Le problème d'uniformité de Serre : le cas des normalisateurs des sous-groupes de Cartan déployés (d'après Y. Bilu, P. Parent et M. Rebolledo)

Richard Griffon
(ENS de Lyon – Université Pierre et Marie Curie)
Sous la direction de Loïc Merel
(Université Paris-Diderot)

– Rapport de Stage –
Master 2 Recherche - Mathématiques Fondamentales
Juillet 2011

TABLE DES MATIÈRES

INTRODUCTION

Soit E une courbe elliptique définie sur $\mathbb{Q}$ et p un nombre premier. L'action de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur les points de p-torsion de E fournit une représentation

$$\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[p]) \simeq \mathbf{GL}_2(\mathbb{Z}/p\mathbb{Z}).$$

Si l'on suppose en outre que E est sans multiplication complexe (CM dans la suite), un théorème de J.-P. Serre ([**Ser71**, Théorème 2, §4.2]) dit que la représentation $\rho_{E,p}$ est surjective pour p suffisamment grand. Bien sûr, ce qu'on entend par « suffisamment grand » dépend a priori de la courbe elliptique E choisie.

J.-P. Serre pose alors la question ([**Ser71**, §4.3]) de savoir si la notion de « suffisamment grand » peut être rendue indépendante de E ; c'est-à-dire :

Question d'uniformité de Serre. — Existe-t-il un nombre entier $P \geqslant 1$ telle que pour tout premier $p > P$ et toute courbe elliptique $E/\mathbb{Q}$ sans CM, la représentation $\rho_{E,p}$ est surjective.

Serre suggère que $P = 19$ serait satisfaisant. Cependant B. Mazur et P. Swinnerton-Dyer ont exhibé une courbe elliptique E définie sur $\mathbb{Q}$ dont la représentation de 37-torsion n'est pas surjective ([**MSD74**]).

La première chose à faire pour répondre à cette question est de comprendre ce à quoi peut ressembler l'image $\mathrm{Im}\,\rho_{E,p}$ si $\rho_{E,p}$ n'est pas surjective. Dans tous les cas, la composée $\det \circ \rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to (\mathbb{Z}/p\mathbb{Z})^\times$ est surjective. D'autre part, $\mathrm{Im}\,\rho_{E,p}$ est contenue dans un sous-groupe maximal de $\mathbf{GL}_2(\mathbb{Z}/p\mathbb{Z})$: ceux-ci sont relativement simples à répertorier (voir [**Ser71**, § 2]). Cinq cas se présentent alors :

(1) $\rho_{E,p}$ est surjective,

(2) l'image de $\rho_{E,p}$ est contenue dans un sous-groupe de Borel, ie. à conjugaison près, le sous-groupe des matrices triangulaires supérieures,

(3) l'image de $\rho_{E,p}$ est contenue dans le normalisateur d'un sous-groupe de Cartan déployé, ie. à conjugaison près, le sous-groupe formé des matrices diagonales et anti-diagonales,

(4) l'image de $\rho_{E,p}$ est contenue dans le normalisateur d'un sous-groupe de Cartan non-déployé, ie. à conjugaison près, le normalisateur de l'image d'un plongement $\mathbb{F}_{p^2}^\times \hookrightarrow \mathbf{GL}_2(\mathbb{Z}/p\mathbb{Z})$,

(5) l'image de $\rho_{E,p}$ est contenue dans un "sous-groupe exceptionnel", ie. un sous-groupe de $\mathbf{GL}_2(\mathbb{Z}/p\mathbb{Z})$ dont l'image dans $\mathbf{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ est isomorphe à $\mathfrak{S}_4$, $\mathfrak{A}_4$ ou $\mathfrak{A}_5$.

Pour répondre affirmativement à la question de Serre, il s'agit donc de montrer que les cas (2) à (5) ne se produisent pas pour p plus grand qu'une constante absolue P. Le cas (5) est facile à écarter : la surjectivité du déterminant montre que l'image de $\rho_{E,p}$ n'est jamais contenue dans l'image inverse de $\mathfrak{A}_4$ ou $\mathfrak{A}_5$, J.-P. Serre ([**Ser71**, § 2.2]) montre que le cas de $\mathfrak{S}_4$ ne se produit pas pour $p > 13$. La situation (2) a été traitée par B. Mazur en 1978 ([**Maz78**]) : si $p > 37$, l'image de $\rho_{E,p}$ ne peut être contenue dans un sous-groupe de Borel. Le cas (4) semble pour l'instant hors de portée.

Dans le cadre de ce programme, nous nous concentrons ici sur l'étude du cas (3). Pour obtenir une borne uniforme sur p (ie. indépendante de E), on construit une courbe projective $X_{split}(p)$ sur $\mathbb{Q}$ qui paramètre les classes d'isomorphisme de courbes elliptiques E sur $\mathbb{Q}$ dont la représentation de p-torsion a une image contenue dans le normalisateur d'un sous-groupe de Cartan déployé de niveau p ([**Maz77b**, §]). On se ramène donc à étudier l'existence ou non de points rationnels (et non CM) sur $X_{split}(p)$.

La première avancée dans cette direction a été faite par B. Mazur ([**Maz77a**, III.§6]) : si $p > 13$, il n'y a qu'un nombre fini de points $\mathbb{Q}$-rationnels sur $X_{split}(p)$. Dans [**Mom84**], F. Momose montre que $X_{split}(p)$ n'a pas de points rationnels pour $p > 37$ tel que la jacobienne de $X_{split}(p)$ vérifie une hypothèse de finitude. Par des techniques différentes, P. Parent ([**Par05**]) et M. Rebolledo ([**Reb08**]) prouvent que l'ensemble des nombres premiers tels que $X_{split}(p)$ n'a que des points rationnels triviaux (ie. des points CM et des pointes) admet une densité positive importante. Dans leur article [**BP09b**], Y. Bilu et P. Parent montrent qu'il existe une constante $P_0 > 0$ telle que $X_{split}(p)(\mathbb{Q})$ est trivial pour tout $p > P_0$. Après une étude plus fine des constantes numériques ([**BPR11**, Sections 1-3]), ils démontrent avec M. Rebolledo que $P_0 = 1,2 \cdot 10^7$ convient. Enfin, un argument de crible sur les nombres

premiers restants ([**BPR11**, Section 4]) leur permet de conclure que $X_{split}(p)(\mathbb{Q})$ n'est composé que de pointes et de points CM pour $p > 13$.

L'objet de ce mémoire est d'exposer en détail l'argument donné par Y. Bilu, P. Parent et M. Rebolledo pour démontrer l'énoncé suivant :

Théorème 0.0.1. — *Soit p un nombre premier plus grand que $1,2 \cdot 10^7$. Un point de $X_{split}(p)(\mathbb{Q})$ est soit une pointe, soit un point CM, si bien que le cas* (3) *est exclu.*

Heuristiquement, la preuve de Y. Bilu et P. Parent consiste à étudier la hauteur des points rationnels de $X_{split}(p)$ en fonction de p. Soit $P \in X_{split}(p)(\mathbb{Q})$: il lui correspond une courbe elliptique E, définie sur $\mathbb{Q}$ et munie d'une structure de sous-groupe de Cartan déployé de niveau p. Par un théorème de B. Mazur, F. Momose et L. Merel ([**Maz78**, Corollary 4.8]), [**Mom84**, Proposition 3.1], [**Mom84**, Corollary 3.6] et [**Mer07**, Theorem 5]), l'invariant j de E est un entier, et la hauteur de E est approximativement la taille de $\log|j(E)|$.

- Le cas de points de « petite » hauteur (par rapport à p) est réglé par le théorème suivant :

  Théorème 0.0.2 **(Proposition 5.2 de [BP09b])**. — *Soit p un nombre premier, et $P \in X_{split}(p)(\mathbb{Q})$ un point non CM. Si $p > 6,3 \cdot 10^6$, on a*

  $$\log|j(P)| \geqslant 12\left(\frac{p}{6,5 \cdot 10^3} - \frac{1}{2}\log p - 3\right).$$

- Il n'y a pas non plus de points de « grande » hauteur par rapport à p pour p grand :

  Théorème 0.0.3 **(Théorème 1.1 de [BP09b])**. — *Soit $p \geqslant 3$ un nombre premier et $P \in Y_{split}(p)(\mathbb{Z})$. On a*

  $$\log|j(P)| \leqslant 2\pi\sqrt{p} + 6\log p + 21\frac{(\log p)^2}{\sqrt{p}}.$$

Pour une bonne définition de ce qu'est une hauteur « petite » ou « grande » par rapport à p, on peut espérer couvrir l'ensemble des courbes elliptiques telle que l'image de la représentation $\rho_{E,p}$ est dans le normalisateur d'un sous-groupe de Cartan déployé de niveau p.

Les quatre premiers chapitres de ce mémoire sont consacrés à des rappels sur les courbes modulaires. Le cinquième chapitre explique la construction des fonctions de Siegel. Les deux derniers chapitres détaillent les preuves des Théorèmes 0.0.3 et 0.0.2 respectivement.

Conventions. — Pour un corps k et un entier $N \geqslant 1$, on notera $\mu_N(k)$ l'ensemble des racines N-ièmes de l'unité dans une clôture algébrique $\overline{k}$ de k, et $k(\mu_N)$ la sous-extension de $\overline{k}$ qu'elles engendrent. Pour $k = \mathbb{Q}$, on fixe une clôture algébrique $\overline{\mathbb{Q}}$ qu'on suppose plongée dans $\mathbb{C}$ de sorte que $\mu_N(\mathbb{Q}) = \mathrm{e}^{2i\pi\mathbb{Z}}$.

CHAPITRE 1

COURBES MODULAIRES SUR $\mathbb{C}$

1.1. Deux rappels sur les courbes elliptiques

Si E est une courbe elliptique sur un corps k quelconque et que N est un entier non nul et premier à la caractéristique de k, on note $E[N]$ le sous-groupe des points de N-torsion non nuls de $E(\overline{k})$. Et on note $k(E[N])$ l'extension engendrée par les coordonnées des points de $E[N]$.

Lemme 1.1.1. — *On suppose que N est premier à la caractéristique de k. Alors, $k(E[N])$ contient une racine primitive N-ième de l'unité. Autrement dit,*

$$k \subset k(\mu_N) \subset k(E[N])$$

Démonstration. — Vu l'hypothèse sur N et la caractéristique de k, on sait que $E[N]$ est un $\mathbb{Z}/N\mathbb{Z}$-module de rang 2 : on peut donc choisir une base (P,Q) de $E[N]$ sur $\mathbb{Z}/N\mathbb{Z}$ et considérer la valeur $e_N(P,Q)$ de l'accouplement de Weil. Comme P et Q sont d'ordre exactement N, on sait même que $e_N(P,Q)$ est une racine primitive N-ième de l'unité ([**DS05**, Corollary 7.4.2]). Par définition, les coordonnées de P et Q sont des éléments de $k(E[N])$, et l'accouplement de Weil $e_N(-,-)$ est défini sur k. Donc $e_N(P,Q) \in k(E[N])$. □

On peut définir une action de $\mathrm{Gal}(\overline{k}/k)$ sur $E(\overline{k})$ en décrétant que celle-ci se fait coordonnée à coordonnée :

$$\forall \sigma \in \mathrm{Gal}(\overline{k}/k),\ \forall P = (x,y) \in E(\overline{k}), \qquad {}^{\sigma}P := (\sigma(x), \sigma(y)).$$

Comme E est définie sur k, ceci définit bien une action sur $E(\overline{k})$. De plus, si P est un point de N-torsion de E, alors ${}^{\sigma}P$ est aussi un point de N-torsion : par conséquent, on peut restreindre l'action ci-dessus à une action sur $E[N]$. On en déduit un morphisme de groupes

$$\mathrm{Gal}(\overline{k}/k) \longrightarrow \mathrm{Aut}(E[N]).$$

L'adjonction des coordonnées des points de N-torsion à k permet de factoriser celui-ci en un morphisme injectif

$$\mathrm{Gal}(k(E[N])/k) \hookrightarrow \mathrm{Aut}(E[N])$$

En effet, le noyau du premier morphisme est égal à $\mathrm{Gal}(\overline{k}/k(E[N]))$ donc : premièrement l'extension $k(E[N])/k$ est galoisienne (car le sous-groupe $\mathrm{Gal}(\overline{k}/k(E[N]))$ est distingué) ; deuxièmement, le morphisme est effectivement injectif.

Enfin, après choix d'une $\mathbb{Z}/N\mathbb{Z}$-base $\mathcal{B}$ de $E[N]$, on obtient par composition un morphisme de groupes

$$\rho_{\mathcal{B}} : \mathrm{Gal}(k(E[N])/k) \hookrightarrow \mathrm{Aut}(E[N]) \xrightarrow{\sim} \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Autrement dit, on obtient une représentation fidèle de dimension 2 de $\mathrm{Gal}(k(E[N])/k)$, appelée *représentation associée à la N-torsion de E*. Cette dernière dépend du choix d'une base de $E[N]$ de la manière suivante : passer d'une base $\mathcal{B}$ à une autre $\mathcal{B}'$ transforme $\rho_{\mathcal{B}}$ en sa conjuguée $A^{-1}\rho_{\mathcal{B}}A$ par la matrice de passage A de $\mathcal{B}$ à $\mathcal{B}'$.

Plus explicitement, si $\mathcal{B} = (P,Q)$ est une telle base, alors l'action de $\mathrm{Gal}(k(E[N])/k)$ sur $E[N]$ est donnée par

$$\forall \sigma \in \mathrm{Gal}(k(E[N])/k), \qquad \begin{pmatrix} {}^{\sigma}P \\ {}^{\sigma}Q \end{pmatrix} = \rho_{\mathcal{B}}(\sigma) \cdot \begin{pmatrix} P \\ Q \end{pmatrix}.$$

On a vu au lemme précédent que $k(E[N])$ contient une racine primitive N-ième de l'unité, donc que l'ensemble μ_N des racines N-ièmes de l'unité est inclus dans $k(E[N])$.

Lemme 1.1.2. — *L'action de $\mathrm{Gal}(k(E[N])/k)$ sur μ_N est donnée par le caractère cyclotomique χ. Plus précisément, pour tout $\zeta \in \mu_N$ et pour tout $\sigma \in \mathrm{Gal}(k(E[N])/k)$, on a*

$$\sigma(\zeta) = \zeta^{\det \rho(\sigma)}.$$

Ou encore $\chi = \det \circ \rho$ (Ceci ne dépend plus du choix d'une base de $E[N]$).

Démonstration. — Soit $\zeta \in \mu_N$ et $\sigma \in \mathrm{Gal}(k(E[N])/k)$, on pose $\rho(\sigma) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ (après choix d'une base de $E[N]$). L'accouplement de Weil étant surjectif, il existe $P, Q \in E[N]$ tels que $e_N(P,Q) = \zeta$. Alors, par Galois-équivariance et bilinéarité de $e_N(-,-)$, on a :

$$\sigma(\zeta) = \sigma\big(e_N(P,Q)\big) = e_N({}^\sigma P, {}^\sigma Q) = e_N(aP + bQ, cP + dQ) = e_N(P,Q)^{ad-bd} = \zeta^{\det \rho(\sigma)}.$$

□

En particulier, si k contient déjà μ_N, alors χ est le caractère trivial, et l'on a

$$\rho_{\mathcal{B}} : \mathrm{Gal}(k(E[N])/k) \hookrightarrow \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

1.2. Rappels rapides sur $\mathbf{SL}_2(\mathbb{Z})$ et ses sous-groupes

On sait que $\mathbf{SL}_2(\mathbb{Z})$ est engendré par

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad \text{et} \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

et que $\mathbf{SL}_2(\mathbb{Z}) = \langle S, T;\ S^2 = 1, (ST)^3 = 1 \rangle$. Soit $N \in \mathbb{N}^*$, on pose

$$\Gamma(N) := \left\{ \gamma \in \mathbf{SL}_2(\mathbb{Z}) \mid \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \right\},$$

$$\Gamma_1(N) := \left\{ \gamma \in \mathbf{SL}_2(\mathbb{Z}) \mid \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N \right\},$$

$$\Gamma_0(N) := \left\{ \gamma \in \mathbf{SL}_2(\mathbb{Z}) \mid \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N \right\}.$$

Plus généralement, on appelle *sous-groupe de congruence* tout sous-groupe Γ de $\mathbf{SL}_2(\mathbb{Z})$ contenant $\Gamma(N)$ pour un certain entier N. Le plus petit entier N tel que $\Gamma(N) \subset \Gamma$ est appelé *niveau de* Γ. Le groupe $\Gamma(N)$ est parfois appelé *sous-groupe de congruence principal de niveau N*.

Proposition 1.2.1. — *Soit $N \in \mathbb{N}^*$.*

- *$\Gamma(N)$ est un sous-groupe distingué de $\Gamma_1(N)$ et $\Gamma_1(N)/\Gamma(N) \simeq \mathbb{Z}/N\mathbb{Z}$,*
- *$\Gamma_1(N)$ est un sous-groupe distingué de $\Gamma_0(N)$ et $\Gamma_0(N)/\Gamma_1(N) \simeq (\mathbb{Z}/N\mathbb{Z})^*$,*
- *$\Gamma(N)$ est un sous-groupe distingué de $\mathbf{SL}_2(\mathbb{Z}) = \Gamma(1)$ et on a*

$$[\mathbf{SL}_2(\mathbb{Z}) : \Gamma(N)] = N^3 \prod_{p \mid N} \left(1 - \frac{1}{p^2}\right)$$

En outre, rappelons que le morphisme de réduction modulo N fournit une suite exacte

$$1 \to \Gamma(N) \to \mathbf{SL}_2(\mathbb{Z}) \to \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z}) \to 1.$$

En effet, on a :

Lemme 1.2.2. — *Pour $N \in \mathbb{N}^*$, la réduction modulo N sur les matrices*

$$\mathbf{SL}_2(\mathbb{Z}) \longrightarrow \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})$$

est surjective.

Démonstration. — Soit $g = \begin{pmatrix} a & b \\ c & 1 \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})$. On commence par relever $a, b, c, d \in \mathbb{Z}/N\mathbb{Z}$ en des entiers, encore notés a, b, c, d. Sachant que $ad - bc \equiv \det g \equiv 1 \mod N$, on fixe $m \in \mathbb{Z}$ tel que

$$ad - bc - mN = 1.$$

On constate alors que c, d et N sont premiers entre eux (dans leur ensemble). A fortiori, il existe $k \in \mathbb{Z}$ tel que c et $d + kN$ soient premiers entre eux. Et l'on peut alors remplacer d par $d + kN$ sans perte de généralité : on suppose donc que c et d sont premiers entre eux.

On écrit alors une relation de Bézout : $ud - vc = -1$ avec $u, v \in \mathbb{Z}^2$. La matrice

$$\gamma = \begin{pmatrix} a - muN & b - mvN \\ c & d \end{pmatrix}$$

est congrue à g modulo N et a pour déterminant

$$\det \gamma = (a - muN)d - c(b - mvN) = ad - bc - mN(ud - vc) = 1 + mN - mN = 1.$$

Donc $\gamma \in \mathbf{SL}_2(\mathbb{Z})$ relève $g \in \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})$! □

En particulier, cela implique que

$$\mathbf{SL}_2(\mathbb{Z})/\Gamma(N) \simeq \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z}),$$

ce qui nous sera souvent utile.

1.3. Rappels rapides sur les fonctions modulaires

On note $\mathfrak{H}$ le demi-plan de Poincaré : il sera toujours muni de son action usuelle de $\mathbf{GL}_2^+(\mathbb{R})$, définie par :

$$\forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{GL}_2^+(\mathbb{R}),\ \forall \tau \in \mathfrak{H}, \qquad \gamma \cdot \tau := \frac{a\tau + b}{c\tau + d}.$$

Pour une fonction $f : \mathfrak{H} \to \mathbb{C}$, on note $f \circ \gamma$ la fonction translatée : $\tau \mapsto f(\gamma \cdot \tau)$.

Définition 1.3.1. — Soit $\Gamma \subset \mathbf{SL}_2(\mathbb{Z})$, un sous-groupe d'indice fini (par exemple, un sous-groupe de congruences). Une fonction $f : \mathfrak{H} \to \mathbb{C}$ est dite *modulaire pour* Γ si c'est une fonction méromorphe sur $\mathfrak{H}$ vérifiant les deux conditions suivantes :

1 – La fonction f est Γ-invariante : $\forall \gamma \in \Gamma$, $f \circ \gamma = f$.

2 – Pour tout $\delta \in \mathbf{SL}_2(\mathbb{Z})$, la fonction $f \circ \delta$ admet un développement de Fourier pour $\operatorname{Im}\tau \to \infty$ de la forme

$$f \circ \delta(\tau) = \sum_{n \geqslant n_0} a_n \mathrm{e}^{2i\pi\tau/M}$$

où $n_0 \in \mathbb{Z}$ et $M \in \mathbb{N}^*$ (ie. f est méromorphe aux pointes).

On note $\mathfrak{M}(\Gamma)$, l'ensemble des fonctions modulaires pour Γ.

Exemple 1.3.2. — Pour $\Gamma = \mathbf{SL}_2(\mathbb{Z})$, on demande que $f \circ \gamma = f$ pour toute matrice $\gamma \in \mathbf{SL}_2(\mathbb{Z})$, et que $f(\tau)$ admette un développement de Fourier pour $q = \mathrm{e}^{2i\pi\tau}$ se rapprochant de 0.

Remarque 1.3.3. — Plusieurs commentaires sur cette définition :

- On peut reformuler ainsi la seconde condition : soit $\delta \in \mathbf{SL}_2(\mathbb{Z})$, étant donné que Γ est d'indice fini dans $\mathbf{SL}_2(\mathbb{Z})$, une des puissances de $\delta \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \delta^{-1}$ est dans Γ : on fixe $M \in \mathbb{N}^*$ une telle puissance. Dès lors, on peut considérer la fonction $F(\mathrm{e}^{2i\pi\tau/M}) := f(\delta \cdot \tau)$ définie sur le disque unité pointé $D^\circ = \{q \in \mathbb{C} \mid 0 < |q| < 1\}$. Par hypothèse, F est méromorphe sur D° : la deuxième condition demande en sus que F se prolonge en une fonction méromorphe sur le disque unité entier $D = \{q \in \mathbb{C} \mid |q| < 1\}$. Et ce, pour tout $\delta \in \mathbf{SL}_2(\mathbb{Z})$.

  De manière plus imagée (cette image deviendra plus précise dans la suite), on exige que f soit "méromorphe aux pointes".
- L'addition et la multiplication des fonctions font de $\mathfrak{M}(\Gamma)$ un corps commutatif. Remarquons que si $\Gamma \subset \Gamma'$ sont deux sous-groupes d'indice fini de $\mathbf{SL}_2(\mathbb{Z})$, alors $\mathfrak{M}(\Gamma') \subset \mathfrak{M}(\Gamma)$ et l'extension de corps ainsi formée est finie.

On peut tout de suite donner la propriété suivante :

Théorème 1.3.4. — *L'extension $\mathfrak{M}(\Gamma(N))/\mathfrak{M}(\Gamma(1))$ est galoisienne, de groupe de Galois*

$$\operatorname{Gal}\left(\mathfrak{M}(\Gamma(N))/\mathfrak{M}(\Gamma(1))\right) \simeq \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}.$$

Démonstration. — Le groupe $\mathbf{SL}_2(\mathbb{Z})$ agit sur $\mathfrak{M}(\Gamma(N))$ par « composition » à droite :

$$\forall \gamma \in \mathbf{SL}_2(\mathbb{Z}), \quad f \mapsto f|_\gamma\ .$$

Cette action se factorise à travers $\mathbf{SL}_2(\mathbb{Z})/\pm\Gamma(N) \simeq \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$, car $-1 \in \mathbf{SL}_2(\mathbb{Z})$ agit trivialement sur $\mathfrak{H}$ et que, par définition de $\mathfrak{M}(\Gamma(N))$, les éléments de $\Gamma(N)$ agissent trivialement. Autrement dit, on a un morphisme

$$\mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\} \longrightarrow \operatorname{Aut}(\mathfrak{M}(\Gamma(N))).$$

Le sous-corps de $\mathfrak{M}(\Gamma(N))$ fixé par $\mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ est exactement $\mathfrak{M}(\Gamma(1))$, par définition des fonctions modulaires pour $\Gamma(1)$. On en conclut que l'extension $\mathfrak{M}(\Gamma(N))/\mathfrak{M}(\Gamma(1))$ est galoisienne, de groupe de Galois isomorphe à $\mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$. □

1.4. Quotients de $\mathfrak{H}$ et de $\mathfrak{H}^*$

On note $\mathfrak{H}$ le demi-plan supérieur de Poincaré, et on définit le *demi-plan supérieur complété* par

$$\mathfrak{H}^* := \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q}) = \mathfrak{H} \cup \mathbb{Q} \cup \{\infty\}.$$

L'action de $\mathbf{SL}_2(\mathbb{Z})$ sur $\mathfrak{H}$ est l'action usuelle par homographies, et on a une action naturelle de $\mathbf{SL}_2(\mathbb{Z})$ sur $\mathbb{P}^1(\mathbb{Q})$:

$$\forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}),\ \forall\ \frac{u}{v} \in \mathbb{P}^1(\mathbb{Q}), \qquad \gamma \cdot \frac{u}{v} := \frac{au+bv}{cu+dv}.$$

où, par convention, $u/0 = \infty$. Ainsi, l'action de $\mathbf{SL}_2(\mathbb{Z})$ sur $\mathfrak{H}$ s'étend en une action sur $\mathfrak{H}^*$.

Remarque 1.4.1. — L'action de $\mathbf{SL}_2(\mathbb{Z})$ sur $\mathbb{P}^1(\mathbb{Q})$ est transitive. Etant donné un sous-groupe Γ d'indice fini de $\mathbf{SL}_2(\mathbb{Z})$, le quotient $\Gamma\backslash\mathbb{P}^1(\mathbb{Q})$ est donc fini. Cet ensemble est appelé *ensemble des pointes de* Γ.

Si maintenant Γ est un sous-groupe d'indice fini de $\mathbf{SL}_2(\mathbb{Z})$, on peut considérer le quotient de $\mathfrak{H}^*$ par cette action, et noter

$$Y(\Gamma) := \Gamma\backslash\mathfrak{H} \qquad \text{et} \qquad X(\Gamma) := \Gamma\backslash\mathfrak{H}^*.$$

1.4.1. Topologie et structure de surface de Riemann. — Commençons par définir une topologie sur $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$.

Définition 1.4.2. — La base d'ouverts de $\mathfrak{H}^*$ choisie est l'ensemble contenant

- les ouverts usuels de $\mathfrak{H}$ (pour la topologie induite par celle de $\mathbb{C}$),
- les ensembles de la forme :
$$\gamma(\{\tau \in \mathfrak{H} \mid \operatorname{Im}\tau > C\}) \cup \{\infty\}$$
pour tous $\gamma \in \mathbf{SL}_2(\mathbb{Z})$ et $C \in \mathbb{R}_+$. Ce sont les "voisinages de $i\infty$" ainsi que leurs translatés.

La projection $\pi : \mathfrak{H}^* \to X(\Gamma)\Gamma\backslash\mathfrak{H}^*$ munit $X(\Gamma)$ de la topologie quotient et en fait un espace topologique connexe et compact (et donc séparé) (voir [**DS05**, Chapters 1 & 2] pour plus de détails).

Pour définir une structure complexe sur $X(\Gamma)$, on va construire un faisceau de fonctions holomorphes de la manière suivante : partons du faisceau $\mathcal{F}$ des fonctions continues sur $X(\Gamma)$, et définissons un sous-faisceau $\mathcal{O}$ de $\mathcal{F}$ en spécifiant les tiges $\mathcal{O}_x \subset \mathcal{F}_x$ pour tout $x \in X(\Gamma)$. On voit ici $\mathcal{F}_x$ comme l'ensemble des classes d'équivalence (f, V) où V est un voisinage ouvert de x et $f \in \mathcal{F}(V)$ pour la relation

$$(f,V) \sim (g,W) \iff \exists U \subset V \cap W,\ x \in U \text{ et } f|_U \equiv g|_U\ .$$

Définition 1.4.3. — Soit $x \in X(\Gamma)$ et $(f,V) \in \mathcal{F}_x$. Alors $(f,V) \in \mathcal{O}_x$ si et seulement si (f,V) vérifie l'une ou l'autre des conditions suivantes :

- Il existe $\tau \in \mathfrak{H}$ et un voisinage ouvert U de τ dans $\mathfrak{H}$ tels que $x = \pi(\tau) = \Gamma \cdot \tau$, $V = \pi(U)$ et $f \circ \pi$ est holomorphe sur U,
- Il existe $c \in \mathbb{P}^1(\mathbb{Q})$ et $C > 0$ pour lesquels on fixe $\delta \in \mathbf{SL}_2(\mathbb{Z})$ et $M \in \mathbb{N}^*$ vérifiant $c = \delta(\infty)$ et
$$(f \circ \pi \circ \delta)(\tau + M) = (f \circ \pi \circ \delta)(\tau)$$
(un tel entier M existe toujours car Γ est d'indice fini dans $\mathbf{SL}_2(\mathbb{Z})$ et π est invariante par Γ).
Avec ces notations, on pose $r = \mathrm{e}^{-2\pi C/M}$ et $D^\circ(r) = \{q \in \mathbb{C} \mid 0 < |q| < r\}$ ainsi que $F : D^\circ(r) \to \mathbb{C}$, la fonction définie par $F(\mathrm{e}^{2i\pi z/M}) = (f \circ \pi \circ \delta)(z)$.
Alors, F est holomorphe sur $D^\circ(r)$ et s'étend en une fonction holomorphe $\widetilde{F}$ sur le disque entier $D(r) = \{q \in \mathbb{C} \mid |q| < r\}$.

On vérifie alors qu'avec ces définitions, chaque point $x \in X(\Gamma)$ a un voisinage ouvert V tel que l'espace localement annelé $(V, \mathcal{O}|_V)$ est isomorphe à un espace localement annelé $(D, \mathcal{O}_{\mathbb{C}}|_D)$ où D est un disque ouvert de $(\mathbb{C}, \mathcal{O}_{\mathbb{C}})$. Les vérifications sont assez longues : voir [**DS05**, Chapter 2] pour les détails.

Le point important est que l'on a choisi les définitions de sorte que l'application

$$f \mapsto (f \circ \pi)|_{\mathfrak{H}}$$

identifie le corps $\mathbb{C}(X(\Gamma))$ des fonctions méromorphes sur $X(\Gamma)$ avec le corps $\mathfrak{M}(\Gamma)$ des fonctions modulaires pour Γ que l'on a défini à la section précédente.

Remarque 1.4.4. — Les objets $X(\Gamma)$ et $\mathfrak{M}(\Gamma)$ ne dépendent que de l'image de Γ dans $\mathbf{SL}_2(\mathbb{Z})/\{\pm 1\}$.

Remarque 1.4.5. — Si Γ et Γ' sont deux groupes d'indice fini de $\mathbf{SL}_2(\mathbb{Z})$ tels qu'il existe $\gamma \in \mathbf{GL}_2^+(\mathbb{Z})$ vérifiant $\Gamma \subset \gamma\Gamma'\gamma^{-1}$, alors la fonction holomorphe $\tau \in \mathfrak{H} \mapsto \gamma\cdot\tau \in \mathfrak{H}$ s'étend en une fonction holomorphe $\mathfrak{H}^* \to \mathfrak{H}^*$ et induit une application holomorphe

$$X(\Gamma) \to X(\Gamma').$$

1.5. Pointes

1.5.1. Pointes de $X(N)$. — Soit $\widetilde{\mathcal{P}} = \left\{ \left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right),\ (u,v) \in \mathbb{Z}^2 \text{ et } \gcd(u,v) = 1 \right\}$. On définit une relation d'équivalence sur $\widetilde{\mathcal{P}}$ de la manière suivante :

$$\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right) \sim \left(\begin{smallmatrix} u' \\ v' \end{smallmatrix}\right) \iff \left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right) \equiv \pm \left(\begin{smallmatrix} u' \\ v' \end{smallmatrix}\right) \bmod N.$$

On note alors $\mathcal{P} = \widetilde{\mathcal{P}}/\sim$ l'ensemble quotient.

Proposition 1.5.1. — *Il y a une bijection entre $\mathcal{P}$ et les pointes de $X(N)$, donnée par*

$$\overline{\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)} \in \mathcal{P} \mapsto \Gamma(N)\cdot\frac{u}{v} \in \Gamma(N)\backslash\mathbb{P}^1(\mathbb{Q}),$$

avec la convention que $\frac{u}{0} = \infty \in \mathbb{P}^1(\mathbb{Q})$.

Démonstration. — Commençons par démontrer que l'application f donnée dans l'énoncé est bien définie : si $\overline{\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)} = \overline{\left(\begin{smallmatrix} u' \\ v' \end{smallmatrix}\right)} \in \mathcal{P}$, alors il existe $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \in \mathbb{Z}^2$ tel que

$$\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right) = \pm \left(\begin{smallmatrix} u' \\ v' \end{smallmatrix}\right) + N \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right).$$

Comme u et v sont premiers entre eux, on peut fixer une relation de Bézout entre eux : $ku + \ell v = 1$. On pose alors $\gamma' = \left(\begin{smallmatrix} 1\pm Nkx & \pm N\ell x \\ \pm Nky & 1\pm N\ell y \end{smallmatrix}\right)$. Clairement $\gamma' \bmod N = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, et l'on peut choisir un relevé γ de γ mod N tel que $\gamma \in \mathbf{SL}_2(\mathbb{Z})$ (car la réduction modulo N est surjective, cf. Lemme 1.2.2). De par l'expression de sa réduction modulo N, on a $\gamma \in \Gamma(N)$, et

$$\gamma\cdot\frac{u}{v} = \frac{(1\pm Nkx)u \pm N\ell xv}{\pm Nkyu + (1\pm N\ell y)v} = \frac{u \pm Nx}{u \pm Ny} = I\cdot f\left(\begin{smallmatrix} u' \\ v' \end{smallmatrix}\right).$$

Donc $f\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right) = f\left(\begin{smallmatrix} u' \\ v' \end{smallmatrix}\right)$. Montrons maintenant la bijectivité de f :

- Si il existe $\gamma = \left(\begin{smallmatrix} 1+Na & Nb \\ Nc & 1+Nd \end{smallmatrix}\right) \in \Gamma(N)$ tel que $\gamma\cdot\frac{u}{v} = \frac{u'}{v'}$, on a

$$\frac{(1+Na)u + Nbv}{Ncu + (1+Nb)v} = \frac{u + N(au+bv)}{v + N(cu+dv)} = \frac{u'}{v'}.$$

  Donc $\left(\begin{smallmatrix} u' \\ v' \end{smallmatrix}\right) = \left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right) + N\left(\begin{smallmatrix} au+bv \\ cu+dv \end{smallmatrix}\right)$ et $\overline{\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)} = \overline{\left(\begin{smallmatrix} u' \\ v' \end{smallmatrix}\right)} \in \mathcal{P}$.
- Enfin, si $\Gamma(N)\cdot\frac{u}{v} \in \mathbb{P}^1(\mathbb{Q})$, on peut supposer que u et v sont des entiers premiers entre eux, et on a

$$\Gamma(N)\cdot\frac{u}{v} = f\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right).$$

□

1.5.2. Pointes de $X(\Gamma)$. — Soit maintenant Γ un sous-groupe de congruences de $\mathbf{SL}_2(\mathbb{Z})$ de niveau N. On pose $G = \pm\Gamma/\pm\Gamma(N)$, qui est un sous-groupe de $\mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$. Le groupe G agit à gauche sur $\mathcal{P}$ via

$$\forall \overline{g} \in G, \forall \overline{\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)} \in \mathcal{P}, \qquad \overline{g} : \overline{\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)} \mapsto \overline{g\cdot\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)}$$

où g désigne un relevé de $\overline{g}$ à $\pm\Gamma$, et $\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)$ un relevé de $\overline{\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)}$ à $\widetilde{\mathcal{P}}$. Il est immédiat que l'action de G sur $\mathcal{P}$ est libre (ie. un élément $p \in \mathcal{P}$ n'est fixé que par l'identité de G)

Proposition 1.5.2. — *Avec ces notations, il y a une bijection entre $G\backslash\mathcal{P}$ et l'ensemble des pointes de $X(\Gamma)$, donnée par*

$$f' : G\cdot\overline{\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)} \in G\backslash\mathcal{P} \mapsto \Gamma\cdot\frac{u}{v} \in \Gamma\backslash\mathbb{P}^1(\mathbb{Q}).$$

Démonstration. — L'inclusion $\Gamma(N) \hookrightarrow \Gamma$ fournit une surjection de l'ensemble des pointes de $X(N)$ sur l'ensemble des pointes de $X(\Gamma)$, et on a un diagramme commutatif

$$\begin{array}{ccc} \Gamma(N)\cdot\dfrac{u}{v} & \longmapsto & \Gamma\cdot\dfrac{u}{v} \\ \uparrow f & & \uparrow f' \\ \overline{\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)} & \longmapsto & G\cdot\overline{\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)}. \end{array}$$

L'application f' est bien définie, on fait le même raisonnement que dans la preuve précédente, en remarquant que $\pm\Gamma/\pm\Gamma(N) = G$. L'injectivité et la surjectivité de f' se montrent comme précédemment, en se servant en outre du diagramme commutatif. □

Si $\overline{\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)} \in \mathcal{P}$ est une pointe de $X(\Gamma)$ (on note $\overline{\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)}$ un représentant de la pointe $G \cdot \overline{\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)}$), il existe une matrice $M \in \mathbf{SL}_2(\mathbb{Z})$ telle que

$$M \cdot \overline{\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)} = \overline{\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)} = \infty.$$

Comme Γ est d'indice fini dans $\mathbf{SL}_2(\mathbb{Z})$, il existe un entier $n \in \mathbb{N}^*$ minimal tel que

$$M \cdot \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) \cdot M^{-1} \in \Gamma.$$

Cet entier est appelé *largeur* de la pointe $M^{-1} \cdot \infty = \overline{\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)}$. Par exemple, la largeur de la pointe ∞ de $X(N)$ est $1/N$. Par définition de la structure de surface de Riemann de $X(N)$, en une pointe $\Gamma(N) \cdot x$ (où $x \in \mathbb{P}^1(\mathbb{Q})$) de largeur h, un paramètre local de $X(N)$ est $q^{1/h}$ (où $q = \mathrm{e}^{2i\pi\tau}$).

1.5.3. Le cas de $\Gamma_{split}(p)$. — Soit p un nombre premier et $G_{split} = \{\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right)\} \cup \{\left(\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right)\}$, le sous-groupe de $\mathbf{SL}_2(\mathbb{Z}/p\mathbb{Z})$ formé des matrices diagonales et antidiagonales. On note $\Gamma_{split}(p)$ le relevé de $G \subset \mathbf{SL}_2(\mathbb{Z}/p\mathbb{Z})$ à $\mathbf{SL}_2(\mathbb{Z})$. On pose aussi $G = G_{split}/\{\pm I\} \simeq \pm\Gamma_{split}(p)/\pm\Gamma(p)$. On a $\#G = p-1$ car $\#G_{split} = 2(p-1)$.

Proposition 1.5.3. — *Un ensemble de représentants de $G\backslash\mathcal{P}$ est donné par*

$$\left\{\overline{\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)},\ \overline{\left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)},\ \overline{\left(\begin{smallmatrix} 1 \\ 2 \end{smallmatrix}\right)},\ \ldots,\ \overline{\left(\begin{smallmatrix} 1 \\ \frac{p-1}{2} \end{smallmatrix}\right)}\right\}.$$

Démonstration. — Soit $\mathcal{S}$ l'ensemble défini dans l'énoncé de la proposition, on a $\#\mathcal{S} = \frac{p+1}{2}$. On peut définir une application $\mathcal{S} \to G\backslash\mathcal{P}$ par $\overline{\left(\begin{smallmatrix} 1 \\ i \end{smallmatrix}\right)} \mapsto G \cdot \overline{\left(\begin{smallmatrix} 1 \\ i \end{smallmatrix}\right)}$ pour $i = 0 \ldots \frac{p-1}{2}$. Montrons que cette application est injective : supposons que $G \cdot \overline{\left(\begin{smallmatrix} 1 \\ i \end{smallmatrix}\right)} = G \cdot \overline{\left(\begin{smallmatrix} 1 \\ j \end{smallmatrix}\right)}$. Fixons $g \in G_{split}$ tel que $\overline{g \cdot \left(\begin{smallmatrix} 1 \\ i \end{smallmatrix}\right)} = \overline{\left(\begin{smallmatrix} 1 \\ j \end{smallmatrix}\right)}$. Deux cas se présentent alors :

- Ou bien g est de la forme $g = \left(\begin{smallmatrix} x & 0 \\ 0 & x^{-1} \end{smallmatrix}\right)$ (avec $x \in (\mathbb{Z}/p\mathbb{Z})^\times$) et on a :

  $$\overline{g \cdot \left(\begin{smallmatrix} 1 \\ i \end{smallmatrix}\right)} = \overline{\left(\begin{smallmatrix} x \\ x^{-1} i \end{smallmatrix}\right)}.$$

  Si bien que $\left(\begin{smallmatrix} 1 \\ j \end{smallmatrix}\right) = \pm \left(\begin{smallmatrix} x \\ x^{-1} i \end{smallmatrix}\right)$. Ceci implique que $x = \pm 1$ et que $i = j$.
- Ou bien g s'écrit $g = \left(\begin{smallmatrix} 0 & -y \\ y^{-1} & 0 \end{smallmatrix}\right)$ (où $y \in (\mathbb{Z}/p\mathbb{Z})^\times$) et on a :

  $$\overline{g \cdot \left(\begin{smallmatrix} 1 \\ i \end{smallmatrix}\right)} = \overline{\left(\begin{smallmatrix} -yi \\ y^{-1} \end{smallmatrix}\right)}.$$

  Si bien que $\left(\begin{smallmatrix} 1 \\ j \end{smallmatrix}\right) = \pm \left(\begin{smallmatrix} -yi \\ y^{-1} \end{smallmatrix}\right)$. Cette relation entraîne que $i = -j$. Puisque i et j sont dans l'intervalle $[\![0, \frac{p-1}{2}]\!]$, ceci n'est possible que si $i = j = 0$.

Donc l'application est bien injective. Or, $\mathcal{P}$ est de cardinal $(p^2-1)/2$ et G agit librement sur $\mathcal{P}$. La formule des classes donne alors

$$\#(G\backslash\mathcal{P}) = \frac{\#\mathcal{P}}{\#G} = \frac{p^2-1}{2(p-1)} = \frac{p+1}{2} = \#\mathcal{S}.$$

Donc l'injection définie plus haut est une bijection ! □

Proposition 1.5.4. — *Un ensemble de représentants des pointes de $X_{split}(p) = \Gamma_{split}(p)\backslash\mathfrak{H}^*$ est donné par*

$$\left\{{\beta_0}^{-1} \cdot \infty,\ {\beta_1}^{-1} \cdot \infty, \ldots,\ {\beta_{\frac{p-1}{2}}}^{-1} \cdot \infty\right\}, \qquad \text{où } \beta_c = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}).$$

Les pointes de $X_{split}(p)$ sont donc toutes de largeur p, sauf la pointe ∞ qui est de largeur 1.

Démonstration. — L'assertion sur les largeurs est immédiate une fois que l'on a montré que les $\beta_i^{-1}\infty$ fournissent un système de représentants des pointes de $X_{split}(p)$.

D'après la proposition précédente et la bijection de la Proposition 1.5.2, les pointes de $X_{split}(p)$ sont

$$\Gamma_{split}(p) \cdot \infty,\ \Gamma_{split}(p) \cdot \tfrac{1}{1},\ \Gamma_{split}(p) \cdot \tfrac{1}{2},\ \ldots,\ \Gamma_{split}(p) \cdot \tfrac{2}{p-1}.$$

Soit $i \in [\![0, \frac{p-1}{2}]\!]$, on pose c un relevé à $[\![0, \frac{p-1}{2}]\!]$ de $-i \bmod p \in \mathbb{Z}/p\mathbb{Z}$. Alors, on a

$$\beta_c \cdot \frac{1}{i} = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \cdot \frac{1}{i} = \frac{1}{c+i} = \infty.$$

□

1.6. Structures sur des courbes elliptiques, espaces de modules

Dans cette section, on fixe un entier $N \in \mathbb{N}^*$ et on se place sur un corps k quelconque de caractéristique p ne divisant pas N (p peut être nul).

1.6.1. Structures de niveau N. —

Définition 1.6.1. — Soit E une courbe elliptique sur k. Une *N-structure sur E* est la donnée d'une base $\mathcal{B} = (P_1, P_2)$ de $E[N]$. L'ensemble des N-structures sur E est noté $\mathscr{B}(E, N)$. À une N-structure $\mathcal{B}$, on peut associer le nombre

$$d(\mathcal{B}) := e_N(P_1, P_2)$$

où e_N désigne l'accouplement de Weil sur $E[N]$. Par les propriétés usuelles de $e_N(-,-)$, $d(\mathcal{B})$ est une racine primitive N-ième de l'unité de k (voir [**Sil09**, Proposition III.8.1]).

Soit ζ_N une racine primitive N-ième de l'unité de k. Une N-structure $\mathcal{B} \in \mathscr{B}(E, N)$ est une ζ_N- *structure* si $d(\mathcal{B}) = \zeta_N$. Leur ensemble est noté $\mathscr{B}(E, \zeta_N)$.

Remarque 1.6.2. — Toute courbe elliptique admet une N-structure $\mathcal{B}_0$: il suffit de prendre une $\mathbb{Z}/N\mathbb{Z}$-base de $E[N]$. Mieux encore, comme l'accouplement de Weil est surjectif ([**Sil09**, Corollary VI.8.1.1]), pour toute racine N-ième de l'unité, il existe N-structure $\mathcal{B}$ sur E telle que $d(\mathcal{B}) = \zeta_N$. Ce qui montre que toute courbe elliptique admet une ζ_N-structure.

On a une action à gauche naturelle de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$ sur $\mathscr{B}(E, N)$:

$$\forall \gamma \in \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z}), \forall \mathcal{B} = (P_1, P_2) \in \mathscr{B}(E, N), \qquad \gamma \star \mathcal{B} := \gamma \cdot \left(\begin{smallmatrix} P_1 \\ P_2 \end{smallmatrix}\right).$$

Par bilinéarité de l'accouplement de Weil, on peut calculer l'action de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$ sur $d(\mathcal{B})$:

$$\forall \gamma \in \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z}), \forall \mathcal{B} \in \mathscr{B}(E, N), \qquad d(\gamma \star \mathcal{B}) = d(\mathcal{B})^{\det \gamma}.$$

Si bien que l'action de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$ sur $\mathscr{B}(E, N)$ induit (par restriction) une action à gauche de $\mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})$ sur $\mathscr{B}(E, \zeta_N)$.

Définition 1.6.3. — Soit E une courbe elliptique sur k et G, un sous groupe de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Une *$G$-structure sur E* est une orbite de N-structures sur E. Leur ensemble est notée $\mathscr{B}(E, G)$. On a donc

$$\mathscr{B}(E, G) = G\backslash\mathscr{B}(E, N).$$

On notera $\mathscr{B}(E, G, \zeta_N)$, l'ensemble des G-structures sur E qui contiennent au moins une ζ_N-structure.

Remarque 1.6.4. — Si le déterminant $\det : G \to (\mathbb{Z}/N\mathbb{Z})^*$ est surjectif, alors $\mathscr{B}(E, G, \zeta_N) = \mathscr{B}(E, G)$. En effet, soit $\beta \in \mathscr{B}(E, G)$ une G-structure quelconque sur E : on choisit une N-structure $\mathcal{B} \in \beta$. On transforme alors $\mathcal{B} = (P_1, P_2)$ en une ζ_N-structure $\mathcal{B}'$ comme suit : on peut écrire $d(\mathcal{B}) = {\zeta_N}^k$ pour un certain $k \in (\mathbb{Z}/N\mathbb{Z})^\times$; notons $k' \in (\mathbb{Z}/N\mathbb{Z})^\times$ l'inverse de k. Comme le déterminant est surjectif, il existe $h \in G$, de déterminant k'. On pose $\mathcal{B}' := h \star \mathcal{B}$. Par construction, on a :

$$d(\mathcal{B}') = d(h \star \mathcal{B}) = d(\mathcal{B})^{\det h} = d(\mathcal{B})^{k'} = {\zeta_N}^{k \cdot k'} = \zeta_N.$$

Par conséquent, $\mathcal{B}'$ est une ζ_N-structure, et on a clairement $G \star \mathcal{B}' = G \star (h \star \mathcal{B}) = G \star \mathcal{B} = \beta$.

D'autre part, on peut définir une action *à gauche* de $\mathrm{Gal}(\overline{k}/k)$ sur $\mathscr{B}(E, N)$ de la manière suivante : pour tout $\mathcal{B} = (P_1, P_2) \in \mathscr{B}(E, N)$ et tout $\sigma \in \mathrm{Gal}(\overline{k}/k)$, on pose

$$^\sigma\mathcal{B} := ({}^\sigma P_1, {}^\sigma P_2).$$

Un calcul montre alors que $d({}^\sigma\mathcal{B}) = d(\mathcal{B})^{\det \rho_{E,N}(\sigma)}$, où $\rho_{E,N} : \mathrm{Gal}(\overline{k}/k) \to \mathrm{Aut}(E[N])$ est la représentation de $\mathrm{Gal}(\overline{k}/k)$ déduite de l'action galoisienne sur les points de N-torsion. Notons au passage que le choix d'une N-structure $\mathcal{B} = (P_1, P_2)$ sur E induit un morphisme $\rho_{\mathcal{B}} : \mathrm{Gal}(\overline{k}/k) \to \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$ donné par

$$\forall \sigma \in \mathrm{Gal}(\overline{k}/k), \qquad \left(\begin{smallmatrix} {}^\sigma P_1 \\ {}^\sigma P_2 \end{smallmatrix}\right) = \rho_{\mathcal{B}}(\sigma) \cdot \left(\begin{smallmatrix} P_1 \\ P_2 \end{smallmatrix}\right).$$

Ainsi définies, les actions de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$ et de $\mathrm{Gal}(\overline{k}/k)$ sont "compatibles" : plus précisément, on a

$$\forall \mathcal{B} \in \mathscr{B}(E, N), \forall \sigma \in \mathrm{Gal}(\overline{k}/k), \forall \gamma \in \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z}), \qquad {}^\sigma(\gamma \star \mathcal{B}) = \gamma \star ({}^\sigma\mathcal{B}). \tag{1}$$

Définition 1.6.5. — Soit E une courbe elliptique sur k et L/k est une sous-extension de corps de $\overline{k}/k$. Une G-structure $\beta \in \mathscr{B}(E, G)$ est dite *L-rationnelle* si l'orbite β est $\mathrm{Gal}(\overline{k}/L)$-stable. On pose alors $\mathscr{B}_L(E, G)$ (resp. $\mathscr{B}_L(E, G, \zeta_N)$) l'ensemble des G-structures (resp. G-structures contenant une ζ_N-structure) L-rationnelles sur E.

Proposition 1.6.6. — *Soit E une courbe elliptique sur k. On fixe une N-structure $\mathcal{B} = (P_1, P_2) \in \mathscr{B}(E, N)$. Le morphisme $\rho_{E,N} : \mathrm{Gal}(\overline{k}/k) \to \mathrm{Aut}(E[N])$ induit une représentation*

$$\rho_{\mathcal{B}} : \mathrm{Gal}(\overline{k}/k) \to \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Soit G, un sous-groupe de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Les deux assertions suivantes sont équivalentes :

1 – *E admet une G-structure k-rationnelle,*

2 – *La représentation $\rho_{\mathcal{B}}$ est à valeurs dans G.*

Démonstration. — Soit $\beta = G \star \mathcal{B}$, la G-structure "engendrée" par $\mathcal{B}$. Par (1), on a les équivalences suivantes :

$$^{\sigma}(G \star \mathcal{B}) = G \star \mathcal{B} \iff G \star {}^{\sigma}\mathcal{B} = G \star \mathcal{B} \iff \forall \sigma \in \mathrm{Gal}(\overline{k}/k),\ {}^{\sigma}\mathcal{B} \in \beta.$$

Il suffit donc de démontrer l'équivalence suivante :

$$\mathrm{Im}\,\rho_{\mathcal{B}} \subset G \iff \forall \sigma \in \mathrm{Gal}(\overline{k}/k),\ {}^{\sigma}\mathcal{B} \in \beta.$$

Or, pour tout automorphisme $\sigma \in \mathrm{Gal}(\overline{k}/k)$, l'action de σ sur $\mathcal{B}$ est donnée par $\rho_{\mathcal{B}}(\sigma)$:

$${}^{\sigma}\mathcal{B} = \begin{pmatrix} {}^{\sigma}P_1 \\ {}^{\sigma}P_2 \end{pmatrix} = \rho_{\mathcal{B}}(\sigma) \cdot \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \rho_{\mathcal{B}}(\sigma) \cdot \mathcal{B}.$$

Si $\mathrm{Im}\,\rho_{\mathcal{B}} \subset G$, l'égalité ci-dessus montre que β est $\mathrm{Gal}(\overline{k}/k)$-stable.

Réciproquement, si β est une G-structure $\mathrm{Gal}(\overline{k}/k)$-stable, pour tout $\sigma \in \mathrm{Gal}(\overline{k}/k)$, on a ${}^{\sigma}\mathcal{B} \in \beta = G \star \mathcal{B}$: il existe donc $h_\sigma \in G$ tel que

$${}^{\sigma}\mathcal{B} = \rho_{\mathcal{B}}(\sigma) \cdot \mathcal{B} = h_\sigma \star \mathcal{B} = h_\sigma \cdot \mathcal{B}.$$

Mais l'action de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$ sur $\mathscr{B}(E, N)$ est libre, donc $\rho_{\mathcal{B}}(\sigma) = h_\sigma \in G$. Et ce, quelque soit $\sigma \in \mathrm{Gal}(\overline{k}/k)$, donc $\mathrm{Im}\,\rho_{\mathcal{B}} \subset G$. □

Définition 1.6.7. — Soit E et E' des courbes elliptiques sur k, munies de N-structures $\mathcal{B} = (P_1, P_2) \in \mathscr{B}(E, N)$ et $\mathcal{B}' = (P_1', P_2') \in \mathscr{B}(E', N)$ respectivement. Un *isomorphisme de courbes elliptiques avec N-structures* est un isomorphisme $\phi : E \to E'$ telle que $\phi(P_i) = P_i'$ $(i = 1, 2)$, ce que l'on notera $\phi(\mathcal{B}) = \mathcal{B}'$.

De même, un *isomorphisme de courbes elliptiques avec G-structures* $\beta \in \mathscr{B}(E, G)$ et $\beta' \in \mathscr{B}(E', G)$ est un isomorphisme $\phi : E \to E'$ telle que, pour tout $\mathcal{B} \in \beta$ on ait $\phi(\mathcal{B}) \in \beta'$.

Remarque 1.6.8. — Si E est une courbe elliptique et que $\varepsilon \in \mathrm{Aut}_{\overline{k}}(E)$, on a

$$(E, \mathcal{B}) \simeq (E, \varepsilon(\mathcal{B})).$$

1.6.2. Exemples. — Soit E une courbe elliptique sur un corps k, de caractéristique première à N. Il est facile de relier ces définitions aux définitions usuelles :

- Soit $G = \{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)\}$ est le sous-groupe des matrices triangulaires supérieures de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$ (sous-groupe de Borel). L'image inverse de $G \cap \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})$ par l'application de réduction modulo N est $\Gamma_0(N)$. Un raisonnement rapide montre qu'il y a une bijection

$$\begin{array}{ccc} \mathscr{B}(E, G) & \longleftrightarrow & \{\text{sous-groupes } N\text{-cycliques de } E[N]\} \\ G \star \left(\begin{smallmatrix} P_1 \\ P_2 \end{smallmatrix}\right) & \longmapsto & \langle P_2 \rangle. \end{array}$$

- De même, pour $G = \{\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)\}$, il y a une bijection

$$\begin{array}{ccc} \mathscr{B}(E, G) & \longleftrightarrow & \{\text{points d'ordre exactement } N \text{ de } E[N]\} \\ G \star \left(\begin{smallmatrix} P_1 \\ P_2 \end{smallmatrix}\right) & \longmapsto & P_2. \end{array}$$

  Dans ce cas, le relevé de $G \subset \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})$ à $\mathbf{SL}_2(\mathbb{Z})$ est $\Gamma_1(N)$.

On peut alors faire agir le groupe de Galois $\mathrm{Gal}(\overline{k}/k)$ sur ces bijections :

- Dans le cas où $G = \{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)\}$, il y a une bijection

$$\begin{array}{ccc} \mathscr{B}_k(E, G) & \longleftrightarrow & \{\text{sous-groupes } N\text{-cycliques et } \mathrm{Gal}(\overline{k}/k)\text{-invariants de } E[N]\} \\ G \star \left(\begin{smallmatrix} P_1 \\ P_2 \end{smallmatrix}\right) & \longmapsto & \langle P_2 \rangle. \end{array}$$

- Similairement, pour $G = \{\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)\}$, il y a une bijection

$$\begin{array}{ccc} \mathscr{B}_k(E, G) & \longleftrightarrow & \{\text{points d'ordre exactement } N \text{ de } E[N](k)\} \\ G \star \left(\begin{smallmatrix} P_1 \\ P_2 \end{smallmatrix}\right) & \longmapsto & P_2. \end{array}$$

  Dans ce cas, le relevé de $G \subset \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})$ à $\mathbf{SL}_2(\mathbb{Z})$ est $\Gamma_1(N)$.

1.6.3. Espaces de modules sur $\mathbb{C}$. — On s'intéresse aux problèmes de modules suivants :

Définition 1.6.9. — Pour toute racine primitive N-ième de l'unité $\zeta_N \in \mu_N(k)^\times$, on définit

$$\mathscr{E}\ell\ell_k(\zeta_N) := \Big\{(E,\mathcal{B}),\ \text{où } E \text{ est une courbe elliptique sur } k \text{ et } \mathcal{B} \in \mathscr{B}(E,\zeta_N)\ \Big\}\Big/ k\text{-isomorphisme}$$

et, plus généralement,

$$\mathscr{E}\ell\ell_k(N) := \Big\{(E,\mathcal{B}),\ \text{où } E \text{ est une courbe elliptique sur } k \text{ et } \mathcal{B} \in \mathscr{B}(E,N)\ \Big\}\Big/ k\text{-isomorphisme.}$$

Pour tout sous-groupe G de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$ et toute racine primitive N-ième de l'unité $\zeta_N \in \mu_N(k)^\times$, on définit

$$\mathscr{E}\ell\ell_k(G,\zeta_N) := \Big\{(E,\beta),\ \text{où } E \text{ est une courbe elliptique sur } k \text{ et } \beta \in \mathscr{B}(E,G,\zeta_N)\ \Big\}\Big/ k\text{-isomorphisme}$$

et

$$\mathscr{E}\ell\ell_k(G) := \Big\{(E,\beta),\ \text{où } E \text{ est une courbe elliptique sur } k \text{ et } \beta \in \mathscr{B}(E,G)\ \Big\}\Big/ k\text{-isomorphisme.}$$

Si (E,β) est une courbe elliptique munie d'une G-structure, on note $[E,\beta]$ sa classe d'isomorhisme.

Théorème 1.6.10. — *Soit $N \in \mathbb{N}^*$, on pose $\zeta_N = \mathrm{e}^{2i\pi/N} \in \mathbb{C}$. Il y a une bijection canonique entre $Y(N)(\mathbb{C})$ et $\mathscr{E}\ell\ell_{\mathbb{C}}(\zeta_N)$, donnée par*

$$\begin{array}{rcl} Y(N)(\mathbb{C}) = \Gamma(N)\backslash\mathfrak{H} & \longrightarrow & \mathscr{E}\ell\ell_{\mathbb{C}}(\zeta_N) \\ \Gamma(N)\cdot\tau & \mapsto & [E_\tau, \mathcal{B}_\tau] \end{array}$$

où $E_\tau = \mathbb{C}/\Lambda_\tau$ et $\mathcal{B}_\tau = (\tau/N \bmod \Lambda_\tau, 1/N \bmod \Lambda_\tau)$.

Démonstration. —

- Commençons par définir une application $\Phi : \mathfrak{H} \to \mathscr{E}\ell\ell_{\mathbb{C}}(\zeta_N)$: soit $\tau \in \mathfrak{H}$, le quotient
$$E_\tau = \mathbb{C}/(\mathbb{Z}\tau \oplus \mathbb{Z}) = \mathbb{C}/\Lambda_\tau$$
est une courbe elliptique sur $\mathbb{C}$ et le couple
$$\mathcal{B}_\tau = \left(\frac{\tau}{N} \bmod \Lambda_\tau, \frac{1}{N} \bmod \Lambda_\tau\right)$$
est une base $E_\tau[N]$ telle que $d(\mathcal{B}) = \mathrm{e}^{2i\pi/N}$. En d'autres termes, le couple $(E_\tau, \mathcal{B}_\tau)$ est une courbe elliptique munie d'une ζ_N-structure. On peut donc poser $\Phi(\tau) = [E_\tau, \mathcal{B}_\tau]$.
- Vérifions maintenant que Φ passe au quotient par $\Gamma(N)$. Soit $\tau, \tau' \in \mathfrak{H}$ tels que $\Gamma(N)\cdot\tau = \Gamma(N)\cdot\tau'$: on peut donc fixer $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(N)$ tel que $\tau = \gamma\cdot\tau'$. On pose $m = c\tau' + d \in \mathbb{C}^*$. On calcule alors :
$$m\Lambda_\tau = (c\tau'+d)\cdot(\mathbb{Z}\tau \oplus \mathbb{Z}) = (c\tau'+d)\cdot\left(\mathbb{Z}\frac{a\tau'+b}{c\tau'+d} \oplus \mathbb{Z}\right) = \mathbb{Z}(a\tau'+b) \oplus \mathbb{Z}(c\tau'+d) = \Lambda_{\tau'}$$
$$m\left(\frac{\tau}{N} \bmod \Lambda_\tau\right) = (c\tau'+d)\cdot\left(\frac{a\tau'+b}{N(c\tau'+d)} \bmod \Lambda_\tau\right) = \left(\frac{a\tau'+b}{N} \bmod \Lambda_{\tau'}\right) = \left(\frac{\tau'}{N} \bmod \Lambda_{\tau'}\right)$$
$$m\left(\frac{1}{N} \bmod \Lambda_\tau\right) = \left(\frac{c\tau'+d}{N} \bmod \Lambda_{\tau'}\right) = \left(\frac{1}{N} \bmod \Lambda_{\tau'}\right).$$
Où l'on a utilisé le fait que $\gamma \in \Gamma(N)$ au travers des deux relations suivantes : $(a,b) \equiv (1,0) \bmod N$ et $(c,d) \equiv (0,1) \bmod N$.

  Donc la multiplication par m est un $\mathbb{C}$-isomorphisme $E_\tau \to E_{\tau'}$, compatible aux ζ_N-structures ! Autrement dit,
$$[E_\tau, \mathcal{B}_\tau] = [E_{\tau'}, \mathcal{B}_{\tau'}]$$
et Φ se factorise à travers le quotient $\Gamma(N)\backslash\mathfrak{H}$. On notera encore $\Phi : Y(N) \to \mathscr{E}\ell\ell_{\mathbb{C}}(\zeta_N)$ l'application induite.
- Soit $[E,\mathcal{B}] \in \mathscr{E}\ell\ell_{\mathbb{C}}(\zeta_N)$. La courbe elliptique E est isomorphe à une courbe $E_{\tau'}$ pour un certain $\tau' \in \mathfrak{H}$: on peut donc supposer sans perte de généralité que $E = E_{\tau'}$.

  On considère donc $(E_{\tau'}, \mathcal{B})$: on veut montrer que Φ est surjective, ie. que
$$\exists\ \tau \in \mathfrak{H}, \qquad [E_{\tau'}, \mathcal{B}] = [E_\tau, \mathcal{B}_\tau].$$
Notons $\mathcal{B} = (P_1, P_2)$. Comme $\mathcal{B}_{\tau'}$ est aussi une base de $E_{\tau'}[N]$, on peut fixer $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{GL}_2(\mathbb{Z})$ telle que
$$P_1 = \frac{a\tau'+b}{N} \qquad \text{et} \qquad P_2 = \frac{c\tau'+d}{N}$$
On a alors
$$\zeta_N = d(\mathcal{B}) = d(\mathcal{B}_{\tau'})^{\det\gamma} = {\zeta_N}^{\det\gamma}.$$

Donc $\det(\gamma) \equiv 1 \bmod N$, c'est-à-dire $\gamma \bmod N \in \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Comme la réduction modulo N est surjective (Lemme 1.2.2), on peut supposer que $\gamma \in \mathbf{SL}_2(\mathbb{Z})$ (car changer les coefficients de γ par un multiple de N ne change pas $\mathcal{B}$).

On pose alors $\tau = \gamma \cdot \tau'$ et $m = c\tau' + d$. Puisque $\gamma \in \mathbf{SL}_2(\mathbb{Z})$, les mêmes calculs que ci-dessus conduisent à

$$m\Lambda_\tau = \Lambda_{\tau'}, \qquad m\left(\frac{\tau}{N} \bmod \Lambda_\tau\right) = P_1 \qquad \text{et} \qquad m\left(\frac{1}{N} \bmod \Lambda_\tau\right) = P_2.$$

Ainsi, la multiplication par m est un $\mathbb{C}$-isomorphisme de $(E_{\tau'}, \mathcal{B})$ sur $(E_\tau, \mathcal{B}_\tau)$. Ce qui se réécrit sous la forme $[E_{\tau'}, \mathcal{B}] = [E_\tau, \mathcal{B}_\tau] = \Phi(\Gamma(N) \cdot \tau)$.

- Enfin, montrons que Φ est injective : si $[E_\tau, \mathcal{B}_\tau] = [E_{\tau'}, \mathcal{B}_{\tau'}]$ dans $\mathscr{E}\ell\ell_{\mathbb{C}}(\zeta_N)$, alors il existe un nombre complexe $m \in \mathbb{C}^\times$ tel que

$$m\Lambda_\tau = \Lambda_{\tau'}, \qquad m\left(\frac{\tau}{N} \bmod \Lambda_\tau\right) = \frac{\tau'}{N} \bmod \Lambda_{\tau'} \quad \text{et} \quad m\left(\frac{1}{N} \bmod \Lambda_\tau\right) = \frac{1}{N} \bmod \Lambda_{\tau'}$$

car une isogénie entre courbes elliptiques sur $\mathbb{C}$ correspond à une homothétie entre réseaux de $\mathbb{C}$ (voir [**Sil09**, Proposition VI.4.1(b)]). La première égalité impose qu'il existe une matrice de changement de base $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z})$ telle que

$$\begin{pmatrix} m\tau \\ m \end{pmatrix} = \gamma \cdot \begin{pmatrix} \tau' \\ 1 \end{pmatrix}.$$

En particulier, on a $m = c\tau' + d$. La seconde condition donne alors

$$\frac{\tau'}{N} \bmod \Lambda_{\tau'} = \frac{m}{N} \cdot \frac{a\tau' + b}{c\tau' + d} \bmod \Lambda_{\tau'} = \frac{a\tau' + b}{N} \bmod \Lambda_{\tau'},$$

c'est-à-dire $(a, b) \equiv (1, 0) \bmod N$. Similairement, la troisième condition impose que $(c, d) \equiv (0, 1) \bmod N$.

Finalement, on a $\gamma \in \Gamma(N)$, et $\Gamma(N) \cdot \tau = \Gamma(N) \cdot \tau'$.

□

Corollaire 1.6.11. — *Soit $N \in \mathbb{N}^*$. Il y a une bijection canonique entre les ensembles suivants :*

$$\begin{array}{ccc} (\mu_N(\mathbb{C}))^\times \times Y(N)(\mathbb{C}) & \longrightarrow & \mathscr{E}\ell\ell_{\mathbb{C}}(N) \\ (\mathrm{e}^{2i\pi k/N}, \Gamma(N) \cdot \tau) & \mapsto & [E_\tau, \left(\begin{smallmatrix} 1 & 0 \\ 0 & k \end{smallmatrix}\right) \star \mathcal{B}_\tau] \end{array}$$

où $E_\tau = \mathbb{C}/\Lambda_\tau$ et $\mathcal{B}_\tau = (\tau/N \bmod \Lambda_\tau, 1/N \bmod \Lambda_\tau)$.

Démonstration. — Vu le théorème précédent, il suffit que les applications canonique ci-dessous sont des bijections inverse l'une de l'autre :

$$\begin{array}{ccc} \mathscr{E}\ell\ell_{\mathbb{C}}(N) & \longleftrightarrow & (\mu_N(\mathbb{C}))^\times \times \mathscr{E}\ell\ell_{\mathbb{C}}(\zeta_N) \\ [E, \mathcal{B}] & \mapsto & \left(d(\mathcal{B}), \left[E, \left(\begin{smallmatrix} 1 & 0 \\ 0 & (d(\mathcal{B}))^{-1} \end{smallmatrix}\right) \star \mathcal{B}\right]\right) \\ [E, \left(\begin{smallmatrix} 1 & 0 \\ 0 & k \end{smallmatrix}\right) \star \mathcal{B}_0] & \hookleftarrow & \left(\mathrm{e}^{2i\pi k/n}, [E, \mathcal{B}_0]\right). \end{array}$$

Mais cela est clair. □

Plus généralement, on a :

Théorème 1.6.12. — *Soit Γ, un sous-groupe de congruences de $\mathbf{SL}_2(\mathbb{Z})$ de niveau N, dont on note H la réduction modulo N. Alors, il y a une bijection canonique entre les deux ensembles suivants :*

$$\begin{array}{ccc} Y(\Gamma)(\mathbb{C}) & \longrightarrow & \mathscr{E}\ell\ell_{\mathbb{C}}(H, \zeta_N) \\ \Gamma \cdot \tau & \mapsto & [E_\tau, H \star \mathcal{B}_\tau]. \end{array}$$

Démonstration. — • Remarquons dans un premier temps que l'inclusion $\Gamma(N) \hookrightarrow \Gamma$ induit une surjection canonique $\pi : Y(N) \twoheadrightarrow Y(\Gamma)$ (qui consiste à envoyer $\Gamma(N) \cdot \tau$ sur $\Gamma \cdot \tau$ pour tout $\tau \in \mathfrak{H}$), et que l'on a

$$\Gamma/\Gamma(N) \simeq H.$$

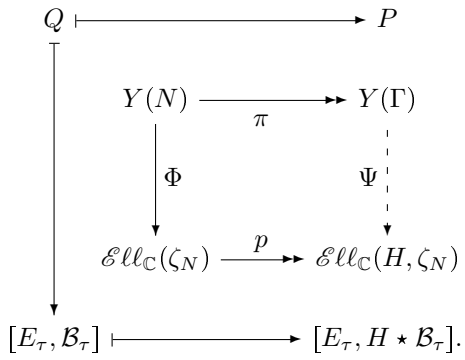
De plus, il y a une surjection $p : \mathscr{E}\ell\ell_{\mathbb{C}}(\zeta_N) \twoheadrightarrow \mathscr{E}\ell\ell_{\mathbb{C}}(H, \zeta_N)$ donnée par

$$[E, \mathcal{B}] \mapsto [E, H \star \mathcal{B}].$$

Soit $P \in Y(\Gamma)$, on peut le relever par un point $Q \in Y(N)$. D'après le théorème précédent, Q correspond de manière canonique à une classe de $\mathbb{C}$-isomorphisme $[E_\tau, \mathcal{B}_\tau] \in \mathscr{E}\ell\ell_{\mathbb{C}}(\zeta_N)$. On pose alors

$$\Psi(P) := p([E_\tau, \mathcal{B}_\tau]) = [E_\tau, H \star \mathcal{B}_\tau] \in \mathscr{E}\ell\ell_{\mathbb{C}}(H, \zeta_N).$$

La situation est la suivante :



- Premièrement, démontrons que $\Psi : Y(\Gamma) \to \mathscr{E}\ell\ell_{\mathbb{C}}(H, \zeta_N)$ est bien définie. Si $Q = \Gamma(N) \cdot \tau$ et $Q' = \Gamma(N) \cdot \tau'$ sont deux relevés de P, on a
$$\pi(Q') = \Gamma \cdot \tau = \Gamma \cdot \tau' = \pi(Q).$$
et on peut fixer $h \in \Gamma/\Gamma(N)$ tel qu'un relevé $\gamma \in \Gamma$ de h vérifie : $\tau' = \gamma \cdot \tau$. Alors
$$p \circ \Phi(Q') = p([E_{\gamma\tau}, \mathcal{B}_{\gamma\tau}]) = p([E_\tau, h \star \mathcal{B}_\tau]) = [E_\tau, H \star (h \star \mathcal{B}_\tau)] = p \circ \Phi(Q).$$
- Deuxièmement, prouvons la surjectivité de Ψ. Soit $[E, \beta] \in \mathscr{E}\ell\ell_{\mathbb{C}}(H, \zeta_N)$, on peut supposer sans perte de généralité que $E = E_{\tau'}$ pour un certain $\tau' \in \mathfrak{H}$. Écrivons $\beta = H \star \mathcal{B}$ avec $\mathcal{B} \in \mathscr{B}(E_\tau, \zeta_N)$. Dans ces conditions, le Théorème 1.6.10 affirme qu'il existe $\tau \in \mathfrak{H}$ tel que $[E_{\tau'}, \mathcal{B}] = [E_\tau, \mathcal{B}_\tau]$. En prenant l'image par p, on obtient :
$$[E_{\tau'}, H \star \mathcal{B}] = p([E_{\tau'}, \mathcal{B}]) = p([E_\tau, \mathcal{B}_\tau]) = p \circ \Phi(\Gamma(N) \cdot \tau).$$
On a donc $[E_{\tau'}, H \star \mathcal{B}] = \Psi(P)$, où $P = \pi(\Gamma(N) \cdot \tau)$.
- Terminons la preuve en montrant que Ψ est injective. Soit $[E_\tau, H \star \mathcal{B}_\tau] = [E_{\tau'}, H \star \mathcal{B}_{\tau'}] \in \mathscr{E}\ell\ell_{\mathbb{C}}(H, \zeta_N)$. Il existe alors $m \in \mathbb{C}^\times$ et $h = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in H$, dont on notera encore h un relevé à Γ, tels que
$$m\Lambda_\tau = \Lambda_{\tau'}, \qquad m\left(\frac{\tau}{N} \bmod \Lambda_\tau\right) = \frac{x\tau' + y}{N} \bmod \Lambda_{\tau'}, \qquad m\left(\frac{z\tau' + w}{N} \bmod \Lambda_\tau\right) = \frac{1}{N} \bmod \Lambda_{\tau'}.$$
La première égalité assure que l'on peut fixer $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z})$ telle que
$$\left(\begin{smallmatrix} m\tau \\ m \end{smallmatrix}\right) = \gamma \cdot \left(\begin{smallmatrix} \tau' \\ 1 \end{smallmatrix}\right).$$
En particulier, on a $m = c\tau' + d$. La seconde condition donne alors
$$\frac{x\tau' + y}{N} \bmod \Lambda_{\tau'} = \frac{m}{N} \cdot \frac{a\tau' + b}{c\tau' + d} \bmod \Lambda_{\tau'} = \frac{a\tau' + b}{N} \bmod \Lambda_{\tau'},$$
c'est-à-dire $(a, b) \equiv (x, y) \bmod N$. Similairement, la troisième condition impose que $(c, d) \equiv (z, w) \bmod N$. Ce qui démontre que $\gamma \bmod N = h$, donc que $\gamma \in \Gamma$.
Finalement, on a bien $\Gamma \cdot \tau = \Gamma \cdot \tau'$.

□

Corollaire 1.6.13. — *Soit G un sous-groupe de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$ contenant $-I$. On note $H = G \cap \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})$, et Γ le relevé de H à $\mathbf{SL}_2(\mathbb{Z})$. Alors, il y a une bijection canonique entre les deux ensembles suivants :*
$$\begin{array}{ccc} Y(\Gamma)(\mathbb{C}) & \longrightarrow & \mathscr{E}\ell\ell_{\mathbb{C}}(G, \zeta_N) \\ \Gamma \cdot \tau & \mapsto & [E_\tau, G \star \mathcal{B}_\tau]. \end{array}$$

Démonstration. — D'après le théorème ci-dessus, il suffit de voir que les applications canoniques ci-dessous sont inverses l'une de l'autre :
$$\begin{array}{cccc} & \mathscr{E}\ell\ell_{\mathbb{C}}(G, \zeta_N) & \longleftrightarrow & \mathscr{E}\ell\ell_{\mathbb{C}}(H, \zeta_N) \\ y : & [E, G \star \mathcal{B}_0] & \mapsto & [E, H \star \mathcal{B}_0] \\ z : & [E, G \star \mathcal{B}] & \hookleftarrow & [E, H \star \mathcal{B}] \end{array}$$
où $\mathcal{B}_0$ désigne une ζ_N-structure de l'orbite $G \star \mathcal{B}_0$. La seule chose qui n'est pas claire est la bonne définition de y. Mais, si $\beta \in \mathscr{B}(E, G, \zeta_N)$ et si $\mathcal{B}_0$ et $\mathcal{B}_0'$ sont deux ζ_N-structure dans l'orbite β, on peut fixer $g \in G$ tel que $\mathcal{B}_0' = g \cdot \mathcal{B}_0$. Auquel cas $\det g = 1$ car $d(\mathcal{B}_0) = d(\mathcal{B}_0') = \zeta_N$. C'est-à-dire que l'on a $g \in H$, donc $H \star \mathcal{B}_0' = H \star g \cdot \mathcal{B}_0 = H \star \mathcal{B}_0$. Donc y est bien définie. □

CHAPITRE 2

ALGÉBRISATION SUR $\mathbb{C}$

Soit Γ, un sous-groupe de congruences de $\mathbf{SL}_2(\mathbb{Z})$. Comme toute surface de Riemann compacte, $X(\Gamma)$ admet une structure de courbe projective lisse sur $\mathbb{C}$. Trouver une équation de cette courbe revient à expliciter un ensemble de générateurs de $\mathfrak{M}(\Gamma)$. Ce chapitre a pour but de déterminer de tels générateurs et d'en déduire un modèle de $X(\Gamma)$ sur un sous-corps de $\mathbb{Q}(\mu_N)$.

2.1. Générateurs de $\mathfrak{M}(\Gamma(N))$

2.1.1. Le cas de $\mathbf{SL}_2(\mathbb{Z})$. —

Proposition 2.1.1. — *On a :*

$$\mathfrak{M}(\Gamma(1)) = \mathbb{C}(j).$$

Démonstration. — On sait (voir **[DS05]**) que j est une fonction holomorphe sur $\mathfrak{H}$, qu'elle ne s'annule pas sur $\mathfrak{H}$ et qu'elle a un pôle simple en $i\infty$ de résidu 1. Autrement dit, $j(\tau)$ admet un développement de Fourier de la forme

$$j(\tau) = \frac{1}{q} + \text{ série entière en } q.$$

Par conséquent, $\mathbb{C}(j)$ est un sous-corps de $\mathfrak{M}(\Gamma(1))$. Réciproquement, soit $f \in \mathfrak{M}(\Gamma(1))$ est une fonction non constante : elle admet un nombre fini de pôles dans un domaine fondamental de $\mathfrak{H}$ pour l'action de $\mathbf{SL}_2(\mathbb{Z})$. Notons $z_1, \ldots, z_n$ ces pôles (comptés avec multiplicités) et posons :

$$\forall \tau \in \mathfrak{H}, \qquad G(\tau) := f(\tau) \cdot \prod_{k=1}^{n} (j(\tau) - j(z_k)).$$

La fonction $G : \mathfrak{H} \to \mathbb{C}$ est holomorphe sur $\mathfrak{H}$, et modulaire pour $\mathbf{SL}_2(\mathbb{Z})$. En particulier, G définit une fonction sur $X(1) = \mathbf{SL}_2(\mathbb{Z})\backslash\mathfrak{H}^*$, qui est une surface de Riemann compacte. Donc G est constante sur $X(1)$, de valeur $C \in \mathbb{C}^*$! On peut ainsi écrire

$$f = \frac{C}{\prod_{k=1}^{n}(j - j(z_k))} \in \mathbb{C}(j).$$

□

2.1.2. Générateurs de $\mathfrak{M}(\Gamma(N))$. —

Définition 2.1.2. — Soir $\Lambda_\tau = \mathbb{Z}\tau \oplus \mathbb{Z}$ un réseau de $\mathbb{C}$. Pour tout $\mathbf{a} = (a_1, a_2) \in (N^{-1}\mathbb{Z})^2 \smallsetminus \mathbb{Z}^2$, on définit la $\mathbf{a}$-ième *fonction de Weber de* Λ_τ par

$$\forall \tau \in \mathfrak{H}, \quad f_{\mathbf{a}}(\tau) = \frac{g_2(\tau)}{g_3(\tau)} \cdot \wp\left(a_1\tau + a_2; \Lambda_\tau\right),$$

où g_2, g_3 et $\wp(-;\Lambda_\tau)$ sont les fonctions usuelles :

$$g_2(\tau) = 60 \cdot \sum_{\omega\in\Lambda_\tau}{}' \frac{1}{\omega^4}, \quad g_3(\tau) = 140 \cdot \sum_{\omega\in\Lambda_\tau}{}' \frac{1}{\omega^4}, \quad \wp(z;\Lambda_\tau) := \frac{1}{z^2} + \sum_{\omega\in\Lambda_\tau}{}' \left(\frac{1}{(z-\omega)^2} - \frac{1}{z^2}\right).$$

Lemme 2.1.3. — *Soit* $\mathbf{a} = (a, b) \in (N^{-1}\mathbb{Z})^2 \smallsetminus \mathbb{Z}^2$*, on note* $q = \mathrm{e}^{2i\pi\tau}$ *et* $\zeta_N = \mathrm{e}^{2i\pi/N}$*. Alors on a*

$$\forall \tau \in \mathfrak{H}, \quad f_{(a,b)}(\tau) = \frac{1}{12} - 2\sum_{n=1}^{\infty} \frac{nq^{Nn}}{1-q^{Nn}} + \frac{{\zeta_N}^b q^a}{1-{\zeta_N}^b q^a} + \sum_{n=1}^{\infty} \frac{nq^n\left({\zeta_N}^{bn}q^{an} + {\zeta_N}^{-bn}q^{-an}\right)}{1-q^n}.$$

Démonstration. — Il s'agit d'écrire les développements en séries de Fourier de $\wp(-;\Lambda_\tau)$, de $g_2(\tau)$ et de $g_3(\tau)$ et de combiner les résultats. Le détail des calculs se trouve dans [**Lan87**, Chapter 4. §2]. □

Donnons quelques propriétés des fonctions de Weber :

Proposition 2.1.4. — *Pour tout* $\mathbf{a} = (a_1, a_2) \in (N^{-1}\mathbb{Z})^2 \smallsetminus \mathbb{Z}^2$*, on a*

- $f_{-\mathbf{a}} = f_{\mathbf{a}}$.
- *Pour tout* $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{SL}_2(\mathbb{Z})$*, on a :*
$$\forall \tau \in \mathfrak{H}, \qquad f_{\mathbf{a}}(\alpha \cdot \tau) = f_{\mathbf{a}\cdot\alpha}(\tau).$$
- *La fonction* $f_{\mathbf{a}}$ *est modulaire pour* $\Gamma(N)$*, ie.* $f_{\mathbf{a}} \in \mathfrak{M}(\Gamma(N))$.
- *Si* $\mathbf{a}' \in (N^{-1}\mathbb{Z})^2 \smallsetminus \mathbb{Z}^2$*, on a*
$$f_{\mathbf{a}} = f_{\mathbf{a}'} \iff \mathbf{a} = \pm\mathbf{a}'.$$

Démonstration. — Le premier point est clair car la fonction $\wp(-;\Lambda_\tau)$ est paire. Pour démontrer le deuxième point, on utilise les propriétés d'homogénéité de g_2, g_3 et $\wp(-;\Lambda_\tau)$: avec les notations de la proposition, on a

$$\begin{aligned} f_{\mathbf{a}}(\alpha\cdot\tau) &= \frac{g_2(\alpha\cdot\tau)}{g_3(\alpha\cdot\tau)} \cdot \wp\left(a_1\frac{a\tau+b}{c\tau+d} + a_2; \Lambda_{\alpha\cdot\tau}\right) \\ &= \frac{(c\tau+d)^6}{(c\tau+d)^4}\cdot\frac{g_2(\tau)}{g_3(\tau)}\cdot\frac{1}{(c\tau+d)^2}\wp\left((a_1a+a_2c)\tau + (a_1b+a_2d); \Lambda_\tau\right) \\ &= \frac{g_2(\tau)}{g_3(\tau)}\cdot\wp\left(a_1'\tau + a_2'; \Lambda_\tau\right) = f_{\mathbf{a}'}(\tau), \end{aligned}$$

où l'on a posé $\mathbf{a}' = \mathbf{a}\cdot\alpha$. En particulier, ceci montre que $f_{\mathbf{a}}$ est $\Gamma(N)$-invariante, puisque $\Gamma(N)$ agit trivialement à droite sur $(N^{-1}\mathbb{Z})^2 \smallsetminus \mathbb{Z}^2$.

D'après leur définition, les fonctions $f_{\mathbf{a}}$ sont clairement méromorphes sur $\mathfrak{H}$, il reste donc à vérifier qu'elles le sont aussi aux pointes de $X(N)$. D'après la deuxième propriété, il suffit de voir qu'elles le sont à la pointe $i\infty$. Mais cela se voit directement sur leur développement en série de Fourier (Lemme 2.1.3).

Enfin, la fonction $\wp(-;\Lambda_\tau)$ vérifie

$$\forall z, z' \in \mathbb{C},\ \wp(z;\Lambda_\tau) = \wp(z';\Lambda_\tau) \iff z \equiv \pm z' \bmod \Lambda_\tau,$$

ce qui montre que $f_{\mathbf{a}} = f_{\mathbf{a}'}$ si et seulement si $\mathbf{a} = \pm\mathbf{a}'$. □

Le dernier point de la proposition prouve que $\left\{f_{\mathbf{a}},\ \mathbf{a} \in (N^{-1}\mathbb{Z})^2 \smallsetminus \mathbb{Z}^2\right\}$ est en bijection avec

$$A = \left((N^{-1}\mathbb{Z})^2 \smallsetminus \mathbb{Z}^2\right)/\{\pm1\} \leftrightarrow \left(\mathbb{Z}/N\mathbb{Z}^2 \smallsetminus \{(0,0)\}\right)/\{\pm1\}.$$

Proposition 2.1.5. — *Les fonctions* j *et* $f_{\mathbf{a}}$ *(pour* $\mathbf{a}$ *parcourant* A*) engendrent* $\mathfrak{M}(\Gamma(N))$*. On a même*

$$\mathfrak{M}(\Gamma(N)) = \mathbb{C}(j, f_{\pm(1,0)}, f_{\pm(0,1)}).$$

Démonstration. — La proposition précédente montre que

$$\mathfrak{M}(\Gamma(1)) \subset \mathbb{C}(j, \{f_{\mathbf{a}}\}) \subset \mathfrak{M}(\Gamma(N)).$$

On a démontré à la Proposition 1.3.4 que le morphisme

$$\theta : \mathbf{SL}_2(\mathbb{Z})/\{\pm I\} \to \mathrm{Gal}\left(\mathfrak{M}(\Gamma(N))/\mathfrak{M}(\Gamma(1))\right), \qquad \overline{\gamma} \mapsto (f \mapsto f|_\gamma),$$

(où γ désigne un relevé de $\overline{\gamma}$ à $\mathbf{SL}_2(\mathbb{Z})$) est un isomorphisme de groupes. Or, on vient de montrer que l'action de $\overline{\gamma} \in \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ sur A coïncide avec celle de $\theta(\overline{\gamma})$ sur $\{f_{\mathbf{a}}\}$ (donc sur $\mathbb{C}(j, \{f_{\mathbf{a}}\})$), au sens où

$$\theta(\overline{\gamma})(f_{\mathbf{a}}) = f_{\mathbf{a}}|_\gamma = f_{\mathbf{a}\cdot\gamma}.$$

Ainsi, l'extension $\mathbb{C}(j, \{f_{\mathbf{a}}\})/\mathfrak{M}(\Gamma(1))$ est fixée par le sous-groupe trivial de $\mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ car l'action de $\mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ sur $\{f_{\mathbf{a}}\}$ est libre. Par théorie de Galois, cela entraîne que $\mathbb{C}(j, \{f_{\mathbf{a}}\}) = \mathfrak{M}(\Gamma(N))$.

De la même manière, considérons les inclusions de corps suivantes :

$$\mathfrak{M}(\Gamma(1)) \subset \mathbb{C}(j, f_{\pm(1,0)}, f_{\pm(0,1)}) \subset \mathfrak{M}(\Gamma(N)).$$

Un élément $\overline{\gamma} \in \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ dont l'image par θ fixe $\mathbb{C}(j, f_{\pm(1,0)}, f_{\pm(0,1)})$ est nécessairement trivial. Donc, par le même argument que ci-dessus, $\mathbb{C}(j, f_{\pm(1,0)}, f_{\pm(0,1)}) = \mathfrak{M}(\Gamma(N))$. □

Remarque 2.1.6. — Des considérations similaires montreraient que

$$\mathfrak{M}(\Gamma_1(N)) = \mathbb{C}(j, \{f_{(0,b)}\}) = \mathbb{C}(j, f_{(0,1)})$$

où b parcourt un ensemble de représentants de $B = (N^{-1}\mathbb{Z} \smallsetminus \mathbb{Z})/\{\pm1\}$. On a également

$$\mathfrak{M}(\Gamma_0(N)) = \mathbb{C}(j, f^0) = \mathbb{C}(j, j_N)$$

où $f^0 = \sum_{b=1}^{N-1} f_{(0,b/N)}$ et $j_N : \tau \mapsto j(N\tau)$.

Ces relations sont utiles lorsque l'on cherche des équations explicites de $X_0(N)$ ou de $X_1(N)$: en effet, comme le degré de transcendance de $\mathfrak{M}(\Gamma_0(N))$ (par exemple) sur $\mathbb{C}$ est 1, on sait qu'il existe une relation polynômiale entre j et j_N :

$$\phi_N(j, j_N) = 0 \qquad \text{où } \phi_N \in \mathbb{C}[X, Y].$$

Expliciter $\phi_N(X, Y)$ revient donc à donner une équation algébrique de $X_0(N)$. On peut même choisir ϕ_N de manière à ce qu'il ait des coefficients rationnels. C'est ce que l'on verra au chapitre suivant.

2.2. Générateurs de $\mathfrak{M}(\Gamma)$

Soit Γ un sous-groupe de congruences de $\mathbf{SL}_2(\mathbb{Z})$ de niveau N, on notera H sa réduction modulo N. Les inclusions $\Gamma(N) \subset \Gamma \subset \mathbf{SL}_2(\mathbb{Z})$ fournissent des inclusions de corps

$$\mathfrak{M}(\mathbf{SL}_2(\mathbb{Z})) \hookrightarrow \mathfrak{M}(\Gamma) \hookrightarrow \mathfrak{M}(\Gamma(N)).$$

Or, on a vu (Théorème 1.3.4) que l'extension $\mathfrak{M}(\Gamma(N))/\mathfrak{M}(\Gamma(1))$ est galoisienne de groupe de Galois $\mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$: la sous-extension $\mathfrak{M}(\Gamma(N))/\mathfrak{M}(\Gamma)$ est donc galoisienne de groupe de Galois isomorphe à $\Gamma/\{\pm I\} \cdot \Gamma(N) \simeq H/\{\pm 1\}$. En d'autres termes, $\mathfrak{M}(\Gamma)$ est le sous-corps de $\mathfrak{M}(\Gamma(N))$ fixé par l'action de $H/\{\pm I\}$. L'isomorphisme entre $\mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ et $\mathrm{Gal}(\mathfrak{M}(\Gamma(N))/\mathfrak{M}(\Gamma(1)))$ est donné par

$$\overline{\gamma} \mapsto (f \mapsto f|_\gamma)$$

où γ désigne un relevé de $\overline{\gamma}$ à $\mathbf{SL}_2(\mathbb{Z})$.

D'autre part, on a démontré que $\mathfrak{M}(\Gamma(N)) = \mathbb{C}(j, \{f_{\mathbf{a}}\})$, donc on a

$$\mathfrak{M}(\Gamma) = \mathbb{C}(j, \{f_{\mathbf{a}}\})^{H/\{\pm I\}}.$$

Donnons maintenant des générateurs explicites de $\mathfrak{M}(\Gamma)$. Rappelons que l'on a posé

$$A = \left((N^{-1}\mathbb{Z})^2 \smallsetminus \mathbb{Z}^2\right)/\{\pm 1\}$$

et que $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ agit naturellement à droite sur A, via

$$\forall \overline{\gamma} \in \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}, \forall \mathbf{a} \in A, \qquad \gamma : \mathbf{a} \mapsto \mathbf{a} \cdot \overline{\gamma}.$$

Le sous-groupe de congruences Γ de $\mathbf{SL}_2(\mathbb{Z})$ se réduit modulo N en un sous-groupe H de $\mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})$, et en un sous-groupe $\overline{H}$ de $\mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$. On notera B le quotient $B := A/\overline{H}$. Pour tout $\mathbf{b} = \mathbf{a} \cdot \overline{H} \in B$, on pose

$$g_{\mathbf{b}} := \sum_{\mathbf{a} \in \mathbf{b}} f_{\mathbf{a}} = \sum_{\overline{\gamma} \in \overline{H}} f_{\mathbf{a} \cdot \overline{\gamma}} \in \mathbb{C}(j, \{f_{\mathbf{a}}\}_{\mathbf{a} \in A}).$$

Théorème 2.2.1. — *Avec les notations précédentes, on a*

$$\mathfrak{M}(\Gamma) = \mathbb{C}(j, \{g_{\mathbf{b}}\}_{\mathbf{b} \in B}).$$

Démonstration. — Posons $M = \mathbb{C}(j, \{g_{\mathbf{b}}\}_{\mathbf{b} \in B})$. Pour tout $\overline{\gamma} \in \overline{H}$, relevé en $\gamma \in \mathbf{SL}_2(\mathbb{Z})$, on a

$$g_{\mathbf{b}}|_\gamma = \sum_{\overline{h} \in \overline{H}} (f_{\mathbf{a} \cdot \overline{h}}|_\gamma) = \sum_{\overline{h} \in \overline{H}} f_{\mathbf{a} \cdot \overline{h} \cdot \overline{\gamma}} = g_{\mathbf{b}}.$$

Donc $M \subset \mathfrak{M}(\Gamma(N))^{\overline{H}} = \mathfrak{M}(\Gamma)$. En fait, le sous-groupe $\overline{K}$ de $\mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ fixant M est *exactement* $\overline{H}$. En effet, on vient de voir que $\overline{H} \subset \overline{K}$; réciproquement, supposons qu'il existe un élément $\overline{k} \in \overline{K} \smallsetminus \overline{H}$, un élément $\mathbf{b} \in B$ est envoyé sur $\mathbf{b} \cdot \overline{k}$ sous l'action de $\overline{k}$. Comme $\overline{k} \notin \overline{H}$, on a $\mathbf{b} \cap (\mathbf{b} \cdot \overline{k}) = \varnothing$: ce qui montre que $g_{\mathbf{b}} \neq g_{\mathbf{b} \cdot \overline{k}}$, car les $f_{\mathbf{a}}$ sont distinctes pour $\mathbf{a} \in A$. Ce qui est contradictoire avec l'hypothèse que $\overline{K}$ fixe M.

Donc, $\overline{H}$ est le sous-groupe de $\mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ fixant M : par correspondance de Galois, M est exactement le sous-corps de $\mathfrak{M}(\Gamma(N))$ fixé par $\overline{H}$. Donc $M = \mathfrak{M}(\Gamma)$. □

2.3. Interprétation en termes de courbes elliptiques

Partons de la paramétrisation de Weierstrass d'une courbe elliptique sur $\mathbb{C}$: soit $\Lambda_\tau = \mathbb{Z}\tau \oplus \mathbb{Z}$ un réseau de $\mathbb{C}$, on considère la courbe elliptique

$$E^0_\tau : y^2 = 4x^3 - g_2(\tau)x - g_3(\tau).$$

Rappelons que la fonction $\wp(-; \Lambda_\tau)$ de Weierstrass du réseau Λ_τ donne un isomorphisme analytique de groupes

$$\Phi_0 : \mathbb{C}/\Lambda_\tau \to E^0_\tau, \quad z \bmod \Lambda_\tau \mapsto \begin{cases} \left(\wp(z; \Lambda_\tau), \wp'(z; \Lambda_\tau)\right) & \text{si } z \notin \Lambda_\tau \\ \infty & \text{si } z \in \Lambda_\tau. \end{cases}$$

Supposons que $\tau \in \mathfrak{H}$ soit tel que $j(\tau) \notin \{0, 1728\}$. Modifions la paramétrisation de E_τ^0 de la manière suivante : comme

$$j(\tau) = \frac{1728 g_2(\tau)^3}{g_2(\tau)^3 - 27 g_3(\tau)^2}$$

n'est ni 0 ni 1728, les valeurs $g_2(\tau)$ et $g_3(\tau)$ ne sont pas nulles. On choisit u, l'une des deux racines carrées de $g_2(\tau)/g_3(\tau)$ dans $\mathbb{C}$, et on réécrit la définition de $j(\tau)$ sous la forme

$$\frac{g_2(\tau)^3}{g_3(\tau)^2} = \frac{27 j(\tau)}{j(\tau) - 1728}.$$

Il est alors clair que le changement de variables

$$x = u^2 x' \qquad \text{et} \qquad y = u^3 y'$$

dans l'équation de Weierstrass de E_τ^0 transforme celle-ci en :

$$E_{j(\tau)} : y'^2 = 4x'^3 - \frac{27 j(\tau)}{j(\tau) - 1728} x' - \frac{27 j(\tau)}{j(\tau) - 1728}.$$

On remarque que l'équation obtenue est indépendante du choix de la racine carrée u. Les deux courbes elliptiques E_τ^0 et $E_{j(\tau)}$ sont donc isomorphes et ce procédé a transformé la paramétrisation Φ_0 en :

$$\Phi : \mathbb{C}/\Lambda_\tau \to E_{j(\tau)},\ z \bmod \Lambda_\tau \mapsto \begin{cases} \left(\frac{g_2(\tau)}{g_3(\tau)} \cdot \wp(z;\Lambda_\tau), \left(\frac{g_2(\tau)}{g_3(\tau)}\right)^{3/2} \cdot \wp'(z;\Lambda_\tau) \right) & \text{si } z \notin \Lambda_\tau \\ \infty & \text{si } z \in \Lambda_\tau. \end{cases}$$

Soit $N \in \mathbb{N}^*$. L'isomorphisme Φ se restreint en un isomorphisme sus les sous-groupes de N-torsion : les points de N-torsion de $\mathbb{C}/\Lambda_\tau$ s'écrivent sous la forme

$$(\mathbb{C}/\Lambda_\tau)[N] = \left\{ a\tau + b,\ (a,b) \in (N^{-1}\mathbb{Z})^2 \smallsetminus \mathbb{Z}^2 \right\} \cup \{0\}.$$

A droite les points de N-torsion sont donc :

$$E_{j(\tau)}[N] = \left\{ \Phi\left(a\tau + b\right),\ (a,b) \in (N^{-1}\mathbb{Z})^2 \smallsetminus \mathbb{Z}^2 \right\} \cup \{\infty\}.$$

Or, si on écrit $\mathbf{a} = (a,b)$, on a

$$\Phi(a\tau + b) = (P_\tau, Q_\tau) = \left(f_{\mathbf{a}}(\tau), \left(\frac{g_2(\tau)}{g_3(\tau)}\right)^{1/2} f_{\mathbf{a}}(\tau) \right).$$

Lorsque l'on change de choix de racine carrée de $g_2(\tau)/g_3(\tau)$, on transforme (P_τ, Q_τ) en $-(P_\tau, Q_\tau)$ (pour la structure de groupe sur $\mathbf{E}_{j(\tau)}$). Modulo ce choix, on vient de construire une base canonique de $E_{j(\tau)}[N]$:

Proposition 2.3.1. — *L'ensemble des coordonnées en x des points de N-torsion de la partie affine de la courbe elliptique $E_{j(\tau)}$ définie sur $\mathbb{C}$ par*

$$E_{j(\tau)} :\ y^2 = 4x^3 - \frac{27 j(\tau)}{j(\tau) - 1728} x - \frac{27 j(\tau)}{j(\tau) - 1728}$$

coïncident avec l'ensemble

$$\left\{ f_{\mathbf{a}}(\tau),\ \mathbf{a} \in A \right\}.$$

Démonstration. — Lorsque le couple $\mathbf{a} = (a,b)$ parcourt un ensemble de représentants de A dans $(N^{-1}\mathbb{Z})^2 \smallsetminus \mathbb{Z}^2$, les valeurs des fonctions $f_{\mathbf{a}}$ en τ sont toutes distinctes. Comme chaque $f_{\mathbf{a}}(\tau)$ est la première coordonnée d'un point de N-torsion de la partie affine de E_j, et que

$$\#\left\{f_{\mathbf{a}}(\tau)\right\} = \#A = \#\left((\mathbb{Z}/N\mathbb{Z}^2 \smallsetminus \{(0,0)\})/\{\pm 1\}\right) = \#\left\{x,\ (x,y) \in E_{j(\tau)}[N]\right\},$$

on conclut que les $f_{\mathbf{a}}(\tau)$ parcourent exactement les coordonnées en x des points de N-torsion de la partie affine de la courbe elliptique $E_{j(\tau)}$. □

On admet l'existence d'un « polynôme de division par N » (cf. [**DS05**, Chapter 7, §1]), ie. un polynôme universel $\mathcal{P}_N(X, A, B) \in \mathbb{Z}[X, A, B]$ tel que, pour tout $x, A, B \in \mathbb{C}$,

$$\mathcal{P}_N(x, A, B) = 0 \iff \begin{cases} x \text{ est la première coordonnée d'un point de } N\text{-torsion} \\ \text{de la partie affine de la courbe elliptique } y^2 = 4x^3 - Ax - B. \end{cases}$$

En particulier, pour la courbe $E_{j(\tau)}$ qu'on étudie, on a

$$\mathcal{P}_N\left(f_{\mathbf{a}}(\tau), \frac{27 j(\tau)}{j(\tau) - 1728}, \frac{27 j(\tau)}{j(\tau) - 1728}\right) = 0.$$

Or, cette relation polynômiale a lieu pour tout $\tau \in \mathfrak{H}$ tel que $j(\tau) \neq 0, 1728$ (c'est-à-dire pour tout τ sauf un nombre fini). Donc, elle a lieu pour *tout* $\tau \in \mathfrak{H}$! Autrement dit, dans le corps des fonctions méromorphes sur $X(N)$, on a

$$\mathcal{P}_N\left(f_{\mathbf{a}}, \frac{27j}{j-1728}, \frac{27j}{j-1728}\right) = 0$$

Plus précisément, considérons la fonction $\mathcal{P}_N\left(f_{\mathbf{a}}, \frac{27j}{j-1728}, \frac{27j}{j-1728}\right) \in \mathfrak{M}(\Gamma(N))$: pour tout $\tau \in \mathfrak{H}$ tel que $j(\tau) \neq 0, 1728$, la courbe $\mathbf{E}_j$ se spécialise en une courbe elliptique $\mathbf{E}_{j(\tau)}$ sur $\mathbb{C}$, et les $f_{\mathbf{a}}$ se spécialisent en $\{f_{\mathbf{a}}(\tau)\}$ qui donnent exactement les premières coordonnées des points de N-torsion de $\mathbf{E}_{j(\tau)}[N]$, on a donc $\mathcal{P}_N\left(f_{\mathbf{a}}(\tau), \frac{27j(\tau)}{j(\tau)-1728}, \frac{27j(\tau)}{j(\tau)-1728}\right) = 0$. Ainsi, la fonction méromorphe $\mathcal{P}_N\left(f_{\mathbf{a}}, \frac{27j}{j-1728}, \frac{27j}{j-1728}\right)$ admet une infinité de zéros sur la surface de Riemann compacte $X(N)$: c'est donc la fonction nulle.

Par conséquent, lorsque l'on considère la courbe elliptique $\mathbf{E}_j$ définie sur $\mathbb{C}(j)$ par

$$\mathbf{E}_j : \ y^2 = 4x^3 - \frac{27j}{j-1728}x - \frac{27j}{j-1728}$$

et que l'on note $x(\mathbf{E}_j[N])$, l'ensemble des premières coordonnées des points de N-torsion de $\mathbf{E}_j$ dans une clôture algébrique $\overline{\mathbb{C}(j)}$ de $\mathbb{C}(j)$ contenant $\mathfrak{M}(\Gamma(N))$, les fonctions $f_{\mathbf{a}}$ (pour $\mathbf{a}$ parcourant A) décrivent exactement $x(\mathbf{E}_j[N])$! Ainsi, les propositions précédentes et la discussion ci-dessus montrent que

Corollaire 2.3.2. — *On a*

$$\mathfrak{M}(\Gamma(N)) = \mathbb{C}(j, x(\mathbf{E}_j[N])).$$

De plus, l'extension $\mathbb{C}(j, x(\mathbf{E}_j[N]))/\mathbb{C}(j)$ est galoisienne de groupe de Galois

$$\mathrm{Gal}\left(\mathbb{C}(j, x(\mathbf{E}_j[N]))/\mathbb{C}(j)\right) \simeq \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}.$$

Pour éliminer le quotient par $\{\pm I\}$ dans ce groupe de Galois, il suffit de rajouter les deuxièmes coordonnées des points de N-torsion de $\mathbf{E}_j[N]$:

Proposition 2.3.3. — *L'extension de corps $\mathbb{C}(j, \mathbf{E}_j[N])/\mathbb{C}(j)$ est galoisienne, de groupe de Galois*

$$\mathrm{Gal}\left(\mathbb{C}(j, \mathbf{E}_j[N])/\mathbb{C}(j)\right) \simeq \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

De plus, un isomorphisme est donné par la restriction de la représentation de N-torsion de $\mathbf{E}_j$,

$$\rho_{\mathbf{E}_j,N} : \mathrm{Gal}\left(\overline{\mathbb{C}(j)}/\mathbb{C}(j)\right) \longrightarrow \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

dans la base $\left(\left(f_{(1,0)}, (g_2/g_3)^{1/2} \cdot f_{(1,0)}\right), \left(f_{(0,1)}, (g_2/g_3)^{1/2} \cdot f_{(0,1)}\right)\right)$.

Démonstration. — On adjoint à $\mathbb{C}(j, x(\mathbf{E}_j[N]))$ les deuxièmes coordonnées $y(\mathbf{E}_j[N])$ des points de N-torsion de $\mathbf{E}_j[N]$: en termes de fonctions, cela revient à considérer l'extension engendrée (dans une clôture algébrique $\overline{\mathbb{C}(j)}$) sur $\mathbb{C}(j)$ par les $f_{\mathbf{a}}$ et les $g_{\mathbf{a}} := (g_2/g_3)^{1/2} f_{\mathbf{a}}$, pour chaque choix de la racine carrée (c'est ce qu'on a vu dans la discussion ci-dessus). Considérons alors la tour de corps suivante :

$$\mathbb{C}(j) \subset \mathbb{C}(j, x(\mathbf{E}_j[N])) \subset \mathbb{C}(j, \mathbf{E}_j[N]) \subset \overline{\mathbb{C}(j)}.$$

- L'extension $\mathbb{C}(j, \mathbf{E}_j[N])/\mathbb{C}(j)$ est galoisienne. C'est un fait général que l'on a rappelé au Chapitre 1.
- Fixons une $\mathbb{Z}/N\mathbb{Z}$-base (P_1, P_2) de $\mathbf{E}_j[N]$: on choisit celle définie par

$$P_1 = \left(f_{(1,0)}, \left(\frac{g_2}{g_3}\right)^{1/2} \cdot f_{(1,0)}\right), \qquad P_2 = \left(f_{(0,1)}, \left(\frac{g_2}{g_3}\right)^{1/2} \cdot f_{(0,1)}\right).$$

  Il s'agit de voir que la représentation

$$\rho_{\mathbf{E}_t,N} : \mathrm{Gal}\left(\overline{\mathbb{C}(j)}/\mathbb{C}(j)\right) \longrightarrow \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

  fournit un isomorphisme

$$\mathrm{Gal}\left(\mathbb{C}(j, \mathbf{E}_j[N])/\mathbb{C}(j)\right) \simeq \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

  Comme $\mathbb{C}(j)$ contient toutes ses racines N-ièmes de l'unité, on sait déjà qu'on a une injection :

$$\rho_{\mathbf{E}_t,N} : \mathrm{Gal}\left(\mathbb{C}(j, \mathbf{E}_j[N])/\mathbb{C}(j)\right) \hookrightarrow \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

  Pour alléger les notations, on pose $H = \mathrm{Gal}\left(\mathbb{C}(j, \mathbf{E}_j[N])/\mathbb{C}(j)\right)$ et $K = \mathrm{Gal}\left(\mathbb{C}(j, \mathbf{E}_j[N])/\mathbb{C}(j, x(\mathbf{E}_j[N]))\right)$. L'action de K sur $\mathbf{E}_j[N]$ fixe les premières coordonnées des points de $\mathbf{E}_j[N]$. Or, deux points de N-torsion qui ont même première coordonnée sont égaux ou opposés (ceci découle du calcul explicite de la loi de groupe sur

une courbe elliptique en fonction des coordonnées). Ainsi, si $\sigma \in K$, on a ${}^{\sigma}P_1 = \pm P_1$ et ${}^{\sigma}P_2 = \pm 1$, c'est-à-dire que l'on a

$$\begin{pmatrix} {}^{\sigma}P_1 \\ {}^{\sigma}P_2 \end{pmatrix} = \rho_{\mathbf{E}_j,N}(\sigma) \cdot \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \begin{pmatrix} \pm P_1 \\ \pm P_2 \end{pmatrix} = \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \cdot \begin{pmatrix} P_1 \\ P_2 \end{pmatrix}.$$

Comme de plus $\rho_{\mathbf{E}_j,N}(\sigma) \in \mathbf{SL}_2(\mathbb{Z})$, on conclut que $\rho_{\mathbf{E}_j,N}(\sigma) = \pm I$.

Réciproquement, si $\rho_{\mathbf{E}_j,N}(\sigma) = \pm I$ pour un automorphisme $\sigma \in H$, alors ${}^{\sigma}P = \pm P$ pour tout point $P \in \mathbf{E}_j[N]$. Donc σ est un élément de K. On vient de montrer que K est exactement $\rho_{\mathbf{E}_j,N}{}^{-1}(\{\pm I\})$.

Comme $\rho_{\mathbf{E}_j,N}$ est injective, K est de cardinal $\#K \leqslant 2$; de plus, on a montré (Corollaire 2.3.2) que

$$\mathrm{Gal}\left(\mathbb{C}(j, x(\mathbf{E}_j[N]))/\mathbb{C}(j)\right) \simeq \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}.$$

Ainsi, on a $\#H = \#\big(\mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}\big) \cdot \#K$ et on en déduit que

$$[\mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z}) : \rho_{\mathbf{E}_j,N}(H)] \leqslant 2.$$

Supposons que l'on ait $[\mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z}) : \rho_{\mathbf{E}_j,N}(H)] = 2$, alors K est réduit à $\{1\}$ et $-I \notin \rho_{\mathbf{E}_j,N}(H)$. Cependant, on a $\{\pm I\} \cdot \rho_{\mathbf{E}_j,N}(H) = \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})$, donc l'une des matrices $\pm \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ appartient à l'image $\rho_{\mathbf{E}_j,N}(H)$. Mais on a alors

$$-I = \left(\pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right)^2 \in \rho_{\mathbf{E}_j,N}(H).$$

Ce qui est contradictoire ! La seule possibilité est donc que l'on ait $[\mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z}) : \rho_{\mathbf{E}_j,N}(H)] = 1$.
Finalement, $\rho_{\mathbf{E}_j,N}(H) = \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})$ et l'on a bien démontré l'isomorphisme souhaité. □

Proposition 2.3.4. — *On pose $\zeta_N = \mathrm{e}^{2i\pi/N}$. La base*

$$(P_1, P_2) = \left(\left(f_{(1,0)}, (g_2/g_3)^{1/2} \cdot f_{(1,0)}\right), \left(f_{(0,1)}, (g_2/g_3)^{1/2} \cdot f_{(0,1)}\right)\right)$$

de $\mathbf{E}_j[N]$ construite dans la preuve ci-dessus est une ζ_N-structure sur $\mathbf{E}_j$.

Démonstration. — Remarquons que le résultat ne dépend pas du choix de la racine carrée de (g_2/g_3) : passer d'un choix à l'autre change (P_1, P_2) en $(-P_1, -P_2)$, comme l'accouplement de Weil est bilinéaire, on a $d(\left(\begin{smallmatrix} P_1 \\ P_2 \end{smallmatrix}\right)) = d(\left(\begin{smallmatrix} -P_1 \\ -P_2 \end{smallmatrix}\right))$.

Soit $\tau \in \mathfrak{H}$ tel que $j(\tau) \neq 0, 1728$. Par construction, la base (P_1, P_2) de $\mathbf{E}_j[N]$ fournit une base $\mathcal{B}_\tau$ de $E_{j(\tau)}[N]$. Cette base $\mathcal{B}_\tau$ est une ζ_N-structure car elle correspond, via la paramétrisation de Weierstrass modifiée (cf. Section 2.3), à la ζ_N-structure $(\frac{\tau}{N} \bmod \Lambda_\tau, \frac{1}{N} \bmod \Lambda_\tau)$ de $\mathbb{C}/\Lambda_\tau$. Donc $d(\mathcal{B}_\tau) = \zeta_N$ pour tout $\tau \in \mathfrak{H}$ tel que $j(\tau) \neq 0, 1728$. Il s'agit d'une relation polynomiale qui a lieu en une infinité de points, donc $d(\mathcal{B}_\tau) = \zeta_N$ pour tout $\tau \in \mathfrak{H}$. Par conséquent, $d(\left(\begin{smallmatrix} P_1 \\ P_2 \end{smallmatrix}\right)) = \zeta_N$. □

2.4. Les courbes modulaires comme courbes projectives sur $\mathbb{C}$

Les courbes $X(N)$ ont été définies au Chapitre 1 comme des surfaces de Riemann :

$$X(N) = \Gamma(N)\backslash\mathfrak{H}^*.$$

On a alors noté $\mathfrak{M}(\Gamma(N))$ des fonctions méromorphes sur $X(N)$. On vient de voir que

$$\mathfrak{M}(\Gamma(N)) = \mathbb{C}(j, \{f_{\mathbf{a}}\})$$

et que l'extension $\mathfrak{M}(\Gamma(N))/\mathfrak{M}(\Gamma(1))$ était galoisienne finie. Comme $\mathbb{C}(j)$ est une extension transcendante de $\mathbb{C}$, de degré de transcendance 1, $\mathfrak{M}(\Gamma(N))/\mathbb{C}$ est une extension de degré de transcendance 1, et engendrée par un nombre fini de générateurs. C'est donc un corps de fonction au sens de la définition suivante :

Définition 2.4.1. — Soit k un corps, on appelle *corps de fonctions sur k* toute extension finiment engendrée K/k de degré de transcendance 1 et telle que k soit algébriquement clos dans K, autrement dit $K \cap \overline{k} = k$.

Rappelons alors que l'on a (voir par exemple [**Har77**, Theorem I.6.9]) :

Théorème 2.4.2. — *Il y a une bijection fonctorielle entre*

$$\left\{\begin{array}{c}\textit{Classes de conjugaison de} \\ \textit{corps de fonctions sur } k\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\textit{Classes d'isomorphisme de} \\ \textit{courbes projectives lisses sur } k\end{array}\right\}$$

On munira maintenant $X(N)$ de cette structure de courbe algébrique. Le corps des fonctions rationnelles sur $X(N)$ (vue comme courbe algébrique) est égal au corps des fonctions méromorphes sur $X(N)$ (vue comme surface de Riemann).

CHAPITRE 3

PASSAGE DE $\mathbb{C}$ À $\mathbb{Q}$

Rappel :

Définition 3.0.3. — Soit $\Gamma \subset \mathbf{SL}_2(\mathbb{Z})$, un sous-groupe de congruences. On note $\mathfrak{M}(\Gamma)$, le corps des fonctions méromorphes sur la surface de Riemann $X(\Gamma) = \Gamma\backslash\mathfrak{H}^*$. De manière équivalente, $\mathfrak{M}(\Gamma)$ est le corps des fonctions méromorphes $f : \mathfrak{H} \to \mathbb{C}$, invariantes par Γ et qui sont méromorphes aux pointes.

Comme $X(\Gamma)$ est une surface de Riemann compacte, on peut lui donner une structure $X_{alg}(\Gamma)$ de courbe algébrique projective lisse sur $\mathbb{C}$. Un moyen de caractériser (à isomorphisme birationnel près) cette structure de variété algébrique est d'imposer que le corps des fonctions rationnelles sur $X_{alg}(\Gamma)$ soit le corps $\mathfrak{M}(\Gamma)$.

Dans la suite, on s'intéresse aux propriétés géométrico-arithmétiques de $X_{alg}(\Gamma)$: il serait donc bon d'en faire une variété algébrique sur $\mathbb{Q}$ (ie. une variété algébrique sur $\overline{\mathbb{Q}}$ définie par des équations à coefficients dans $\mathbb{Q}$). Pour ce faire, nous allons d'abord "décomposer" $\mathfrak{M}(\Gamma)$ en un produit de corps

$$\mathfrak{M}(\Gamma) = \mathbb{C} \cdot \mathscr{M}_\Gamma$$

où $\mathscr{M}_\Gamma$ pourra être considéré comme le corps des fonctions rationnelles d'une variété algébrique lisse sur $\overline{Q}$. Il nous faut aussi définir des actions de groupes de Galois pour espérer redescendre à une variété définie sur $\mathbb{Q}$.

3.1. Les corps $\mathscr{M}_\Gamma$

Soit N un entier non nul.

Définition 3.1.1. — Soit $f \in \mathfrak{M}(\Gamma)$ et $K/\mathbb{Q}$ une sous-extension de corps de $\mathbb{Q}(\mu_N)/\mathbb{Q}$. On dit que f *est définie sur* K si les développements en série de Fourier de f aux pointes sont tous à coefficients dans K. On notera $\mathscr{M}_N^{(K)}$ leur ensemble. Par souci de légèreté des notations, on notera $\mathscr{M}_\Gamma$ l'ensemble $\mathscr{M}_\Gamma^{(\mathbb{Q}(\mu_N))}$ et on désignera $\mathscr{M}_{\Gamma(N)}^{(\mathbb{Q}(\mu_N))}$ par $\mathscr{M}_N$.

Plus précisément, si $f \in \mathfrak{M}(\Gamma)$, on peut lui associer son développement à la pointe ∞ :

$$\sum a_n^{(0)} \left(q^{1/h}\right)^n \in \mathbb{C}[[q^{1/h}]]$$

où h désigne la largeur de la pointe ∞. Et on peut faire de même pour toutes les autres pointes de $X(\Gamma)$: si $c = \gamma^{-1} \cdot \infty \in X(\Gamma)$ est une pointe de largeur h_c :

$$f\,|_\gamma = \sum a_n^{(\gamma)} \left(q^{1/h_c}\right)^n \in \mathbb{C}[[q^{1/h'}]]$$

Alors, $f \in \mathscr{M}_\Gamma$ signifie exactement que tous les coefficients $a_n^{(\gamma)}$ sont éléments de $\mathbb{Q}(\mu_N)$.

Exemple 3.1.2. — L'invariant j est défini sur $\mathbb{Q} = \mathbb{Q}(\mu_1)$. Les fonctions de Siegel, qu'on définira au Chapitre 5, sont aussi définies sur $\mathbb{Q}(\mu_N)$.

Lemme 3.1.3. — *Soit* $\mathbf{a} \in (N^{-1}\mathbb{Z})^2 \smallsetminus \mathbb{Z}^2$. *La* $\mathbf{a}$*-ième fonction de Weber* $f_{\mathbf{a}}$ *est définie sur* $\mathbb{Q}(\mu_N)$.

Démonstration. — Pour tout $\gamma \in \mathbf{SL}_2(\mathbb{Z})$ et tout $\mathbf{a} = (a, b) \in (N^{-1}\mathbb{Z})^2 \smallsetminus \mathbb{Z}^2$, on a $f_{\mathbf{a}}\,|_\gamma = f_{\mathbf{a}\cdot\gamma}$ (Proposition 2.1.4). Il suffit donc de montrer que le développement en série de Fourier à l'infini de toutes les $f_{\mathbf{a}}$ est à coefficients dans $\mathbb{Q}(\mu_N)$. Mais on a vu au Lemme 2.1.3 que

$$\forall \tau \in \mathfrak{H}, \quad f_{(a,b)}(\tau) = \frac{1}{12} - 2\sum_{n=1}^{\infty} \frac{nq^{Nn}}{1-q^{Nn}} + \frac{{\zeta_N}^b q^a}{1-{\zeta_N}^b q^a} + \sum_{n=1}^{\infty} \frac{nq^n\left({\zeta_N}^{bn} q^{an} + {\zeta_N}^{-bn} q^{-an}\right)}{1-q^n}$$

où $\zeta_N = \mathrm{e}^{2i\pi/N} \in \mathbb{Q}(\mu_N)$. □

3.1.1. Générateurs de $\mathscr{M}_N$. — Pour utiliser cette notion, nous aurons besoin du lemme suivant :

***Lemme 3.1.4* (Restriction des scalaires).** — *Soit $K/\mathbb{Q}$, une sous-extension de $\mathbb{Q}(\mu_N)/\mathbb{Q}$. Supposons avoir fixé un ensemble S tel que*

$$\mathfrak{M}(\Gamma(N)) = \mathbb{C}(S) \qquad et \qquad S \subset \mathscr{M}_N^{(K)}.$$

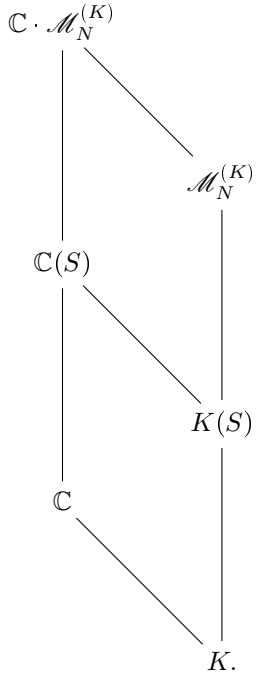
Alors S engendre $\mathscr{M}_N^{(K)}$ sur K, ie. on a :

$$\mathscr{M}_N^{(K)} = K(S).$$

Démonstration. — Montrons d'abord que $\mathbb{C}$ et $K(S)$ sont linéairement disjoints sur K : soit $\gamma_1, \dots, \gamma_m$ des éléments de $\mathbb{C}$ qui sont linéairement indépendants sur K. Supposons qu'on aie une relation $\sum_{k=1}^m \gamma_k f_k = 0$, avec des fonctions $f_k \in \mathscr{M}_N^{(K)}$: on écrit $f_k = \sum_{n=-\infty}^{\infty} c_{k,n} q^{n/h}$ avec $c_{k,n} \in K$. Alors on a,

$$\sum_{k=1}^m \gamma_k f_k = \sum_{k=1}^m \gamma_k \cdot \sum_{n=-\infty}^{\infty} c_{k,n} q^{n/h} = \sum_{n=-\infty}^{\infty} \left(\sum_{k=1}^m c_{k,n} \gamma_k \right) q^{n/h} = 0.$$

Et ceci impose que, pour tout $n \in \mathbb{Z}$, on aie $\sum_{k=1}^m c_{k,n}\gamma_k = 0$. Or, les $\gamma_k \in \mathbb{C}$ ont été choisis de sorte qu'ils soient indépendants sur K. D'où $c_{k,n} = 0$ pour tout k, n. Donc $f_1 = \cdots = f_m = 0$. Ce qui prouve que $\mathbb{C}$ et $K(S)$ sont linéairement disjoints sur K. On a donc un diagramme de corps comme suit :



Finalement, on a les inégalités suivantes :

$$1 \leqslant [\mathscr{M}_N^{(K)} : K(S)] \leqslant [\mathbb{C} \cdot \mathscr{M}_N^{(K)} : \mathbb{C}(S)] \leqslant [\mathfrak{M}(\Gamma(N)) : \mathfrak{M}(\Gamma(N))] = 1$$

car $\mathbb{C}$ et $K(S)$ sont linéairement disjoints sur K. □

A partir de ce lemme, on déduit directement les trois propositions suivantes :

Proposition 3.1.5. — *On a $\mathscr{M}_1 = \mathbb{Q}(j)$.*

Démonstration. — À partir de l'égalité $\mathfrak{M}(\mathbf{SL}_2(\mathbb{Z})) = \mathbb{C}(j)$, il suffit d'utiliser le lemme avec

$$N = 1, \quad K = \mathbb{Q} \quad \text{et} \quad S = \{j\} \subset \mathscr{M}_1^{(\mathbb{Q})}.$$

□

Proposition 3.1.6. — *On a $\mathscr{M}_N = \mathbb{Q}(\mu_N, j, \{f_{\mathbf{a}}\})$.*

Démonstration. — On sait que $\mathfrak{M}(\Gamma(N)) = \mathbb{C}(j, \{f_{\mathbf{a}}\})$ et on utilise le lemme avec

$$K = \mathbb{Q}(\mu_N) \quad \text{et} \quad S = \{j\} \cup \{f_{\mathbf{a}}, \mathbf{a} \in A\} \subset \mathscr{M}_N.$$

On obtient que $\mathscr{M}_N = \mathbb{Q}(\mu_N)(j, \{f_{\mathbf{a}}\})$. □

Proposition 3.1.7. — *Si l'on reprend les notations du Théorème 2.2.1, on a $\mathscr{M}_\Gamma = \mathbb{Q}(\mu_N, j, \{g_{\mathbf{b}}\})$.*

Démonstration. — Au Théorème 2.2.1, on a montré que $\mathfrak{M}(\Gamma) = \mathbb{C}(j, \{g_{\mathbf{b}}\})$. On applique le lemme de restriction avec

$$K = \mathbb{Q}(\mu_N), \quad \text{et} \quad S = \{j\} \cup \{g_{\mathbf{b}}, \mathbf{b} \in A/\overline{H}\} \subset \mathscr{M}_\Gamma.$$

□

On montrera plus loin un résultat plus précis pour $\mathscr{M}_\Gamma$.

3.1.2. Action galoisienne. — Dans le cas complexe, on avait vu que $\mathfrak{M}(\Gamma(N)) = \mathbb{C}(j, \{f_{\mathbf{a}}\})$ (où les $f_{\mathbf{a}}$ sont les fonctions de Weber) et que

$$\mathrm{Gal}(\mathfrak{M}(\Gamma(N))/\mathfrak{M}(\Gamma(1))) \simeq \mathbf{SL}_2(\mathbb{Z})/\pm\Gamma(N) \simeq \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}.$$

On pourrait obtenir le même résultat dans le cas d'un corps de base quelconque (ici $\mathbb{Q}$ ou $\mathbb{Q}(\mu_N)$) : la seule différence tient à l'absence (partielle) de racines N-ièmes de l'unité.

Décrivons plus explicitement l'action de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ sur $\mathscr{M}_N$:

- L'action de $\mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ sur $\mathfrak{M}(\Gamma(N))$ se restreint en une action sur $\mathscr{M}_N$: on considère d'abord l'action de $\mathbf{SL}_2(\mathbb{Z})$ sur $\mathscr{M}_N$ par « composition » :

  $$\forall \alpha \in \mathbf{SL}_2(\mathbb{Z}), \forall f \in \mathscr{M}_N, \qquad f \mapsto f|_\alpha \,.$$

  Comme $-I \in \mathbf{SL}_2(\mathbb{Z})$ agit trivialement sur $\mathfrak{H}$, et que $f \in \mathscr{M}_N$ est $\Gamma(N)$-invariante, cette action se factorise par $\pm\Gamma(N)$ pour donner une action de $\mathbf{SL}_2(\mathbb{Z})/\pm\Gamma(N) \simeq \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ sur $\mathscr{M}_N$. Remarquons que, par définition de $\mathscr{M}_N$, pour toute fonction $f \in \mathscr{M}_N$, la fonction « translatée » $f|_\alpha$ est aussi dans $\mathscr{M}_N$. Vue en terme d'opération sur les développements en séries de Fourier, cette action est donnée par

  $$\forall \alpha \in \mathbf{SL}_2(\mathbb{Z}), \forall \tau \in \mathfrak{H}, \qquad q_\tau \mapsto q_{\alpha\cdot\tau}.$$

- Définissons comme suit une action de $G_N = \{\left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right),\ d \in (\mathbb{Z}/N\mathbb{Z})^\times\}$ sur $\mathscr{M}_N$: soit $\left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right)$, il existe un automorphisme $\sigma_d \in \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$ uniquement déterminé par la condition que $\forall \zeta \in \mu_N, \sigma_d(\zeta) = \zeta^d$. Alors σ_d s'étend en un automorphisme de $\mathscr{M}_N$ par la formule

  $$\sigma_d\left(\sum_n a_n q^{n/N}\right) := \sum_n \sigma_d(a_n) q^{n/N}.$$

  On pose donc :

  $$\begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix} \star \left(\sum_n a_n q^{n/N}\right) := \sum_n \sigma_d(a_n) q^{n/N}.$$

- Enfin, on remarque que $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z}) \simeq G_N \cdot \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})$ où $G_N = \{\left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right),\ d \in (\mathbb{Z}/N\mathbb{Z})^\times\}$. Et cette décomposition passe au quotient par $\{\pm I\}$: c'est-à-dire que l'on a

  $$\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\} \simeq G_N \cdot \Big(\mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}\Big).$$

  On peut donc utiliser cette décomposition pour définir une action de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ sur $\mathscr{M}_N$: pour $\alpha \in \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$, on peut écrire $\alpha = \left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right) \cdot \alpha_0$ où $\left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right) \in G_N$ et $\alpha_0 \in \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$, on pose

  $$\forall f = \sum_n a_n {q_\tau}^{n/N} \in \mathscr{M}_N, \qquad \alpha \bullet \left(\sum_n a_n {q_\tau}^{n/N}\right) := \sum_n \sigma_d(a_n) \cdot {q_{\alpha_0\cdot\tau}}^{n/N}.$$

Avec cette définition, on a

Théorème 3.1.8. — *L'extension de corps $\mathscr{M}_N/\mathscr{M}_1$ est galoisienne, de groupe de Galois,*

$$\mathrm{Gal}(\mathscr{M}_N/\mathscr{M}_1) \simeq \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}.$$

Démonstration. — Comme $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ agit sur $\mathscr{M}_N$, on a un morphisme

$$\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\} \longrightarrow \mathrm{Aut}(\mathscr{M}_N).$$

Or, le sous-corps de $\mathscr{M}_N$ fixé par $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ est exactement $\mathscr{M}_1$. En effet, si $f = \sum a_n {q_\tau}^{n/N}$ est fixée par l'action $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$, alors :

- L'action de $\mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ est triviale, ie. $f|_\gamma = f$ pour tout $\gamma \in \mathbf{SL}_2(\mathbb{Z}/)\mathbb{Z}$. Donc f est une fonction modulaire de niveau 1 : $f \in \mathfrak{M}(\Gamma(1)) = \mathbb{C}(j)$. Comme f est astreinte à avoir des coefficients de Fourier dans $\mathbb{Q}(\mu_N)$, on a même $f = \sum a_n {q_\tau}^n \in \mathbb{Q}(\mu_N)(j)$.
- Mais l'action de G_N sur f est, elle aussi, triviale. C'est-à-dire que $\sigma_d(a_n) = a_n$ pour tout $\sigma_d \in \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$: les coefficients de Fourier de f sont donc $\mathbb{Q}$-rationnels. Par définition cela signifie que $f \in \mathscr{M}_1$.

Et réciproquement, il est clair que $\mathscr{M}_1$ est fixé par $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$.

Dès lors, par théorie de Galois, l'extension $\mathscr{M}_N/\mathscr{M}_1$ est galoisienne, de groupe de Galois isomorphe à $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$. □

Au cours de la preuve ci-dessus, on a même montré que

Corollaire 3.1.9. — *L'extension $\mathscr{M}_N/\mathbb{Q}(\mu_N, j)$ est galoisienne, de groupe de Galois,*

$$\mathrm{Gal}(\mathscr{M}_N/\mathbb{Q}(\mu_N, j)) \simeq \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\} \simeq \mathrm{Gal}(\mathfrak{M}(\Gamma(N))/\mathfrak{M}(\Gamma(1))).$$

C'est la partie « géométrique » du groupe de Galois $\mathrm{Gal}(\mathscr{M}_N/\mathscr{M}_1)$; la partie « arithmétique » est décrite par la proposition suivante :

Proposition 3.1.10. — *On a*

$$\mathrm{Gal}(\mathbb{Q}(\mu_N, j)/\mathscr{M}_1) \simeq \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \simeq (\mathbb{Z}/N\mathbb{Z})^\times$$

Démonstration. — On part de la suite exacte

$$1 \longrightarrow \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\} \longrightarrow \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\} \longrightarrow (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow 1,$$

dans laquelle on remplace les groupes de matrices par des groupes de Galois (selon le Théorème 3.1.8 et le Corollaire 3.1.9) : on obtient

$$1 \longrightarrow \mathrm{Gal}(\mathscr{M}_N/\mathbb{Q}(\mu_N, j)) \longrightarrow \mathrm{Gal}(\mathscr{M}_N/\mathscr{M}_1) \longrightarrow (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow 1.$$

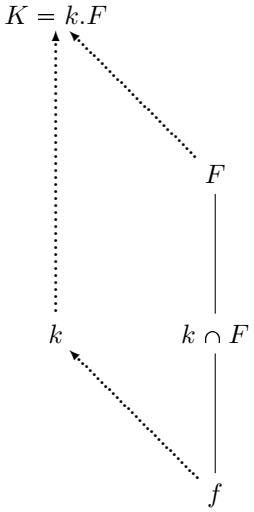
Par théorie de Galois, ceci est équivalent à dire que la sous-extension $\mathbb{Q}(\mu_N, j)/\mathscr{M}_1$ de $\mathscr{M}_N/\mathscr{M}_1$ est galoisienne de groupe de Galois isomorphe à $(\mathbb{Z}/N\mathbb{Z})^\times$. □

***Lemme 3.1.11* (Restriction des groupes de Galois)**. — *Soit k/f et F/f deux sous-extensions de corps d'une extension K/f. On suppose que $K = k.F$ et que F/f est galoisienne. Dans cette situation, K/k est galoisienne et il existe une injection naturelle*

$$\mathrm{Gal}(K/k) \hookrightarrow \mathrm{Gal}(F/f)$$

d'image $\mathrm{Gal}(F/k \cap F)$.

La situation est la suivante :



Les traits plein correspondent à des extensions supposées galoisiennes.

Démonstration. — Commençons par montrer que K/k est bien une extension galoisienne : soit $\sigma : K \to \overline{K}$, un morphisme de corps fixant k. On peut restreindre σ en $\sigma' : F \to \overline{F}$, un morphisme fixant $k \cap F$. Vu que l'extension $F/k \cap F$ est galoisienne, la restriction σ' est en fait un automorphisme $\sigma' : F \to F$. Dès lors, comme $K = k.F$ et que σ agit trivialement sur k et via σ' sur F, le morphisme "recollé" $\sigma : K \to \overline{K}$ est en fait à valeurs dans K. Ainsi, K/k est galoisienne.

En outre, on vient de voir l'existence d'un morphisme de groupes

$$r : \mathrm{Gal}(K/k) \to \mathrm{Gal}(F/k \cap F) \hookrightarrow \mathrm{Gal}(F/f)$$

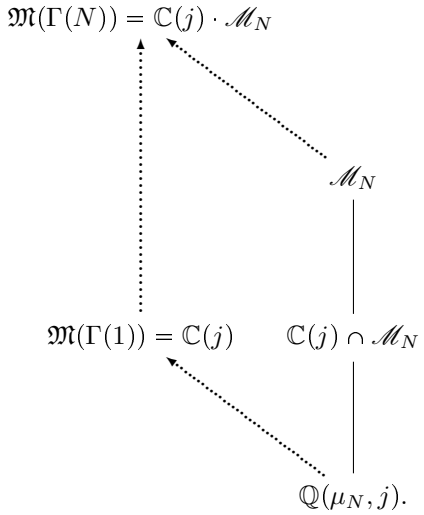
qui à σ associe sa resctriction σ' comme ci-dessus. Si la restriction $\sigma' = r(\sigma)$ d'un élément $\sigma \in \mathrm{Gal}(K/k)$ est triviale, alors σ' fixe non seulement $k \cap F$, mais F tout entier. En conséquence, σ fixe k (par définition) et F (car σ agit comme σ' sur F) et par suite, σ fixe $K = k.F$. Donc $\sigma = 1 \in \mathrm{Gal}(K/k)$. Donc r est bien injectif.

Enfin, on sait que le sous-corps de K fixé par $\mathrm{Gal}(K/k)$ est k : on voit donc immédiatement que le sous-corps de F fixé par $r(\mathrm{Gal}(K/k))$ est $k \cap F$. Ce qui prouve que r envoie surjectivement $\mathrm{Gal}(K/k)$ dans $\mathrm{Gal}(F/k \cap F)$. □

Proposition 3.1.12. — *La clôture algébrique de $\mathbb{Q}$ dans $\mathscr{M}_N$ est $\mathbb{Q}(\mu_N)$: autrement dit, on a*

$$\mathscr{M}_N \cap \overline{\mathbb{Q}} = \mathbb{Q}(\mu_N).$$

Démonstration. — Appliquons le lemme précédent à la situation suivante :



Le lemme affirme qu'on a un isomorphisme :

$$\mathrm{Gal}(\mathfrak{M}(\Gamma(N))/\mathfrak{M}(\Gamma(1))) \xrightarrow{\sim} \mathrm{Gal}(\mathscr{M}_N/\mathbb{C}(j) \cap \mathscr{M}_N) \hookrightarrow \mathrm{Gal}(\mathscr{M}_N/\mathbb{Q}(\mu_N, j)).$$

Or, on peut compléter ce diagramme de chaque côté avec les Théorèmes 1.3.4 et 3.1.9 :

$$\mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\} \simeq \mathrm{Gal}(\mathfrak{M}(\Gamma(N))/\mathfrak{M}(\Gamma(1))) \xrightarrow{\sim} \mathrm{Gal}(\mathscr{M}_N/\mathbb{C}(j)\cap\mathscr{M}_N) \hookrightarrow \mathrm{Gal}(\mathscr{M}_N/\mathbb{Q}(\mu_N, j)) \simeq \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}.$$

Donc $\mathrm{Gal}(\mathscr{M}_N/\mathbb{C}(j) \cap \mathscr{M}_N) \simeq \mathrm{Gal}(\mathscr{M}_N/\mathbb{Q}(\mu_N, j))$. Ainsi, on a

$$\mathbb{C}(j) \cap \mathscr{M}_N = \mathbb{Q}(\mu_N, j).$$

La fonction j est transcendante sur $\mathbb{C}$ donc, a fortiori, elle l'est sur $\mathbb{Q}$. En particulier, $j \notin \overline{\mathbb{Q}}$ et lorsqu'on intersecte la dernière égalité avec $\overline{\mathbb{Q}}$, on trouve

$$\overline{\mathbb{Q}} \cap \mathscr{M}_N = \overline{\mathbb{Q}} \cap \mathbb{C}(j) \cap \mathscr{M}_N = \overline{\mathbb{Q}} \cap \mathbb{Q}(\mu_N, j) = \mathbb{Q}(\mu_N).$$

□

Corollaire 3.1.13. — *L'extension $\mathscr{M}_N/\mathbb{Q}(\mu_N)$ est un corps de fonctions.*

3.1.3. Générateurs de $\mathscr{M}_\Gamma$. — Soit G, un sous-groupe de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$ contenant $-I$, on note $H = G \cap \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})$ et Γ le relevé à $\mathbf{SL}_2(\mathbb{Z})$ de H. Alors Γ est un sous-groupe de congruences de niveau N de $\mathbf{SL}_2(\mathbb{Z})$.

L'action de $\overline{G} := G/\{\pm I\}$ sur $\mathscr{M}_N/\mathscr{M}_1$ (définie à la section 3.1.2) induit une action de $\overline{G}$ sur $\mathbb{Q}(\mu_N)/\mathbb{Q}$ via le déterminant :

$$\forall \overline{g} \in \overline{G}, \forall \zeta \in \mathbb{Q}(\mu_N), \qquad \det \overline{g} : \zeta \mapsto \zeta^{\det g}.$$

D'autre part, on définit $B := A/\overline{G}$, et pour tout $\mathbf{b} = \mathbf{a} \cdot \overline{G} \in B$, on pose

$$g_{\mathbf{b}} = \sum_{\mathbf{a} \in \mathbf{b}} f_{\mathbf{a}} = \sum_{\overline{g} \in \overline{G}} f_{\mathbf{a} \cdot \overline{g}}$$

Proposition 3.1.14. — *Avec ces notations, les fonctions $g_{\mathbf{b}}$ (pour $\mathbf{b} \in B$) sont définies sur $k_G := \mathbb{Q}(\mu_N)^{\det G}$.*

Démonstration. — Pour tout $\gamma \in \mathbf{SL}_2(\mathbb{Z})$, on note $\overline{\gamma}$ sa réduction modulo $\{\pm I\} \cdot \Gamma(N)$. On a

$$g_{\mathbf{b}} \,|_\gamma = \sum_{\overline{g} \in \overline{G}} (f_{\mathbf{a} \cdot \overline{g}} \,|_\gamma) = \sum_{\overline{g} \in \overline{G}} f_{\mathbf{a} \cdot \overline{g} \cdot \overline{\gamma}} = g_{\mathbf{b} \cdot \overline{\gamma}}.$$

Ce qui montre que $g_{\mathbf{b}}$ est Γ-invariante (si $\gamma \in \Gamma$ alors $\overline{\gamma} \in \overline{H} \subset G$), et donc que $g_{\mathbf{b}} \in \mathfrak{M}(\Gamma)$ (car les $f_{\mathbf{a}}$ sont des éléments de $\mathscr{M}_N \subset \mathfrak{M}(\Gamma(N))$). Pour terminer la preuve, il reste à voir que les coefficients de Fourier du développement à l'infini de toutes les $g_{\mathbf{b}}$ sont $(\det G)$-invariants. Tout $g \in G$ s'écrit de manière unique $g = g_0 \cdot \left(\begin{smallmatrix} \det g & 0 \\ 0 & 1 \end{smallmatrix}\right)$ avec $h_0 \in \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})$. On a donc

$$g_{\mathbf{b}} = \sum_{\overline{g} \in \overline{G}} f_{\mathbf{a} \cdot \overline{g}} = \sum_{d \in \det G} \sum_{\overline{h_0}} f_{\mathbf{a} \cdot \overline{h_0} \cdot \left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right)} = \sum_{d \in \det G} \sum_{\overline{h_0}} \left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right) \bullet (f_{\mathbf{a} \cdot \overline{h_0}}).$$

Soit $n \in \det G \subset (\mathbb{Z}/N\mathbb{Z})^\times$, n agit sur $g_{\mathbf{b}}$ comme suit :

$$\left(\begin{smallmatrix} n & 0 \\ 0 & 1 \end{smallmatrix}\right) \bullet g_{\mathbf{b}} = \sum_{d \in \det G} \sum_{\overline{h_0}} \left(\left(\begin{smallmatrix} n & 0 \\ 0 & 1 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right)\right) \bullet (f_{\mathbf{a}\cdot\overline{h_0}}) = \sum_{d \in \det G} \sum_{\overline{h_0}} \left(\begin{smallmatrix} dn & 0 \\ 0 & 1 \end{smallmatrix}\right) \bullet (f_{\mathbf{a}\cdot\overline{h_0}}) = \sum_{d' \in \det G} \sum_{\overline{h_0'}} \left(\begin{smallmatrix} d' & 0 \\ 0 & 1 \end{smallmatrix}\right) \bullet (f_{\mathbf{a}\cdot\overline{h_0'}}) = g_{\mathbf{b}}.$$

car $\det G$ est un sous-groupe de $(\mathbb{Z}/N\mathbb{Z})^\times$. Donc les coefficients de Fourier à l'infini de $g_{\mathbf{b}}$ sont $(\det G)$-invariants. □

Proposition 3.1.15. — *On a $\mathscr{M}_\Gamma^{(k_G)} = k_G(j, \{g_{\mathbf{b}}\})$.*

Démonstration. — Le Théorème 2.2.1 montre que $\mathfrak{M}(\Gamma) = \mathbb{C}(j, \{g_{\mathbf{b}}\})$. On applique le lemme de restriction des scalaires (Lemme 3.1.4) avec

$$K = k_G, \quad \text{et} \quad S = \{j\} \cup \{g_{\mathbf{b}}, \mathbf{b} \in A/\overline{G}\} \subset \mathscr{M}_\Gamma^{(k_G)}.$$

□

Proposition 3.1.16. — *Avec les mêmes notations, $\mathscr{M}_G^{(k_G)}$ est le sous corps de $\mathscr{M}_N$ fixé par $\overline{G} \subset \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$.*

Démonstration. — C'est la correspondance de Galois pour le sous-groupe $G/\{\pm 1\} \subset \mathrm{Gal}(\mathscr{M}_N/\mathscr{M}_1)$. □

Proposition 3.1.17. — *L'extension $\mathscr{M}_\Gamma^{(k_G)}/k_G$ est un corps de fonctions.*

Démonstration. — Il reste à voir que k_G est algébriquement clos dans $\mathscr{M}_\Gamma^{(k_g)}$, c'est-à-dire que $\overline{\mathbb{Q}} \cap \mathscr{M}_\Gamma^{(k_g)} = k_G$. Pour le montrer, on utilise les mêmes raisonnements que ci-dessus. □

3.2. Modèles des courbes modulaires

3.2.1. Modèle de $X(N)$. — La courbe modulaire $X(N)$ a d'abord été définie comme quotient de $\mathfrak{H}^*$, puis comme courbe projective lisse sur $\mathbb{C}$ dont le corps des fonctions rationnelles est $\mathfrak{M}(\Gamma)$. Ce qu'on vient de faire montre qu'il existe une courbe projective lisse et géométriquement irréductible $\mathscr{X}(N)$ sur $\mathbb{Q}(\mu_N)$ (c'est la conjonction du Théorème 2.4.2 et du Corollaire 3.1.13) dont le corps des fonctions est $\mathscr{M}_N$ et telle que

$$\mathscr{X}(N)(\mathbb{C}) \simeq X(N).$$

Désormais, on notera $X(N)$ le modèle canonique sur $\mathbb{Q}(\mu_N)$ ainsi défini.

3.2.2. Modèle de $X(\Gamma)$. — Soit G un sous-groupe de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$ contenant $-I$, on note $H = G \cap \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})$ et Γ le relevé à $\mathbf{SL}_2(\mathbb{Z})$ de H. Alors Γ est un sous-groupe de congruences de niveau N de $\mathbf{SL}_2(\mathbb{Z})$.

Pour les mêmes raisons que ci-dessus, il existe une courbe projective lisse et géométriquement irréductible $\mathscr{X}(G)$ sur $k_G = \mathbb{Q}(\mu_N)^{\det G}$ telle que

$$\mathscr{X}(G)(\mathbb{C}) \simeq X(\Gamma).$$

On notera maintenant $X(G)$ le modèle canonique sur k_G ainsi défini.

3.2.3. Remarques. —

- L'inclusion de corps $\mathscr{M}_1 = \mathbb{Q}(j) \hookrightarrow \mathscr{M}_N$ induit une application rationnelle $X(N) \to X(1)$ définie sur $\mathbb{Q}$. De même l'inclusion $k_G \hookrightarrow \mathscr{M}_\Gamma^{(k_G)}$ induit une application rationnelle $X(G) \to X(1)$ définie sur $\mathbb{Q}$.
- On peut naturellement considérer $X(N)$ comme une courbe sur $\mathbb{Q}$, mais celle-ci n'est alors plus géométriquement irréductible (car $\mathbb{Q}$ n'est pas algébriquement clos dans le corps des fonctions de $X(N)$).
- On a vu que $\mathscr{M}_1 = \mathbb{Q}(j)$, donc $X(1) \simeq \mathbb{P}^1(\mathbb{Q})$ car une courbe projective lisse est déterminée à isomorphisme près par son corps des fonctions rationnelles.
- En tant que courbe définie sur $\mathbb{C}$, l'objet $X(G)$ ne dépend que de $H = G \cap \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

3.2.4. Exemples. — Si $N = p \geqslant 5$ est un nombre premier, un sous-groupe maximal G de $\mathbf{GL}(\mathbb{Z}/N\mathbb{Z})$ est conjugué à l'un des sous-groupes suivants (voir **[Ser71**, Section 2] et **[Maz77b]**) :

Sous-groupe G	$X(G)$ est notée	Corps k_G de définition	Remarques
Sous-groupe de Borel $\{\left(\begin{smallmatrix}*&*\\0&*\end{smallmatrix}\right)\}$	$X_0(p)$	$\mathbb{Q}$	-
Normalisateur d'un sous-groupe de Cartan déployé $\{\left(\begin{smallmatrix}*&0\\0&*\end{smallmatrix}\right)\} \cup \{\left(\begin{smallmatrix}0&*\\*&0\end{smallmatrix}\right)\}$	$X_{split}(p)$	$\mathbb{Q}$	-
Normalisateur d'un sous-groupe de Cartan non-déployé $(\mathbb{F}_{p^2})^\times \subset \mathbf{GL}_2(\mathbb{Z}/p\mathbb{Z})$	$X_{n.split}(p)$	$\mathbb{Q}$	-
Pullback de $\mathfrak{S}_4 \subset \mathbf{PGL}_2(\mathbb{Z}/N\mathbb{Z})$	$X_{\mathfrak{S}_4}(p)$	$\begin{cases}\mathbb{Q} & \text{si } p \equiv \pm 3 \bmod 8\\ \mathbb{Q}^+(\zeta_p) & \text{si } p \not\equiv \pm 3 \bmod 8\end{cases}$	possible seulement si $p \equiv \pm 1 \bmod 5$
Pullback de $\mathfrak{S}_5 \subset \mathbf{PGL}_2(\mathbb{Z}/N\mathbb{Z})$	$X_{\mathfrak{S}_5}(p)$	$\mathbb{Q}^+(\zeta_p)$	-
Pullback de $\mathfrak{A}_4 \subset \mathbf{PGL}_2(\mathbb{Z}/N\mathbb{Z})$	$X_{\mathfrak{A}_4}(p)$	$\mathbb{Q}^+(\zeta_p)$	-

3.3. Intégralité

Soit $N \in \mathbb{N}^*$. On a les inclusions d'anneaux suivantes :

$$\begin{array}{ccc} & & \mathfrak{M}(\Gamma(N)) \\ & & \uparrow \\ \mathbb{Z}[j] & \hookrightarrow & \mathbb{Q}(j) \end{array}$$

On peut alors considérer la clôture intégrale de $\mathbb{Z}[j]$ dans $\mathfrak{M}(\Gamma(N))$. Pour étudier cela, on définit

Définition 3.3.1. — Une série formelle $f = \sum_{n\in\mathbb{Z}} a_n q^{n/N} \in \mathbb{C}((q^{1/N}))$ est dite *entière algébrique* si
- La partie négative de f est finie, ie. il existe $n_0 \in \mathbb{Z}$ tel que $a_n = 0$ pour tout $n \leqslant n_0$,
- Les coefficients a_n sont des entiers algébriques.

On appelle alors *coefficient dominant* de f le terme a_{n_0} tel que $a_{n_0} \neq 0$ et $a_n = 0$ pour tout $n < n_0$.

Les séries entières algébriques forment un anneau. Les éléments inversibles de cet anneau sont les séries formelles dont le coefficient dominant est inversible. Dans ce langage, on a une caractérisation des fonctions entières sur $\mathbb{Z}[j]$ parmi celle qui sont $\Gamma(N)$-modulaires.

Proposition 3.3.2 (**[KL81**, Chapter 2.2, Lemma 2.1**]**). — *Soit $f : \mathfrak{H} \to \mathbb{C}$ une fonction $\Gamma(N)$-invariante holomorphe sur $\mathfrak{H}$ telle que le développement de Fourier de $f|_\gamma$ est une série algébrique entière en $q^{1/N}$ pour tout $\gamma \in \mathbf{SL}_2(\mathbb{Z})$. Alors f est entière sur $\mathbb{Z}[j]$.*

Démonstration. — Comme f est $\Gamma(N)$-modulaire, l'ensemble $T := \{f|_\gamma, \gamma \in \mathbf{SL}_2(\mathbb{Z})\}$ est fini. On considère alors le polynôme

$$F(X) := \prod_{g\in T}(X - g) = \sum_{n\in\mathbb{N}} a_n X^n.$$

Les coefficients de F sont des fonctions holomorphes $a_n : \mathfrak{H} \to \mathbb{C}$ qui sont $\mathbf{SL}_2(\mathbb{Z})$-invariantes sur $\mathfrak{H}$. Les a_n n'ayant aucun pôle sur $\mathfrak{H}$ ce sont des éléments de $\mathbb{C}[j]$ (car $\mathfrak{M}(\mathbf{SL}_2(\mathbb{Z})) = \mathbb{C}(j)$). De plus, les séries de Fourier en q des a_n sont algébriques entières (par hypothèse sur f) : donc $a_n \in \overline{\mathbb{Z}}[j]$ (où $\overline{\mathbb{Z}}$ est l'anneau des entiers algébriques) car les coefficients de leur développement en série de Fourier sont des entiers algébriques.

La fonction f étant un zéro de $F(X)$, elle est entière sur $\overline{\mathbb{Z}}[j]$, donc sur $\mathbb{Z}[j]$. □

Ce critère nous sera utile au Chapitre 5.

CHAPITRE 4

COURBES MODULAIRES SUR $\mathbb{Q}$

4.1. Interprétation de $\mathscr{M}_N$ en termes de courbes elliptiques

4.1.1. Une courbe elliptique universelle. — On considère la courbe elliptique $\mathbf{E}_j$ définie sur $\mathbb{Q}(j)$ par une équation de Weierstrass :

$$\mathbf{E}_j : \ y^2 = 4x^3 - \frac{27j}{j-1728}x - \frac{27j}{j-178}.$$

Son invariant $j(\mathbf{E}_j)$ vaut j, et on rappelle que l'on regarde seulement les points affines de $E \subset \overline{\mathbb{Q}(j)}^2$.

On applique les remarques générales de la section 1.1 dans le cas où $k = \mathbb{Q}(j)$:

– Premièrement, on sait qu'il y a une racine primitive N-ième de l'unité dans le corps $\mathbb{Q}(j, \mathbf{E}_j[N])$.

– Deuxièmement, pour tout choix de base de $\mathbf{E}_j[N]$, on dispose d'une injection de groupes

$$\rho := \rho_{\mathbf{E}_j,N} : \mathrm{Gal}(\mathbb{Q}(j, \mathbf{E}_j[N])/\mathbb{Q}(j)) \hookrightarrow \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

– Troisièmement, on peut aussi considérer $\mathbf{E}_j$ comme une courbe elliptique sur $\mathbb{Q}(\mu_N, j)$ (par extension des scalaires). Le corps $\mathbb{Q}(j, \mathbf{E}_j[N])$ ne change pas car$\mathbb{Q}(j, \mu_N) \subset \mathbb{Q}(j, \mathbf{E}_j[N])$, mais le corps de base $k' = \mathbb{Q}(\mu_N, j)$ contient maintenant toutes les racines N-ièmes de l'unité : la représentation de N-torsion fournit une injection (après choix d'une base de la N-torsion) :

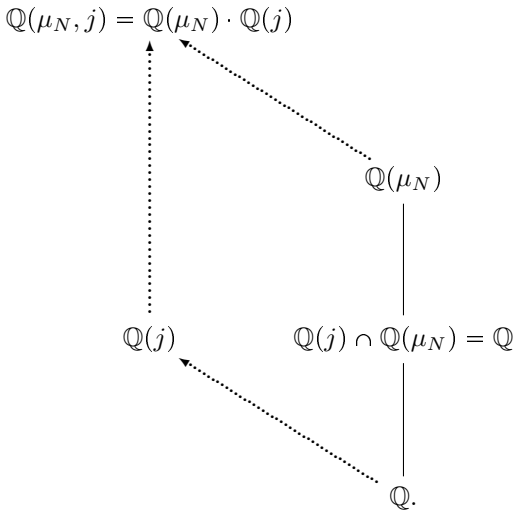
$$\rho' := \rho_{\mathbf{E}_j,N} : \mathrm{Gal}(\mathbb{Q}(j, \mathbf{E}_j[N])/\mathbb{Q}(\mu_N, j)) \hookrightarrow \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})$$

Afin d'alléger les notations, on écrira $\mathcal{G}(k)$ pour désigner $\mathrm{Gal}(k(j, \mathbf{E}_j[N])/k(j))$ pour $k = \mathbb{Q}, \mathbb{Q}(\mu_N)$ ou $\mathbb{C}$. Noter que

$$\mathcal{G}(\mathbb{Q}(\mu_N)) = \mathrm{Gal}(\mathbb{Q}(\mu_N, j, \mathbf{E}_j[N])/\mathbb{Q}(\mu_N, j)) = \mathrm{Gal}(\mathbb{Q}(j, \mathbf{E}_j[N])/\mathbb{Q}(\mu_N, j)).$$

Lemme 4.1.1. — *Le caractère cyclotomique $\chi : \mathcal{G}(\mathbb{Q}) \to (\mathbb{Z}/N\mathbb{Z})^\times$ est surjectif.*

Démonstration. — L'extension galoisienne de corps $\mathbb{Q}(j, \mathbf{E}_j[N])/\mathbb{Q}(j)$ contient $\mathbb{Q}(\mu_N, j)/\mathbb{Q}(j)$. On applique alors le Lemme 3.1.11 à la situation suivante :



Ce qui montre que l'extension $\mathbb{Q}(\mu_N, j)/\mathbb{Q}(j)$ est galoisienne de groupe de Galois isomorphe à $\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}(\mu_N) \cap \mathbb{Q}(j)) = \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \simeq (\mathbb{Z}/N\mathbb{Z})^\times$.

Le caractère χ se décompose alors comme composition de plusieurs surjections :

$$\mathcal{G}(\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\mu_N, j)/\mathbb{Q}(j)) \simeq \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \simeq (\mathbb{Z}/N\mathbb{Z})^\times.$$

□

À la Proposition 2.3.3, on a montré que la représentation de N-torsion de $\mathbf{E}_j$, vue comme une courbe elliptique sur $\mathbb{C}(j)$, réalise un isomorphisme

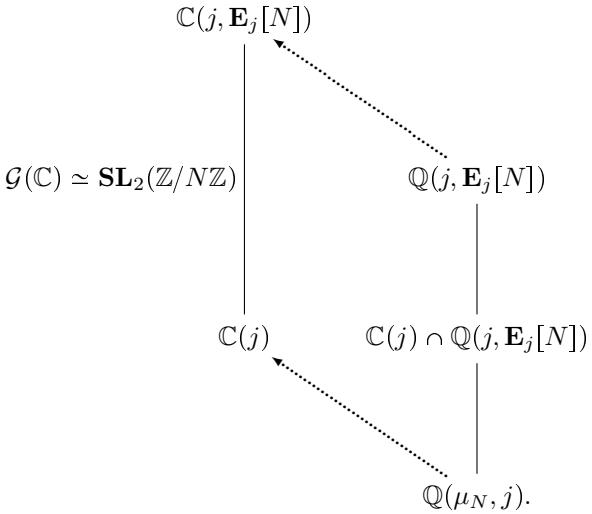
$$\rho : \mathcal{G}(\mathbb{C}) \xrightarrow{\sim} \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

La « restriction des scalaires » de $\mathbb{C}(j)$ à $\mathbb{Q}(\mu_N, j)$ ne change pas la conclusion de cette proposition. En effet,

Proposition 4.1.2. — *Le morphisme ρ' est un isomorphisme*

$$\rho' : \mathcal{G}(\mathbb{Q}(\mu_N)) \xrightarrow{\sim} \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Démonstration. — Par construction, ρ' est injective, il ne reste qu'à montrer la surjectivité. Pour ce faire, on applique le Lemme 3.1.11 au diagramme suivant :



Où l'on a utilisé la Proposition 2.3.3 pour écrire que $\mathcal{G}(\mathbb{C}) \simeq \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Le Lemme 3.1.11 montre que l'on a a un isomorphisme

$$\mathrm{Gal}(\mathbb{C}(j, \mathbf{E}_j[N])/\mathbb{C}(j)) \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(j, \mathbf{E}_j[N])/\mathbb{C}(j) \cap \mathbb{Q}(j, \mathbf{E}_j[N])) \subset \mathrm{Gal}(\mathbb{Q}(j, \mathbf{E}_j[N])/\mathbb{Q}(\mu_N, j)).$$

En reprenant les notations utilisées plus haut, on obtient la forme plus compacte suivante :

$$\mathcal{G}(\mathbb{C}) \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(j, \mathbf{E}_j[N])/\mathbb{C}(j) \cap \mathbb{Q}(j, \mathbf{E}_j[N])) \subset \mathcal{G}(\mathbb{Q}(\mu_N)).$$

Et on peut compléter ce diagramme de chaque côté par

$$\mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z}) \xrightarrow{\sim} \mathcal{G}(\mathbb{C}) \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(j, \mathbf{E}_j[N])/\mathbb{C}(j) \cap \mathbb{Q}(j, \mathbf{E}_j[N])) \hookrightarrow \mathcal{G}(\mathbb{Q}(\mu_N)) \underset{\rho'}{\hookrightarrow} \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Manifestement, les deux injections à droite doivent être des isomorphismes :
- Le fait que ρ' est un isomorphisme est ce qu'on cherche à démontrer !
- On gagne au passage l'égalité

$$\mathrm{Gal}(\mathbb{Q}(j, \mathbf{E}_j[N])/\mathbb{C}(j) \cap \mathbb{Q}(j, \mathbf{E}_j[N])) = \mathrm{Gal}(\mathbb{Q}(j, \mathbf{E}_j[N])/\mathbb{Q}(\mu_N, j)).$$

  C'est-a-dire que l'on a $\mathbb{C}(j) \cap \mathbb{Q}(j, \mathbf{E}_j[N]) = \mathbb{Q}(\mu_N, j)$.

En intersectant cette dernière égalité avec $\overline{\mathbb{Q}}$, et en remarquant que j étant transcendant sur $\mathbb{C}$, il l'est a fortiori sur $\mathbb{Q}$, et $j \notin \overline{\mathbb{Q}}$, on obtient $\overline{\mathbb{Q}} \cap \mathbb{Q}(j, \mathbf{E}_j[N]) = \mathbb{Q}(\mu_N)$. Ce qui termine la preuve. □

Au cours de cette preuve, on a constaté que $\overline{\mathbb{Q}} \cap \mathbb{Q}(j, \mathbf{E}_j[N]) = \mathbb{Q}(\mu_N)$. Ce que l'on reformule en un corollaire :

Corollaire 4.1.3. — *L'extension $\mathbb{Q}(j, \mathbf{E}_j[N])/\mathbb{Q}(\mu_N)$ est un corps de fonctions.*

On peut alors démontrer le fait suivant :

Proposition 4.1.4. — *Le morphisme ρ réalise un isomorphisme*

$$\rho : \mathcal{G}(\mathbb{Q}) \xrightarrow{\sim} \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Démonstration. — On sait que ρ est injectif et on a déjà montré que :
- Le caractère $\chi : \mathcal{G}(\mathbb{Q}) \to (\mathbb{Z}/N\mathbb{Z})^\times$ est surjectif (Lemme 4.1.1),
- Le morphisme $\rho' : \mathcal{G}(\mathbb{Q}(\mu_N)) \hookrightarrow \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})$ est un isomorphisme (Proposition 4.1.2).

Soit $\gamma \in \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$, alors $\det\gamma$ est un élément de $(\mathbb{Z}/N\mathbb{Z})^\times$ et peut donc s'écrire $\chi(\sigma)$ pour un certain $\sigma \in \mathcal{G}(\mathbb{Q})$. D'autre part, on sait que $\det\circ\rho = \chi$, donc

$$\det\rho(\sigma) = \chi(\sigma) = \det\gamma$$

et la matrice $\rho(\sigma)\cdot\gamma^{-1}$ est donc de déterminant 1. Par conséquent, on peut fixer $\sigma_0 \in \mathcal{G}(\mathbb{Q}(\mu_N))$ tel que

$$\rho'(\sigma_0) = \rho(\sigma)\cdot\gamma^{-1}$$

Autrement dit, $\gamma = \rho(\sigma)\cdot\rho'(\sigma_0)^{-1}$. Mais ρ' n'est autre que la restriction à $\mathcal{G}(\mathbb{Q}(\mu_N)) \subset \mathcal{G}(\mathbb{Q})$ de ρ, et cela donne

$$\gamma = \rho(\sigma\cdot{\sigma_0}^{-1}).$$

□

Corollaire 4.1.5. — *Soit* $\mathbf{E}$ *une courbe elliptique sur* $\mathbb{Q}(j)$ *d'invariant* $j(\mathbf{E}) = j$ *et* N *un entier non-nul. La représentation de* N*-torsion de* $\mathbf{E}$ *donne un isomorphisme*

$$\rho_{\mathbf{E},N} : \mathrm{Gal}(\mathbb{Q}(j,\mathbf{E}[N])/\mathbb{Q}(j)) \longrightarrow \mathrm{Aut}(\mathbf{E}[N]) \simeq \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

De plus, on a $\mathscr{M}_N = \mathbb{Q}(j, x(\mathbf{E}[N]))$.

Démonstration. — La courbe $\mathbf{E}$ a même invariant que $\mathbf{E}_j$, pas conséquent elles sont isomorphes sur $\overline{\mathbb{Q}(j)}$. Fixons $\phi : \mathbf{E}_j \to \mathbf{E}$ un tel isomorphisme et $\mathcal{B}$ une N-structure sur $\mathbf{E}_j$. Alors $\phi(\mathcal{B})$ est une N-structure sur $\mathbf{E}$ et les représentations associées $\rho_{\mathbf{E}_j,N} : \mathrm{Gal}(\overline{\mathbb{Q}(j)}/\mathbb{Q}(j)) \to \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$ et $\rho_{\mathbf{E},N} : \mathrm{Gal}(\overline{\mathbb{Q}(j)}/\mathbb{Q}(j)) \to \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$ sont égales.

En particulier, $\rho_{\mathbf{E},N}$ est un isomorphisme de $\mathrm{Gal}(\mathbb{Q}(j,\mathbf{E}[N])/\mathbb{Q}(j))$ sur $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$. En outre, le corps fixé dans l'extension galoisienne $\mathbb{Q}(j,\mathbf{E}[N])/\mathbb{Q}(j)$ par le sous-groupe $\rho^{-1}_{\mathbf{E},N}(\{\pm I\})$ est égal à $\mathbb{Q}(j, x(\mathbf{E}_j[N]))$. Donc on a

$$\mathscr{M}_N = \mathbb{Q}(j, x(\mathbf{E}_j[N])) = \mathbb{Q}(j, x(\mathbf{E}[N]))$$

(car sa caractérisation comme sous-corps fixé par $\{\pm I\}$ est indépendante du choix de $\mathbf{E}$). □

4.2. Problème de modules pour $X(N)$

4.2.1. Le cas de $X(1)$. —

Théorème 4.2.1. — *On a un isomorphisme de courbes algébriques sur* $\mathbb{Q}$ *:*

$$X(1) \simeq \mathbb{P}^1.$$

Démonstration. — Les corps des fonctions rationnelles de $X(1)$ et $\mathbb{P}^1$ sont tous deux isomorphes à $\mathbb{Q}(X)$. Le Theorème 2.4.2 montre donc que ces deux courbes sont isomorphes. □

Grâce au Théorème 4.2.1, on peut poser la définition suivante :

Définition 4.2.2. — Pour toute courbe modulaire $X(G)$, on note $J : X(G) \to X(1) = \mathbb{P}^1$ le morphisme canonique provenant de l'inclusion $\mathbb{Q}(j) \hookrightarrow \mathbb{Q}(j, \{f_{\mathbf{a}}\})^G = \mathscr{M}_N^{(k_G)}$. Les *pointes de* $X(G)$ sont les éléments de $J^{-1}(\{\infty\})$. On pose $Y(G) = X(G) \smallsetminus j^{-1}(\{\infty\})$. C'est une courbe affine lisse sur k_G.

Remarque 4.2.3. — Cette définition des pointes est cohérente avec celle que l'on avait faite au Chapitre 1. Par définition du modèle de $X(N)$ sur $\mathbb{Q}(\mu_N)$, on a

$$X(N)\otimes\mathbb{C} \simeq \Gamma(N)\backslash\mathfrak{H}^*.$$

Et le morphisme $X(N) \to X(1)$ donne un morphisme $\Gamma(N)\backslash\mathfrak{H}^* \to \Gamma(1)\backslash\mathfrak{H}^*$. Or $\Gamma(1)\backslash\mathfrak{H}^* = \mathbb{P}^1(\mathbb{C}) = \mathbb{C}\cup\{\infty\}$. La composée $\Gamma(N)\backslash\mathfrak{H}^* \to \mathbb{C}\cup\{\infty\}$ est la fonction modulaire j, vue comme fonction méromorphe sur $\Gamma(N)\backslash\mathfrak{H}^*$. Comme j n'a pas de pôle sur $\mathfrak{H}$, un point x de $\Gamma(N)\backslash\mathfrak{H}^*$ est une pointe si et seulement si $j(x) = \infty$. Ce qui correspond à la définition qu'on en a donné ici.

Théorème 4.2.4. — *Il y a une bijection canonique entre*

$$Y(1) \leftrightarrow \mathscr{E}\ell\ell_{\overline{\mathbb{Q}}}(1) = \big\{E,\ \textit{courbe elliptique sur } \overline{\mathbb{Q}}\big\}\Big/\overline{\mathbb{Q}}\textit{-isomorphisme.}$$

Démonstration. — On utilise les deux résultats suivants :

- Deux courbes elliptiques E et E' définies sur un corps k sont $\overline{k}$-isomorphes si et seulement si $j(E) = j(E')$ (voir [**Sil09**, Chapter III, Proposition 1.4 (b)]).
- Pour tout $\alpha \in k$, il existe une courbe elliptique E définie sur k telle que $j(E) = \alpha$ (voir [**Sil09**, Chapter III, Proposition 1.4 (c)]).

Ces deux faits montrent qu'il y a une bijection entre $\overline{\mathbb{Q}} = \mathbb{A}^1$ et $\mathscr{E}\ell\ell_{\overline{\mathbb{Q}}}(1)$. Il suffit alors de composer cette bijection par la restriction de l'isomorphisme $X(1) \to \mathbb{P}^1$. □

4.2.2. Injectivité de l'application de réduction. —

Proposition 4.2.5. — *Soit E une courbe elliptique sur un corps local K et N un entier non-nul. On note R l'anneau des entiers de K, π l'idéal maximal de R, et k le corps résiduel. On suppose que N est premier à la caractéristique de k et que E a bonne réduction en π. Alors l'application de réduction modulo π se restreint en une* injection *de groupes*

$$E[N](K) \hookrightarrow (E \bmod \pi)[N](k).$$

Démonstration. — Voir **[Sil09**, Chapter VII, Proposition 3.1(b)]. □

On en déduit immédiatement la version globale suivante :

Corollaire 4.2.6. — *Soit $\mathcal{F}/\mathbb{Q}(j)$ une extension finie de corps, on note $\mathscr{A}$ la clôture intégrale de $\mathbb{Q}[j]$ dans $\mathcal{F}$. Soit $\mathbf{E}$ une courbe elliptique sur K et N un entier non-nul. Soit enfin $\mathfrak{m}$ un idéal maximal de $\mathscr{A}$ où $\mathbf{E}$ a bonne réduction. Alors l'application de réduction modulo $\mathfrak{m}$ se restreint en une injection :*

$$\iota : \mathbf{E}[N](K) \hookrightarrow (E \bmod \mathfrak{m})[N]\big(\mathscr{A}/\mathfrak{m}\big).$$

4.2.3. Espace de modules. — Soit $N \geqslant 3$ un entier. A partir de maintenant, on considère le modèle de $X(N)$ sur $\mathbb{Q}$ construit au chapitre précédent (la courbe $X(N)$ n'est donc plus absolument irréductible), de sorte que le morphisme canonique $J : X(N) \to X(1) = \mathbb{P}^1$ est défini sur $\mathbb{Q}$. Si $S \subset \overline{\mathbb{Q}}$ est un ensemble fini, on note $Y(N)(\overline{\mathbb{Q}})_S = \big\{t \in Y(N)(\overline{\mathbb{Q}}) \text{ tel que } j(t) \notin S\big\}$ et

$$\mathscr{E}\ell\ell_{\overline{\mathbb{Q}}}(N)_S = \big\{(E, \mathcal{B}),\ E \text{ une courbe elliptique sur } \overline{\mathbb{Q}} \text{ telle que } j(E) \notin S,\ \mathcal{B} \in \mathscr{B}(E, N)\big\}\Big/\overline{\mathbb{Q}} - \text{isomorphisme.}$$

Soit $\mathbf{E}_j$ la courbe elliptique définie sur $\mathbb{Q}(j)$ par l'équation de Weierstrass :

$$\mathbf{E}_j :\ y^2 = 4x^3 - \frac{27j}{j-1728}x - \frac{27j}{j-178}.$$

Son invariant $j(\mathbf{E}_j)$ vaut j et son discriminant est

$$\Delta(\mathbf{E}_j) = 27^3 \cdot 12^3 \cdot \frac{j^2}{(1728-j)^3}.$$

La courbe a donc mauvaise réduction en les idéaux maximaux $(j-0)$ et $(j-1728)$ de $\mathbb{Q}[j]$ et bonne réduction en tous les autres idéaux maximaux.

Remarque 4.2.7. — Si l'on considère $\mathbf{E}_j$ comme une courbe elliptique sur $K = \mathbb{Q}(j, j^{1/3}, (j-1728)^{1/2})$, on peut faire un changement de coordonnées $(x, y) = (u^2x', u^3y')$ avec $u = \frac{j^{1/6}}{(1728-j)^{1/4}}$ dans l'équation de Weierstrass et obtenir

$$\mathbf{E}'_j :\ y'^2 = 4x'^3 - 27j^{1/3}x - 27(1728-j)^{1/2}.$$

Cette dernière courbe elliptique a bonne réduction modulo tous les idéaux maximaux de $\mathbb{Q}[j^{1/3}, (1728-j)^{1/2}]$ car $\Delta(\mathbf{E}'_j) = 27^3 12^3$.

Proposition 4.2.8. — *Soit $S = \{0, 1728\} \subset \overline{\mathbb{Q}}$. Il y a une bijection canonique*

$$\begin{array}{ccc} Y(N)_S & \longrightarrow & \mathscr{E}\ell\ell_{\overline{\mathbb{Q}}}(N)_S \\ t & \mapsto & [E_t, \mathcal{B}_t] \end{array}$$

Démonstration. — Soit $t \in Y(N)(\overline{\mathbb{Q}})$. L'image de t par le morphisme canonique $J : X(N) \to X(1)$ est un point de $Y(1)(\overline{\mathbb{Q}}) = \mathbb{P}^1(\overline{\mathbb{Q}})$: on pose $\alpha = J(t) \in \overline{\mathbb{Q}} \smallsetminus S$ et on note $f(X) \in \mathbb{Q}[X]$ le polynôme minimal unitaire de α sur $\mathbb{Q}$. L'idéal $\mathfrak{m}_t$ de $\mathbb{Q}[j]$ engendré par $f(j)$ est maximal et

$$\mathbb{Q}[j]/\mathfrak{m}_t \simeq \mathbb{Q}(\alpha) \subset \overline{\mathbb{Q}}.$$

On pose $\mathcal{F}_N = \mathbb{Q}(j, \mathbf{E}_j[N])$: c'est une extension galoisienne de $\mathbb{Q}(j)$, de groupe de Galois $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$ (cf. Corollaire 4.1.5), l'isomorphisme entre $\mathrm{Gal}(\mathcal{F}_N/\mathbb{Q}(j))$ et $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$ est donné par la représentation de N-torsion de $\mathbf{E}_j$ dans la N-structure canonique $(\mathbf{P}_1, \mathbf{P}_2)$ sur $\mathbf{E}_j$ (voir Proposition 2.3.4). Soit $\mathcal{A}_N$ la clôture intégrale de $\mathbb{Q}[j]$ dans $\mathscr{F}_N$. L'extension d'anneaux $\mathscr{A}_N/\mathbb{Q}[j]$ est finie et entière. D'autre part, on sait que $\mathscr{M}_N/\mathbb{Q}(j)$ est une sous-extension galoisienne de $\mathcal{F}_N/\mathbb{Q}(j)$, son groupe de Galois est isomorphe à $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$. On notera $\mathscr{B}_N$ la clôture intégrale de $\mathbb{Q}[j]$ dans $\mathscr{M}_N$, si bien que $\mathscr{B}_N$ est contenue dans $\mathscr{A}_N$. Si l'on voit $\mathscr{M}_N$ comme le corps

des fonctions rationnelles sur $X(N)$, l'anneau $\mathscr{B}_N$ est l'anneau des fonctions régulières sur $X(N)$. Résumons la situation sur un diagramme :

$$\begin{array}{ccccc} \mathbb{Q}(j) & \xhookrightarrow{\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}} & \mathscr{M}_N & \xhookrightarrow{\{\pm I\}} & \mathcal{F}_N \\ \uparrow & & \uparrow & & \uparrow \\ \mathbb{Q}[j] & \hookrightarrow & \mathscr{B}_N & \hookrightarrow & \mathscr{A}_N. \end{array}$$

Par Nullstellensatz, le point $t \in Y(N)_S$ correspond à un idéal maximal $\mathfrak{M}_t$ de $\mathscr{B}_N$. Clairement, on a

$$\mathfrak{M}_t \cap \mathbb{Q}[j] = \mathfrak{m}_t.$$

Par théorème de « going-up » (cf. [**Sam67**, § VI.1]), il existe un idéal maximal $\mathfrak{N}_t$ de $\mathcal{A}_N$ tel que

$$\mathfrak{N}_t \cap \mathscr{B}_N = \mathfrak{M}_t.$$

De plus, deux tels idéaux $\mathfrak{N}_t$ et $\mathfrak{N}'_t$ sont conjugués par le groupe de Galois $\mathrm{Gal}(\mathcal{F}_N/\mathscr{M}_N)$, ie. il existe $\sigma \in \mathrm{Gal}(\mathcal{F}_N/\mathscr{M}_N) \simeq \{\pm 1\}$ tel que $\mathfrak{N}'_t = \sigma(\mathfrak{N}_t) = \pm\mathfrak{N}_t$.

Après extension des scalaires à $\mathcal{F}_N$, $\mathbf{E}_j$ a bonne réduction en $\mathfrak{N}_t$. En effet, $\mathbf{E}_{j\,/\mathbb{Q}(j)}$ a bonne réduction en $\mathfrak{m}_t$: on note $E_{\alpha\,/\mathbb{Q}(\alpha)}$ la courbe obtenue. Alors la réduction de $\mathbf{E}_{j\,/\mathcal{F}_N}$ modulo $\mathfrak{N}_t$ est l'extension des scalaires de $E_{\alpha\,/\mathbb{Q}(\alpha)}$ à $K = \mathscr{A}_N/\mathfrak{N}_t$ et $K/\mathbb{Q}(\alpha)$ est une extension finie de corps car $\mathfrak{N}_t$ est un idéal maximal de $\mathscr{A}_N$.

Remarquons que, par définition, $\mathbf{E}_j(\mathcal{F}_N)$ contient $\mathbf{E}_j[N]$. La proposition 4.2.5 montre que l'application de réduction modulo $\mathfrak{N}_t$ se restreint en une injection :

$$\iota : \mathbf{E}_j[N](\mathcal{F}_N) \hookrightarrow E_\alpha[N](K).$$

Or, $\mathbf{E}_j$ possède une N-structure canonique $\mathcal{B}_j = (\mathbf{P}_1, \mathbf{P}_2)$ (celle donnée par $f_{\pm(1,0)}$ et $f_{\pm(0,1)}$). L'image de $\mathcal{B}_j$ réduite modulo $\mathfrak{N}_t$ par ι est donc une N-structure sur E_α : on la note $\mathcal{B}_\alpha = (P_1(\alpha), P_2(\alpha))$.

On peut maintenant définir une application $\Phi : Y(N)(\overline{\mathbb{Q}})_S \to \mathscr{E}\ell\ell_{\overline{\mathbb{Q}}}(N)_S$ par :

$$\Phi(t) := [E_\alpha, \mathcal{B}_\alpha] \qquad \text{où} \quad \alpha = J(t) \in \overline{\mathbb{Q}} \smallsetminus S.$$

Il reste à voir que Φ est une bijection :

- Premièrement, cette application est bien définie : il faut voir que la classe d'isomorphie de $(E_\alpha, \mathcal{B}_\alpha)$ ne dépend pas du choix d'un idéal maximal $\mathfrak{N}_t \subset \mathscr{A}_N$ au-dessus de $\mathfrak{M}_t \subset \mathscr{B}_N$. Remarquons déjà que la courbe E_α est indépendante d'un tel choix car c'est la réduction modulo $\mathfrak{m}_t = \mathfrak{M}_t \cap \mathbb{Q}[j]$ de $\mathbf{E}_j$. Comme on l'a fait remarquer ci-dessus, deux idéaux maximaux $\mathfrak{N}_t$ et $\mathfrak{N}'_t$ de $\mathscr{A}_N$ au-dessus de $\mathfrak{M}_t$ vérifient $\mathfrak{N}'_t = \pm\mathfrak{N}_t$. Soit $\mathcal{B}_\alpha$ (resp. $\mathcal{B}'_\alpha$) la N-structure sur E_α obtenue par réduction modulo $\mathfrak{N}_t$ (resp $\mathfrak{N}'_t$) de $(\mathbf{P}_1, \mathbf{P}_2)$. Comme $\mathfrak{N}'_t = \pm\mathfrak{N}_t$, on a $\mathcal{B}'_\alpha = \pm\mathcal{B}_\alpha$. Or, comme $\mathrm{Aut}_{\overline{\mathbb{Q}}}(E_\alpha)$ contient $\{\pm 1\}$, on a $[E_\alpha, \mathcal{B}_\alpha] = [E_\alpha, \pm\mathcal{B}_\alpha]$.
- Soit $t, t' \in Y(N)(\overline{\mathbb{Q}})_S$ auxquels on associe les idéaux maximaux $\mathfrak{M}_t$ et $\mathfrak{M}_{t'}$ de $\mathscr{B}_N$. Supposons que $\Phi(t) = \Phi(t')$, ie. $[E_\alpha, \mathcal{B}_\alpha] = [E_{\alpha'}, \mathcal{B}_{\alpha'}]$. En particulier, les courbes E_α et $E_{\alpha'}$ sont isomorphes et leurs invariants modulaires sont égaux. Puisque $j(E_\alpha) = \alpha$, on a $\alpha = \alpha'$. Autrement dit, les idéaux maximaux $\mathfrak{m}_t$ et $\mathfrak{m}_{t'}$ de $\mathbb{Q}[j]$ sont égaux. De plus, comme E_α est définie comme la réduction de $\mathbf{E}_j$ modulo $\mathfrak{m}_t$, on a même $E_\alpha = E_{\alpha'}$. Vu que $j(E_\alpha) \neq 0, 1728$, le groupe des automorphismes de E_α est réduit à $\{\pm I\}$, ce qui impose $\mathcal{B}_\alpha = \pm\mathcal{B}_{\alpha'}$. Soit $\mathfrak{N}_t$ et $\mathfrak{N}_{t'}$ les deux idéaux maximaux de $\mathscr{A}_N$ au-dessus de $\mathfrak{m}_t = \mathfrak{m}_{t'}$ correspondant à $\mathcal{B}_\alpha$ et $\mathcal{B}_{\alpha'}$ respectivement. Le fait que $\mathcal{B}_\alpha = \pm\mathcal{B}_{\alpha'}$ implique que $\mathfrak{N}_t = \pm\mathfrak{N}_{t'}$. On a finalement

$$\mathfrak{M}_t = \mathfrak{N}_t \cap \mathscr{B}_N = (\pm\mathfrak{N}_t) \cap \mathscr{B}_N = \mathfrak{N}_{t'} \cap \mathscr{B}_N = \mathfrak{M}_{t'}.$$

  Finalement, $t = t'$ et Φ est injective.
- Soit $(E, \mathcal{B})$ une courbe elliptique sur $\overline{\mathbb{Q}}$ munie d'une N-structure. Comme toute courbe elliptique sur $\overline{\mathbb{Q}}$ est isomorphe à une courbe E_α pour un certain $\alpha \in \overline{\mathbb{Q}}$, on peut supposer que $E = E_\alpha$ sans perte de généralité. Dans cette situation, soit $f \in \mathbb{Q}[X]$ le polynôme minimal de α sur $\mathbb{Q}$, et $\mathfrak{m}$ l'idéal maximal de $\mathbb{Q}[j]$ qu'il engendre. Il existe alors (par « going-up ») un idéal maximal $\mathfrak{N}_0$ de $\mathscr{A}_N$ au-dessus de $\mathfrak{m}$: on dispose donc d'un idéal maximal $\mathfrak{M}_0 = \mathfrak{N}_0 \cap \mathscr{B}_N$ de $\mathscr{B}_N$, ie. d'un point $t_0 \in Y(N)_S$ auquel on peut associer $\Phi(t_0) = [E_\alpha, \mathcal{B}_{\alpha,0}]$. Le groupe $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$ agit transitivement sur l'ensemble des N-structures sur E_α donc il existe $g \in \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$ tel que $g \star \mathcal{B}_{\alpha,0} = \mathcal{B}$. Par l'isomorphisme $\mathrm{Gal}(\mathcal{F}_N/\mathbb{Q}(j)) \simeq \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$, l'action de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$ sur les N-structures sur E_α correspond à l'action de $\mathrm{Gal}(\mathcal{F}_N/\mathbb{Q}(j))$ sur l'ensemble des idéaux maximaux de $\mathscr{A}_N$ au-dessus de $\mathfrak{m}$. Plus précisément, notons $\rho : \mathrm{Gal}(\mathcal{F}_N/\mathbb{Q}(j)) \to \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$ l'isomorphisme donné par la représentation de N-torsion de $\mathbf{E}_j$ dans la base $(\mathbf{P}_1, \mathbf{P}_2)$. Si $\mathfrak{N}$ et $\mathfrak{N}'$ sont deux idéaux maximaux de $\mathscr{A}_N$ au-dessus de $\mathfrak{m}$, il existe

$\sigma \in \mathrm{Gal}(\mathcal{F}_N/\mathbb{Q}(j))$ tel que $\sigma(\mathfrak{N}) = \mathfrak{N}'$ car l'action de $\mathrm{Gal}(\mathcal{F}_N/\mathbb{Q}(j))$ sur l'ensemble des idéaux maximaux de $\mathscr{A}_N$ au-dessus de $\mathfrak{m}$ est transitive. Auquel cas, on a

$$(\mathbf{P}_1, \mathbf{P}_2) \bmod \mathfrak{N}' = (\mathbf{P}_1, \mathbf{P}_2) \bmod \sigma(\mathfrak{N}) = ({}^{\sigma^{-1}}\mathbf{P}_1, {}^{\sigma^{-1}}\mathbf{P}_2) \bmod \mathfrak{N} = \rho(\sigma^{-1}) \cdot (\mathbf{P}_1, \mathbf{P}_2) \bmod \mathfrak{N}.$$

Notons $\mathcal{B}$ et $\mathcal{B}'$ les N-structures sur E_α déduites de $(\mathbf{P}_1, \mathbf{P}_2)$ par résuction modulo $\mathfrak{N}$ et $\mathfrak{N}'$ respectivement : on a $\mathcal{B}' = \rho(\sigma^{-1}) \cdot \mathcal{B}$. On a fixé $g \in \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$ tel que $g \star \mathcal{B}_{\alpha,0} = \mathcal{B}$. Par conséquent, il existe $\sigma \in \mathrm{Gal}(\mathcal{F}_N/\mathbb{Q}(j))$ tel que $\rho(\sigma^{-1}) = g$. Soit alors $\mathfrak{N} := \sigma(\mathfrak{N}_0)$, $\mathfrak{M} = \mathfrak{N} \cap \mathscr{A}_N$ et $t \in Y(N)_S$ le point correspondant. Par construction $\Phi(t) = [E_\alpha, \mathcal{B}]$. Donc Φ est surjective.

□

Proposition 4.2.9. — *Soit N un entier non-nul. Il y a des bijections*

$$j^{-1}(\{0\}) \subset Y(N) \longrightarrow \left\{ \begin{array}{c} (E, \mathcal{B}),\ E \text{ une courbe elliptique sur } \overline{\mathbb{Q}} \\ \text{telle que } j(E) = 0,\ \mathcal{B} \in \mathscr{B}(E, N) \end{array} \right\} \Big/ \overline{\mathbb{Q}} - \text{isomorphisme.}$$

et

$$j^{-1}(\{1728\}) \subset Y(N) \longrightarrow \left\{ \begin{array}{c} (E, \mathcal{B}),\ E \text{ une courbe elliptique sur } \overline{\mathbb{Q}} \\ \text{telle que } j(E) = 1728,\ \mathcal{B} \in \mathscr{B}(E, N) \end{array} \right\} \Big/ \overline{\mathbb{Q}} - \text{isomorphisme.}$$

Démonstration. — On admet cette proposition. Pour la démontrer, il faudrait choisir une autre courbe elliptique "universelle" ayant bonne réduction en $j = 0$ (resp. $j = 1728$) et munie d'une N-structure "universelle". Pour des éléments d'une démonstration proche de la preuve de la Proposition 4.2.8, on pourra consulter [**Shi71**, Chapter 6, §A - §B]. □

Corollaire 4.2.10. — *Il y a une bijection canonique*

$$Y(N) \longleftrightarrow \left\{ \begin{array}{c} (E, \mathcal{B}),\ E \text{ une courbe elliptique} \\ \text{sur } \overline{\mathbb{Q}} \text{ et } \mathcal{B} \in \mathscr{B}(E, N) \end{array} \right\} \Big/ \overline{\mathbb{Q}} - \text{isomorphisme.}$$

Remarque 4.2.11. — Si l'on considère le modèle de $X(N)_{/\,\mathbb{Q}(\mu_N)}$ sur $\mathbb{Q}(\mu_N)$, la courbe $Y(N)$ paramètre les courbes elliptiques avec ζ_N-structures (pour un choix préalable d'une racine primitive N-ième de l'unité ζ_N). C'est-à-dire qu'il y a une bijection :

$$Y(N)_{/\,\mathbb{Q}(\mu_N)} \longleftrightarrow \left\{ \begin{array}{c} (E, \mathcal{B}),\ E \text{ une courbe elliptique} \\ \text{sur } \overline{\mathbb{Q}} \text{ et } \mathcal{B} \in \mathscr{B}(E, \zeta_N) \end{array} \right\} \Big/ \overline{\mathbb{Q}} - \text{isomorphisme.}$$

4.2.4. Rigidité. —

Lemme 4.2.12 (**[KM85**, Corollary 2.6.2.2**]**). — *Soit E une courbe elliptique sur un corps k et $f \in \mathrm{End}_{\overline{k}}(E)$. Alors f est une racine dans $\mathrm{End}_{\overline{k}}(E)$ du polynôme*

$$P_f := X^2 - \mathrm{Tr}(f)X + \deg(f) \in \mathbb{Z}[X],$$

où $\mathrm{Tr}(f) = f + \widehat{f} \in \mathbb{Z}$. De plus, on a $(\mathrm{Tr}(f))^2 \leqslant 4\deg(f)$.

Démonstration. — Tout d'abord, remarquons que $\mathrm{Tr}(f)$ est bien un entier : on a en effet

$$\deg(1 + f) = (1 + f) \circ \widehat{(1 + f)} = (1 + f) \circ (1 + \widehat{f}) = 1 + \deg(f) + \mathrm{Tr}(f).$$

Par ailleurs, on a

$$P_f(f) = f^2 - (f + \widehat{f}) \circ f + f \circ \widehat{f} = f^2 - f^2 - \widehat{f} \circ f + f \circ \widehat{f} = 0$$

car $\widehat{f} \circ f = f \circ \widehat{f} = [\deg(f)]$. Enfin, pour tout $\frac{m}{n} \in \mathbb{Q}$, on a

$$0 \leqslant \deg(n - mf) = n^2 - \mathrm{Tr}(f)nm + \deg(f)m^2 = m^2 P_f(\tfrac{m}{n}).$$

Donc P_f ne prend que des valeurs positives sur $\mathbb{Q}$, donc sur $\mathbb{R}$ par continuité. Ainsi, son discriminant est négatif. Et cela donne exactement la dernière assertion du lemme. □

Corollaire 4.2.13. — *Soit $\psi \in \mathrm{Aut}_{\overline{k}}(E)$. On a $\psi^2 - \mathrm{Tr}(\psi)\psi + 1 = 0$ dans $\mathrm{End}_{\overline{k}}(E)$ où $\mathrm{Tr}(\psi) \in \{0, \pm 1, \pm 2\}$.*

Démonstration. — Comme ψ est un automorphisme, on a $\deg(\psi) = 1$. Donc on a $\psi^2 - \mathrm{Tr}(\psi)\psi + 1 = 0$ d'après le lemme précédent, où $(\mathrm{Tr}(\psi)) \leqslant 4(\deg(\psi))^2 = 4$. □

Proposition 4.2.14. — *Soit $N \geqslant 3$ un entier et $\psi \in \mathrm{Aut}_{\overline{k}}(E)$. On suppose que ψ induit l'identité sur $E[N]$. Alors ψ est l'identité sur E.*

Démonstration. — Par hypothèse, on a $\psi - 1 = 0$ sur $E[N]$: autrement dit, on a

$$E[N] \subset \mathrm{Ker}(\psi - 1).$$

Il existe donc une factorisation $(\psi - 1) = g \circ [N]$ où $g \in \mathrm{End}_{\overline{k}}(E)$. Dès lors, on a

$$\deg(\psi) = 1 + N\,\mathrm{Tr}(g) + N^2 \deg(g) \qquad \text{et} \qquad \mathrm{Tr}(\psi) = 2 + N\,\mathrm{Tr}(g).$$

Or, $\deg(\psi) = 1$ et $|\,\mathrm{Tr}(\psi)| \leqslant 2$. Avec les deux relations ci-dessus, cela implique que $|N\,\mathrm{Tr}(g)| \leqslant 4$ et que $|N^2 \deg(g)| \leqslant 4$. D'autre part, le Lemme 4.2.12 montre que $(\mathrm{Tr}(g))^2 \leqslant 4\deg(g)$.

Ce qui impose $|\deg(g)| < 1$ dès que $N > 2$. Donc $g = 0$ et ψ est l'identité de E. □

Proposition 4.2.15. — *Soit E, E' deux courbes elliptiques sur $\mathbb{Q}$. Soit $\phi : (E, \mathcal{B}) \to (E', \mathcal{B}')$ un isomorphisme de courbes elliptiques avec N-structures $\mathbb{Q}$-rationnelles. Si $N \geqslant 3$, alors ϕ est définie sur $\mathbb{Q}$.*

Démonstration. — Soit $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, il s'agit de voir que $\phi^\sigma = \phi$. Par définition, on a $\phi^\sigma = \sigma \circ \phi \circ \sigma^{-1}$. Soit $\psi = \phi^{-1} \circ \phi^\sigma$: comme E et E' sont définies sur $\mathbb{Q}$, ψ est un automorphisme de E. De plus, la N-structure $\psi(\mathcal{B})$ est égale à $\mathcal{B}$ car $\mathcal{B}$ est $\mathbb{Q}$-rationnelle : c'est-à-dire que ψ est un automorphisme de $(E, \mathcal{B})$. L'automorphisme ψ fixe donc point à point $E[N]$ car il fixe une $\mathbb{Z}/N\mathbb{Z}$-base de $E[N]$. La Proposition 4.2.14 montre que $\psi = 1$, donc que $\phi = \phi^\sigma$. Et ce, pour tout $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Donc ϕ est définie sur $\mathbb{Q}$. □

4.2.5. Action de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$ et de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. — Rappelons que $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$ agit sur $\mathscr{M}_N = \mathbb{Q}(\mu_n, j, \{f_{\mathbf{a}}\})$ par

$$\forall \gamma \in \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z}), \qquad f_{\mathbf{a}}|_\gamma = f_{\mathbf{a}\cdot\gamma} \qquad \text{et} \qquad \zeta|_\gamma = \zeta^{\det\gamma}.$$

Cette action se factorise en une action de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ sur $\mathscr{M}_N$. Par fonctorialité de la correspondance « corps de fonctions $\leftrightarrow$ courbes projectives », l'action ci-dessus induit une action (définie sur $\mathbb{Q}$) de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ sur $X(N)$:

$$\forall \gamma \in \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}, \qquad \gamma : X(N) \longrightarrow X(N).$$

Proposition 4.2.16. — *L'action de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ sur $X(N)$ se restreint en une action sur $Y(N)$. Celle-ci est donnée par*

$$\forall g \in \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}, \qquad [E, \mathcal{B}] \mapsto [E, g \star \mathcal{B}].$$

Démonstration. — Par définition, on a $Y(N) = X(N) \smallsetminus J^{-1}(\{\infty\})$. On note à nouveau $\mathscr{B}_N$ la clôture intégrale de $\mathbb{Q}[j]$ dans $\mathscr{M}_N$. L'action de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ préserve les fibres de J. En effet, l'isomorphisme $\rho' : \mathrm{Gal}(\mathscr{M}_N/\mathbb{Q}(j)) \to \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ permet de reformuler l'action de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ sous la forme suivante :

$$\forall g \in \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}, \forall \mathfrak{M} \subset \mathscr{B}_N, \qquad \mathfrak{M} \mapsto {\rho'}^{-1}(g)(\mathfrak{M}).$$

En particulier, comme $\sigma := {\rho'}^{-1}(g)$ fixe $\mathbb{Q}(j)$ et que J correspond à l'inclusion de $\mathbb{Q}(j)$ dans $\mathscr{M}_N$, les fibres de J sont préservées par action de g. En particulier, l'action de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ induit une action sur sur $Y(N)$.

Le fait que celle-ci est donnée par $[E, \mathcal{B}] \mapsto [E, g \star \mathcal{B}]$ (pour $g \in \mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$) suit immédiatement de la définition de la bijection entre $Y(N)$ et $\mathscr{E}\ell\ell_{\overline{\mathbb{Q}}}(N)$. □

La courbe $Y(N)$ étant une courbe algébrique affine sur $\mathbb{Q}$, il y a une action de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur ses points $\overline{\mathbb{Q}}$-rationnels : celle-ci se traduit par

$$\forall \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \qquad [E, \mathcal{B}] \mapsto [E^\sigma, {}^\sigma\mathcal{B}],$$

où $E^\sigma = \{{}^\sigma P,\ P \in E\}$. On note $Y(N)(\mathbb{Q})$ l'ensemble des points $\mathbb{Q}$-rationnels de $Y(N)$, ie. l'ensemble des points $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariants.

Définition 4.2.17. — Un point $t \in Y(N)$ est dit *entier* si $J(t) \in \mathbb{Z}$.

Proposition 4.2.18. — *Il y a une bijection*

$$Y(N)(\mathbb{Q}) \leftrightarrow \Big\{(E, \mathcal{B}),\ E \text{ une courbe elliptique sur } \mathbb{Q} \text{ et } \mathcal{B} \in \mathscr{B}_{\mathbb{Q}}(E, N)\Big\} \Big/ \overline{\mathbb{Q}} - \text{isomorphisme.}$$

Démonstration. — Si $(E, \mathcal{B})$ est une courbe elliptique sur $\mathbb{Q}$ munie d'une N-structure $\mathbb{Q}$-rationnelle, alors la classe d'isomorphisme $[E, \mathcal{B}]$ est clairement un point $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant de $Y(N)$ via la bijection du Corollaire 4.2.10. Réciproquement, soit $[E, \mathcal{B}]$ un point $\mathbb{Q}$-rationnel de $Y(N)$: comme le morphisme $J : X(N) \to \mathbb{P}^1$ est défini sur $\mathbb{Q}$, on a $J([E, \mathcal{B}]) \in \mathbb{Q}$. Donc il existe un représentant $(E_0, \mathcal{B}_0)$ de $[E, \mathcal{B}]$ où E_0 est définie sur $\mathbb{Q}$. En outre, la N-structure $\mathcal{B}_0$ est nécessairement $\mathbb{Q}$-rationnelle car le seul automorphisme de $(E_0, \mathcal{B}_0)$ est l'identité (cf. Proposition 4.2.14). □

Avec le Corollaire 4.2.15, on voit même que

Proposition 4.2.19. — *Il y a une bijection*

$$Y(N)(\mathbb{Q}) \leftrightarrow \Big\{(E,\mathcal{B}),\ E \text{ une courbe elliptique sur } \mathbb{Q} \text{ et } \mathcal{B} \in \mathscr{B}_{\mathbb{Q}}(E,N)\Big\}\Big/\mathbb{Q}-\text{isomorphisme.}$$

4.3. Problèmes de modules pour $X(G)$

Soit G un sous-groupe de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$. On suppose pour simplifier que $\det : G \to \mathbb{Z}/N\mathbb{Z}^\times$ surjectif (on suppose aussi que $-I \in G$, comme au chapitre précédent). On notera $\overline{G} = G/\{\pm I\}$.

Le modèle canonique de $X(G)$ (construit à la section 3.2.2) est alors défini sur $k_G = \mathbb{Q}$. L'inclusion de corps $\mathscr{M}_\Gamma^{(k_G)} = \mathscr{M}_\Gamma^{(\mathbb{Q})} \hookrightarrow \mathscr{M}_N$ correspond canoniquement à un morphisme $\pi : X(N) \to X(G)$ défini sur $\mathbb{Q}$. Au vu de la proposition 4.2.16, π peut se donner de manière plus maniable sur les parties affines $Y(N) \to Y(G)$ par

$$\pi([E,\mathcal{B}]) = [E, G\star\mathcal{B}] = [E, \overline{G}\star\mathcal{B}].$$

Il est alors clair que pour tout point $t \in Y(G)$, l'image inverse $\pi^{-1}(\{t\})$ est exactement une $\overline{G}$-orbite de $Y(N)$ pour l'action de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$.

Proposition 4.3.1. — *Avec les notations et hypothèses de cette section, il y a une bijection*

$$Y(G) \leftrightarrow \Big\{(E,\beta),\ E \text{ une courbe elliptique sur } \overline{\mathbb{Q}} \text{ et } \beta \in \mathscr{B}(E,G)\Big\}\Big/\overline{\mathbb{Q}}-\text{isomorphisme.}$$

Démonstration. — Commençons par remarquer qu'il y a un diagramme naturel :

$$\begin{array}{ccccc}
t & & Y(N) & \xrightarrow[\pi]{} & Y(G) \\
\big\downarrow & & \big\downarrow \Phi & & \big\vdots \Psi \\
[E_{J(t)},\mathcal{B}_{J(t)}] & & \mathscr{E}\ell\ell_{\overline{\mathbb{Q}}}(N) & \xrightarrow{p} & \mathscr{E}\ell\ell_{\overline{\mathbb{Q}}}(G) \\
 & & [E,\mathcal{B}] & \longmapsto & [E, G\star\mathcal{B}].
\end{array}$$

Soit $s \in Y(G)$, pour un relevé $t \in Y(N)$ de s par π, on pose

$$\Psi(t) := p\circ\Phi(s) = [E_{J(s)}, G\star\mathcal{B}_{J(s)}] \in \mathscr{E}\ell\ell_{\overline{\mathbb{Q}}}(G).$$

- Cette application est bien définie. En effet, si $s' \in Y(N)$ est un autre relevé de t par π est dans la même $\overline{G}$-orbite que s donc $J(s) = J(s')$ (car l'action de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ préserve les fibres de J) et il existe $g \in G$ tel que $[E_{J(s')},\mathcal{B}_{J(s')}] = [E_{J(s)}, g\star\mathcal{B}_{J(s)}]$. Ainsi, on a $p\circ\Phi(s') = p\circ\Phi(s)$.
- L'injectivité et la surjectivité se démontrent facilement, en suivant le même raisonnement que sur $\mathbb{C}$ (voir la preuve de la Proposition 1.6.12).

□

L'action de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur $Y(N)$ se factorise en une action sur $Y(G)$, donnée par

$$\forall\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \qquad [E, G\star\mathcal{B}] \mapsto [E^\sigma, G\star^\sigma\mathcal{B}].$$

On a déjà démontré que cette action est bien définie (cf. Section 1.6, en particulier l'équation (1)). On peut donc décrire les points $\mathbb{Q}$-rationnels de $Y(G)$:

Théorème 4.3.2. — *Il y a une bijection*

$$Y(G)(\mathbb{Q}) \leftrightarrow \Big\{(E,\beta),\ E \text{ une courbe elliptique sur } \mathbb{Q} \text{ et } \beta \in \mathscr{B}_{\mathbb{Q}}(E,G)\Big\}\Big/\overline{\mathbb{Q}}-\text{isomorphisme.}$$

Démonstration. — La démonstration est en tout point similaire à celle de la Proposition 4.2.18 : on utilise en plus le fait que les actions de $\mathbf{GL}_2(\mathbb{Z}/N\mathbb{Z})$ et de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur les N-structures sont compatibles (au sens de (1)). □

4.4. Le cas des sous-groupes de Cartan déployés

Dans ce qui suit, $N = p$ est un nombre premier impair. Et G est le sous-groupe de $\mathbf{GL}_2(\mathbb{Z}/p\mathbb{Z})$ formé des matrices diagonales et anti-diagonales.

Proposition 4.4.1. — *Soit k un corps de caractéristique différente de p. Les G-structures k-rationnelles sur une courbe elliptique E définie sur k sont en bijection avec les paires de sous-groupes p-cycliques distincts de $E[p]$ qui sont* $\mathrm{Gal}(\overline{k}/k)$*-invariantes, via*

$$\begin{array}{ccc} \mathscr{B}_k(E,G) & \to & \left\{ \begin{array}{c} \{C_1,C_2\},\ \ C_1,C_2 \text{ des sous-groupes } p\text{-cycliques distincts} \\ \text{de } E[p] \text{ tels que } \{C_1,C_2\} \text{ est } \mathrm{Gal}(\overline{k}/k)\text{-invariante} \end{array} \right\} \\ G \star \left(\begin{smallmatrix} P_1 \\ P_2 \end{smallmatrix}\right) & \mapsto & \{\langle P_1\rangle, \langle P_2\rangle\}. \end{array}$$

Démonstration. — Notons f l'application définie dans l'énoncé.

- En premier lieu vérifions que f est bien définie. Supposons que $G \star \left(\begin{smallmatrix} P_1 \\ P_2 \end{smallmatrix}\right) = G \star \left(\begin{smallmatrix} P_1' \\ P_2' \end{smallmatrix}\right)$. Alors on peut fixer $g \in G$ tel que $g \star \left(\begin{smallmatrix} P_1 \\ P_2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} P_1' \\ P_2' \end{smallmatrix}\right)$. Deux cas se présentent alors :
  - ou bien $g = \left(\begin{smallmatrix} a & 0 \\ 0 & a' \end{smallmatrix}\right)$ est diagonale, et l'on a
  $$\left(\begin{smallmatrix} P_1' \\ P_2' \end{smallmatrix}\right) = g \star \left(\begin{smallmatrix} P_1 \\ P_2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} aP_1 \\ a'P_2 \end{smallmatrix}\right).$$
  Auquel cas, on a $\langle P_1'\rangle = \langle aP_1\rangle = \langle P_1\rangle$ car a est un élément de $\mathbb{Z}/p\mathbb{Z}^\times$. De même $\langle P_2'\rangle = \langle P_2\rangle$.
  - ou bien $g = \left(\begin{smallmatrix} 0 & a \\ a' & 0 \end{smallmatrix}\right)$ est anti-diagonale, et l'on a
  $$\left(\begin{smallmatrix} P_1' \\ P_2' \end{smallmatrix}\right) = g \star \left(\begin{smallmatrix} P_1 \\ P_2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} aP_2 \\ a'P_1 \end{smallmatrix}\right).$$
  Auquel cas, on a $\langle P_1'\rangle = \langle P_2\rangle$ et $\langle P_2'\rangle = \langle P_1\rangle$ pour les mêmes raisons que ci-dessus. Finalement, on a bien $\{\langle P_1'\rangle, \langle P_2'\rangle\} = \{\langle P_1\rangle, \langle P_2\rangle\}$.

  Comme $\beta = G \star \left(\begin{smallmatrix} P_1 \\ P_2 \end{smallmatrix}\right)$ est $\mathrm{Gal}(\overline{k}/k)$-stable, la paire $\{\langle P_1\rangle, \langle P_2\rangle\}$ est $\mathrm{Gal}(\overline{k}/k)$-stable.
- Si $\{\langle P_1'\rangle, \langle P_2'\rangle\} = \{\langle P_1\rangle, \langle P_2\rangle\}$, il existe $g \in G$ tel que
$$g \cdot \left(\begin{smallmatrix} P_1 \\ P_2 \end{smallmatrix}\right) = \left(\begin{smallmatrix} P_1' \\ P_2' \end{smallmatrix}\right).$$
Donc f est injective.
- Enfin, si $\{C_1, C_2\}$ est une paire $\mathrm{Gal}(\overline{k}/k)$-invariante de sous-groupes p-cycliques distincts de $E[p]$, on choisit des générateurs P_i de C_i $(i = 1, 2)$. Dans ce cas, $\left(\begin{smallmatrix} P_1 \\ P_2 \end{smallmatrix}\right)$ est une p-structure sur E, et l'orbite $G \star \left(\begin{smallmatrix} P_1 \\ P_2 \end{smallmatrix}\right)$ est $\mathrm{Gal}(\overline{k}/k)$-stable. Donc on a $\{C_1, C_2\} = f\left(G \star \left(\begin{smallmatrix} P_1 \\ P_2 \end{smallmatrix}\right)\right)$.

□

Théorème 4.4.2. — *Il y a une bijection*

$$Y_{split}(p)(\mathbb{Q}) \leftrightarrow \Big\{(E,\beta),\ E \text{ une courbe elliptique sur } \mathbb{Q} \text{ et } \beta \in \mathscr{B}_{\mathbb{Q}}(E,G)\Big\}\Big/ \text{isomorphisme}.$$

Démonstration. — C'est un cas particulier du Théorème 4.3.2. □

CHAPITRE 5

FONCTIONS DE SIEGEL

5.1. Préliminaires

Soit L un réseau de $\mathbb{C}$. On dispose de plusieurs fonctions utiles attachées à ce réseau : premièrement, la *fonction $\wp$ de Weierstrass* :

$$\forall z \in \mathbb{C}, \qquad \wp(z;L) = \frac{1}{z^2} + \sum_{\omega \in L \smallsetminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right),$$

qui permet de paramétrer la courbe elliptique $\mathbb{C}/L$ par une équation de Weierstrass dans $\mathbb{P}^2(\mathbb{C})$ de manière biholomorphe. Deuxièmement, on utilisera la *fonction σ de Weierstrass* :

$$\forall z \in \mathbb{C}, \qquad \sigma(z;L) = z \cdot \prod_{\omega \in L \smallsetminus \{0\}} \left(1 - \frac{z}{\omega}\right) \exp\left(\frac{z}{\omega} + \frac{z^2}{2\omega^2} \right),$$

et sa dérivée logarithmique, la *fonction ζ de Weierstrass* :

$$\forall z \in \mathbb{C}, \qquad \zeta(z;L) = \frac{\sigma'(z;L)}{\sigma(z;L)} = \frac{1}{z} + \sum_{\omega \in L \smallsetminus \{0\}} \left(\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2} \right).$$

On voit que la fonction $\zeta(-;L)$ n'est pas L-périodique. Cependant, pour $\omega \in L$ fixé, comme la dérivée de $z \mapsto \zeta(z+\omega;L) - \zeta(z;L)$ est nulle, il existe un nombre complexe $\eta(\omega;L)$ tel que

$$\forall z \in \mathbb{C}, \qquad \zeta(z+\omega;L) - \zeta(z;L) = \eta(\omega;L).$$

L'application η qui à $\omega \in L$ associe $\eta(\omega;L)$ est appelée *fonction η de Weierstrass*. C'est une fonction $\mathbb{Z}$-linéaire, qui vérifie la *relation de Liouville* : pour toute base (ω_1, ω_2) de L, on a

$$\eta(\omega_2;L)\omega_1 - \eta(\omega_1;L)\omega_2 = 2i\pi.$$

En outre, la fonction $\sigma(-;L)$ est impaire : $\sigma(-z;L) = -\sigma(z;L)$ pour tout $z \in \mathbb{C}$.

On rappelle enfin que la fonction $\sigma(-;L)$ vérifie une relation qui palie à sa non-périodicité : après le choix d'une base (ω_1, ω_2) de L, pour tout $\omega = b_1\omega_1 + b_2\omega_2 \in L$, on a

$$\forall z \in \mathbb{C}, \qquad \sigma(z+\omega;L) = (-1)^{b_1 b_2 + b_1 + b_2} \cdot \exp\left(\eta(\omega;L) \cdot \left(z + \frac{\omega}{2} \right) \right) \cdot \sigma(z;L).$$

Pour des preuves détaillées, on pourra consulter **[Lan87]**.

5.2. Formes de Klein et fonctions de Siegel

5.2.1. Définitions, premières propriétés. —

Définition 5.2.1. — Pour tout $\mathbf{a} = (a_1, a_2) \in \mathbb{Q}^2 \smallsetminus \mathbb{Z}^2$, on définit la $\mathbf{a}$-*ième forme de Klein* par la formule suivante :

$$\forall \tau \in \mathfrak{H}, \qquad K_{\mathbf{a}}(\tau) := \exp\left(-\frac{a_1\tau + a_2}{2} \cdot \big(a_1\eta(\tau;\Lambda_\tau) + a_2\eta(1;\Lambda_\tau) \big) \right) \cdot \sigma\left(a_1\tau + a_2; \Lambda_\tau\right)$$

où Λ_τ est le réseau de $\mathbb{C}$ dont une base est $(\tau, 1)$.

Ainsi définies, les formes de Klein sont méromorphes sur $\mathfrak{H}$, et l'on peut dès à présent donner quelques propriétés de cette famille de fonctions. On rappelle que $\mathbf{SL}_2(\mathbb{Z})$ agit à droite sur $\mathbb{Q}^2 \smallsetminus \mathbb{Z}^2$.

Proposition 5.2.2. — *Pour tout $\mathbf{a} \in \mathbb{Q}^2 \smallsetminus \mathbb{Z}^2$, on a*

- $K_{-\mathbf{a}} = -K_{\mathbf{a}}$.

- *Pour tout* $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z})$, *on a :*

$$\forall \tau \in \mathfrak{H}, \qquad K_{\mathbf{a}}(\alpha \cdot \tau) = (c\tau + d)^{-1} \cdot K_{\mathbf{a}\cdot\alpha}(\tau).$$

- *Pour tout* $v = (v_1, v_2) \in \mathbb{Z}^2$, *on a :*

$$K_{\mathbf{a}+v} = \varepsilon(\mathbf{a}, v) \cdot K_{\mathbf{a}}$$

où $\varepsilon(\mathbf{a}, v) = \exp(-i\pi(v_1 a_2 - v_2 a_1)) \cdot (-1)^{v_1 v_2 + v_1 + v_2}$.

Démonstration. — Le premier point ne pose pas de problème : la fonction $\sigma(-; \Lambda_\tau)$ est impaire et le facteur exponentiel ne change pas lorsqu'on change le signe de $\mathbf{a}$. Pour prouver la seconde relation, raisonnons séparément sur le facteur $\sigma(-; \Lambda_\tau)$ et sur le terme exponentiel ; pour simplifier les calculs, on pose $\tau' = \alpha \cdot \tau = \frac{a\tau+b}{c\tau+d}$, et $\mathbf{a}' = \mathbf{a} \cdot \alpha = (a_1', a_2')$. D'abord, comme σ est homogène de degré 1, on a

$$\begin{aligned} \sigma(a_1\tau' + a_2; \Lambda_{\tau'}) &= \sigma\left(\tfrac{1}{c\tau+d} \cdot (a_1(a\tau+b) + a_2(c\tau+d)); \Lambda_{\tau'}\right) \\ &= (c\tau+d)^{-1} \cdot \sigma\left(a_1(a\tau+b) + a_2(c\tau+d); (c\tau+d)\Lambda_{\tau'}\right) \\ &= (c\tau+d)^{-1} \cdot \sigma\left(a_1'\tau + a_2'; \Lambda_\tau\right). \end{aligned}$$

Pour ce qui est du terme exponentiel, on remarque dans un premier temps que $\eta(-; \Lambda_{\tau'})$ est $\mathbb{Z}$-linéaire et homogène de degré -1, ce qui permet de calculer

$$\eta(\tau'; \Lambda_{\tau'}) = \eta\left(\frac{a\tau+b}{c\tau+d}; \Lambda_{\tau'}\right) = (c\tau+d) \cdot \eta(a\tau+b; \Lambda_\tau) = (c\tau+d) \cdot \big(a \cdot \eta(\tau; \Lambda_\tau) + b \cdot \eta(1; \Lambda_\tau)\big)$$

De la même manière, on trouve que $\eta(1; \Lambda_{\tau'}) = (c\tau+d) \cdot \big(c \cdot \eta(\tau; \Lambda_\tau) + d \cdot \eta(1; \Lambda_\tau)\big)$. Si bien que,

$$\frac{\exp\left(-\frac{a_1\tau'+a_2}{2} \cdot \big(a_1\eta(\tau'; \Lambda_\tau') + a_2\eta(1; \Lambda_\tau')\big)\right)}{\exp\left(-\frac{a_1'\tau+a_2'}{2} \cdot \big(a_1'\eta(\tau; \Lambda_\tau) + a_2'\eta(1; \Lambda_\tau)\big)\right)} = 1.$$

La preuve de la troisième relation est longue et calculatoire : on utilise la relation de Liouville

$$\eta(\omega_2; L)\omega_1 - \eta(\omega_1; L)\omega_2 = 2i\pi,$$

et la relation de transformation pour $\sigma(-; L)$:

$$\forall L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2, \forall \omega = b_1\omega_1 + b_2\omega_2 \in L, \forall z \in \mathbb{C}, \quad \sigma(z+\omega; L) = (-1)^{b_1 b_2 + b_1 + b_2} \cdot \exp\left(\eta(\omega; L) \cdot \left(z + \frac{\omega}{2}\right)\right) \cdot \sigma(z; L).$$

□

Lorsque l'on a construit les courbes modulaires, on a modifié la paramétrisation de Weierstrass

$$\mathbb{C}/L \to E_L, \qquad z \mapsto (\wp(z), \wp'(z))$$

par un facteur $(g_2(z)/g_3(z))^{3/2}$, pour l'adapter à nos besoins sur les points de torsion : on avait alors obtenu les fonctions de Fricke (Teilwert), dont les propriétés algébriques étaient en outre meilleures. On va faire de même pour les formes de Klein : ici, le facteur à rajouter est la puissance 12-ième d'un facteur d'automorphie de fonctions theta.

Définition 5.2.3. — Pour tout $\mathbf{a} \in \mathbb{Q}^2 \smallsetminus \mathbb{Z}^2$, on définit la $\mathbf{a}$-*ième fonction de Siegel* par :

$$\forall \tau \in \mathfrak{H}, \qquad g_{\mathbf{a}}(\tau) = K_{\mathbf{a}}(\tau)^{12} \cdot \Delta(\tau)$$

où Δ est la fonction usuelle :

$$\forall \tau \in \mathfrak{H}, \qquad \Delta(\tau) = (2i\pi)^{12} \cdot q \cdot \prod_{n=1}^{\infty} (1-q^n)^{24} \qquad (q = \mathrm{e}^{2i\pi\tau}).$$

Remarque 5.2.4. — On attire l'attention du lecteur sur le fait que la définition des fonctions de Siegel choisie ici ne corresponde pas à celles de [**KL81**] ou [**Lan87**] : nos fonctions $g_{\mathbf{a}}$ sont les puissances 12-ièmes de celles utilisées dans les références citées.

D'autre part, on rappelle que la fonction Δ est modulaire de poids 12 pour $\mathbf{SL}_2(\mathbb{Z})$:

$$\forall \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}), \ \forall \tau \in \mathfrak{H}, \qquad \Delta(\alpha \cdot \tau) = (c\tau+d)^{-12}\Delta(\tau).$$

La Proposition 5.2.2 donnant les propriétés de la famille des formes de Klein se traduit ici par :

Proposition 5.2.5. — *Soit* $\mathbf{a} \in \mathbb{Q}^2 \smallsetminus \mathbb{Z}^2$, *les relations suivantes sont vérifiées :*

- $g_{-\mathbf{a}} = g_{\mathbf{a}}$.

- *Pour tout* $\alpha \in \mathbf{SL}_2(\mathbb{Z})$*, on a*
$$g_{\mathbf{a}} \circ \alpha = g_{\mathbf{a}\cdot\alpha}.$$
- *Pour tout* $v = (v_1, v_2) \in \mathbb{Z}^2$*, on a*
$$g_{\mathbf{a}+v} = \varepsilon(\mathbf{a}, v)^{12} g_{\mathbf{a}}$$
où, comme plus haut, $\varepsilon(\mathbf{a}, v) = \exp(-i\pi(v_1 a_2 - v_2 a_1)) \cdot (-1)^{v_1 v_2 + v_1 + v_2}$.

Démonstration. — La majeure partie des calculs a déjà été faite dans la démonstration de la Proposition 5.2.2. Le premier point est clair. Le second point est la conjonction de la deuxième relation vérifiée par les formes de Klein et du fait que Δ est modulaire de poids 12. Enfin, le troisième point découle directement de la relation correspondante pour les $K_{\mathbf{a}}$. □

5.3. Analyse du comportement aux pointes

Les $g_{\mathbf{a}}$ admettent un développement en q-produit de la forme suivante :

Proposition 5.3.1. — *Pour* $\mathbf{a} = (a_1, a_2) \in \mathbb{Q}^2 \smallsetminus \mathbb{Z}^2$*, posons* $q_z = \mathrm{e}^{2i\pi(a_1\tau + a_2)}$*. On a*
$$\forall \tau \in \mathfrak{H}, \qquad g_{\mathbf{a}}(\tau) = q^{6\cdot B_2(a_1)} \cdot \mathrm{e}^{12i\pi a_2(a_1-1)} \cdot (1-q_z)^{12} \cdot \prod_{n=1}^{\infty} \left((1-q_z\cdot q^n)(1-{q_z}^{-1}\cdot q^n)\right)^{12}$$
où $B_2(X) = X^2 - X + 1/6$ *désigne le second polynôme de Bernoulli. On peut aussi écrire ceci sans faire apparaitre* z*,*
$$\forall \tau \in \mathfrak{H}, \qquad g_{\mathbf{a}}(\tau) = q^{6\cdot B_2(a_1)} \cdot \mathrm{e}^{12i\pi a_2(a_1-1)} \cdot \prod_{n=0}^{\infty} \left((1-\mathrm{e}^{2i\pi a_2}\cdot q^{n+a_1})(1-\mathrm{e}^{-2i\pi a_2}\cdot q^{n+1-a_1})\right)^{12}.$$

Démonstration. — Pour tout $\tau \in \mathfrak{H}$, on pose $q = \mathrm{e}^{2i\pi\tau}$ comme d'habitude, $z = a_1\tau + a_2$ et $q_z = \mathrm{e}^{2i\pi(a_1\tau+a_2)}$. Partons du développement en q-produit de la fonction $\sigma(-;\Lambda_\tau)$ (la preuve se trouve dans [**Lan87**, Chapter 18, § 2, Theorem 4]) :
$$\sigma(z;\Lambda_\tau) = \frac{1}{2i\pi}\mathrm{e}^{\eta(1;\Lambda_\tau)\frac{z^2}{2}} \cdot (\mathrm{e}^{i\pi z} - \mathrm{e}^{-i\pi z}) \cdot \prod_{n=1}^{\infty} \frac{(1-q_z\cdot q^n)(1-{q_z}^{-1}\cdot q^n)}{(1-q^n)^2}.$$
On a par ailleurs :
$$\Delta(\tau) = (2i\pi)^{12} \cdot q \cdot \prod_{n=1}^{\infty}(1-q^n)^{24}.$$
Si bien que
$$g_{\mathbf{a}}(\tau) = \underbrace{\mathrm{e}^{-6z\cdot\left(a_1\eta(\tau;\Lambda_\tau)+a_2\eta(1;\Lambda_\tau)\right)} \cdot \mathrm{e}^{6\eta(1;\Lambda_\tau)\cdot z^2} \cdot q \cdot (\mathrm{e}^{i\pi z} - \mathrm{e}^{-i\pi z})^{12}}_{:=e(z)} \cdot \prod_{n=1}^{\infty} \left((1-q_z\cdot q^n)(1-{q_z}^{-1}\cdot q^n)\right)^{12}.$$

Le facteur $e(z)$ devant le produit se simplifie en utilisant la relation de Liouville pour la fonction $\eta(-;L)$ et quelques astuces de calcul :
$$\begin{aligned}
e(z) &= \mathrm{e}^{-6z\cdot\left(a_1\eta(\tau;\Lambda_\tau)+a_2\eta(1;\Lambda_\tau)\right)} \cdot \mathrm{e}^{6\eta(1;\Lambda_\tau)\cdot z^2} \cdot q \cdot (\mathrm{e}^{i\pi z} - \mathrm{e}^{-i\pi z})^{12} \\
&= \mathrm{e}^{2i\pi\tau} \cdot \mathrm{e}^{-6\cdot(a_1\tau+a_2)\cdot\left(a_1\eta(\tau;\Lambda_\tau)+a_2\eta(1;\Lambda_\tau)\right)} \cdot \mathrm{e}^{6\eta(1;\Lambda_\tau)\cdot(a_1\tau+a_2)^2} \cdot (\mathrm{e}^{i\pi z} - \mathrm{e}^{-i\pi z})^{12} \\
&= \exp\left(2i\pi\tau + 12i\pi {a_1}^2\tau + 12i\pi a_1 a_2\right) \cdot (\mathrm{e}^{i\pi z} - \mathrm{e}^{-i\pi z})^{12} \\
&= \exp\left(12i\pi\tau\cdot B_2(a_1) + 12i\pi a_1\tau + 12i\pi a_1 a_2\right) \cdot (\mathrm{e}^{i\pi z} - \mathrm{e}^{-i\pi z})^{12} \\
&= q^{6B_2(a_1)} \cdot \exp\left(12i\pi z + 12i\pi a_2(a_1-1)\right) \cdot (\mathrm{e}^{i\pi z} - \mathrm{e}^{-i\pi z})^{12} \\
&= q^{6B_2(a_1)} \cdot \mathrm{e}^{12i\pi a_2(a_1-1)} \cdot \mathrm{e}^{12i\pi z} \cdot (\mathrm{e}^{i\pi z} - \mathrm{e}^{-i\pi z})^{12} \\
&= q^{6B_2(a_1)} \cdot \mathrm{e}^{12i\pi a_2(a_1-1)} \cdot (1-q_z)^{12}.
\end{aligned}$$
Comme annoncé. La seconde égalité s'obtient immédiatement à partir de la première. □

Remarquons qu'on peut lire sur le q-produit d'une fonction $f(\tau)$ sur $\mathfrak{H}$ son comportement lorsque $\tau \to i\infty$. En d'autres termes, on peut savoir si f a un zéro ou un pôle en $q = 0$ en regardant son q-produit.

Définition 5.3.2. — Soit $f : \mathfrak{H} \to \mathbb{C}$. L'ordre de f en ∞ est l'unique rationnel ℓ tel que la limite $\lim_{\tau\to\infty} q^{-\ell} f(\tau)$ existe et soit non-nulle. On le note $\mathrm{ord}_x f$.

Avec cette définition, on peut énoncer le

Lemme 5.3.3. — *Soit* $\mathbf{a} = (a_1, a_2) \in \mathbb{Q}^2 \smallsetminus \mathbb{Z}^2$ *avec* $0 \leqslant a_1 < 1$. *L'ordre de* $g_{\mathbf{a}}$ *en la pointe* ∞ *de* $\mathfrak{H}$ *vaut*

$$\mathrm{ord}_\infty\, g_{\mathbf{a}} = 6 \cdot B_2(a_1).$$

Démonstration. — Ceci est clair au vu du développement en q-produit de $g_{\mathbf{a}}$. □

Analysons de manière plus détaillée le comportement de $g_{\mathbf{a}}$ en $q = 0$ dans le cas particulier où $\mathbf{a} \in \mathbb{Q}^2 \smallsetminus \mathbb{Z}^2$ est de dénominateur N (c'est-à-dire que $N\mathbf{a} \in \mathbb{Z}^2$ et que N est le plus petit entier tel que cela se produise). Soit $\mathbf{a} = (a_1, a_2) \in (N^{-1}\mathbb{Z})^2 \smallsetminus \mathbb{Z}^2$ avec $0 \leqslant a_1 < 1$. On a vu que

$$g_{\mathbf{a}} = \boxed{q^{6\cdot B_2(a_1)}}_{(1)} \cdot \boxed{\mathrm{e}^{12i\pi a_2(a_1-1)}}_{(2)} \cdot \prod_{n=0}^{\infty} \left(\boxed{(1 - \mathrm{e}^{2i\pi a_2} \cdot q^{n+a_1})(1 - \mathrm{e}^{-2i\pi a_2} \cdot q^{n+1-a_1})}_{(3)} \right)^{12}.$$

Dans ce produit :

Le terme (1) : détermine l'ordre du pôle/zéro de $g_{\mathbf{a}}$ en $q = 0$.

Le terme (2) : est une racine de l'unité, dont l'ordre divise N^2 car a_1 et a_2 sont des éléments de $N^{-1}\mathbb{Z}$.

Le terme (3) : s'analyse en plusieurs temps :

- Pour $n = 0$ et $a_1 = 0$, il vaut $(1 - \mathrm{e}^{-2i\pi a_2} q)$: c'est une racine N-ième de l'unité !
- Pour $n = 0$ et $a_1 > 0$, ce terme s'écrit
$$(1 - \mathrm{e}^{2i\pi a_2} \cdot q^{a_1})(1 - \mathrm{e}^{-2i\pi a_2} \cdot q^{1-a_1}),$$
c'est donc un élément inversible de $\mathbb{Z}[\mu_N][[q^{1/N}]]$.
- Pour $n > 0$, il vaut
$$(1 - \mathrm{e}^{2i\pi a_2} \cdot q^{n})(1 - \mathrm{e}^{-2i\pi a_2} \cdot q^{n+1}),$$
c'est encore un élément inversible de $\mathbb{Z}[\mu_N][[q^{1/N}]]$.

Si bien que, mis à part le terme (1), on obtient une série entière inversible :

$$g_{\mathbf{a}} \cdot q^{-6B_2(a_1)} \in \left(\mathbb{Q}(\mu_N)[[q^{1/N}]]\right)^\times.$$

Et cela "repousse les pôles et zéros de $g_{\mathbf{a}}$ à l'infini". Plus précisément,

Proposition 5.3.4. — *Les fonctions* $g_{\mathbf{a}}$ *n'ont ni pôles ni zéros sur le demi-plan* $\mathfrak{H}$.

Démonstration. — Soit $\mathbf{a} \in \mathbb{Q}^2 \smallsetminus \mathbb{Z}^2$, de dénominateur N. Comme on vient de le voir,

$$g_{\mathbf{a}} \cdot q^{-6B_2(a_1)} \in \left(\mathbb{Q}(\mu_N)[[q^{1/N}]]\right)^\times \subset \mathbb{C}[[q^{1/N}]]^\times$$

Donc il existe une série entière $h \in \mathbb{C}[[q^{1/N}]]^\times$ telle que

$$g_{\mathbf{a}} \cdot q^{-6B_2(a_1)} \cdot h = 1$$

et h induit une fonction méromorphe sur $\mathfrak{H}$. Si $\tau \in \mathfrak{H}$ est un zéro de $g_{\mathbf{a}}$, alors

$$0 = g_{\mathbf{a}}(\tau) \cdot {q_\tau}^{-6B_2(a_1)} \cdot h(\tau) = 1$$

Ce qui est contradictoire. On raisonne de même pour les pôles. □

5.3.1. Modularité. — En tant que telles, les $g_{\mathbf{a}}$ ne sont pas des fonctions modulaires, car

$$\forall \alpha \in \mathbf{SL}_2(\mathbb{Z}), \qquad g_{\mathbf{a}} \circ \alpha = g_{\mathbf{a}\cdot\alpha}$$

Il y a cependant un certain nombres de théorèmes donnant des conditions nécessaires et suffisantes pour qu'un produit de fonctions de Siegel soit modulaire pour un sous-groupe de congruences donné (cf. le Chapitre 2 de [**KL81**]). On se borne ici au cas le plus simple qui nous sera utile :

Proposition 5.3.5. — *Soit* $\mathbf{a} \in (N^{-1}\mathbb{Z})^2 \smallsetminus \mathbb{Z}^2$. *Alors* ${g_{\mathbf{a}}}^N$ *est modulaire pour* $\Gamma(N)$.

Démonstration. — Écrivons $\mathbf{a} = (\frac{a_1}{N}, \frac{a_2}{N})$, avec a_1, a_2 des entiers premiers à N. Soit $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(N)$.

Calculons d'abord

$$\mathbf{a} \cdot \alpha = \left(\frac{a_1}{N}, \frac{a_2}{N}\right) + \left(\frac{(a-1)a_1 + ca_2}{N}, \frac{ba_1 + (d-1)a_2}{N}\right).$$

Posons $v = \left(\frac{(a-1)a_1+ca_2}{N}, \frac{ba_1+(d-1)a_2}{N}\right)$. Comme $\alpha \in \Gamma(N)$, le vecteur v est à coordonnées entières, et l'on peut utiliser les propriétés des fonctions de Siegel (deuxième relation donnée dans la Proposition 5.2.5) : on trouve que

$$g_{\mathbf{a}} \circ \alpha = g_{\mathbf{a}\cdot\alpha} = g_{\mathbf{a}+v} = \varepsilon(\mathbf{a}, v)^{12} g_{\mathbf{a}}.$$

Or,

$$\varepsilon(\mathbf{a},v)^{12} = \exp(-12i\pi(v_1a_2 - v_2a_1)) = \exp\left(-\frac{12i\pi}{N}\cdot(c{a_1}^2 - b{a_2}^2 + (a-d)a_1a_2)\right)$$

est clairement une racine N-ième de l'unité ! □

5.4. Propriétés d'intégralité

Lemme 5.4.1. — *Soit* $\mathbf{a} \in (N^{-1}\mathbb{Z})^2 \smallsetminus \mathbb{Z}^2$. *La fonction* $u_{\mathbf{a}} := {g_{\mathbf{a}}}^N$ *est un élément de* $\mathscr{M}_N$.

Démonstration. — Le fait que $u_{\mathbf{a}}$ est modulaire pour $\Gamma(N)$ a déjà été démontré (cf. Proposition 5.3.5). De plus, on a vu que

$$g_{\mathbf{a}} \in q^{6B_2(a_1)}\cdot\mathbb{Q}(\mu_N)[[q^{1/N}]]$$

donc les coefficients du développement à l'infini de $u_{\mathbf{a}}$ sont dans $\mathbb{Q}(\mu_N)$. De plus, pour $\gamma \in \mathbf{SL}_2(\mathbb{Z})$, les propriétés des fonctions de Siegel (Proposition 5.2.5) imposent que

$$u_{\mathbf{a}}|_\gamma = (\text{ une racine } N\text{-ième de l'unité})\cdot u_{\mathbf{a}\cdot\gamma}$$

Donc, les coefficients de Fourier de $u_{\mathbf{a}}$ à toutes les pointes sont dans $\mathbb{Q}(\mu_N)$. □

Proposition 5.4.2. — *Soit* $\mathbf{a} = (a_1,a_2) \in (N^{-1}\mathbb{Z})^2 \smallsetminus \mathbb{Z}^2$ *et* $\zeta_N := \mathrm{e}^{2i\pi/N}$. *Les fonctions* $g_{\mathbf{a}}$ *et* $(1-\zeta_N)^{12}{g_{\mathbf{a}}}^{-1}$ *sont entières sur* $\mathbb{Z}[j]$.

Démonstration. — On utilise le critère de la Proposition 3.3.2. La fonction $u_{\mathbf{a}} = {g_{\mathbf{a}}}^N : \mathfrak{H} \to \mathbb{C}$ est $\Gamma(N)$-modulaire et holomorphe sur $\mathfrak{H}$. De plus, son développement en série de Fourier en $q = \mathrm{e}^{2i\pi\tau}$ est algébrique entier (cela se voit facilement en développant le q-produit de la Proposition 5.3.1 en une série entière en q). De plus, pour tout $\gamma \in \mathbf{SL}_2(\mathbb{Z})$, on a montré à la Proposition 5.2.5 que

$$u_{\mathbf{a}}|_\gamma = (\text{ une racine } N\text{-ième de l'unité})\cdot u_{\mathbf{a}\cdot\gamma}.$$

Donc le développement en série de Fourier de $u_{\mathbf{a}}|_\gamma$ est algébrique entier.

La Proposition 3.3.2 assure alors que $u_{\mathbf{a}}$ est entière sur $\mathbb{Z}[j]$. Donc $g_{\mathbf{a}}$ l'est aussi.

De plus,

- Si $a_1 = 0$, la série formelle en q donnant le développement en série de Fourier de $g_{\mathbf{a}}$ est inversible. Le développement de Fourier de ${g_{\mathbf{a}}}^{-1}$ est donc algébrique entier.
- Si $a_1 \neq 0$, la série de Fourier de $g_{\mathbf{a}}$ s'écrit $(1-\mathrm{e}^{\pm 2i\pi a_2})^{12}$ fois une série inversible. Ainsi, la série de Fourier en q de $(1-\mathrm{e}^{\pm 2i\pi a_2})\cdot{g_{\mathbf{a}}}^{-1}$ est algébrique entière. Dans ce cas, comme N est le dénominateur de a_2, le nombre $(1-\zeta_N)/(1-\mathrm{e}^{\pm 2i\pi a_2})$ est une unité algébrique.

Dans les deux cas, $(1-\zeta_N)^{12}\cdot{g_{\mathbf{a}}}^{-1}$ a une série de Fourier algébrique entière. Le même résultat vaut pour tous les $g_{\mathbf{a}}|_\gamma$ (γ parcourant $\mathbf{SL}_2(\mathbb{Z})$) par la Proposition 5.2.5.

On applique alors la Proposition 3.3.2 à la fonction $(1-\zeta_N)^{12N}\cdot{g_{\mathbf{a}}}^{-N}$ pour conclure. □

CHAPITRE 6

LE PREMIER INGRÉDIENT : ESTIMATIONS ANALYTIQUES

Dans ce chapitre, nous utilisons les fonctions de Siegel pour construire une unité modulaire, afin de démontrer le résultat suivant :

Théorème 6.0.3. — *Soit p un nombre premier impair et $P \in Y_{split}(p)(\mathbb{Z})$. On a*

$$\log|j(P)| \leqslant 2\pi\sqrt{p} + 6\log p + 21\frac{(\log p)^2}{\sqrt{p}}.$$

Pour obtenir un tel théorème, il s'agit de construire une fonction rationnelle sur X_{split}, sans pôle ni zéro sur Y_{split} et dont on peut relier le comportement aux pointes à celui de j. Une telle fonction sera construite à partir d'un certain produit de fonctions de Siegel.

Pour la démonstration du Théorème 6.0.3, nous suivrons la preuve du Théorème 1.1 de [**BP09b**] en incluant les améliorations de [**BP09a**] et [**BPR11**].

Remarque 6.0.4. — Les constantes 2π et 6 sont optimales pour la méthode utilisée, mais la constante 21 peut-être diminuée pour p suffisamment grand ([**BPR11**, Section 2] annonce qu'il est possible de remplacer 21 par 3).

Soit G le sous-groupe des matrices diagonales et antidiagonales de $\mathbf{GL}_2(\mathbb{Z}/p\mathbb{Z})$. On relève $G \cap \mathbf{SL}_2(\mathbb{Z}/N\mathbb{Z})$ en un sous-groupe$\Gamma_{split}(p)$ de $\mathbf{SL}_2(\mathbb{Z})$.

On notera encore $\mathcal{D}^\circ$ l'intérieur du triangle hyperbolique de sommets $\mathrm{e}^{i\pi/3}, \mathrm{e}^{2i\pi/3}$ et $i\infty$, et

$$\mathcal{D} := \mathcal{D}^\circ \cup \{\text{les segments hyperboliques } [i, \mathrm{e}^{2i\pi/3}] \text{ et } [\mathrm{e}^{2i\pi/3}, i\infty]\ \}.$$

6.1. Estimations préliminaires sur l'invariant j

Tout d'abord, rappelons que la fonction modulaire $j : \mathfrak{H} \to \mathbb{C}$ est définie par

$$j(\tau) = \frac{(12E_4(\tau))^3}{\Delta(\tau)}$$

où, en posant $q = \mathrm{e}^{2i\pi\tau}$,

$$E_4(\tau) = \frac{(2\pi)^4}{12}\left(1 + 240\sum_{n=1}^{\infty}\frac{n^3q^n}{1-q^n}\right) \qquad \text{et} \qquad \Delta(\tau) = (2\pi)^{12}q\prod_{n=1}^{\infty}(1-q^n)^{24}.$$

Les constantes multiplicatives étant choisies afin de normaliser j en un élément de $q^{-1}\mathbb{Z}[[q]]$:

$$j(\tau) = q^{-1} + 744 + 196884q + \dots$$

Lemme 6.1.1. — *Pour tout $\tau \in \mathcal{D} + \mathbb{Z}$, on a*

$$|j(\tau) - q^{-1} - 744| \leqslant 309000|q| \tag{2}$$

Démonstration. — Comme $\tau \in \mathcal{D} + \mathbb{Z}$, on a $\operatorname{Im}\tau \geqslant \operatorname{Im}\mathrm{e}^{2i\pi/3} = \sqrt{3}/2$; ou encore, en termes de $q = \mathrm{e}^{2i\pi\tau}$,

$$|q| = \mathrm{e}^{-2\pi\operatorname{Im}\tau} \leqslant \mathrm{e}^{-\pi\sqrt{3}} < 0,0044.$$

Dans un premier temps, écrivons des développements de E_4 et Δ.

- Pour $n \geqslant 3$, on a $n^3 \leqslant 3^n$: on en déduit les inégalités ci-dessous, valables pour $|q| < 1/3$:

$$\begin{aligned}\left|\frac{12}{(2\pi)^4}E_4(\tau) - 1 - 240q\right| &\leqslant 240\left(\left|\frac{q}{1-q} - q\right| + \frac{8|q|^2}{1-|q|^2} + \sum_{n=3}^{\infty}\frac{3^n|q|^n}{1-|q|}\right)\\ &\leqslant 240\left(\frac{|q|^2}{1-|q|} + \frac{8|q|^2}{1-|q|^2} + \sum_{n=3}^{\infty}\frac{3^n|q|^n}{1-|q|}\right)\\ &\leqslant \frac{240}{1-|q|}\left(|q|^2 + 8|q|^2 + \sum_{n=3}^{\infty}|3q|^n\right)\\ &\leqslant \frac{240}{1-|q|}\sum_{n=2}^{\infty}|3q|^n = \frac{2160}{(1-|q|)(1-3|q|)}|q|^2.\end{aligned}$$

  En outre, pour $|q| < \mathrm{e}^{-\pi\sqrt{3}}$, un calcul numérique nous donne que $\frac{2160}{(1-|q|)(1-3|q|)} \leqslant 2199$.
- D'autre part, on a

$$\left|\log\frac{(2\pi)^{12}q(1-q)^{24}}{\Delta(\tau)}\right| = 24\left|\sum_{n=2}^{\infty}\log(1-q^n)\right| \leqslant 24\sum_{n=2}^{\infty}|\log(1-q^n)| \leqslant 24\sum_{n=2}^{\infty} -\log(1-|q|^n)$$

  où l'on a utilisé le fait que, si $|z| < 1$, on a $|\log|1+z|| \leqslant -\log(1-|z|)$. Tirons à présent parti de la majoration classique (obtenue avec le principe du maximum, par exemple) :

$$\forall |z| \leqslant r < 1, \qquad |\log(1+z)| \leqslant \frac{|\log(1-r)|}{r}|z|$$

  avec $r = \mathrm{e}^{-\pi\sqrt{3}}$ et $z = q^n$, pour obtenir

$$\sum_{n=2}^{\infty} -\log(1-|q|^n) \leqslant \frac{|\log(1-\mathrm{e}^{-\pi\sqrt{3}})|}{\mathrm{e}^{-\pi\sqrt{3}}}\cdot\frac{|q|^2}{1-|q|} \leqslant \mathrm{e}^{\pi\sqrt{3}}\cdot\frac{|\log(1-\mathrm{e}^{-\pi\sqrt{3}})|}{1-\mathrm{e}^{-\pi\sqrt{3}}}\cdot|q|^2 \leqslant 1,0066|q|^2.$$

  Ainsi, on trouve que

$$\left|\log\frac{(2\pi)^{12}q(1-q)^{24}}{\Delta(\tau)}\right| \leqslant 24\times 1,0066|q|^2 \leqslant 24,2|q|^2.$$

  En utilisant l'inégalité classique

$$\forall |z| \leqslant r < 1, \qquad |\mathrm{e}^z - 1| \leqslant \frac{|\mathrm{e}^r - 1|}{r}|z| \tag{3}$$

  avec $z = \log\frac{(2\pi)^{12}q(1-q)^{24}}{\Delta(\tau)}$ et $r = 24,2|q|^2$, on obtient la majoration suivante :

$$\begin{aligned}\left|\frac{(2\pi)^{12}q(1-q)^{24}}{\Delta(\tau)} - 1\right| &\leqslant \frac{\left|\mathrm{e}^{24,2|q|^2} - 1\right|}{24,2|q|^2}\cdot\left|\log\frac{(2\pi)^{12}q(1-q)^{24}}{\Delta(\tau)}\right|\\ &\leqslant \frac{\left|\mathrm{e}^{24,2|q|^2} - 1\right|}{24,2|q|^2}\cdot 24,2|q|^2 \leqslant \left|\mathrm{e}^{24,2|q|^2} - 1\right|\end{aligned}$$

  On réutilise alors la même inégalité (3) avec cette fois $z = 24,2|q|^2$ et $r = 24,2\mathrm{e}^{-2\pi\sqrt{3}}$: cela fournit

$$\left|\mathrm{e}^{24,2|q|^2} - 1\right| \leqslant \frac{\left|\mathrm{e}^{24,2\mathrm{e}^{-2\pi\sqrt{3}}} - 1\right|}{24,2\mathrm{e}^{-2\pi\sqrt{3}}}\cdot 24,2|q|^2 \leqslant 24,21|q|^2.$$

  On a donc prouvé que

$$\left|\frac{(2\pi)^{12}q(1-q)^{24}}{\Delta(\tau)} - 1\right| \leqslant 24,21|q|^2.$$

  Ce qui permet d'obtenir le développement suivant :

$$\begin{aligned}\left|\frac{(2\pi)^{12}q}{\Delta(\tau)} - 1 - 24q\right| &\leqslant \frac{1}{|1-q|^{24}}\cdot\left|\frac{(2\pi)^{12}q(1-q)^{24}}{\Delta(\tau)} - 1\right| + \left|\frac{1}{(1-q)^{24}} - 1 - 24q\right|\\ &\leqslant \frac{1}{(1-\mathrm{e}^{2\pi\sqrt{3}})^{24}}\cdot 24,21|q|^2 + 312|q|^2 \leqslant 340|q|^2.\end{aligned}$$

  En effet, toujours grâce au principe du maximum, on peut démontrer que

$$\forall |z| \leqslant r < 1, \left|\frac{1}{(1-z)^{24}} - 1 - 24z\right| \leqslant \frac{\left|(1-r)^{-24} - 1 + 24r\right|}{r^2}|z|^2.$$

Ce qui donne bien, avec $z = q$ et $r = \mathrm{e}^{-\pi\sqrt{3}}$:

$$\left|\frac{1}{(1-q)^{24}} - 1 - 24q\right| \leqslant \frac{\left|(1-\mathrm{e}^{-\pi\sqrt{3}})^{-24} - 1 + 24r\right|}{r^2}|q|^2 \leqslant 312|q|^2.$$

Si l'on écrit

$$\frac{12E_4(\tau)}{(2\pi)^4} = 1 + 240q + \alpha(q) \qquad \text{et} \qquad \frac{(2\pi)^4}{\Delta(\tau)}q = 1 + 24q + \beta(q),$$

on vient donc de montrer que

$$|\alpha(q)| \leqslant 2199|q|^2 \qquad \text{et} \qquad |\beta(q)| \leqslant 340|q|^2.$$

Utilisons alors ces développements dans la définition de j :

$$\begin{aligned}
j(\tau) &= \frac{(12E_4(\tau))^3}{\Delta(\tau)} = \frac{1}{q}\cdot\left(\frac{12E_4(\tau)}{(2\pi)^4}\right)^3\cdot\left(\frac{(2\pi)^{12}q}{\Delta(\tau)}\right)\\
&= \frac{1}{q}\cdot(1+240q+\alpha(q))^3\cdot(1+24q+\beta(q)).\\
&= \frac{1}{q}\cdot\Big(172800\alpha(q)\beta(q)\cdot q^2 + 720\alpha(q)^2\beta(q)\cdot q + 1440\alpha(q)\beta(q)\cdot q + \alpha(q)^3\beta(q) + 3\alpha(q)^2\beta(q)\\
&\quad + 3\alpha(q)\beta(q) + 4147200\alpha(q)\cdot q^3 + 17280\alpha(q)^2\cdot q^2 + 207360\alpha(q)\cdot q^2 + 24\alpha(q)^3\cdot q\\
&\quad + 792\alpha(q)^2\cdot q + 1512\alpha(q)\cdot q + \alpha(q)^3 + 3\alpha(q)^2 + 3\alpha(q) + 13824000\beta(q)\cdot q^3\\
&\quad + 172800\beta(q)\cdot q^2 + 720\beta(q)\cdot q + \beta(q) + 331776000\cdot q^4 + 17971200\cdot q^3\\
&\quad + 190080\cdot q^2 + 744\cdot q + 1\Big).
\end{aligned}$$

En regroupant les termes de même ordre en q, on trouve que :

$$\begin{aligned}
\left|j(\tau) - q^{-1} - 744\right| &\leqslant |q|\cdot\Big(3615385443660|q|^6 + 1438958803176|q|^5 + 228320632899|q|^4\\
&\qquad + 18726279192|q|^3 + 863262423|q|^2 + 21540888|q| + 197017\Big)\\
&\leqslant 308180,3\cdot|q| \leqslant 309000|q|.
\end{aligned}$$

Ce qui conclut la preuve. □

Cet encadrement nous sera utile sous la forme suivante :

Proposition 6.1.2. — *Pour tout $\tau \in \mathcal{D} + \mathbb{Z}$, ou bien $|j(\tau)| < 3500$, ou bien $|j(\tau) - q^{-1}| \leqslant 963$.*

Démonstration. — Si $|j(\tau)| \geqslant 3500$, on commence par utiliser l'encadrement (2) sous la forme

$$|q^{-1}| \geqslant |j(\tau)| + 744 - 309000|q|,$$

ce qui se reécrit

$$|q| \leqslant \frac{1}{|j(\tau)| - 744 - 309000|q|}.$$

Or, on a supposé que $|j(\tau)| \geqslant 3500$ et que $|q| \leqslant \mathrm{e}^{-\pi\sqrt{3}}$, on a donc

$$|q| \leqslant \frac{1}{3500 - 744 - 309000\cdot\mathrm{e}^{-\pi\sqrt{3}}} \leqslant 0.00071.$$

Ceci donne alors

$$|j(\tau) - q^{-1}| \leqslant 309000|q| + 744 \leqslant \frac{30900}{3500 - 744 - 309000\cdot\mathrm{e}^{-\pi\sqrt{3}}} + 744 \leqslant 963.$$

C'est bien la majoration annoncée. □

6.1.1. Développement aux pointes de $g_{\mathbf{a}}$. — Dans la section 5.3, on a déjà donné une estimation du type

$$\log g_{\mathbf{a}}(\tau) = \mathrm{ord}_q\, g_{\mathbf{a}}\cdot\log|q| + \mathcal{O}(1)$$

Pour la suite de la démonstration, il nous faut cependant un terme de plus dans ce développement :

Proposition 6.1.3. — *Soit $\mathbf{a} = (a_1, a_2) \in (p^{-1}\mathbb{Z}^2) \smallsetminus \mathbb{Z}^2$, avec $0 \leqslant a_1 < 1$. Pour tout $\tau \in \mathcal{D} + \mathbb{Z}$, on a*

$$\log|g_{\mathbf{a}}(\tau)| = 6B_2(a_1)\cdot\log|q| + 12\log\left|1 - q^{a_1}\mathrm{e}^{2i\pi a_2}\right| + 12\log\left|1 - q^{1-a_1}\mathrm{e}^{-2i\pi a_2}\right| + \gamma(q)$$

où γ est une fonction vérifiant $|\gamma(q)| \leqslant 25|q|^2$.

Démonstration. — D'après l'expression du q-produit de $g_{\mathbf{a}}$ trouvé à la Proposition 5.3.1 :

$$g_{\mathbf{a}}(\tau) = q^{6\cdot B_2(a_1)} \cdot \mathrm{e}^{12i\pi a_2(a_1-1)} \cdot \prod_{n=0}^{\infty} \left((1-\mathrm{e}^{2i\pi a_2}\cdot q^{n+a_1})(1-\mathrm{e}^{-2i\pi a_2}\cdot q^{n+1-a_1})\right)^{12},$$

on a :

$$\log|g_{\mathbf{a}}(\tau)| = 6B_2(a_1)\cdot\log|q| + \sum_{n=0}^{\infty}\left(12\log\left|1-q^{n+a_1}\mathrm{e}^{2i\pi a_2}\right| + 12\log\left|1-q^{n+1-a_1}\mathrm{e}^{-2i\pi a_2}\right|\right).$$

Il faut donc montrer que

$$\left|\sum_{n=1}^{\infty}\left(\log\left|1-q^{n+a_1}\mathrm{e}^{2i\pi a_2}\right| + \log\left|1-q^{n+1-a_1}\mathrm{e}^{-2i\pi a_2}\right|\right)\right| \leqslant \frac{25}{12}|q|.$$

Or, pour $\tau \in \mathcal{D}+\mathbb{Z}$ on a vu que $|q| < \mathrm{e}^{-\pi\sqrt{3}}$: par conséquent, chaque terme $|q^{n+a_1}|$ ou $|q^{n+1-a_1}|$ est plus petit que $\mathrm{e}^{-\pi\sqrt{3}}$. On a donc :

$$\begin{aligned}
\left|\sum_{n=1}^{\infty}\left(\log\left|1-q^{n+a_1}\mathrm{e}^{2i\pi a_2}\right| + \log\left|1-q^{n+1-a_1}\mathrm{e}^{-2i\pi a_2}\right|\right)\right| &\leqslant \sum_{n=1}^{\infty}\left|\log\left|1-q^{n+a_1}\mathrm{e}^{2i\pi a_2}\right|\right| \\
&\quad + \sum_{n=1}^{\infty}\left|\log\left|1-q^{n+1-a_1}\mathrm{e}^{-2i\pi a_2}\right|\right| \\
&\leqslant -\sum_{n=1}^{\infty}\log(1-|q|^{n+a_1}) - \sum_{n=1}^{\infty}\log(|1-|q|^{n+1-a_1}) \\
&\leqslant \frac{|\log(1-\mathrm{e}^{-\pi\sqrt{3}})|}{\mathrm{e}^{-\pi\sqrt{3}}}\cdot\left(\frac{|q|^{1+a_1}}{1-|q|} + \frac{|q|^{2-a_1}}{1-|q|}\right) \\
&\leqslant \frac{|\log(1-\mathrm{e}^{-\pi\sqrt{3}})|}{\mathrm{e}^{-\pi\sqrt{3}}}\cdot\frac{2}{1-|q|}\cdot|q| \\
&\leqslant 2,02|q| \leqslant \frac{25}{12}|q|.
\end{aligned}$$

□

6.2. Une unité modulaire

6.2.1. Construction, premières propriétés. — On pose tout d'abord

$$A := \left\{(\tfrac{k}{p}, 0),\ k=1,\dots,p-1\right\} \cup \left\{(0,\tfrac{k}{p}),\ k=1,\dots,p-1\right\} \subset (p^{-1}\mathbb{Z})^2 \smallsetminus \mathbb{Z}^2.$$

Notons que l'action à droite de $\mathbf{SL}_2(\mathbb{Z})$ sur $(p^{-1}\mathbb{Z})^2 \smallsetminus \mathbb{Z}^2$ se factorise à travers $\mathbf{SL}_2(\mathbb{Z}/p\mathbb{Z})$ et que le stabilisateur de A dans $\mathbf{SL}_2(\mathbb{Z})$ est $\Gamma_{split}(p)$.

Définition 6.2.1. — L'unité modulaire U est définie par

$$U := \prod_{\mathbf{a}\in A} u_{\mathbf{a}} \qquad \text{où } u_{\mathbf{a}} = {g_{\mathbf{a}}}^p.$$

Pour l'étude de U aux pointes, on aura aussi besoin de

$$U_c := U\,|_{\beta_c} = \prod_{\mathbf{a}\in A\cdot\beta_c} u_{\mathbf{a}} \qquad \text{où } \beta_c = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}).$$

Remarque 6.2.2. — Comme on l'a vu à la section 1.5.3, l'ensemble

$$\left\{{\beta_0}^{-1}\cdot\infty,\ {\beta_1}^{-1}\cdot\infty,\dots,\ {\beta_{\frac{p-1}{2}}}^{-1}\cdot\infty\right\}$$

est un système de représentants des pointes de $X_{split}(p)$.

Proposition 6.2.3. — *La fonction U est modulaire pour $\Gamma_{split}(p)$.*

Démonstration. — Soit $\beta \in \Gamma_{split}(p) \subset \mathbf{SL}_2(\mathbb{Z})$. D'après la Proposition 5.3.5, on a

$$U\,|_{\beta} = \prod_{a\in A}(u_{\mathbf{a}}\,|_{\beta}) = \prod_{a\in A} u_{\mathbf{a}\cdot\beta} = \prod_{a'\in A\cdot\beta} u_{\mathbf{a}'} = U$$

car $A\cdot\beta = A$. □

On déduit immédiatement de la Proposition 5.3.4 que :

Proposition 6.2.4. — *La fonction U n'a ni pôle ni zéro sur la partie affine $Y_{split}(p)$ de $X_{split}(p)$.*

6.2.2. Intégralité, et majoration globale de U. — On a vu à la Proposition 5.4.2 que les fonctions $g_{\mathbf{a}}$ et $(1-\zeta_p)^{12}{g_{\mathbf{a}}}^{-1}$ sont entières sur $\mathbb{Z}[j]$. Cela fournit des renseignements sur U, que l'on donne ici sous la forme d'un encadrement analytique :

Proposition 6.2.5. — *Pour tout $P \in Y_{split}(p)(\mathbb{Z})$, on a*

$$0 \leqslant \log|U(P)| \leqslant 24p\log p.$$

Démonstration. — Soit $P \in Y_{split}(p)(\mathbb{Z})$: par définition cela signifie que $j(P) \in \mathbb{Z}$. Comme U n'a aucun pôle ou zéro sur $Y_{split}(p)$ et que U est une fonction rationnelle sur $X_{split}(p)$, on a

$$U(P) \in \mathbb{Q} \smallsetminus \{0\}.$$

D'autre part, si l'on fixe ζ_p, une racine primitive p-ième de l'unité dans $\mathbb{C}$, on a démontré (Proposition 5.4.2) que les fonctions $g_{\mathbf{a}}$ et $(1-\zeta_p)^{12}{g_{\mathbf{a}}}^{-1}$ sont entières sur $\mathbb{Z}[j]$. Or, U est un produit de $2(p-1)$ fonctions ${g_{\mathbf{a}}}^p$. Donc U et $(1-\zeta_p)^{24p(p-1)}U^{-1}$ sont des fonctions entières sur $\mathbb{Z}[j]$. En particulier, leurs valeurs en des points entiers de $Y_{split}(p)$ sont des entiers algébriques. Ceci a deux conséquences :

- $U(P)$ est un entier algébrique, qui est aussi un rationnel non nul. Donc $U(P)$ est un entier non nul.
  Ainsi, $\log|U(P)| \geqslant 0$.
- Dans $\mathbb{Z}[\zeta_p]$, la valeur de U en P divise $(1-\zeta_p)^{24p(p-1)}$. Si l'on note $\mathbf{N} = \mathbf{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}$, cela entraîne que $\mathbf{N}(U(P)) = U(P)^{p-1}$ divise $\mathbf{N}((1-\zeta_p)^{24p(p-1)}) = p^{24p(p-1)}$ dans $\mathbb{Z}$, car $\mathbf{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1-\zeta_p) = p$. En particulier, cela fournit :
$$|U(P)|^{p-1} = U(P)^{p-1} \leqslant p^{24p(p-1)}.$$

Ce qui donne le résultat escompté en passant au logarithme. □

6.2.3. Justification de la construction de U. —

Proposition 6.2.6. — *L'unité modulaire U peut se mettre sous la forme :*

$$\forall \tau \in \mathfrak{H}, \qquad U(\tau) = p^{12p} \cdot \left(\frac{\Delta(p\tau)\cdot\Delta(\tau/p)}{\Delta(\tau)^2}\right)^p.$$

Démonstration. — Pour $\mathbf{a} = (a_1, a_2) \in (p^{-1}\mathbb{Z})^2 \smallsetminus \mathbb{Z}^2$ avec $0 \leqslant a_1 < 1$, on a vu (Proposition 5.3.1) que

$$\forall \tau \in \mathfrak{H}, \qquad g_{\mathbf{a}}(\tau) = q^{6\cdot B_2(a_1)} \cdot \mathrm{e}^{12i\pi a_2(a_1-1)} \cdot \prod_{n=0}^{\infty} \left((1-\mathrm{e}^{2i\pi a_2}\cdot q^{n+a_1})(1-\mathrm{e}^{-2i\pi a_2}\cdot q^{n+1-a_1})\right)^{12}.$$

Comme A est l'ensemble des $(\frac{k}{p}, 0)$ et des $(0, \frac{k}{p})$ pour $k = 1 \dots p-1$, on regarde seulement les expressions de ${g_{(\frac{k}{p},0)}}^p$ et ${g_{(0,\frac{k}{p})}}^p$: on a

$$\left(g_{(\frac{k}{p},0)}(\tau)\right)^p = q^{6p\cdot B_2(k/p)} \cdot \prod_{n=0}^{\infty} \left((1-q^{n+k/p})(1-q^{n+1-k/p})\right)^{12p}$$

et

$$\left(g_{(0,\frac{k}{p})}(\tau)\right)^p = q^{6p\cdot B_2(0)} \cdot \prod_{n=0}^{\infty} \left((1-\mathrm{e}^{2i\pi k/p}\cdot q^n)(1-\mathrm{e}^{-2i\pi k/p}\cdot q^{n+1})\right)^{12p}.$$

Par conséquent, à partir de la définition de U, on obtient :

$$\begin{aligned}
U(\tau) &= \prod_{\mathbf{a}\in A} (g_{\mathbf{a}}(\tau))^p = \prod_{k=1}^{p-1} \left(g_{(\frac{k}{p},0)}(\tau)\right)^p \cdot \prod_{k=1}^{p-1} \left(g_{(0,\frac{k}{p})}(\tau)\right)^p \\
&= q^{6p\cdot\left(\sum_{k=1}^{p-1} B_2(k/p) + \sum_{k=1}^{p-1} B_2(0)\right)} \cdot \prod_{n=0}^{\infty} \left(\prod_{k=1}^{p-1} \left((1-q^{n+k/p})(1-q^{n+1-k/p})(1-\mathrm{e}^{2i\pi k/p}\cdot q^n)(1-\mathrm{e}^{-2i\pi k/p}\cdot q^{n+1})\right)\right)^{12p} \\
&= q^{-(p-1)^2} \cdot \prod_{n=0}^{\infty} \left(\prod_{k=1}^{p-1} \left((1-q^{n+k/p})(1-q^{n+1-k/p})(1-\mathrm{e}^{2i\pi k/p}\cdot q^n)(1-\mathrm{e}^{-2i\pi k/p}\cdot q^{n+1})\right)\right)^{12p}.
\end{aligned}$$

Traitons séparément chacun des facteurs du produit infini :

- Premièrement, on remarque que
$$\prod_{k=1}^{p-1}(1-\mathrm{e}^{2i\pi k/p}\cdot q^n) = \begin{cases} p & \text{si } n = 0, \\ \frac{1-q^{np}}{1-q^n} & \text{si } n \neq 0. \end{cases}$$
  Ce qui permet de simplifier l'expression suivante :
$$\prod_{n=0}^{\infty}\prod_{k=1}^{p-1}(1-\mathrm{e}^{2i\pi k/p}\cdot q^n) = \prod_{k=1}^{p-1}(1-\mathrm{e}^{2i\pi k/p}) \cdot \prod_{n=1}^{\infty}\prod_{k=1}^{p-1}(1-\mathrm{e}^{2i\pi k/p}\cdot q^n) = p\cdot\prod_{n=1}^{\infty}\frac{1-q^{np}}{1-q^n}.$$

- En appliquant la même identité, on obtient
$$\prod_{n=0}^{\infty}\prod_{k=1}^{p-1}(1-\mathrm{e}^{-2i\pi k/p}\cdot q^{n+1}) = \prod_{n=1}^{\infty}\frac{1-q^{np}}{1-q^n}.$$
- Deuxièmement, en faisant une réindexation, on a
$$\prod_{k=1}^{p-1}(1-q^{n+k/p}) = \frac{\prod_{k=np}^{(n+1)p-1}(1-q^{k/p})}{1-q^n} \qquad \text{si } n\neq 0.$$
Si bien que :
$$\prod_{n=0}^{\infty}\prod_{k=1}^{p-1}(1-q^{n+k/p}) = \prod_{k=1}^{p-1}(1-q^{k/p})\cdot\prod_{n=1}^{\infty}\prod_{k=1}^{p-1}(1-q^{n+k/p}) = \prod_{k=1}^{p-1}(1-q^{k/p})\cdot\prod_{n=1}^{\infty}\frac{\prod_{k=np}^{(n+1)p-1}(1-q^{k/p})}{1-q^n}$$
$$= \prod_{k=1}^{p-1}(1-q^{k/p})\cdot\frac{\prod_{n=p}^{\infty}(1-q^{k/p})}{\prod_{n=1}^{\infty}(1-q^n)} = \frac{\prod_{n=1}^{\infty}(1-q^{k/p})}{\prod_{n=1}^{\infty}(1-q^n)}.$$
- Enfin, par une autre réindexation, on tire :
$$\prod_{k=1}^{p-1}(1-q^{n+1-k/p}) = \frac{\prod_{k=np+1}^{(n+1)p}(1-q^{k/p})}{1-q^{n+1}}.$$
D'où l'on déduit que
$$\prod_{n=0}^{\infty}\prod_{k=1}^{p-1}(1-q^{n+1-k/p}) = \prod_{n=0}^{\infty}\frac{\prod_{k=np+1}^{(n+1)p}(1-q^{k/p})}{1-q^{n+1}} = \frac{\prod_{n=1}^{\infty}(1-q^{k/p})}{\prod_{n=0}^{\infty}(1-q^{n+1})} = \frac{\prod_{n=1}^{\infty}(1-q^{k/p})}{\prod_{n=1}^{\infty}(1-q^n)}.$$

Combinant enfin ces égalités avec les définitions de U et de $\Delta(\tau)=(2\pi)^{12}q\prod_{n=1}^{\infty}(1-q^n)^{24}$, on obtient :
$$U(\tau) = q^{-(p-1)^2}\cdot\left(p\cdot\prod_{n=1}^{\infty}\frac{1-q^{np}}{1-q^n}\cdot\prod_{n=1}^{\infty}\frac{1-q^{np}}{1-q^n}\cdot\frac{\prod_{n=1}^{\infty}(1-q^{k/p})}{\prod_{n=1}^{\infty}(1-q^n)}\cdot\frac{\prod_{n=1}^{\infty}(1-q^{k/p})}{\prod_{n=1}^{\infty}(1-q^n)}\right)^{12p}$$
$$= p^{12p}\cdot q^{-(p-1)^2}\cdot\left(\frac{\left(\prod_{n=1}^{\infty}(1-q^{np})\right)^2\cdot\left(\prod_{n=1}^{\infty}(1-q^{n/p})\right)^2}{\left(\prod_{n=1}^{\infty}(1-q^n)\right)^4}\right)^{12p}$$
$$= p^{12p}\cdot q^{-(p-1)^2}\cdot\left(\frac{\prod_{n=1}^{\infty}(1-q^{np})^{24}\cdot\prod_{n=1}^{\infty}(1-q^{n/p})^{24}}{\prod_{n=1}^{\infty}(1-q^n)^{24}\cdot\prod_{n=1}^{\infty}(1-q^n)^{24}}\right)^{p}$$
$$= p^{12p}\cdot q^{-(p-1)^2}\cdot\left(\frac{\Delta(p\tau)}{(2\pi)^{12}q^p}\cdot\frac{\Delta(\tau/p)}{(2\pi)^{12}q^{1/p}}\cdot\frac{(2\pi)^{12}q}{\Delta(\tau)}\cdot\frac{(2\pi)^{12}q}{\Delta(\tau)}\right)^{p}$$
$$= p^{12p}\cdot q^{-(p-1)^2}\cdot q^{p(2-p-1/p)}\cdot\left(\frac{\Delta(p\tau)\cdot\Delta(\tau/p)}{\Delta(\tau)^2}\right)^{p} = p^{12p}\cdot\left(\frac{\Delta(p\tau)\cdot\Delta(\tau/p)}{\Delta(\tau)^2}\right)^{p}$$

Ce qui conclut la preuve. □

Corollaire 6.2.7. — *La fonction U est définie sur $\mathbb{Q}$.*

Remarque 6.2.8. — Ceci illustre un théorème de **[KL81]** qui affirme qu'une fonction sur $X_{split}(p)$ dont le diviseur est concentré aux pointes est, à une constante près, une certaine puissance d'un produit de fonctions de Siegel (on calculera le diviseur de U plus bas).

6.3. Etude de U aux pointes

6.3.1. Etre proche d'une pointe. — Lors de l'estimation de l'invariant j faite à la section 6.1, on a pris comme « définition » :
$$\tau\in\mathfrak{H} \text{ est proche de la pointe } i\infty\in\mathfrak{H}^* \iff \tau\in\mathcal{D}+\mathbb{Z} \iff |q|<\mathrm{e}^{-\pi\sqrt{3}}$$
Il semble alors naturel de prolonger cette « définition » à la courbe modulaire $X_{split}(p)(\mathbb{C})=\Gamma_{split}(p)\backslash\mathfrak{H}^*$ par l'équivalence suivante : si ${\beta_c}^{-1}\infty$ est une pointe de $X_{split}(p)$, on décrète que
$$P\in Y_{split}(p)(\mathbb{C}) \text{ est proche de } {\beta_c}^{-1}\infty \iff \text{un relevé } \tau\in\mathfrak{H} \text{ de } P \text{ vérifie } \beta_c\cdot\tau\in\mathcal{D}+\mathbb{Z}$$
Démontrons que les « voisinages des pointes » ainsi définis recouvrent entièrement $Y_{split}(p)(\mathbb{C})$:

Lemme 6.3.1. — *Pour tout point $P\in Y_{split}(p)(\mathbb{C})$, il existe $c\in[\![0,\frac{p-1}{2}]\!]$ et $\tau\in\mathcal{D}+\mathbb{Z}$ tels que*
$$j(P)=j(\tau) \qquad \text{et} \qquad U(P)=U_c(\tau)$$

Démonstration. — Un point $P \in Y_{split}(p)(\mathbb{C})$ se relève par un point $\tau' \in \mathfrak{H}$ tel que

$$j(\tau') = j(P) \qquad \text{et} \qquad U(\tau') = U(P)$$

via la surjection canonique $\mathfrak{H} \twoheadrightarrow Y_{split}(p)(\mathbb{C})$. En premier lieu, fixons $\beta \in \mathbf{SL}_2(\mathbb{Z})$ tel que $\tau = \beta^{-1} \cdot \tau'$ soit dans $\mathcal{D}$: cela est toujours possible car $\mathcal{D}$ est un domaine fondamental pour l'action de $\mathbf{SL}_2(\mathbb{Z})$ sur $\mathfrak{H}$.

Ensuite, on a démontré plus haut (Proposition 1.5.3) que les matrices $\beta_0, \beta_1, \ldots, \beta_{\frac{p-1}{2}}$ fournissent un système complet de représentants des pointes de $Y_{split}(p)(\mathbb{C})$. Ceci signifie qu'il existe $c \in [\![0, \frac{p-1}{2}]\!]$ tel que

$$\beta = \gamma \cdot \beta_c$$

pour un certain $\gamma \in \Gamma_{split}(p)$. Alors $\tau = \beta^{-1} \cdot \tau'$ satisfait aux conditions demandées. □

6.3.2. Ordres de U aux pointes. — Dans cette section, on réutilise les estimations faites sur les fonctions $g_{\mathbf{a}}$ pour en déduire des résultats sur le comportement de U aux pointes de $Y_{split}(p)$. Donnons dans un premier temps l'ordre de U_c à la pointe ∞ de $Y_{split}(p)(\mathbb{C})$.

Proposition 6.3.2. — *Soit $c \in [\![0, \frac{p-1}{2}]\!]$. Alors on a*

$$\mathrm{ord}_\infty(U_c) = \begin{cases} (p-1)^2 & \text{si } c = 0, \\ -2(p-1) & \text{sinon.} \end{cases}$$

Démonstration. — On somme les ordres à l'infini des fonctions $g_{\mathbf{a}}$, que l'on a calculé au Lemme 5.3.3. De manière générale, à partir de la définition de U comme produit de ${g_{\mathbf{a}}}^{12p}$, on déduit que l'ordre de U en $q = 0$ doit être

$$\mathrm{ord}_\infty U_c = p \cdot \sum_{\mathbf{a} \in A\beta_c} \mathrm{ord}_\infty g_{\mathbf{a}} = p \cdot \sum_{\mathbf{a} \in A\beta_c} 6 \cdot B_2(a_1) = 6p \cdot \sum_{\mathbf{a} \in A\beta_c} B_2(a_1). \tag{4}$$

Un calcul facile montre par ailleurs que

$$\sum_{k=1}^{p-1} B_2\left(\tfrac{k}{p}\right) = -\frac{p-1}{6p}.$$

Distinguons maintenant deux cas :

- Si $c = 0$, alors $\beta_c = I$ et $U_c = U$. Ce qui conduit au calcul suivant :

$$\mathrm{ord}_\infty U = 6p \cdot \sum_{\mathbf{a} \in A} B_2(a_1) = 6p \cdot \left(\sum_{k=1}^{p-1} B_2\left(\tfrac{k}{p}\right) + (p-1) \cdot B_2(0) \right) = (p-1)^2.$$

- Si maintenant $c \neq 0$, on peut fixer un entier b tel que $bc = 1 \bmod p$. Dans ce cas, β_c agit non trivialement sur A. En effet,

$$A\beta_c = \big\{(a_1, 0),\ a_1 \in (p^{-1}\mathbb{Z}/\mathbb{Z}) \smallsetminus \{0\}\big\} \cup \big\{(a_2, a_2 \cdot b),\ a_2 \in (p^{-1}\mathbb{Z}/\mathbb{Z}) \smallsetminus \{0\}\big\},$$

  si bien que la formule générale (4) devient ici :

$$\mathrm{ord}_\infty U_c = 6p \cdot 2 \cdot \sum_{k=1}^{p-1} B_2\left(\tfrac{k}{p}\right) = -2(p-1).$$

□

Cette proposition se traduit immédiatement en :

***Corollaire 6.3.3* (Ordre aux pointes).** — *Pour une pointe P de $X_{split}(p)$, on fixe $c \in [\![0, \frac{p-1}{2}]\!]$ tel que $P = \beta_c^{-1}\infty$. Alors*

$$\mathrm{ord}_P(U) = \begin{cases} (p-1)^2 & \text{si } c = 0, \\ -2(p-1) & \text{sinon.} \end{cases}$$

Remarque 6.3.4. — Comme U n'a ni pôle ni zéro en dehors des pointes, on vient en fait de calculer son diviseur : si $P_0 = \infty, P_1, \ldots, P_{\frac{p-1}{2}}$ désignent les pointes de $X_{split}(p)$, on a

$$\mathrm{div}\, U = 2(p-1) \cdot \left(\frac{p-1}{2} \cdot \infty - \left(P_1 + \cdots + P_{\frac{p-1}{2}} \right) \right).$$

6.3.3. Développement de U aux pointes. — Il nous faut aussi décrire le terme suivant dans le développement aux pointes de U.

Proposition 6.3.5. — *Pour $c \in [\![0, \frac{p-1}{2}]\!]$, on a*

$$\forall \tau \in \mathcal{D}+\mathbb{Z}, \quad \Big|\log|U_c(\tau)| - \mathrm{ord}_\infty U_c \cdot \log|q|\Big| \leqslant \begin{cases} -4\pi^2 \frac{p^2}{\log|q|} + 12p\log p + 55p^2|q| & \text{si } c=0, \\ -8\pi^2 \frac{p^2}{\log|q|} + 50p^2|q| & \text{sinon.} \end{cases}$$

Démonstration. — Soit $\mathbf{a}=(a_1,a_2)\in A$. Rappelons que l'expression trouvée à la Proposition 6.1.3 :

$$\forall \tau \in \mathcal{D}+\mathbb{Z},\ \log|g_{\mathbf{a}}(\tau)| = \mathrm{ord}_\infty g_{\mathbf{a}} \cdot \log|q| + 12\log\left|1-q^{a_1}\mathrm{e}^{2i\pi a_2}\right| + 12\log\left|1-q^{1-a_1}\mathrm{e}^{-2i\pi a_2}\right| + \gamma(q)$$

où $|\gamma(q)|\leqslant 25|q|$. En passant à la puissance p et en prenant le produit sur tous les $\mathbf{a}\in A\beta_c$, on obtient :

$$\log|U_c(\tau)| = \mathrm{ord}_\infty U_c \cdot \log|q| + 12p\cdot \sum_{\mathbf{a}\in A\beta_c} \Big(\log\left|1-q^{a_1}\mathrm{e}^{2i\pi a_2}\right| + \log\left|1-q^{1-a_1}\mathrm{e}^{-2i\pi a_2}\right|\Big) + 2p(p-1)\gamma(q).$$

Ce que l'on réécrit sous la forme

$$\Big|\log|U_c(\tau)| - \mathrm{ord}_\infty U_c \cdot \log|q|\Big| \leqslant 12p\cdot \left|\sum_{\mathbf{a}\in A\beta_c} \Big(\log\left|1-q^{a_1}\mathrm{e}^{2i\pi a_2}\right| + \log\left|1-q^{1-a_1}\mathrm{e}^{-2i\pi a_2}\right|\Big)\right| + 50p^2|q|.$$

Il s'agit donc de majorer en valeur absolue la somme

$$S_c(\tau) := \sum_{\mathbf{a}\in A\beta_c} \Big(\log\left|1-q^{a_1}\mathrm{e}^{2i\pi a_2}\right| + \log\left|1-q^{1-a_1}\mathrm{e}^{-2i\pi a_2}\right|\Big).$$

Distinguons maintenant les deux cas de la proposition :

- Si $c=0$, alors β_c est la matrice identité et $A\beta_c = A$, si bien que

$$\begin{aligned} S_0(\tau) &= \sum_{k=1}^{p-1}\Big(\log\left|1-q^{k/p}\right| + \log\left|1-q^{1-k/p}\right|\Big) + \sum_{k=1}^{p-1}\Big(\log\left|1-\mathrm{e}^{2i\pi k/p}\right| + \log\left|1-\mathrm{e}^{-2ik/p}\right|\Big) \\ &= 2\sum_{k=1}^{p-1}\log\left|1-q^{k/p}\right| + \sum_{k=1}^{p-1}\log\left|1-\mathrm{e}^{2i\pi k/p}\right| + \sum_{k=1}^{p-1}\log\left|1-q\mathrm{e}^{-2ik/p}\right| \\ &= 2\sum_{k=1}^{p-1}\log\left|1-q^{k/p}\right| + \log p + \log\left|\frac{1-q^p}{1-q}\right|. \end{aligned}$$

- Si $c\neq 0$, on fixe à nouveau $b\in\mathbb{Z}$ tel que $bc = 1 \bmod p$. Dès lors, on connait l'action de β_c sur A :

$$A\beta_c = \big\{(a_1,0),\ a_1\in(p^{-1}\mathbb{Z}/\mathbb{Z})\smallsetminus\{0\}\big\} \cup \big\{(a_2, a_2\cdot b),\ a_2\in(p^{-1}\mathbb{Z}/\mathbb{Z})\smallsetminus\{0\}\big\}.$$

Et on trouve que :

$$\begin{aligned} S_c(\tau) &= \sum_{k=1}^{p-1}\Big(\log\left|1-q^{k/p}\right| + \log\left|1-q^{1-k/p}\right|\Big) + \sum_{k=1}^{p-1}\Big(\log\left|1-q^{k/p}\mathrm{e}^{2i\pi bk/p}\right| + \log\left|1-q^{1-k/p}\mathrm{e}^{-2i\pi bk/p}\right|\Big) \\ &= 2\sum_{k=1}^{p-1}\log\left|1-q^{k/p}\right| + \sum_{k=1}^{p-1}\log\left|1-\left(q^{1/p}\mathrm{e}^{2i\pi b/p}\right)^k\right| + \sum_{k=1}^{p-1}\log\left|1-q\left(q^{-1/p}\mathrm{e}^{-2i\pi b/p}\right)^k\right| \\ &= 2\sum_{k=1}^{p-1}\log\left|1-q^{k/p}\right| + 2\sum_{k=1}^{p-1}\log\left|1-\left(q^{1/p}\mathrm{e}^{2i\pi b/p}\right)^k\right|. \end{aligned}$$

On voit donc, dans les deux cas, la nécessité de maîtriser l'ordre de grandeur de sommes de la forme

$$\forall |z|<1, \quad \left|\sum_{n=1}^{N}\log|1-z^n|\right|.$$

Lemme 6.3.6. — *Pour tout $z\in\mathbb{C}^*$ de module $|z|<1$ et tout $N\in\mathbb{N}^*$, on a*

$$\left|\sum_{n=1}^{N}\log|1-z^n|\right| \leqslant -\frac{\pi^2}{6}\frac{1}{\log|z|}.$$

Démonstration. — Pour $|z|<1$, on sait que $|\log|1+z|| \leqslant -\log(1-|z|)$, on a donc

$$\left|\sum_{n=1}^{N}\log|1-z^n|\right| \leqslant \sum_{n=1}^{N}|\log|1-z^n|| \leqslant -\sum_{n=1}^{N}\log(1-|z|^n).$$

Ainsi, il suffit de montrer que la majoration suivante est vraie :

$$\forall q=|z|\in]0,1[, \qquad -\sum_{n=1}^{\infty}\log(1-q^n) \leqslant -\frac{\pi^2}{6}\frac{1}{\log q}.$$

Distinguons alors deux cas :

- Pour $q = |z| < 1/2$, on peut utiliser la majoration classique

$$\forall q \in]0, r] \subset]0, 1[, \qquad |\log(1+q)| \leqslant \frac{|\log(1-r)|}{r} q \tag{5}$$

avec $r = 1/2$ et on obtient :

$$-\sum_{n=1}^{\infty} \log(1-q^n) \leqslant 2\log 2 \cdot \sum_{n=1}^{\infty} q^n = 2\log 2 \cdot \frac{q}{1-q} \leqslant 4\log 2 \cdot q.$$

Une étude rapide montre par ailleurs que

$$4\log 2 \cdot q \leqslant -\frac{\pi^2}{6}\frac{1}{\log q}.$$

Ce qui termine la preuve du lemme dans ce cas.

- Pour $q \geqslant 1/2$, on pose $\tau = \log q / 2i\pi$ et on utilise la fonction η de Dedekind, définie par

$$\eta(\tau) = q^{1/24} \cdot \prod_{n=1}^{\infty} (1-q^n).$$

Cette fonction vérifie une équation fonctionnelle (cf. par exemple **[Lan87]**), que l'on traduit ici par

$$\log|\eta(-\tau^{-1})| = \log|\eta(\tau)| - \frac{1}{2}\log|\tau|.$$

On peut de plus relier η à la somme qu'on cherche à majorer par

$$-\sum_{n=1}^{\infty} \log(1-q^n) = \frac{1}{24}\log q - \log|\eta(\tau)| \qquad \text{et} \qquad -\sum_{n=1}^{\infty} \log(1-Q^n) = \frac{1}{24}\log Q - \log|\eta(-\tau^{-1})|$$

où l'on a posé $Q = \mathrm{e}^{2i\pi(-\tau^{-1})} = \mathrm{e}^{4\pi^2/\log q}$. D'où l'égalité suivante :

$$-\sum_{n=1}^{\infty} \log(1-q^n) = -\frac{1}{24}\log Q + \frac{1}{24}\log q + \frac{1}{2}\log|\tau| - \sum_{n=1}^{\infty} \log(1-Q^n).$$

Or, du côté droit de cette égalité,

- le premier terme vaut $-\frac{\pi^2}{6}\frac{1}{\log q}$,
- le second terme est négatif car $q \in]0, 1[$,
- la somme des deux derniers termes est négative. En effet, le fait que $q \geqslant 1/2$ implique que

$$\log|\tau| \leqslant \log\frac{2\pi}{\log 2} \qquad \text{et} \qquad Q \leqslant \mathrm{e}^{-4\pi^2/\log 2} \leqslant 10^{-24}.$$

D'autre part, en appliquant (5) avec $Q \leqslant r = 10^{-24}$, on a

$$\begin{aligned}\left|-\sum_{n=1}^{\infty} \log(1-Q^n)\right| &\leqslant \left|\frac{\log(1-10^{-24})}{10^{-24}}\right| \cdot \sum_{n=1}^{\infty} Q^n \leqslant \left|\frac{\log(1-10^{-24})}{10^{-24}}\right| \cdot \frac{Q}{1-Q} \\ &\leqslant \frac{|\log(1-10^{-24})|}{10^{-24}} \cdot \frac{10^{-24}}{1-10^{-24}} \leqslant 10^{-23}.\end{aligned}$$

Et cela permet de conclure que l'on a

$$\frac{1}{2}\log|\tau| - \sum_{n=1}^{\infty} \log(1-Q^n) \leqslant -\frac{1}{2}\log\frac{2\pi}{\log 2} - \sum_{n=1}^{\infty} \log(1-Q^n) \leqslant -1 + 10^{-23} \leqslant 0.$$

Finalement, on a montré que

$$-\sum_{n=1}^{\infty} \log(1-q^n) \leqslant -\frac{\pi^2}{6}\frac{1}{\log q}$$

dans le cas où $q \geqslant 1/2$ aussi. Ce qui conclut la preuve du lemme.

□

Revenons aux calculs en cours : on avait trouvé que

$$S_c(\tau) = \begin{cases} 2\displaystyle\sum_{k=1}^{p-1} \log\left|1-q^{k/p}\right| + \log p + \log\left|\frac{1-q^p}{1-q}\right| & \text{si } c = 0, \\ 2\displaystyle\sum_{k=1}^{p-1} \log\left|1-q^{k/p}\right| + 2\sum_{k=1}^{p-1} \log\left|1-(q^{1/p}\mathrm{e}^{2i\pi b/p})^k\right| & \text{sinon.} \end{cases}$$

- Dans le cas $c = 0$, on applique le lemme avec $z = q^{1/p}$ à la somme :

$$\begin{aligned}|S_0(\tau)| &\leqslant 2\left|\sum_{k=1}^{p-1}\log\left|1-q^{k/p}\right|\right| + \log p + \left|\log\left|\frac{1-q^p}{1-q}\right|\right| \\ &\leqslant -\frac{2\pi^2}{6}\cdot\frac{p}{\log|q|} + \log p + |\log|1-q^p|| + |\log|1-q||.\end{aligned}$$

  Le fait que τ appartienne à $\mathcal{D}+\mathbb{Z}$ garantit que $|q| \leqslant \mathrm{e}^{-\pi\sqrt{3}}$. Donc, en utilisant à nouveau (5), on a

$$|\log|1-q|| \leqslant \frac{|\log(1-\mathrm{e}^{-\pi\sqrt{3}})|}{\mathrm{e}^{-\pi\sqrt{3}}}|q| \leqslant 1{,}0022|q|$$

  et

$$|\log|1-q^p|| \leqslant 1{,}0022|q|^p \leqslant 0{,}00002|q|.$$

  En sommant ces deux majorations, on trouve que

$$|S_0(\tau)| \leqslant \frac{\pi^2}{3}\cdot\frac{p}{\log|q|} + \log p + 1{,}0023|q|.$$

  D'où la majoration attendue dans le cas $c = 0$:

$$\begin{aligned}\big|\log|U_0(\tau)| - \mathrm{ord}_\infty U_0\cdot\log|q|\big| &\leqslant 12p\cdot\left(\frac{\pi^2}{3}\cdot\frac{p}{\log|q|} + \log p + 1{,}02|q|\right) + 50p^2|q| \\ &= -4\pi^2\frac{p^2}{\log|q|} + 12p\log p + 12p\cdot 1{,}0023|q| + 50p^2|q| \\ &\leqslant -4\pi^2\frac{p^2}{\log|q|} + 12p\log p + 55p^2|q|,\end{aligned}$$

  car, pour $p \geqslant 3$, on a clairement $12\times 1{,}0023\cdot p|q| \leqslant 5p^2|q|$.
- Si $c \neq 0$, on avait trouvé que :

$$|S_c(\tau)| \leqslant 2\left|\sum_{k=1}^{p-1}\log\left|1-q^{k/p}\right|\right| + 2\left|\sum_{k=1}^{p-1}\log\left|1-(q^{1/p}\mathrm{e}^{2i\pi b/p})^k\right|\right|.$$

  On applique alors deux fois le Lemme 6.3.6 avec $z = q^{1/p}$ et $z = q^{1/p}\mathrm{e}^{2i\pi b/p}$ et l'on obtient la majoration suivante :

$$|S_c(\tau)| \leqslant -\frac{\pi^2}{3}\frac{p}{\log|q|} - \frac{\pi^2}{3}\frac{p}{\log|q|} = -\frac{2\pi^2}{3}\frac{p}{\log|q|}.$$

  D'où finalement,

$$\begin{aligned}\big|\log|U_c(\tau)| - \mathrm{ord}_\infty U_c\cdot\log|q|\big| &\leqslant -12p\cdot\frac{2\pi^2}{3}\frac{p}{\log|q|} + 50p^2|q| \\ &\leqslant -8\pi^2\frac{p^2}{\log|q|} + 50p^2|q|.\end{aligned}$$

Ce qui conclut la preuve de la proposition. □

Réécrivons le résultat de la proposition sous la forme qui nous servira plus loin :

***Corollaire 6.3.7* (Version utilitaire).** — *Soit $c \in [\![0, \frac{p-1}{2}]\!]$ et $\tau \in \mathcal{D}+\mathbb{Z}$. On a*

$$\log|q^{-1}| \leqslant \begin{cases} -\dfrac{\log|U_0(\tau)|}{(p-1)^2} - \dfrac{4\pi^2p^2}{(p-1)^2\log|q|} + \dfrac{12p\log p}{(p-1)^2} + 55\dfrac{p^2}{(p-1)^2}|q| & \text{si } c = 0, \\ \dfrac{\log|U_c(\tau)|}{2(p-1)} - \dfrac{4\pi^2p^2}{(p-1)\log|q|} + 25\dfrac{p^2}{p-1}|q| & \text{sinon.}\end{cases}$$

6.4. Conséquences sur j

Le but de l'étude est d'obtenir une majoration uniforme de $\log|j|$ sur les points entiers de $Y_{split}(p)(\mathbb{C})$: il est donc temps de revenir à l'invariant j et de conclure la preuve du Théorème 6.0.3.

Lemme 6.4.1. — *Soit $P \in Y_{split}(p)(\mathbb{Z})$: on fixe $\tau \in \mathcal{D}+\mathbb{Z}$ et $c \in [\![0, \frac{p-1}{2}]\!]$ comme au Lemme 6.3.1. On a alors :*

$$\log|q^{-1}| \leqslant 2\pi\sqrt{p} + 6\log p + 20\frac{(\log p)^2}{\sqrt{p}}.$$

Démonstration. — Procédons en deux temps : q « grand » et q « petit », en fonction de la position de $|q|$ par rapport à

$$\rho := \frac{\mathrm{e}^{-2\pi\sqrt{p}}}{p^6}.$$

- Si $|q| > \rho$, il n'y a rien à démontrer. En effet, on a $\log|q^{-1}| \leqslant -\log\rho = 2\pi\sqrt{p} + 6\log p$ donc, a fortiori,

$$\log|q^{-1}| \leqslant 2\pi\sqrt{p} + 6\log p + 20\frac{(\log p)^2}{\sqrt{p}}.$$

- Pour traiter le cas où $|q| \leqslant \rho$, on utilise les estimations de U_c à l'infini.
  - Pour $c = 0$, on a vu au Corollaire 14 que

$$\log|q^{-1}| \leqslant -\frac{\log|U_0(\tau)|}{(p-1)^2} - \frac{4\pi^2p^2}{(p-1)^2\log|q|} + \frac{12p\log p}{(p-1)^2} + 55\frac{p^2}{(p-1)^2}|q|,$$

  où $U_0(\tau) = U(\tau) = U(P)$ est encadré par (cf. Proposition 6.2.5)

$$-24p\log p \leqslant -\log|U(P)| \leqslant 0.$$

  Ceci et le fait que $|q| \leqslant \rho$ entraînent les majorations suivantes :

$$\begin{aligned}\log|q^{-1}| &\leqslant 0 - \frac{4\pi^2p^2}{(p-1)^2\log\rho} + \frac{12\cdot p\log p}{(p-1)^2} + 55\frac{p^2}{(p-1)^2}\rho \\ &\leqslant \frac{4\pi^2p^2}{(p-1)^2}\cdot\frac{1}{2\pi\sqrt{p}+p^6} + \frac{12\cdot p\log p}{(p-1)^2} + \frac{55\cdot\mathrm{e}^{-2\pi\sqrt{p}}}{(p-1)^2p^4} \\ &\leqslant \frac{2\pi\cdot p^{3/2}}{(p-1)^2} + \frac{12\cdot p\log p}{(p-1)^2} + \frac{55\cdot\mathrm{e}^{-2\pi\sqrt{p}}}{(p-1)^2p^4}.\end{aligned}$$

  En outre, on voit facilement que la fonction majorante est décroissante pour $p \geqslant 3$. Par conséquent,

$$\log|q^{-1}| \leqslant \frac{\pi}{2}\cdot 3^{3/2} + 9\log 3 + \frac{55}{324}\cdot\mathrm{e}^{-2\pi\sqrt{3}} \leqslant 13$$

  Ce qui est même beaucoup plus précis que la majoration annoncée !
  - Pour $c \neq 0$, le Corollaire 14 donne :

$$\log|q^{-1}| \leqslant \frac{\log|U_c(\tau)|}{2(p-1)} - \frac{4\pi^2p^2}{(p-1)\log|q|} + 25\frac{p^2}{p-1}|q|.$$

  De manière similaire au cas précédent, on tire parti de l'encadrement de $U_c(\tau) = U(P)$ trouvé à la Proposition 6.2.5 :

$$0 \leqslant \log|U(P)| = \log|U_c(\tau)| \leqslant 24p\log p$$

  pour avoir

$$\log|q^{-1}| \leqslant \frac{12\cdot p\log p}{p-1} - \frac{4\pi^2p^2}{p-1}\cdot\frac{1}{\log|q|} + 25\frac{p^2}{p-1}|q|.$$

  Modifions quelques termes pour se débarrasser des p^2 :
  - Comme $p \geqslant 3$, on a $\frac{p}{p-1} \leqslant \frac{3}{2}$, donc on peut remplacer

$$25\frac{p^2}{p-1}|q| \leqslant \frac{3}{2}\cdot 25p|q| \leqslant 38p|q|.$$

  - Formellement, on a $\frac{p^2}{p-1} = \frac{p(p-1)+p}{p-1} = p + \frac{p}{p-1}$ et

$$-\frac{4\pi^2p^2}{p-1}\cdot\frac{1}{\log|q|} = -\frac{4\pi^2p}{\log|q|} - \frac{4\pi^2p}{p-1}\cdot\frac{1}{\log|q|}.$$

  - De même, $\frac{p}{p-1} = 1 + \frac{1}{p-1}$. On a donc

$$\frac{12\cdot p\log p}{p-1} = 12\log p + \frac{12\cdot\log p}{p-1}.$$

Continuons maintenant les majorations, en sachant que $|q| \leqslant \rho$:

$$\begin{aligned}\log|q^{-1}| &\leqslant \frac{12\cdot p\log p}{p-1} - \frac{4\pi^2p^2}{p-1}\cdot\frac{1}{\log|q|} + 25\frac{p^2}{p-1}|q| \\ &\leqslant 12\log p + \frac{12\cdot\log p}{p-1} - \frac{4\pi^2p}{\log\rho} - \frac{4\pi^2p}{p-1}\cdot\frac{1}{\log|q|} + 38p\cdot\rho \\ &\leqslant 12\log p - \frac{4\pi^2p}{\log|q|} + \frac{12\cdot\log p}{p-1} + \frac{2\pi\sqrt{p}}{p-1} + 38\frac{\mathrm{e}^{-2\pi\sqrt{p}}}{p^5}.\end{aligned}$$

Or, dans cette inégalité, on peut utiliser la majoration suivante, valable pour $p \geqslant 3$:

$$\frac{12\cdot\log p}{p-1} + \frac{2\pi\sqrt{p}}{p-1} + 38\frac{\mathrm{e}^{-2\pi\sqrt{p}}}{p^5} \leqslant \frac{21}{\sqrt{p}}$$

et l'on obtient

$$\log|q^{-1}| \leqslant 12\log p - \frac{4\pi^2p}{\log|q|} + \frac{21}{\sqrt{p}}.$$

On réécrit cette dernière inégalité sous la forme

$$(\log|q^{-1}|)^2 - \left(12\log p + \frac{21}{\sqrt{p}}\right)\cdot\log|q^{-1}| - 4\pi^2p \leqslant 0,$$

de sorte que $\log|q^{-1}|$ est plus petit que la plus grande des deux racines du polynôme

$$f(T) = T^2 - \left(12\log p + \frac{21}{\sqrt{p}}\right)\cdot T - 4\pi^2p.$$

C'est-à-dire que l'on a

$$\log|q^{-1}| \leqslant 6\log p + \frac{21}{2\sqrt{p}} + \sqrt{4\pi^2p + \left(6\log p + \frac{21}{2\sqrt{p}}\right)^2}.$$

Inégalité sur laquelle on utilise la « formule de Taylor » suivante :

$$\sqrt{x+y} \leqslant \sqrt{x} + \frac{1}{2\sqrt{x}}\cdot y$$

pour avoir

$$\begin{aligned}\log|q^{-1}| &\leqslant 6\log p + \frac{21}{2\sqrt{p}} + \sqrt{\left(6\log p + \frac{21}{2\sqrt{p}}\right) + 4\pi^2p} \\ &\leqslant 6\log p + \frac{21}{2\sqrt{p}} + 2\pi\sqrt{p} + \frac{\left(6\log p + \frac{21}{2\sqrt{p}}\right)^2}{4\pi\sqrt{p}} \\ &\leqslant 6\log p + 2\pi\sqrt{p} + \frac{21}{2\sqrt{p}} + \frac{9(\log p)^2}{\pi\sqrt{p}} + \frac{63\log p}{2\pi p} + \frac{21^2}{64\pi p\sqrt{p}} \\ &\leqslant 6\log p + 2\pi\sqrt{p} + \frac{21}{2\sqrt{p}} + \frac{9(\log p)^2}{\pi\sqrt{p}} + \frac{63\log p}{2\pi p} + \frac{21}{2p\sqrt{p}}. \qquad (6)\end{aligned}$$

En effet, on a $\frac{21^2}{64\pi} \leqslant \frac{21^2}{64\cdot 3} = \frac{147}{16} \leqslant \frac{147}{14} = \frac{21}{2}$. Enfin, par une étude de fonctions, on trouve que, pour $p \geqslant 3$, l'inégalité suivante est vraie

$$\frac{21}{2\sqrt{p}} + \frac{9(\log p)^2}{\pi\sqrt{p}} + \frac{63\log p}{2\pi p} + \frac{21}{2p\sqrt{p}} \leqslant 20\frac{(\log p)^2}{\sqrt{p}}. \qquad (7)$$

En combinant (6) et (7), on tire

$$\log|q^{-1}| \leqslant 6\log p + 2\pi\sqrt{p} + 20\frac{(\log p)^2}{\sqrt{p}}.$$

Dans les deux cas, on a bien

$$\log|q^{-1}| \leqslant 2\pi\sqrt{p} + 6\log p + 20\frac{(\log p)^2}{\sqrt{p}}.$$

Donc le lemme est démontré. □

Lemme 6.4.2. — *Soit $\tau \in \mathcal{D} + \mathbb{Z}$ tel que $|j(\tau)| \geqslant 3500$. Alors on a*

$$\log|j(\tau)| \leqslant \log|q^{-1}| + \frac{1}{2}\cdot\frac{963}{|j(\tau)| - 963}.$$

Démonstration. — Remarquons que, pour tout réel $x > 1/2$, on a

$$\log(x) \leqslant \frac{1}{2} \cdot \frac{|1-x|}{|x| - |1-x|}. \tag{8}$$

En effet, la fonction $f : x \mapsto \frac{1}{2} \cdot \frac{|1-x|}{|x|-|1-x|} - \log(x)$ est décroissante sur $]1/2, 1]$ puis croissante sur $[1, +\infty[$, et $f(1) = 0$. Pour $\tau \in \mathcal{D} + \mathbb{Z}$ comme dans l'énoncé du lemme, le Corollaire 6.1.2 donne

$$\big||j(\tau)| - |q^{-1}|\big| \leqslant |j(\tau) - q^{-1}| \leqslant 963. \tag{9}$$

D'où l'on tire la minoration suivante :

$$\frac{|j(\tau)|}{|q^{-1}|} \geqslant \frac{|j(\tau)|}{963 + |j(\tau)|}.$$

Or, la fonction $g : x \in \mathbb{R}_+^* \mapsto \frac{x}{1+x}$ tend vers 1 en croissant lorsque $x \to +\infty$. Donc on a

$$\frac{|j(\tau)|}{|q^{-1}|} \geqslant \frac{|j(\tau)|}{963 + |j(\tau)|} = g(|j(\tau)|) \geqslant g(3500) = \frac{3500}{963 + 3500} = 0,784\ldots \geqslant \frac{1}{2}.$$

On peut donc appliquer (8) à $x = |j(\tau)|/|q^{-1}|$, et on obtient, en utilisant à nouveau (9),

$$\begin{aligned}
\log|j(\tau)| &\leqslant \log|q^{-1}| + \frac{1}{2} \cdot \frac{\left|1 - \frac{|j(\tau)|}{|q^{-1}|}\right|}{\frac{|j(\tau)|}{|q^{-1}|} - \left|1 - \frac{|j(\tau)|}{|q^{-1}|}\right|} \\
&= \log|q^{-1}| + \frac{1}{2} \cdot \frac{\big||j(\tau)| - |q^{-1}|\big|}{|j(\tau)| - \big||j(\tau)| - |q^{-1}|\big|} \\
&\leqslant \log|q^{-1}| + \frac{1}{2} \cdot \frac{963}{|j(\tau)| - 963}.
\end{aligned}$$

□

A partir de ces résultats, concluons enfin la preuve du Théorème 6.0.3, annoncé en début de chapitre.

Démonstration du Théorème 6.0.3. — Il s'agit de montrer que

$$\forall P \in Y_{split}(\mathbb{Z}), \qquad \log|j(P)| \leqslant 2\pi\sqrt{p} + 6\log p + 21\frac{(\log p)^2}{\sqrt{p}}.$$

On peut se limiter au cas où $|j(\tau)| \geqslant 3500$. En effet, si $|j(\tau)| < 3500$ alors,

$$\log|j(\tau)| \leqslant \log 3500 = 8,2\cdots < 31,4... = 2\pi\sqrt{3} + 6\log 3 + 20\frac{(\log 3)^2}{\sqrt{3}} \leqslant 2\pi\sqrt{p} + 6\log p + 20\frac{(\log p)^2}{\sqrt{p}}.$$

Supposons donc que $|j(\tau)| \geqslant 3500$. Le Lemme 6.4.2 donne alors la majoration :

$$\log|j(\tau)| \leqslant \log|q^{-1}| + \frac{1}{2}\frac{963}{|j(\tau)| - 963}.$$

Dès lors, au vu du Lemme 6.4.1, il s'agit donc de voir que $\frac{963}{2(|j(\tau)|-963)}$ est plus petit que $\frac{(\log p)^2}{\sqrt{p}}$:

- Si $\log|j(\tau)| < 2\pi\sqrt{p} + 6\log p$, il n'y a rien à démontrer.
- Si maintenant $\log|j(\tau)| \geqslant 2\pi\sqrt{p} + 6\log p$, on a

$$\frac{963}{2(|j(\tau)| - 963)} \leqslant \frac{963}{2(p^6 e^{2\pi\sqrt{p}} - 963)} \leqslant \frac{(\log p)^2}{\sqrt{p}}.$$

Ce qui conclut la preuve. □

CHAPITRE 7

FIN DE L'ARGUMENT

Dans ce chapitre, nous terminons la preuve du Théorème 0.0.1. Nous suivrons principalement l'argument donné dans [**BPR11**], ainsi que les preuves exposées dans [**BP09b**] et [**BP09a**].

7.1. Encore une estimation de l'invariant j

Démontrons tout de suite deux minorations pour usage futur. Dans toute la suite, on pose $q = \mathrm{e}^{2i\pi\tau}$.

Lemme 7.1.1. — *Pour tout $\tau \in \mathcal{D} + \mathbb{Z}$, on a*

$$|j(\tau)| \geqslant \mathrm{e}^{2\pi \cdot \mathrm{Im}\,\tau} - 740.$$

Démonstration. — On a démontré à la Proposition 6.1.1) que

$$\forall \tau \in \mathcal{D} + \mathbb{Z}, \qquad \left|j(\tau) - q^{-1} - 744\right| \leqslant 309000|q|^2.$$

Comme $\tau \in \mathcal{D} + \mathbb{Z}$, on a $|q| \leqslant \mathrm{e}^{-\pi\sqrt{3}}$. Cela entraîne que

$$\left|j(\tau) - q^{-1} - 744\right| \leqslant 309000 \cdot \mathrm{e}^{-2\pi\sqrt{3}} \leqslant 5,9$$

après application numérique. Dans ce cas, l'inégalité triangulaire fournit :

$$|q|^{-1} - 740 \leqslant |q|^{-1} - 744 + 5,9 \leqslant |j(\tau)|.$$

Ce qui donne bien le résultat escompté. □

Lemme 7.1.2. — *Soit $\tau \in \mathcal{D}$, on a*

$$\log|\Delta(\tau)| \geqslant \log|q| - \frac{1}{9} + 12\log(2\pi).$$

Démonstration. — On a tout d'abord

$$\left|\log\left|\frac{\Delta(\tau)}{(2\pi)^{12}q}\right|\right| = \left|24\sum_{n=1}^{\infty}\log|1-q^n|\right| \leqslant 24\sum_{n=1}^{\infty}|\log|1-q^n|| \leqslant 24\sum_{n=1}^{\infty} -\log(1-|q|^n) \tag{10}$$

où l'on a utilisé l'inégalité $|\log|1+z|| \leqslant -\log(1-|z|)$ (valable pour $|z|<1$). Et on se sert maintenant de

$$\forall |z| \leqslant r < 1, \qquad |\log(1+z)| \leqslant \frac{|\log(1-r)|}{r}|z|$$

avec $z = q$ et $r = \mathrm{e}^{-\pi\sqrt{3}}$, pour trouver que

$$\sum_{n=1}^{\infty} -\log(1-|q|^n) \leqslant \frac{|\log(1-\mathrm{e}^{-\pi\sqrt{3}})|}{\mathrm{e}^{-\pi\sqrt{3}}} \cdot \frac{|q|}{1-|q|} \leqslant \frac{|\log(1-\mathrm{e}^{-\pi\sqrt{3}})|}{\mathrm{e}^{-\pi\sqrt{3}}} \cdot \frac{\mathrm{e}^{-\pi\sqrt{3}}}{1-\mathrm{e}^{-\pi\sqrt{3}}} = \frac{|\log(1-\mathrm{e}^{-\pi\sqrt{3}})|}{1-\mathrm{e}^{-\pi\sqrt{3}}} \leqslant 0,0045.$$

Ce que l'on combine avec (10) : on otbient :

$$\left|\log\left|\frac{\Delta(\tau)}{(2\pi)^{12}q}\right|\right| \leqslant 24 \times 0,0045 \leqslant 0,11 \leqslant \frac{1}{9}.$$

D'où, en particulier,

$$\log\left|\frac{\Delta(\tau)}{(2\pi)^{12}q}\right| \geqslant -\frac{1}{9}.$$

On a donc obtenu la minoration voulue. □

7.2. Hauteurs

7.2.1. Hauteur d'un nombre algébrique. — Soit K un corps de nombres. Pour chaque place v de K, on notera n_v le degré de $K_v/\mathbb{Q}_v$, $|.|_v$ la valeur absolue normalisée associée à v et $\|.\|_v$ la valeur absolue définie par

$$\forall x \in K, \qquad \|x\|_v = |x|_v^{\,n_v}.$$

On note M_K, l'ensemble des places normalisées de K, M_K^0 l'ensemble de celles qui sont finies et M_K^∞ l'ensemble de celles qui sont archimédiennes.

Définition 7.2.1. — La *hauteur relative* d'un élément $\alpha \in K^*$ est définie par

$$\mathrm{H}_K(\alpha) := \prod_{v \in M_K} \max\{1, \|\alpha\|_v\}.$$

On utilisera aussi la *hauteur logarithmique* de α, donnée par $\mathrm{h}_K(\alpha) = \log \mathrm{H}_K(\alpha)$.

Si L/K est une extension finie de corps, on a $\mathrm{H}_L(\alpha) = \mathrm{H}_K(\alpha)^{[L:K]}$. Pour que la hauteur d'un nombre algébrique $\alpha \in \overline{\mathbb{Q}}$ soit indépendante du corps dans lequel on le considère, on peut donc poser :

Définition 7.2.2. — La *hauteur absolue* d'un élément $\alpha \in K^*$ est définie par

$$\mathrm{H}(\alpha) := \mathrm{H}_K(\alpha)^{[K:\mathbb{Q}]}.$$

On utilisera aussi la *hauteur logarithmique* associée, donnée par

$$\mathrm{h}(\alpha) = \log \mathrm{H}(\alpha) = \frac{1}{[K:\mathbb{Q}]} \cdot \sum_{v \in M_K} \log \max\{1, \|\alpha\|_v\}.$$

On peut alors décomposer la hauteur d'un nombre en deux parties : une contribution « archimédienne » et une contribution des places finies :

Lemme 7.2.3. — *Soit K un corps de nombres, et $\alpha \in K^*$. On écrit l'idéal (α) comme un produit $(\alpha) = \mathfrak{a}\mathfrak{b}^{-1}$ de deux idéaux entiers de K, premiers entre eux. Alors ona*

$$\mathrm{H}_K(\alpha) = \mathbf{N}_{K/\mathbb{Q}}(\mathfrak{b}) \cdot \prod_{v \in M_K^\infty} \max\{1, \|\alpha\|_v\}.$$

Démonstration. — Soit $v \in M_K^0$, une place finie de K : on peut fixer un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ tel que $|.|_v = |.|_\mathfrak{p}$. Avec les notations de l'énoncé, on a l'équivalence suivante :

$$\max\{1, \|\alpha\|_v\} > 1 \iff \mathfrak{p} \mid \mathfrak{b}.$$

On notera $e(\mathfrak{p})$ et $f(\mathfrak{p})$, l'indice de ramification et le degré du corps résiduel respectivement. Soit aussi p la caractéristique résiduelle de $\mathfrak{p}$. Si $\mathfrak{p} \mid \mathfrak{b}$, il existe $\pi_\mathfrak{b} \in \mathfrak{b}$ qui vérifie $|{\pi_\mathfrak{b}}^e|_\mathfrak{p} = |p|_\mathfrak{p}$. Rappelons enfin que l'on a $n_v = e(\mathfrak{p}) \cdot f(\mathfrak{p})$. On alors

$$\|{\pi_\mathfrak{b}}^{-e}\|_v = \left|{\pi_\mathfrak{b}}^{-e}\right|_v^{n_v} = (p^{1/e(\mathfrak{p})})^{n_v} = p^{f(\mathfrak{p})} = \mathbf{N}_{K/\mathbb{Q}}(\mathfrak{p}).$$

Si $\mathfrak{b}$ se décompose en produits d'idéaux premiers comme suit :

$$\mathfrak{b} = \prod_\mathfrak{p} \mathfrak{p}^{m_\mathfrak{p}},$$

alors, on a :

$$\begin{aligned}\prod_{v \in M_K^0} \max\{1, \|\alpha\|_v\} &= \prod_{v \in M_K^0 \text{ tq. } \|\alpha\|_v > 1} \max\{1, \|\alpha\|_v\} \\ &= \prod_{\mathfrak{p} \mid \mathfrak{b}} \|\alpha\|_\mathfrak{p} = \prod_{\mathfrak{p} \mid \mathfrak{b}} {\|\pi_b\|_\mathfrak{p}}^{m_\mathfrak{p}} \\ &= \prod_{\mathfrak{p} \mid \mathfrak{b}} \mathbf{N}_{K/\mathbb{Q}}(\mathfrak{p})^{m_\mathfrak{p}} = \mathbf{N}_{K/\mathbb{Q}}(\mathfrak{b}).\end{aligned}$$

En multipliant ce résultat par la contribution des places infinies de K, on trouve l'égalité recherchée. □

7.2.2. Application à $j(E)$. — Soit E, une courbe elliptique définie sur un corps de nombres K. Alors E se met sous la forme d'une cubique de Weierstrass

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

à laquelle on associe le discriminant $\Delta(E)$ de la cubique, et l'invariant $j(E) = \frac{{c_4}^3}{\Delta(E)}$ où $c_4 = ({a_1}^2 + 4a_2)^2 - 24(2a_4 + a_1a_3)$. Soit $v \in M_K^0$, une place finie de K, on considère la courbe E comme une courbe elliptique sur K_v : on peut choisir une équation de Weierstrass

$$E_v : y_v^2 + a_{1,v}x_vy_v + a_{3,v}y_v = x_v^3 + a_{2,v}x_v^2 + a_{4,v}x_v + a_{6,v}$$

qui soit une équation minimale de E en v, au sens où les $a_{i,v}$ vérifient : $v(a_{i,v}) \geqslant 0$ et $v(\Delta(E_v))$ est minimal : on notera Δ_v ce discriminant minimal de E sur K_v, et $c_{4,v}$ le polynôme correspondant en les $a_{i,v}$.

Définition 7.2.4. — Le *discriminant minimal de E/K* est l'idéal entier de K défini par le produit

$$\Delta_{E/K} := \prod_{v \in M_K^0} {\mathfrak{p}_v}^{v(\Delta_v)}$$

où $\mathfrak{p}_v$ est l'idéal premier de $\mathcal{O}_K$ associé à v.

Rappelons qu'une courbe elliptique E/K est dite de *réduction semi-stable en v* si la réduction modulo v de son équation de Weierstrass n'est pas additive (ie. la réduction de E modulo v est soit une courbe elliptique, soit une cubique avec un point double). On dit alors que E est *semi-stable* si elle admet une équation de Weierstrass qui a réduction semi-stable en toutes les places finies de K.

Lemme 7.2.5. — *Soit une courbe elliptique E définie sur un corps de nombres K. On suppose que E/K a réduction semi-stable, alors*

$$(j(E)) = \mathfrak{a} \cdot \Delta_{E/K}^{-1}$$

où $\mathfrak{a}$ est un idéal entier de K, premier à $\Delta_{E/K}$.

Démonstration. — On choisit une équation de Weierstrass de E dont la réduction modulo les places finies de K est semi-stable :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{11}$$

à laquelle on associe les quantités Δ et c_4 usuelles. D'autre part, pour chaque place finie v de K, on a choisi une équation de Weierstrass minimale de E en v :

$$E_v : y_v^2 + a_{1,v}x_vy_v + a_{3,v}y_v = x_v^3 + a_{2,v}x_v^2 + a_{4,v}x_v + a_{6,v}. \tag{12}$$

On peut alors fixer un changement de coordonnées

$$(x, y) = (\alpha^2x + r, \alpha^3y + s\alpha^2x + t), \qquad \alpha \in {K_v}^\times,\ r, s, t, u \in K_v$$

qui transforme la réduction de (11) modulo v en (12). Ceci affecte les quantités Δ et c_4 de la manière suivante :

$$\Delta(E \bmod v) = \alpha^{12}\Delta_v, \qquad c_4 = \alpha^4 c_{4,v}.$$

Par unicité de la décomposition d'un idéal en produit d'idéaux premiers de $\mathcal{O}_K$, il suffit de voir que l'idéal fractionnaire $\mathfrak{a} := (j(E)) \cdot \Delta_{E/K}$ est un idéal entier de K. Pour montrer cela, on étudie localement $\mathfrak{a}$ en calculant $\mathrm{ord}_v(\mathfrak{a})$ pour tout $v \in M_K^0$. Soit donc v, une place finie de K : on a

$$\begin{aligned}\mathrm{ord}_v(\mathfrak{a}) &= \mathrm{ord}_v(\Delta_{E/K}) + v(j(E)) = v(\Delta_v) - v(\Delta(E)) + 3v(c_4)\\ &= v(\Delta_v) - 12v(\alpha) - v(\Delta_v) + 12v(\alpha) + 3v(c_{4,v})\\ &= 3v(c_{4,v}).\end{aligned}$$

Comme $c_{4,v}$ est un polynôme à coefficients entiers en les $a_{i,v}$ et que les $a_{i,v}$ sont entiers en v, on a $v(c_{4,v}) \geqslant 0$, ie. $\mathrm{ord}_v(\mathfrak{a}) \geqslant 0$. Et ce, quelque soit la place finie v de K. Donc $\mathfrak{a}$ est un idéal entier de K. □

Proposition 7.2.6. — *Soit E une courbe elliptique semi-stable sur un corps de nombres K. On a alors*

$$\mathrm{h}(j(E)) = \frac{1}{[K : \mathbb{Q}]} \cdot \left(\log \left| \mathbf{N}_{K/\mathbb{Q}} \Delta_{E/K} \right| + \sum_{\sigma : K \hookrightarrow \mathbb{C}} \log \max\{1, |j(\tau_\sigma)|\} \right)$$

où $\Delta_{E/K}$ est le dicriminant minimal de E sur K et où la somme est prise sur toutes les places archimédiennes de K.

Démonstration. — Sachant que E est définie sur K, on peut écrire l'idéal fractionnaire de K engendré par $j(E)$ comme un produit $\mathfrak{a}\mathfrak{d}^{-1}$ d'idéaux entiers de K, premiers entre eux. Comme E/K est semi-stable, on sait même que $\mathfrak{d} = \Delta_{E/K}$ (Lemme 7.2.5). Dans cette situation, on peut utiliser le Lemme 7.2.3 : on obtient que

$$\mathrm{H}_K(j(E)) = \mathbf{N}_{K/\mathbb{Q}}(\Delta_{E/K}) \cdot \prod_{v \in M_K^{\infty}} \max\{1, ||j(E)||_v\}.$$

Or, pour une place archimédienne v de K, on peut choisir $\tau_v \in \mathcal{D}$ tel que

$$E_v(\mathbb{C}) \simeq \mathbb{C}/(\mathbb{Z}\tau_v + \mathbb{Z})$$

Autrement dit, on a $\|j(E)\|_v = |j(\tau_v)|^{n_v}$. Ce qui fournit

$$\mathrm{h}(j(E)) = \frac{1}{[K:\mathbb{Q}]} \cdot \log|\mathrm{H}_K(j(E))| = \frac{1}{[K:\mathbb{Q}]} \cdot \left(\log\left|\mathbf{N}_{K/\mathbb{Q}}\Delta_{E/K}\right| + \sum_{v \in M_K^{\infty}} \log\max\{1, |j(\tau_v)|^{n_v}\} \right).$$

Et l'on réindexe la somme pour conclure : en effet, une place $v \in M_K^{\infty}$ réelle (resp. complexe) correspond à un plongement (resp. deux plongements conjugués) de K dans $\mathbb{C}$, d'où la « simplification » des exposants n_v. □

7.2.3. Hauteur de Faltings d'une courbe elliptique. — La définition générale de la hauteur de Faltings d'une variété abélienne dépassant un peu le cadre de ce mémoire, nous nous contenterons du cas particulier suivant :

Définition 7.2.7. — Soit E une courbe elliptique définie sur un corps de nombres K, on définit la *hauteur de Faltings de E/K* par la formule suivante :

$$\mathrm{h}_{\mathcal{F}}(E/K) = \frac{1}{2}\log\pi + \frac{1}{12[K:\mathbb{Q}]} \cdot \left(\log\left|\mathbf{N}_{K/\mathbb{Q}}\Delta_{E/K}\right| - \sum_{\sigma : K \hookrightarrow \mathbb{C}} \log\left(|\Delta(\tau_\sigma)| \cdot (\operatorname{Im}\tau_\sigma)^6 \right) \right)$$

où la somme est prise sur toutes places archimédiennes de K, pour lesquelles on choisit des $\tau_\sigma \in \mathcal{D}$ tels que $E_\sigma(\mathbb{C}) \simeq \mathbb{C}/(\mathbb{Z}\tau_\sigma + \mathbb{Z})$.

Voir l'article [**Sil84**] pour une preuve que cette formule correspond bien à la définition de [**Fal84**]. Voir aussi [**GR11**, Section 2.3] pour les questions de normalisation.

Exemple 7.2.8. — Si le corps de définition est $\mathbb{Q}$, la formule se simplifie quelque peu : la norme $\mathbf{N}_{\mathbb{Q}/\mathbb{Q}}\Delta_{E/\mathbb{Q}}$ n'est autre que le discriminant de E (vue comme une cubique plane), et il n'y a qu'une place archimédienne, pour laquelle on choisit $\tau \in \mathcal{D}$ tel que $E(\mathbb{C}) \simeq \mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z})$. La définition devient donc

$$\mathrm{h}_{\mathcal{F}}(E/\mathbb{Q}) = \frac{1}{2}\log\pi + \frac{1}{12} \cdot \left(\log\Delta_E - \log\left|\Delta(\tau) \cdot (\operatorname{Im}\tau)^6\right| \right).$$

On admet le résultat suivant (voir [**Fal84**, Lemma 5]) qui relie les hauteurs de Faltings de deux courbes elliptiques isogènes :

Proposition 7.2.9. — *Si E_1 et E_2 sont des courbes elliptiques définies sur un corps de nombres K, et qu'elles sont reliées par une isogénie $\varphi : E_1 \to E_2$, alors on a*

$$\mathrm{h}_{\mathcal{F}}(E_1/K) \leqslant \mathrm{h}_{\mathcal{F}}(E_2/K) + \frac{1}{2}\log\deg\varphi.$$

7.2.4. Lien entre hauteurs et invariant j. — Pour pouvoir finalement trouver une minoration de $\log|j(E)|$ à partir des considérations ci-dessus, il faut expliciter un lien entre la hauteur de Faltings d'une courbe elliptique E et $\log|j(E)|$. Nous faisons un premier pas dans cette direction dans la proposition suivante.

Proposition 7.2.10 **(Gaudron - Rémond [GR11**, Lemme 7.9**]).** — *Soit E une courbe elliptique définie sur un corps de nombres K, d'invariant $j(E)$. On a alors :*

$$\mathrm{h}_{\mathcal{F}}(E/K) \leqslant \frac{1}{12}\mathrm{h}(j(E)) + 3.$$

Démonstration. — Les deux membres de l'équation sont invariants par extension (finie) de corps : on peut donc supposer sans perte de généralité que E/K est semi-stable ([**Sil09**, Chapter VII, Proposition 5.4]). La Proposition 7.2.6 donne alors

$$\mathrm{h}(j(E)) = \frac{1}{[K:\mathbb{Q}]} \cdot \left(\log\left|\mathbf{N}_{K/\mathbb{Q}}\Delta_{E/K}\right| + \sum_{\sigma : K \hookrightarrow \mathbb{C}} \log\max\{1, |j(\tau_\sigma)|\} \right),$$

et la Définition 7.2.7 s'écrit

$$\mathrm{h}_{\mathcal{F}}(E/K) = \frac{1}{2}\log\pi + \frac{1}{12[K:\mathbb{Q}]} \cdot \left(\log\left|\mathbf{N}_{K/\mathbb{Q}}\Delta_{E/K}\right| - \sum_{\sigma : K \hookrightarrow \mathbb{C}} \log\left(|\Delta(\tau_\sigma)| \cdot (\operatorname{Im}\tau_\sigma)^6 \right) \right).$$

En combinant ces deux égalités, on trouve

$$\mathrm{h}_{\mathcal{F}}(E/K) - \frac{1}{12}\mathrm{h}(j(E)) = \frac{1}{2}\log\pi - \frac{1}{12[K:\mathbb{Q}]} \cdot \sum_{\sigma:K\hookrightarrow\mathbb{C}} \log\Big(|\Delta(\tau_\sigma)| \cdot (\operatorname{Im}\tau_\sigma)^6 \cdot \max\{1, |j(\tau_\sigma)|\}\Big).$$

Pour alléger les notations, on pose $f(\sigma) = |\Delta(\tau_\sigma)| \cdot (\operatorname{Im}\tau_\sigma)^6 \cdot \max\{1, |j(\tau_\sigma)|\}$.

D'après les Lemmes 7.1.1 et 7.1.2, on obtient que

$$\begin{aligned} f(\sigma) &\geqslant \Big((2\pi)^{12}\mathrm{e}^{-1/9}|q|\Big) \cdot (\operatorname{Im}\tau_\sigma)^6 \cdot \max\left\{1, \mathrm{e}^{2\pi\operatorname{Im}\tau_\sigma} - 740\right\} \\ &\geqslant (2\pi)^{12}\mathrm{e}^{-1/9} \cdot \max\left\{(\operatorname{Im}\tau_\sigma)^6\mathrm{e}^{-2\pi\operatorname{Im}\tau_\sigma}, (\operatorname{Im}\tau_\sigma)^6\left(1 - 740\mathrm{e}^{-2\pi\operatorname{Im}\tau_\sigma}\right)\right\} \\ &\geqslant (2\pi)^{12}\mathrm{e}^{-1/9} \cdot g(\operatorname{Im}\tau_\sigma) \qquad \text{où } g(y) = \max\{y^6\mathrm{e}^{-2\pi y}, y^6\left(1 - 740\mathrm{e}^{-2\pi y}\right)\}. \end{aligned}$$

Une étude de fonction assez technique révèle alors que g est croissante sur $[\sqrt{3}/2, 3/\pi]$, puis décroissante sur $[3/\pi, (\log 741)/2\pi]$ et à nouveau croissante sur $[(\log 741)/2\pi, +\infty[$. De plus, le calcul montre que

$$g\left(\frac{\sqrt{3}}{2}\right) = 0,0018281\cdots > 0,0018263\cdots = g\left(\frac{\log 741}{2\pi}\right).$$

Au final, on a :

$$\forall y \geqslant \frac{\sqrt{3}}{2}, \qquad g(y) \geqslant g\left(\frac{\log 741}{2\pi}\right) = \frac{(\log 741)^6}{(2\pi)^6 \cdot 741}.$$

Par suite, pour tous les plongements $\sigma : K \hookrightarrow \mathbb{C}$, on a

$$f(\sigma) \geqslant f_{min} = \frac{(2\pi)^6\mathrm{e}^{-1/9} \cdot (\log 741)^6}{741}.$$

Ces plongements sont au nombre de $[K:\mathbb{Q}]$, d'où finalement

$$\mathrm{h}_{\mathcal{F}}(E/K) - \frac{1}{12}\mathrm{h}(j(E)) \leqslant \frac{1}{2}\log\pi - \frac{1}{12}\log f_{min} \leqslant \frac{1}{2}\log\pi - \frac{1}{12} \cdot \log\left(\frac{(2\pi)^6\mathrm{e}^{-1/9} \cdot (\log 741)^6}{741}\right) \leqslant 3$$

après l'application numérique. □

7.3. Le deuxième ingrédient

Au chapitre précédent, on a majoré $\log|j(P)|$ pour $P \in X_{split}(p)(\mathbb{Z})$. Cela soulève deux questions :
- Quel est le lien entre $\log|j(P)|$ que l'on a majoré au Théorème 6.0.3 et $\mathrm{h}(j(P))$ que l'on vient de définir ?
- Le Théorème 0.0.1 promet un résultat sur les points rationnels de $X_{split}(p)$, et pas seulement sur les points entiers : y a-t-il une différence ?

Le théorème suivant, que nous admettons, donne une réponse à ces deux questions :

***Théorème 7.3.1* (Mazur - Momose - Merel).** — *Si $p \geqslant 17$, un point $P \in Y_{split}(p)(\mathbb{Q})$ non CM vérifie :*

$$j(P) \in \mathbb{Z}.$$

La preuve est la combinaison de résultats de B. Mazur ([**Maz78**, Corollary 4.8]), F. Momose ([**Mom84**, Proposition 3.1] et [**Mom84**, Corollary 3.6]) et L. Merel ([**Mer07**, Theorem 5]), une esquisse de démonstration unifiée est donnée dans [**BP09b**, Section 6].

Ce théorème nous sera utile sous la forme suivante :

Corollaire 7.3.2. — *Soit $p \geqslant 17$. Pour tout point $P \in Y_{split}(p)(\mathbb{Q})$, correspondant à une courbe elliptique E définie sur $\mathbb{Q}$ et munie d'une structure de sous-groupe de Cartan déployé de niveau p, on a*

$$\log|j(P)| = \log|j(E)| = \mathrm{h}(j(E)).$$

7.4. Le dernier ingrédient, conséquences

7.4.1. Isogénies minimales. — Soit E_1 et E_2 deux courbes elliptiques définies sur un corps de nombres K. Si on suppose qu'elles sont isogènes sur $\overline{K}$, l'ensemble $\mathrm{Hom}_{\overline{K}}(E_1, E_2)$ n'est pas réduit à $\{0\}$ et l'on peut poser

$$\delta = \min\{\deg\varphi,\ \phi \in \mathrm{Hom}_{\overline{K}}(E_1, E_2) \smallsetminus \{0\}\} \in \mathbb{N}^*.$$

Une isogénie $E_1 \to E_2$ est alors appelée *minimale* si elle est de degré δ. Par ailleurs, on rappelle qu'une isogénie est dite *cyclique* si son noyau est un groupe cyclique.

Lemme 7.4.1. — *Une isogénie minimale est cyclique.*

Démonstration. — Soit $\varphi : E_1 \to E_2$, une isogénie minimale. Son noyau $\operatorname{Ker}\varphi$ est un sous-groupe de $E_1[\deg\varphi] = E_1[\delta]$. Comme $E[\delta]$ est isomorphe à $(\mathbb{Z}/\delta\mathbb{Z})^2$, le théorème de structure des groupes abéliens finis affirme que le noyau de φ est de la forme $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ où $0 < a \mid b \mid \delta$. Ainsi, il existe un sous-groupe de $\operatorname{Ker}\varphi$ isomorphe à $(\mathbb{Z}/a\mathbb{Z})^2$, qui est nécessairement $E_1[a]$. Autrement dit, on a $\operatorname{Ker}[a] \subset \operatorname{Ker}\varphi$. L'isogénie φ se factorise donc en $\varphi = \varphi' \circ [a]$, avec $\varphi' : E_1 \to E_2$ une isogénie non-nulle. Mais alors,

$$\deg\varphi = \deg[a] \cdot \deg\varphi' = a^2 \cdot \deg\varphi'.$$

Par minimalité de $\deg\varphi$, on a $a = 1$. C'est pourquoi $\operatorname{Ker}\varphi \simeq \mathbb{Z}/b\mathbb{Z}$ est un groupe cyclique. □

Lemme 7.4.2. — *On suppose de plus que E_1 est sans CM. Alors toute isogénie cyclique est minimale.*

Démonstration. — Soit $\varphi : E_1 \to E_2$ est une isogénie cyclique. Pour toute isogénie non-nulle $\psi : E_1 \to E_2$, on note $\widehat{\psi} : E_1 \to E_2$ l'isogénie duale. Comme E_1 n'a pas de CM, l'endomorphisme $\widehat{\psi} \circ \phi$ de E_1 est nécessairement la multiplication par un entier $n \in \mathbb{Z}^*$. Auquel cas, $n^2 = \deg[n] = \deg\widehat{\psi} \cdot \deg\phi = \deg\psi \cdot \deg\phi$. Mais φ est cyclique donc $\deg\varphi \leqslant |n|$. De la sorte, $\deg\varphi \leqslant \deg\psi$. Et ce, quelque soit $\psi \in \operatorname{Hom}(E_1, E_2) \smallsetminus \{0\}$. □

7.4.2. Une majoration du degré minimal. — On admet le théorème suivant :

***Théorème 7.4.3* (E. Gaudron - G. Rémond).** — *Soit une courbe elliptique E définie sur un corps de nombres K de degré d, et soit $\phi : E \to E'$ une isogénie (définie sur $\overline{K}$).*

Alors il existe une isogénie $\phi_0 : E \to E'$ (définie sur $\overline{K}$) telle que

$$\deg\phi_0 \leqslant 10^7 d^2 \left(\max\{\mathrm{h}_{\mathcal{F}}(E), 985\} + 4\log d\right)^2.$$

La démonstration se trouve dans [**GR11**, Théorème 1.4]. Il s'agit d'une amélioration de résultats antérieurs :

- D.W. Masser et G. Wüstholz [**MW90**] ont démontré qu'il existe une constante $\kappa(d)$ ne dépendant que de d telle que :
$$\deg\phi_0 \leqslant \kappa(d)(1 + \mathrm{h}(j(E)))^4.$$
- Ensuite, F. Pellarin [**Pel01**] a raffiné l'argument précédent pour une courbe elliptique E sans CM : il montre que l'on a
$$\deg\phi_0 \leqslant \kappa'(d)(1 + \mathrm{h}(j(E)))^2,$$
où $\kappa'(d) = 10^{70} d^4 \max\{\log d, 1\}^2$ est une constante explicite.
- Enfin, E. Gaudron et G. Rémond ([**GR11**]) diminuent à la fois la constante et l'exposant du degré d.

Corollaire 7.4.4. — *Soit E une courbe elliptique sans CM définie sur un corps de nombres K de degré d, et une isogénie cyclique φ de E de degré δ. Alors on a*

$$\delta \leqslant 10^7 d^2 \left(\max\{\mathrm{h}_{\mathcal{F}}(E), 985\} + 4\log d\right)^2.$$

Démonstration. — Il s'agit de la conjonction du Théorème 7.4.3 et du Lemme 7.4.2. □

7.4.3. Interlude : un exemple d'application. — Grâce à ce corollaire, on peut retrouver un résultat de Serre ([**Ser71**]) :

Proposition 7.4.5. — *Soit E une courbe elliptique définie sur $\mathbb{Q}$ sans CM. Il existe une constante $B_E > 0$ telle que, pour tout $p \geqslant B_E$, l'image de la représentation $\rho_{E,p}$ n'est pas contenue dans un sous-groupe de Borel de $\mathbf{GL}_2(\mathbb{Z}/p\mathbb{Z})$.*

Démonstration. — Soit $p \geqslant 3$ un nombre premier et C un sous-groupe p-cyclique $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant de $E(\overline{\mathbb{Q}})$. La courbe elliptique quotient $E' := E/C$ est alors définie sur $\mathbb{Q}$ et il y a une isogénie cyclique π de degré p entre E et E'. Le Corollaire 7.4.4 (appliqué avec $K = \mathbb{Q}$) affirme qu'il existe une isogénie $\phi : E' \to E$ de degré

$$\delta := \deg\phi \leqslant 10^7 (\max\{\mathrm{h}_{\mathcal{F}}(E), 985\})^2.$$

Comme E est sans CM, la composée $\phi \circ \pi$ est de la forme $[n] : E \to E$ pour un certain $n \in \mathbb{Z} \smallsetminus \{0\}$. On a donc $n^2 = \deg[n] = \deg\phi \cdot \deg\pi = \delta \cdot p$. Par conséquent, p divise δ et, a fortiori, on a

$$p \leqslant 10^7 (\max\{\mathrm{h}_{\mathcal{F}}(E), 985\})^2.$$

Il suffit alors de poser $B_E = 10^7 (\max\{\mathrm{h}_{\mathcal{F}}(E), 985\})^2$ pour conclure la preuve (voir la Section 1.6.2). □

7.5. Fin de la preuve

Démonstration du Théorème 0.0.1. — Soit P, un point non CM de $Y_{split}(p)(\mathbb{Q})$. Il lui correspond une courbe elliptique E définie sur $\mathbb{Q}$ et munie d'une structure de normalisateur de Cartan déployé de niveau p : c'est-à-dire que l'image de $\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbf{GL}_2(\mathbb{Z}/p\mathbb{Z})$ est incluse dans le sous-groupe G de $\mathbf{GL}_2(\mathbb{Z}/p\mathbb{Z})$ formé des matrices diagonales et anti-diagonales. De manière équivalente, E est munie d'une paire $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariante $\{C_1, C_2\}$ de sous-groupes p-cycliques de $E[p](\overline{\mathbb{Q}})$.

Pour $p > 163$, le théorème de Mazur ([**Maz78**, Theorem 1]) montre que l'image de $\rho_{E,p}$ ne peut pas être contenue dans le sous-groupe $D = \{\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right)\}$ des matrices diagonales. On peut supposer sans perte de généralité que $p > 163$: dans ce cas, l'inclusion de $\mathrm{Im}\,\rho_{E,p} \cap D$ dans $\mathrm{Im}\,\rho_{E,p}$ est d'indice 2. Par théorie de Galois, il existe une extension quadratique K de $\mathbb{Q}$ correspondant à cette inclusion. Dès lors, les courbes elliptiques $E_i := E/C_i$ $(i = 1, 2)$ sont définies sur K et il existe des isogénies (définies sur K)

$$E_1 \to E \qquad \text{et} \qquad E \to E_2$$

qui sont toutes deux p-cycliques.On peut alors utiliser la Proposition 7.2.9 et la Proposition 7.2.10 avec l'isogénie $E_1 \to E$ de degré p :

$$\mathrm{h}_{\mathcal{F}}(E_1/K) \leqslant \mathrm{h}_{\mathcal{F}}(E/K) + \frac{1}{2}\log p \leqslant \frac{1}{12}\mathrm{h}(j(E)) + \frac{1}{2}\log p + 3$$

En faisant appel au Corollaire 7.3.2, ceci devient

$$\log|j(E)| \geqslant 12 \cdot \left(\mathrm{h}_{\mathcal{F}}(E_1/K) - \frac{1}{2}\log p - 3\right) \tag{13}$$

D'autre part, on utilise le Corollaire 7.4.4 avec l'isogénie p^2-cyclique obtenue par composition $E_1 \to E \to E_2$:

$$p^2 \leqslant 10^7 2^2 \left(\max\{\mathrm{h}_{\mathcal{F}}(E_1), 985\} + 4\log 2\right)^2 \tag{14}$$

car K est une extension de degré 2 de $\mathbb{Q}$. Par conséquent,

- Ou bien $p \leqslant 2 \cdot 10^{7/2} \cdot (985 + 4\log 2) \leqslant 6,3 \cdot 10^6$, et l'on a fini.
- Ou bien $p \leqslant 2 \cdot 10^{7/2} \cdot \mathrm{h}_{\mathcal{F}}(E_1/K)$. Auquel cas, on a $\mathrm{h}_{\mathcal{F}}(E_1/K) \geqslant p/6,5 \cdot 10^3$, et on peut combiner l'inégalité (13) avec le Théorème 6.0.3 :

$$\begin{aligned} 2\pi\sqrt{p} + 6\log p + 21\frac{(\log p)^2}{\sqrt{p}} \geqslant \log|j(E)| &\geqslant 12 \cdot \left(\mathrm{h}_{\mathcal{F}}(E_1/K) - \frac{1}{2}\log p - 3\right) \\ &\geqslant 12 \cdot \left(\frac{p}{6,5 \cdot 10^3} - \frac{1}{2}\log p - 3\right). \end{aligned}$$

  Soit encore

$$p \leqslant 6,3 \cdot 10^3 \cdot \left(\frac{\pi}{6}\sqrt{p} + \log p + \frac{21}{12} \cdot \frac{(\log p)^2}{\sqrt{p}} + 3\right).$$

  Une résolution numérique indique alors que $p \leqslant 1,2 \cdot 10^7$.

□

BIBLIOGRAPHIE

[BP09a] Y. Bilu & P. Parent – « Runge's method and Modular curves », *International Mathematics Research Notices* **2011** (2009), no. 9, p. 1997–2027.

[BP09b] ———, « Serre's uniformity problem in the split Cartan case », *Annals of Mathematics* **173** (2009), no. 1, p. 569–584.

[BPR11] Y. Bilu, P. Parent & M. Rebolledo – « Rational points on $X_0^+(p^r)$ », *Preprint arXiv : http ://arxiv.org/abs/1104.4641* (2011).

[CS84] G. Cornell & J. H. Silverman (éds.) – *Arithmetic geometry*, Springer-Verlag, 1984.

[CSS97] G. Cornell, J. Silverman & G. Stevens (éds.) – *Modular forms and Fermat's Last Theorem*, Springer-Verlag, 1997.

[DI95] F. Diamond & J. Im – « Modular forms and modular curves », in *Seminar on Fermat's last theorem : 1993-1994, the Fields Institute for Research in the Mathematical Sciences, Toronto.*, vol. 17, 1995, p. 39.

[DR73] P. Deligne & M. Rapoport – « Les schémas de modules de courbes elliptiques », in *Modular functions of one variable II*, Springer, 1973, p. 143–316.

[DS05] F. Diamond & J. M. Shurman – *A first course in modular forms*, Springer, 2005.

[Fal84] G. Faltings – « Finiteness theorems for abelian varieties over number fields », in *Arithmetic geometry*, 1984, p. 9–27.

[GR11] É. Gaudron & G. Rémond – « Théorème des périodes et degrés minimaux d'isogénies », *Arxiv preprint : http ://arxiv.org/abs/1105.1230* (2011).

[Har77] R. Hartshorne – *Algebraic geometry*, Springer-Verlag, 1977.

[KL81] D. S. Kubert & S. Lang – *Modular units*, Springer, 1981.

[KM85] N. M. Katz & B. Mazur – *Arithmetic moduli of elliptic curves*, Princeton University Press, 1985.

[Lan83] S. Lang – *Fundamentals of diophantine geometry*, Springer, 1983.

[Lan87] ———, *Elliptic functions*, Springer, 1987.

[Lig77] G. Ligozat – « Courbes modulaires de niveau 11 », in *Modular Functions of one Variable V*, Springer, 1977, p. 149–237.

[Maz77a] B. Mazur – « Modular curves and the Eisenstein ideal », *Publ. Math. Inst. Hautes Étud. Sci.* **47** (1977), p. 33–186.

[Maz77b] ———, « Rational points on modular curves », in *Modular Functions of one Variable V*, Springer, 1977, p. 107–148.

[Maz78] ———, « Rational isogenies of prime degree », *Inventiones mathematicae* **44** (1978), no. 2, p. 129–162.

[Mer99] L. Merel – « Arithmetic of elliptic curves and diophantine equations », *J. Théor. Nombres Bordeaux* **11** (1999), no. 1, p. 173–200.

[Mer07] ———, « Normalizers of split Cartan subgroups and supersingular elliptic curves », *Diophantine Geometry. Pisa : Edizioni della Normale* (2007), p. 237–55.

[Mom84] F. Momose – « Rational points on the modular curves $X_{split}(p)$. », *Compositio Mathematica* **52** (1984), no. 1, p. 115–137.

[Mom86] ———, « Rational points on the modular curves $X_0^+(p^r)$ », *J. Fac. Sci. Univ. Tokyo Sect. IA Math* **33** (1986), no. 3, p. 441–466.

[MSD74] B. Mazur & P. Swinnerton-Dyer – « Arithmetic of Weil curves », *Inventiones Mathematicae* **25** (1974), no. 1, p. 1–61.

[MW90] D. W. Masser & G. Wüstholz – « Estimating isogenies on elliptic curves », *Inventiones Mathematicae* **100** (1990), no. 1, p. 1–24.

[Ogg72] A. Ogg – « Rational points on certain elliptic modular curves », in *Analytic number theory (Proc. Sympos. Pure Math., St. Louis Univ.)*, 1972, p. 221–231.

[Ogg73] A. Ogg – « Survey of modular functions of one variable », in *Modular functions of one variable I*, Springer, 1973, p. 1–35.

[Par05] P. Parent – « Towards the triviality of $X_0^+(p^r)(\mathbb{Q})$ for $r > 1$ », *Compositio Mathematica* **141** (2005), no. 03, p. 561–572.

[Pel01] F. Pellarin – « Sur une majoration explicite pour un degré d'isogénie liant deux courbes elliptiques », *Acta Arithmetica* **100** (2001), no. 3, p. 203–243.

[Reb08] M. Rebolledo – « Module supersingulier, formule de Gross-Kudla et points rationnels de courbes modulaires », *Pacific journal of mathematics* **234** (2008), no. 1, p. 167.

[Roh96] D. E. Rohrlich – « Modular curves, hecke correspondences, and L-functions », in *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, 1996, p. 41–100.

[Sam67] P. Samuel – *Théorie algébrique des nombres*, Hermann, 1967.

[Ser71] J.-P. Serre – « Propriétés galoisiennes des points d'ordre fini des courbes elliptiques », *Inventiones mathematicae* **15** (1971), no. 4, p. 259–331.

[Shi71] G. Shimura – *Introduction to the arithmetic theory of automorphic functions*, vol. 1, Princeton University Press, 1971.

[Sil84] J. H. Silverman – « Heights and elliptic curves », in *Arithmetic geometry*, 1984, p. 166.

[Sil94] ———, *Advanced topics in the arithmetic of elliptic curves*, Springer, 1994.

[Sil09] ———, *The arithmetic of elliptic curves*, Springer, 2009.