]$ a été calculé en 1.15, 2.2 permet d'expliciter la structure à l'infini de $\mathcal{M}_H$.

2.3. Nous traiterons le cas de $\mathcal{M}_n$ $(n \geq 3)$, considéré comme champ algébrique sur $\mathbb{Z}[\zeta_n]$. Si de $\mathcal{M}_n$ on ôte les points supersinguliers de caractéristique $p|n$, le champ $\mathcal{M}_n^h$ obtenu est un schéma, décrit en termes modulaires en V 4.

Soit C le polygone de Néron à n côtés standard sur $\mathbb{Z}[\zeta_n]$, muni de sa structure de courbe elliptique généralisée (1.9) et de l'isomorphisme naturel

$$C_n = \mu_n \times \mathbb{Z}/n \quad .$$

Cette courbe définit une section à l'infini

(2.3.1) $$f_n : \mathrm{Spec}(\mathbb{Z}[\zeta_n]) \longrightarrow \mathcal{M}_n \quad .$$

Sur $\mathbb{Z}[\zeta_n]\,[[q^{1/n}]]$, considérons la courbe elliptique généralisée

$$C' = \overline{\mathcal{C}}_m^{q^{1/n}} / q^{\mathbb{Z}} \quad .$$

L'application (1.16.3) : $\mu_n \to C'_n$ et la section d'ordre n "$q^{1/n}$" ($x_1 = 1$) définissent un isomorphisme

$$C'_n = \mu_n \times \mathbb{Z}/n \quad .$$

Le morphisme correspondant

$$\text{(2.3.2)} \qquad \mathrm{Spec}(\mathbb{Z}[\zeta_n]\,[[q^{1/n}]]) \longrightarrow \mathcal{M}_n$$

prolonge (2.3.1) et, d'après 1.14, le diagramme

$$\begin{array}{ccc} \mathrm{Spec}(\mathbb{Z}[\zeta_n]\,[[q^{1/n}]] & \longrightarrow & \mathcal{M}_n \\ \downarrow & & \downarrow \\ \mathrm{Spec}(\mathbb{Z}[[q]]) & \longrightarrow & \mathcal{M}_1 \end{array}$$

est commutatif.

Corollaire 2.4. *Le morphisme (2.3.2) identifie $\mathbb{Z}[\zeta_n]\,[[q^{1/n}]]$ au complété formel de $\mathcal{M}_n$ le long de la section à l'infini f_n.*

Preuve: On peut le déduire de 2.2. Il est plus simple de reprendre la démonstration de 2.1, en utilisant que

a) $\mathcal{M}_n$ est lisse sur $\mathbb{Z}[\zeta_n]$ au voisinage de l'infini;

b) L'image sur $\mathrm{Spec}(\mathbb{Z}[\zeta_n]\,[[q^{1/n}]])$ du lieu de non lissité de $\overline{\mathcal{C}}_m^{q^{1/n}}$ est défini par l'équation $q^{1/n} = 0$.

Supposons que $n \geq 3$. Dans ce cas, $\mathcal{M}_n^h$ est un schéma. Le groupe $\mathrm{SL}(2, \mathbb{Z}/n)$ agit sur le $\mathbb{Z}[\zeta_n]$-schéma $\mathcal{M}_n^h = M_n^h$, et le stabilisateur de la section à l'infini f_n est le sous-groupe

$$\pm U = \begin{pmatrix} \pm 1 & * \\ 0 & \pm 1 \end{pmatrix} \quad .$$

Corollaire 2.5. Si $n \geq 3$, le complété de $\mathcal{M}_n$ le long de l'infini est somme d'un ensemble de copies de $\mathrm{Spec}(\mathbb{Z}[\zeta_n][[q^{1/n}]])$, indexées par $SL(2, \mathbb{Z}/n)/\pm U$.

Corollaire 2.6. Soit C une courbe elliptique généralisée sur A local complet. On suppose que C n'est pas lisse; soit (t) l'idéal de A qui définit le sous-schéma de non lissité. On suppose que la fibre spéciale C_s de C à k côtés, et que $\mathrm{Gal}(\bar{s}/s)$ agit trivialement sur le diagramme $\Gamma(C_{\bar{s}})$ des composantes irréductibles de $C_{\bar{s}}$. Alors, il existe $u \in A^*$ tel que

$$C \simeq \mathbb{G}_m^t / (ut^k)^{\mathbb{Z}} \quad .$$

Preuve : Soit X_v le schéma en groupes sur $\mathbb{Z}[v,v^{-1}]$, extension de $\mathbb{Z}/k$ par μ^k,

$$0 \to \mu_k \to X_v \xrightarrow{\varphi} \mathbb{Z}/k \to 0 \quad ,$$

tel que $\varphi^{-1}(1)$ soit le μ_k-torseur des racines $k^{\text{ièmes}}$ de v . Soit $\mathcal{G}_v$ le champ algébrique sur $\mathbb{Z}[v,v^{-1}]$ qui classifie les courbes elliptiques généralisées E sur un $\mathbb{Z}[v,v^{-1}]$-schéma, lisses ou à k côtés, munies d'un isomorphisme $E_k \simeq X_v$. Après extension des scalaires à $\mathbb{Z}[v^{1/k}]$, X_v devient isomorphe à $\mu_k \times \mathbb{Z}/k$, et $\mathcal{G}_v$ à $\mathcal{G}$ de V 4.4. L'application

$$\mathrm{Spec}(\mathbb{Z}[v,v^{-1}][[\tau]]) \longrightarrow \mathcal{G}_v$$

définie par la courbe $\mathbb{G}_m^\tau / (v\tau^k)^{\mathbb{Z}}$ identifie donc $\mathrm{Spec}(\mathbb{Z}[v,v^{-1}][[\tau]])$ au complété formel de $\mathcal{G}_v$ le long d'une section à l'infini.

Sous les hypothèses de 2.6, il existe $v \in A^*$ tel que C_k soit isomorphe à X_v et C_s à $\mathbb{G}_m / (v\tau^k)^{\mathbb{Z}}$ sur k(s) . La courbe C est donc image réciproque de la courbe $\mathbb{G}_m^t / (v\tau^k)^{\mathbb{Z}}$ sur $\mathbb{Z}[v,v^{-1}][[\tau]]$, et 2.6 en résulte.

2.7. Prouvons VI 6.14. Avec les notations de loc.cit., on se ramène à supposer V complet à corps résiduel séparablement clos. Soit C le modèle de Néron de la courbe elliptique E sur le corps des fractions, et appliquons 2.6 à C . On trouve

$$C \simeq \mathbb{G}_m^t / (ut^k)^{\mathbb{Z}}$$

et, puisque C est régulier, t est une uniformisante. D'après 2.1 et VI 1.1, on a

$$j(E)^{-1} = \pm(ut^k) + \sum_{n>0} d_n (ut^k)^n \quad ,$$

et $j(E)$ est donc de valuation $-k$.

3. Application : développement d'une forme modulaire en série de Fourier.

Nous montrerons au § 4 que, après extension des scalaires à $\mathbb{C}$, les notions introduites dans ce paragraphe coïncident avec des notions classiques.

Définition 3.1. L'algèbre des formes modulaires entières est l'algèbre graduée

$$\bigoplus_k H^0(\mathfrak{M}_1, \omega^{\otimes k})$$

En d'autres termes, une forme modulaire entière de poids k est une loi, compatible au changement de base, qui à C/S , une courbe elliptique généralisée irréductible sur un schéma S , associe une section sur S de $\omega^{\otimes k}$.

Définition 3.2. L'algèbre des formes modulaires entières de niveau $H \subset GL(2, \mathbb{Z}/n)$ est l'algèbre graduée

$$\bigoplus_k H^0(\mathfrak{M}_H, \omega^{\otimes k}) \quad .$$

Le lemme suivant, permet, dans certains cas, de ne considérer que les $\mathfrak{M}_n$.

Lemme 3.3. On a $H^0(\mathfrak{M}_H, \omega^{\otimes k}) \xrightarrow{\sim} H^0(\mathfrak{M}_n, \omega^{\otimes k})^H$.

Preuve : Puisque $\mathfrak{M}_H^0[1/n] \simeq [\mathfrak{M}_n^0[1/n] / H]$, (notations comme dans [8], § 4), on a

$$H^0(\mathfrak{M}_H^0[1/n], \omega^{\otimes k}) \simeq H^0(\mathfrak{M}_n^0[1/n], \omega^{\otimes k})^H \quad .$$

On conclut par la normalité de $\mathfrak{M}_H$: pour qu'une section rationnelle de $\omega^{\otimes k}$ sur $\mathfrak{M}_H$ soit partout définie, il suffit que son image réciproque sur le revêtement fini

$\mathfrak{M}_n$ le soit.

Théorème 3.4. L'algèbre des formes modulaires entières de niveau H est une $\mathbb{Z}$ - algèbre de type fini.

Preuve : D'après 3.3, il suffit de traiter le cas de $\mathfrak{M}_n$, n grand. Dans ce cas, $\mathfrak{M}_n = M_n$ est un schéma projectif sur $\mathbb{Z}$, et ω est un faisceau inversible ample sur M_n . Le diviseur de la section Δ de $\omega^{\otimes 12}$ est en effet un multiple de M_n^∞ (sur $\mathfrak{M}_1$, $\mathrm{div}(\Delta) = \mathfrak{M}_1^\infty$) ; il rencontre chaque composante irréductible de chaque fibre de M_n sur $\mathbb{Z}$, donc est ample. Le théorème résulte donc du théorème général EGA III, 2.3.4.1.

3.5. On peut aussi considérer des formes modulaires à coefficients dans des algèbres sur $\mathbb{Z}$. Comme nous ne sommes pas sûr de la définition correcte dans le cas général, nous nous limiterons pour l'essentiel au cas des $\mathfrak{M}_n$, vus comme $\mathbb{Z}[\zeta_n]$-champs.

Définition 3.6. Soit A une algèbre sur $\mathbb{Z}[\zeta_n]$. Une forme modulaire de niveau n et de poids k sur la $\mathbb{Z}[\zeta_n]$-algèbre A est un élément de

$$H^0(\mathfrak{M}_n \otimes_{\mathbb{Z}[\zeta_n]} A,\ \omega^{\otimes k}) \quad .$$

3.7. Soit φ une forme modulaire (cf. 3.6). Evaluons φ sur la courbe de Tate à n côtés

$$\overline{Q}_m^{q^{1/n}} / q^{\mathbb{Z}} \quad \text{sur} \quad A[[q^{1/n}]] \ :$$

la courbe de Tate définit un morphisme (2.1)

$$\tau : \mathrm{Spec}(A[[q^{1/n}]]) \longrightarrow \mathfrak{M}_n \otimes_{\mathbb{Z}[\zeta_n]} A \quad ;$$

l'image inverse de ω par τ est trivialisé (par la section $\frac{dx}{x}$ (1.12.)); on a donc

$$\tau^*\varphi = f_\varphi(q).(\tfrac{dx}{x})^{\otimes k} \quad \text{avec} \quad f_\varphi(q) \in A[[q^{1/n}]] \ .$$

On appelle f_φ le développement en série de Fourier de φ . Puisque la courbe

de Tate à n côtés est définie déjà sur $\mathbb{Z}[[q^{1/n}]] \otimes_{\mathbb{Z}} A$ (le sous-anneau de $A[[q^{1/n}]]$ formé des séries formelles dont les coefficients engendrent un $\mathbb{Z}$-module de type fini) on a

$$f_\varphi(q) \in \mathbb{Z}[[q^{1/n}]] \otimes_{\mathbb{Z}} A \subset A[[q^{1/n}]] \ . \tag{3.7.1}$$

3.8. Soit φ une forme modulaire (cf. 3.6). Pour $g \in SL(2, \mathbb{Z}/n)$, nous noterons $g\varphi$ la forme modulaire qui à une courbe avec structure de niveau n (C,α) sur S associe la section $(g\varphi)(C,\alpha) = \varphi(C,g^{-1}\alpha)$ de $\omega^{\otimes k}$ sur S .

Les $f_{g\varphi}$ sont les <u>développements aux pointes</u> de φ . Si $u = \pm\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, et que $f_\varphi = \Sigma\, c_m\, q^m$ $(m \in \frac{1}{n}\mathbb{Z})$, on a

$$f_{u\varphi} = (-1)^k \Sigma\, c_m\, \zeta_n^{amn}\, q^m \ . \tag{3.8.1}$$

<u>Théorème</u> 3.9. <u>Soit φ une forme modulaire de niveau n et de poids k à coefficients dans la $\mathbb{Z}[\zeta_n]$-algèbre A</u> .

(i) <u>Si les développements aux pointes $f_{g\varphi}$ sont nuls, alors φ est nul</u>.

(ii) <u>Si B est une sous-algèbre de A , et que les $f_{g\varphi}$ sont dans $B[[q^{1/n}]]$, alors φ est à coefficients dans B (provient par extension des scalaires d'une unique forme sur B)</u>.

<u>Preuve</u> : Si A est un $\mathbb{Z}[\zeta_n]$-module, on définit une forme modulaire de niveau n et poids k à coefficients dans A comme un élément de

$$H^0(\mathfrak{M}_n,\ A \otimes_{\mathbb{Z}[\zeta_n]} \omega^{\otimes k}) \ .$$

Pour A une algèbre, cette définition coïncide avec 3.6. Le développement en série de Fourier f_φ d'une telle forme φ se définit comme en 3.7. On a

$$f_\varphi \in A \otimes \mathbb{Z}[[q^{1/n}]] \subset A[[q^{1/n}]] \ .$$

Nous prouverons (i) et (ii) en supposant seulement que A et B soient des modules.

Prouvons (i). Si A est une limite inductive $\varinjlim A_i$, on a

$$H^0(\mathfrak{M}_n, A \otimes \omega^{\otimes k}) = \varinjlim H^0(\mathfrak{M}_n, A_i \otimes \omega^{\otimes k}) .$$

Il suffit donc de traiter le cas où A est un $\mathbb{Z}[\zeta_n]$-module de type fini. Si les $f_{g\varphi}$ sont nuls, (2.4) montre que φ s'annulle sur le complété formel de $\mathfrak{M}_n$ le long de l'infini. Le support de φ, disjoint d'au moins un point de chaque composante irréductible de chaque fibre géométrique de $\mathfrak{M}_n$, est donc fini sur $\mathbb{Z}[\zeta_n]$. Puisque $\mathfrak{M}_n$ est de Cohen-Macaulay sur $\mathbb{Z}[\zeta_n]$ et que $A \otimes \omega^{\otimes k}$ est localement l'image réciproque d'un module sur $\mathbb{Z}[\zeta_n]$, ceci est absurde si $\varphi \neq 0$.

Prouvons (ii). Soit $\mathrm{Spec}(\hat{D})$ la somme des complétés formels de $\mathfrak{M}_n$ le long des sections à l'infini gf_n ($g \in SL(2, \mathbb{Z}/n)$). Les développements aux pointes définissent une application

$$H^0(\mathfrak{M}_n, A \otimes \omega^{\otimes k}) \longrightarrow A \otimes_{\mathbb{Z}[\zeta_n]} \hat{D} .$$

On prouve (ii) en contemplant le diagramme suivant, dont la 2e ligne est exacte car $\hat{D}$ est plat sur $\mathbb{Z}[\zeta_n]$

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^0(\mathfrak{M}_n, B \otimes \omega^{\otimes k}) & \longrightarrow & H^0(\mathfrak{M}_n, A \otimes \omega^{\otimes k}) & \longrightarrow & H^0(\mathfrak{M}_n, A/B \otimes \omega^{\otimes k}) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & B \otimes \hat{D} & \longrightarrow & A \otimes \hat{D} & \longrightarrow & A/B \otimes \hat{D} \end{array}$$

Théorème 3.10. (i) *On a*

$$H^0(\mathfrak{M}_n, \omega^{\otimes k}) \otimes_{\mathbb{Z}[\zeta_n]} \mathbb{Q}(\zeta_n) \xrightarrow{\sim} H^0(\mathfrak{M}_n \otimes \mathbb{Q}, \omega^{\otimes k}) .$$

(ii) *Soient* $\varphi \in H^0(\mathfrak{M}_n \otimes \mathbb{Q}, \omega^{\otimes k})$, $f_\varphi(q) = \Sigma a_i q^i$ ($i \in \frac{1}{n}\mathbb{Z}$, $a_i \in \mathbb{Q}(\zeta_n)$) *le développement de* φ *en série de Fourier, et* π *une place de* $\mathbb{Q}(\zeta_n)$. *Alors,*

$$v_\pi(f_\varphi) \underset{\text{dfn}}{=} \inf(v_\pi(a_i))$$

est l'ordre du zéro (ou - l'ordre du pôle) de φ *au point générique de celle des composantes irréductibles de la fibre de* $\mathfrak{M}_n$ *en* π *qui intersecte la section à l'infini* f_n.

Du point de vue adopté ici, ce théorème est trivial; il résulte de

Corollaire 3.11. Soit $\Sigma a_i q^i$ le développement en série de Fourier de $\varphi \in H^0$ $\varphi \in H^0(\mathbb{m}_n \otimes \mathbb{Q}, \omega^{\otimes k})$. Le dénominateur des a_i est borné.

Corollaire 3.12. Soient π une place de $\mathbb{Q}(\zeta_n)$ de caractéristique p , p^m la plus grande puissance de p qui divise n et g un élément de $SL(2, \mathbb{Z}/n)$ dont l'image dans $SL(2, \mathbb{Z}/p^m)$ est dans le groupe triangulaire supérieur. Alors

$$v_\pi(f_\varphi) = v_\pi(f_{g\varphi}) \quad .$$

Les pointes f_n et gf_n rencontrent en effet la même composante irréductible de caractéristique p .

Corollaire 3.13. Si le développement en une pointe de $\varphi \in H^0(\mathbb{m}_n \otimes \mathbb{Q}, \omega^{\otimes k})$ est à coefficients dans $\mathbb{Z}[\zeta_n][1/n]$, alors le développement aux autres pointes a la même propriété.

3.14. Soit $\varphi \in H^0(\mathbb{m}_n, \omega^{\otimes k})$. Si π est une place de $\mathbb{Q}(\zeta_n)$, de caractéristique p , et que les premiers coefficients du développement de φ en série de Fourier de φ sont divisibles par π , la réduction de φ mod π s'annule un certain nombre de fois au point à l'infini f_n . Notons $\nu(\pi, g, \varphi)$ l'ordre du 0 de $g\varphi$:

$$\text{si} \quad \underset{g\varphi}{f}(g) = \Sigma a_i q^i \qquad (i \in \tfrac{1}{n}\mathbb{Z}) \ ,$$

$$\text{alors} \quad a_i \equiv 0 \quad (\pi) \qquad \text{pour} \quad ni < \nu(\pi, g, \varphi) \ .$$

On peut calculer à l'aide de φ le degré de $\omega^{\otimes k}$ sur $\mathbb{m}_n$. Le résultat est déjà connu (cf. VI 4.4). On obtient, tout calcul fait :

Corollaire 3.14 Soit π une place de $\mathbb{Q}(\zeta_n)$ de caractéristique p , p^m la plus grande puissance de p qui divise n , et $\varphi \in H^0(\mathbb{m}_n, \omega^{\otimes k})$. Pour g parcourant l'ensemble BSL des éléments de $SL(2, \mathbb{Z}/n)$ dont l'image dans $SL(2, \mathbb{Z}/p^m)$ est dans le groupe triangulaire supérieur, on a

$$\frac{1}{|SL(2,\mathbb{Z}/n)|}\sum_{g\in BSL}\nu(\pi,g,\varphi) \leq \frac{1}{|\mathbb{P}^1(\mathbb{Z}/p^m)|}\ \frac{k}{12}\ .$$

Pour $n = 1$, ce résultat se reformule comme suit.

Corollaire 3.15. Soient p un nombre premier et $\varphi \in H^0(\mathfrak{M}_1, \omega^{\otimes k})$ une forme modulaire de développement en série $f_\varphi(q) = \Sigma\, a_n q^n$. On a

$$v_p(f_\varphi) = \inf\{v_p(a_i) \mid i \leq \frac{k}{12}\}\ .$$

En d'autres termes, pour vérifier que les coefficients d'une forme modulaire de poids k sont divisibles par une puissance de p, il suffit de le vérifier pour ceux d'indice $\leq \frac{k}{12}$.

3.16. On peut aussi relier ce qui se passe sur les diverses composantes irréductibles de caractéristique p. A titre d'exemple, nous allons traiter le cas des formes modulaires de niveau $\Gamma_0(p)$. Les mêmes arguments s'appliquent à l'étude, en p, des formes modulaires de niveau $\Gamma_0(p) \cap \Gamma(n)$ (n premier à p). Passer à un tel niveau nous dispenserait de l'usage de nombres d'intersection fractionnaires, introduits sur le modèle de VI 4.

3.17. Soit $\varphi \in H^0(\mathfrak{M}_{\Gamma_0(p)} \otimes \mathbb{Q}, \omega^{\otimes k})$. Une telle forme a deux "développements aux pointes".

a) On évalue φ sur la courbe de Tate

$$\mathbb{G}_m^q/q^{\mathbb{Z}} \quad \text{sur} \quad \mathbb{Z}[[q]] \otimes \mathbb{Q}\ ,$$

munie de son sous-groupe μ_p (1.16.3); on obtient

$${}_1f_\varphi(q).(\frac{dx}{x})^k\ , \text{ avec } {}_1f_\varphi(q) \in \mathbb{Z}[[q]] \otimes \mathbb{Q}$$

b) On évalue φ sur la courbe de Tate

$$\mathbb{G}_m^{q^{1/p}}/q^{\mathbb{Z}} \quad \text{sur} \quad \mathbb{Z}[[q^{1/p}]] \otimes \mathbb{Q}\ ,$$

munie de son sous-groupe isomorphe à $\mathbb{Z}/p$ engendré par q . On obtient

$$ {}_2f_\varphi(q).(\frac{dx}{x})^k \quad , \quad \text{avec} \quad {}_2f_\varphi(q) \in \mathbb{Z}[[q^{1/p}]] \otimes \mathbb{Q} \quad . $$

Pour $\ell \neq p$, les valuations ℓ-adiques de ${}_1f_\varphi$ et ${}_2f_\varphi$ (borne inférieure des valuations ℓ-adiques des coeffients) coincident. Nous noterons $\nu_1(\varphi)$ et $\nu_2(\varphi)$, ou simplement ν_1 et ν_2 les valuations p -adiques de ${}_1f_\varphi$ et ${}_2f_\varphi$.

3.18. Nous étendrons comme suit l'involution w (V.1.3) aux formes modulaires. La forme $w\varphi$ associe à la courbe elliptique C/S , munie d'un sous-groupe $A \subset C_p$, l'image réciproque dans $\omega^{\otimes k}$ de la section $\varphi(C/A, C_p/A)$ de $(\omega_{(C/A)/S})^{\otimes k}$. On a

$$ ww\varphi = p^k\varphi \quad . $$

On vérifie que

$$ {}_1f_{w\varphi}(q) = p^k \, {}_2f_\varphi(q^p) $$

$$ {}_2f_{w\varphi}(q) = {}_1f_\varphi(q^{1/p}) \quad . $$

On a donc

$$ (\nu_1(w\varphi), \nu_2(w\varphi)) = (k+\nu_2(\varphi), \nu_1(\varphi)) \ , $$

et $\nu_2 - \nu_1 + \frac{k}{2}$ change de signe par passage de φ à $w\varphi$.

3.19. Nous nous proposons d'estimer $\nu_1 - \nu_2$. Le nombre ne change pas quand on multiplie φ par un entier; on peut donc supposer que

$$ \varphi \in H^0(\mathfrak{M}_{\Gamma_0(p)} \ , \ \omega^{\otimes k}) \quad . $$

On suppose que φ n'est pas identiquement nul. Si N_1 et N_2 sont les deux composantes irréductibles de $\mathfrak{M}_{\Gamma_0(p)} \otimes \mathbb{F}_p$, correspondant respectivement aux courbes (C,A) avec A infinitésimal et A discret, le diviseur de φ s'écrit

$$ \mathrm{div}(\varphi) = D + \nu_1 N_1 + \nu_2 N_2 \ , $$

où le diviseur D ne rencontre N_1 et N_2 qu'en un nombre fini de points. Sur le champ régulier $\mathfrak{M}_{\Gamma_o(p)}$, $\mathrm{div}(p) = N_1 + N_2$, d'où la nullité des nombres d'intersection

$$(N_1 + N_2, N_1) = (N_1 + N_2, N_2) = 0 \quad .$$

Sur $N_1 \simeq \mathfrak{M}_1 \otimes \mathbb{F}_p$, ω est de degré $\frac{1}{24}$; on a donc

$$(\mathrm{div}(\varphi), N_1) = \frac{k}{24} \quad .$$

De même, puisque sur $\mathfrak{M}_{\Gamma_o(p)}$ ω est de degré $\frac{1}{24} \cdot \left[\mathfrak{M}_{\Gamma_o(p)} : \mathfrak{M}_1\right] = \frac{p+1}{24}$, on a

$$\deg(D) = (D,N_1)+(D,N_2) = \frac{p+1}{24} \cdot k \quad .$$

D'après VI.4.9., $(N_2,N_1) = \frac{p-1}{24}$.

On a

$$(D + \nu_1 \cdot N_1 + \nu_2 \cdot N_2, N_1) = (D,N_1) + \nu_1(N_1+N_2,N_1) + (\nu_2-\nu_1)\cdot(N_2,N_1)$$

$$= \tfrac{1}{2}((D,N_1) + (D,N_2)) + \tfrac{1}{2}((D,N_1) - (D,N_2)) + (\nu_2-\nu_1+\tfrac{k}{2})(N_2,N_1) - \tfrac{k}{2}(N_2,N_1) \quad .$$

Insérant les expressions plus haut, on obtient

$$\tfrac{1}{2}.k.\ \frac{p+1}{24} + \tfrac{1}{2}((D,N_1) - (D,N_2)) + (\nu_2-\nu_1+\frac{k}{2}).\ \frac{p-1}{24} - \frac{k}{2} \cdot \frac{p-1}{24} = \frac{k}{24} \quad .$$

$$(\nu_2-\nu_1+\frac{k}{2})\ \frac{p-1}{24} = \tfrac{1}{2}((D,N_2) - (D,N_1)) \quad .$$

Proposition 3.20. On a

$$\begin{cases} \nu_2-\nu_1+\dfrac{k}{2} = \tfrac{1}{2} \cdot \dfrac{24}{p-1}\ ((D,N_2) - (D,N_1)) \\ (D,N_1) + (D,N_2) = k \cdot \dfrac{p+1}{24} \end{cases}$$

et donc

$$\left|\nu_2-\nu_1+\frac{k}{2}\right| \leq \tfrac{1}{2} \cdot k. \frac{p+1}{p-1} \quad .$$

En particulier, si ${}_1f_\varphi(q)$ est p-entier, alors la valuation p-adique de ${}_1f_{w\varphi}(q)$ est $\geq \frac{-k}{p-1}$.

4. Comparaison avec la théorie transcendante.

4.1. Nous noterons D le disque unité ouvert $\subset \mathbb{C}$, q la coordonnée courante sur D (= l'inclusion $D \hookrightarrow \mathbb{C}$) et D^* le disque épointé $D - \{0\}$.

Nous noterons $D[q^{1/k}]$ la surface de Riemann de $q^{1/k}$: c'est une copie du disque unité, dont la coordonnée courante s'appelle $q^{1/k}$, munie de l'application $u : D[q^{1/k}] \to D$ telle que

$$q \circ u = (q^{1/k})^k \quad .$$

4.2. Une construction identique à la construction 1.1. fournit un espace analytique $\bar{\mathcal{C}}_m^q$ sur D ; la translation par la section q $(x_1 = 1)$ définit une action de $\mathbb{Z}$ sur $\bar{\mathcal{C}}_m^q$; cette action est libre (car $|q| < 1$) . Par passage au quotient, on obtient un espace analytique $\bar{\mathcal{C}}_m^q / q^{\mathbb{Z}}$ sur D , qui est une famille de courbes elliptiques généralisées paramétrée par D (la courbe de Tate).

La fibre du morphisme $\bar{\mathcal{C}}_m^q / q^{\mathbb{Z}} \to D^*$ en le point $q \in D^*$ est la courbe elliptique $\mathbb{C}^*/q^{\mathbb{Z}} \simeq \mathbb{C}/(\mathbb{Z} + \frac{\log q}{2\pi i} \cdot \mathbb{Z})$.

4.3. De même, la courbe de Tate à k côtés sur $D[q^{1/k}]$ est le quotient

$$\bar{\mathcal{C}}_m^{q^{1/k}} / q^{\mathbb{Z}} \quad .$$

4.4. Les constructions 4.2 et 1.15 sont compatibles au sens suivant. On dispose d'un système cohérent d'isomorphismes d'espaces analytiques

$$(\bar{\mathcal{C}}_m^q / q^{\mathbb{Z}} \text{ , analytique, restreint à } \mathrm{Spec}(\mathbb{C}[[q]]/(q^N)) \subset D) \xleftrightarrow{\sim}$$

$$(\bar{\mathcal{C}}_m^q / q^{\mathbb{Z}} \text{ , algébrique}) \otimes_{\mathbb{Z}[[q]]} \mathbb{C}[[q]]/(q^N))^{an} \quad .$$

De même, on dispose d'isomorphismes d'espaces analytiques sur $\mathbb{C}[[q^{1/k}]] / (q^N)$

$$(\bar{\mathcal{Q}}_m^{q^{1/k}} / q^{\mathbb{Z}} \text{ , analytique, restreint à } \mathrm{Spec}(\mathbb{C}[[q^{1/k}]]/(q^N)) \subset D[q^{1/k}]) \longleftrightarrow$$

$$((\bar{\mathcal{Q}}_m^{q^{1/k}} / q^{\mathbb{Z}} \text{ , algébrique}) \otimes_{\mathbb{Z}[[q^{1/k}]]} \mathbb{C}[[q^{1/k}]] / (q^N))^{an} \quad ;$$

ces isomorphismes respectent les structures 1.16 des deux membres.

4.5. Classiquement, une forme modulaire de poids k et de niveau n est une fonction holomorphe f sur le demi-plan de Poincaré $X = \{z \mid \mathrm{Im}(z) > 0\}$ vérifiant les conditions suivantes.

(A) Si $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z})$ est congru à $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod n$,

$$f(z) = (cz + d)^{-k} \; f(\tfrac{az+b}{cz+d}) \quad .$$

Cette condition implique que pour $\gamma \in SL(2, \mathbb{Z}/n)$ image de $\gamma_o = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z})$, la fonction

$$f|\gamma_o : z \to (cz+d)^{-k} \; f(\tfrac{az+b}{cz+d})$$

ne dépend que de γ , non du choix de γ_o . On la note $f|\gamma$.

(B) Pour tout $\gamma \in SL(2, \mathbb{Z}/n)$,

$$(f|\gamma)(z) \quad \text{reste borné pour} \quad \mathrm{Im}(z) \to \infty$$

(il revient au même, et est plus honnête, de demander que $f|\gamma$ soit à croissance polynomiale dans les bandes verticales, pour $\mathrm{Im}(z) \to \infty$) .

Une telle fonction est périodique de période n , donc admet un développement en série de Fourier

$$f(z) = \Sigma \, a_m \, e^{2\pi i m z} \qquad (m \in \tfrac{1}{n}\mathbb{Z} \; , \; m \geq 0) \; .$$

Construction 4.6. Les formes modulaires de poids k et de niveau n s'identifient aux sections de

$$H^0(\mathcal{M}_n \otimes_{\mathbb{Z}[\zeta_n]} \mathbb{C},\ \omega^{\otimes k}) = H^0(\mathcal{M}_n,\ \omega^{\otimes k}) \otimes_{\mathbb{Z}[\zeta]} \mathbb{C} \quad .$$

Preuve : Supposons tout d'abord que $n \geq 3$. Dans ce cas, $\mathcal{M}_n \otimes_{\mathbb{Z}[\zeta]} \mathbb{C} = M_n \otimes_{\mathbb{Z}[\zeta]} \mathbb{C}$ est un schéma. L'espace analytique sous-jacent à $M_n^o \otimes_{\mathbb{Z}[\zeta]} \mathbb{C}$ est $X/\mathrm{Ker}(SL(2, \mathbb{Z}) \to SL(2, \mathbb{Z}/n))$, et les sections holomorphes de $\omega^{\otimes k}$ sur cet espace s'identifient aux fonctions holomorphes sur X vérifiant 4.5 (A). L'espace analytique sous-jacent à $M_n \otimes_{\mathbb{Z}[\zeta_n]} \mathbb{C}$ s'en déduit en ajoutant un nombre fini de points. Une section holomorphe de $\omega^{\otimes k}$ sur $M_n^o \otimes_{\mathbb{Z}[\zeta_n]} \mathbb{C}$ se prolonge à $M_n \otimes_{\mathbb{Z}[\zeta_n)} \mathbb{C}$ si et seulement si elle vérifie (B). D'après GAGA , ces sections sont les sections algébriques de $\omega^{\otimes k}$ sur $M_n \otimes_{\mathbb{Z}[\zeta_n]} \mathbb{C}$.

On ramène le cas où n est quelconque au précédent en passant aux invariants par $\mathrm{Ker}(SL(2, \mathbb{Z}/3n)) \to SL(2, \mathbb{Z}/n))$ dans l'espace des formes modulaires de poids $3n$. On pourrait aussi invoquer GAGA pour le champ algébrique $\mathcal{M}_n \otimes_{\mathbb{Z}[\zeta_n]} \mathbb{C}$.

4.7. Pour $n \geq 3$, $(M_n \otimes_{\mathbb{Z}[\zeta]} \mathbb{C})^{an}$ est aussi l'espace analytique classifiant les courbes elliptiques généralisées C/S sur des espaces analytiques S , munies d'une structure de niveau n , α , telle que $\det(\alpha) = 1$. De ce point de vue, une forme modulaire f est une loi qui, à toute telle courbe, associe une section de $\omega^{\otimes k}$ sur S . Le développement en série de Fourier s'obtient alors en évaluant la forme sur la courbe de Tate (4.3) (et en multipliant le résultat par une puissance de $2\pi i$ dépendant des normalisations choisies). Pour $\varphi \in H^0(M_n \otimes_{\mathbb{Z}[\zeta]} \mathbb{C}\ ,\ \omega^{\otimes k})$, la compatibilité 4.4. montre que ce développement coïncide avec le développement défini de façon purement algébrique au § 3.

4.8. De ce point de vue, les résultats du § 3 fournissent des propriétés arithmétiques des coefficients des développements en série de Fourier aux diverses pointes des fonctions sur X vérifiant 2.5 (A) et (B) . Par exemple

- L'algèbre graduée des formes modulaires de niveau n (2.5) est le produit tensoriel avec $\mathbb{C}$ sur $\mathbb{Z}[\zeta_n]$ de la sous-algèbre de type fini sur $\mathbb{Z}[\zeta_n]$ formée de celles

pour lesquelles les développements en série de Fourier des $f|\gamma$ sont à coefficients dans $\mathbb{Z}[\zeta_n]$.

- Si le développement de f est à coefficients dans $\mathbb{Z}[\zeta_n][1/n]$, celui de $f|\gamma$ a la même propriété.

Bibliographie

[1] M. Artin : The implicit function theorem in algebraic geometry; Proc. Colloq. Alg. Geom.; Bombay, 1968.

[2] M. Artin : Algebraization of formal moduli, in A Collection of Mathematical Papers in Honor of K. Kodaira, University of Tokyo Press 1969.

[3] M. Artin : Construction Techniques for Algebraic Spaces; Actes du Congrès Intern. Math. 1970; Tome 1; pg. 419.

[4] M. Artin, G. Winters : Degenerate Fibres and Stable Reduction of curves; Topology 10 (1971), pg. 373.

[5] W. Casselman : On Abelian Varieties with many Endomorphisms and a Conjecture of Shimura's; Inventiones Math. 12 (1971), pg. 225.

[6] P. Deligne : Formes modulaires et représentations ℓ-adiques; Sém. Bourbaki 355, Février 1969; Springer Lecture Notes 179 (1971).

[7] P. Deligne : Formes modulaires et représentations de GL_2 ; dans ce volume des Proceedings du congrès.

[8] P. Deligne, D. Mumford : The irreducibility of the space of curves of given genus; Publ. Math. IHES, 36 (1969).

[9] M. Deuring : Invarianten und Normalformen elliptischer Funktionenkörper; Math. Z. 47 (1941) pg. 47.

[10] R. Hartshorne : Residues and Duality; Springer Lecture Notes, 20 (1966)

[11] J. Igusa : Fibre systems of Jacobian varieties; Ann. J. Math. 81 (1959), pg. 453.

[12] L. Illusie : Complexe cotangent et déformations I; Springer Lecture Notes, 239 (1971).

[13] N. Katz : P-adic properties of moduli schemes; dans le 2^e volume des Proccedings du congrès.

[14] K. Kodaira : On compact analytic surfaces; in Analytic Functions, Princeton Univ. Press, 1960.

[15] M. Lichtenbaum : Curves over discrete valuation rings; Am. J. Math. 90 (1968), pg. 380.

[16] J. Lipman : Rational Singularities; Publ. Math. IHES, 36 (1969).

[17] D. Mumford : Picard Groups of Moduli Problems; in Arithmetical Algebraic Geometry; Harper & Row, 1965, pg. 33.

[18] D. Mumford : Abelian Varieties; Oxford University Press 1970.

[19] D. Mumford : Geometric invariant theory; Springer, Berlin 1965.

[20] A. Néron : Modèles minimaux des variétés abéliennes sur les corps locaux et globaux, Publ. Math. IHES, 21.

[22] F. Oort, J. Tate : Group schemes of prime order; Ann. Scient. Ec. Norm. Sup. 3 (1970) pg.1.

[23] M. Raynaud : Spécialisation du foncteur de Picard; Comptes Rendus Acad. Sci. 264, pg. 941 et pg. 1001.

[24] M. Raynaud : Modèles de Néron; Comptes Rendus Acad. Sci. 262, pg. 413.

[25] M. Schlessinger : Functors of Artin Rings; Trans. Amer. Soc. 130 (1968) pg. 205.

[26] J.-P. Serre : Rigidité du foncteur de Jacobi d'échelon $n \geq 3$; app. à l'exposé 17 du séminaire Cartan 60/61.

[27] J.-P. Serre : Groupes algébriques et corps de classes; Hermann 1959.

[29] J.-P. Serre, J. Tate : Good reduction of abelian varieties; Ann. of Math. 88 (1968), pg. 492.

[30] G. Shimura : Introduction to the arithmetic theory of automorphic functions; Princeton Univ. Press, 1971.

[31] T. Shioda : On rational points of the generic elliptic curve with level N structure over a field of modular functions of level N ; à paraître.

[32] J. Tate : Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda); Sém. Bourbaki 352 (1968/69); Springer Lecture Notes 179.

[33] J. Tate : Courbes elliptiques : formulaire; mis au goût du jour par P. Deligne; dans un des volumes des Proceedings du congrès.

[34] J.-L. Verdier : Base change for twisted inverse image of coherent sheaves; Proc. Colloq. Alg. Geom., Bombay, 1968.

[35] J. Igusa : On the algebraic theory of elliptic modular functions; J. Math. Soc. Japan 20, 1968, pg. 96.

[36] J. Igusa : Class number of a definite quaternion with prime discriminant, Proc. Nat. Acad. Sci. 44, 1958, pg. 312.

SIGLES :

EGA - Eléments de géométrie algébrique, par A. Grothendieck et J. Dieudonné, Publ. Math. IHES, 4,8,11,17,20,24,28,32.

SGA - Séminaire de géométrie algébrique du Bois-Marie, Notes miméographiées par l'IHES; aussi Springer Lecture Notes, 224,225,269,270,288,305.

TDTE - Techniques de descente et théorèmes d'existence; Exposés de A. Grothendieck au séminaire Bourbaki; Secrétariat mathématique, Paris 1962.

Une grande partie du matériel du présent article est mieux traitée dans le livre:

N. Katz and B. Mazur - Arithmetic moduli of elliptic curves. Annals of Math. Studies 108, Princeton Univ. Press, Princeton. 1985.