CONSTRUCTION DE SHIMURA DES COURBES ELLIPTIQUES MODULAIRES SUR Q

JEAN-PIERRE WINTENBERGER

1. Introduction

Soit N un entier ≥ 1. Soient $\Gamma_0(N)$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),\ c \equiv 0 \text{ mod. } N,$$

et $\Gamma_1(N)$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), c \equiv 0 \text{ mod.} N, a \equiv 1 \text{ mod.} N.$$

On définit $\Gamma(N)$ comme étant le noyau de la réduction de $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Soit $\mathcal{H}$ le demi-plan de Poincaré $\{z \in \mathbb{C}, \mathrm{im}(z) > 0\}$. On fait agir $\mathrm{GL}_2(\mathbb{R})^+$ ($+$: déterminant > 0) sur $\mathcal{H}$ par : $z \mapsto \frac{az+b}{cz+d}$ (on a $\mathrm{im}(\gamma(\mathrm{z})) = \frac{\det(\gamma)\mathrm{im}(\mathrm{z})}{|\mathrm{cz+d}|^2}$). Soit k un entier ≥ 2. Une forme modulaire pour $\Gamma_*(N)$ est une fonction holomorphe sur $\mathcal{H}$ qui vérifie :

$$f(\gamma(z)) = (cz+d)^k f(z)$$

pour tout $\gamma \in \Gamma_*(N)$, et une condition de croissance. On peut écrire l'équation ci dessus (automorphie) de la façon suivante. Pour $\gamma \in \mathrm{GL}_2(\mathbb{C})$, posons $j(\gamma, z) = cz + d$. On a dans $(\mathbb{C})^2$:

$$\gamma(z, 1) = (az + b, cz + d) = j(\gamma, z)(\gamma(z), 1)$$

d'où $j(\gamma_1\gamma_2, z) = j(\gamma_2, z)j(\gamma_1, \gamma_2(z))$. Pour $\gamma \in \mathrm{GL}_2(\mathbb{R})^+$, on pose : $(f_{|k}\gamma)(z) = \det(\gamma)^{k/2} j(\gamma, z)^{-k} f(\gamma(z))$. Alors $f_{|k}\gamma_1\gamma_2 = (f_{|k}\gamma_1)_{|k}\gamma_2$, et l'action ainsi définie se factorise à travers $\mathrm{PGL}(\mathbb{R})^+$. La condition d'automorphie est $f_{|k}\gamma = f$ pour tout $\gamma \in \Gamma_*(N)$. Dans le cas de $\mathrm{SL}_2(\mathbb{Z}) = \Gamma(1)$ la condition d'automorphie dit que f est une fonction homogène $\tilde{f}$ de poids $-k$ sur l'ensemble des réseaux de $\mathbb{C}$. Si $L_z = \mathbb{Z}z \oplus \mathbb{Z}1$, $f(z) = \tilde{f}(L_z)$. On a pour $\gamma \in \Gamma(1)$:

$$f(\gamma(z)) = \tilde{f}(L_{\gamma(z)}) = \tilde{f}(j(\gamma, z)^{-1}\gamma(L_z)) = j(\gamma, z)^k \tilde{f}(\gamma(L_z)) = j(\gamma, z)^k f(z).$$

En particulier, on demande que $f(z+N) = f(z)$. On pose $q_N = \exp(2\pi iz/N)$ et $q = \exp(2\pi iz)$. On a donc une fonction g définie sur le disque unité épointé (en 0) par $g(q_N) = f(z)$. On a un développement de Laurent convergent : $g(q) = \sum_{n\in\mathbb{Z}} a_n q_N^n$. La condition de croissance à la pointe ∞ est que $a_n = 0$ si $n < 0$. La condition de cuspidalité est que de plus $a_0 = 0$. On impose que

pour tout $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ la condition d'holomorphie (resp. de cuspidalité) soit vérifiée pour $f_{|k}\gamma$. Il suffit de le vérifier pour des γ décrivant un système de représentants des doubles classes $\Gamma_*(N)\backslash\Gamma(1)/\Gamma_\infty$ (Γ_∞ est le stabilisateur de ∞ i.e. les matrices triangulaires supérieures dans $\mathrm{SL}_2(\mathbb{Z})$). On peut dire aussi que l'on doit vérifier les conditions pour des γ tels que les $\gamma^{-1}(\infty)$ décrivent toutes les pointes modulo l'action de $\Gamma_*(N)$.

La condition de croissance (pour toutes les pointes) est équivalente à ce que le développement à la pointe infinie de f vérifie que $\mid a_n \mid \leq Cn^r$ ([3] prop. 1.2.4.). La condition de cuspidalité (pour toutes les pointes) est équivalente à $f(z)\mathrm{im(z)}^{\mathrm{k}/2}$ borné. ([4] th. 2.1.5.)

Notons $\Gamma = \Gamma_*(N)$. On définit une structure de surface de Riemann sur $Y_*(N) = \Gamma\backslash\mathcal{H}$. On dit que $z \in \mathcal{H}$ est elliptique pour Γ s'il existe $\gamma \in \Gamma$, $\gamma \neq \pm\mathrm{id}$ tel que $\gamma(z) = z$. Les z qui sont elliptiques pour $\mathrm{SL}_2(\mathbb{Z})$ sont les orbites de i et de $\exp(\frac{2\pi i}{3})$. Pour Γ, c'est un sous-ensemble de ces points. Si z n'est pas elliptique, il existe ouvert non vide U voisinage de z tel que $\gamma(U)\cap U = \emptyset$ si $\gamma \neq \pm\mathrm{id}$. Autrement dit, si π est la projection de $\mathcal{H} \to \Gamma\backslash\mathcal{H}$, la restriction de π à U est injective. On prend comme carte au voisinage de $\pi(z)$ le voisinage U. En particulier, $z - z_0$ est un paramètre local en z_0 si z_0 n'est pas elliptique. Par exemple pour $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ et pour le point elliptique i, la fonction $(\frac{(z-i)}{(z+i)})^2$ est un paramètre local. On complète la surface de Riemann : $X_*(N) = \Gamma\backslash(\mathcal{H} \cup \mathrm{P}_1(\mathbb{Q}))$. Cas $\Gamma = \mathrm{SL}_2(\mathbb{Z})$: $X(1)$ est isomorphe à $\mathrm{P}_1(\mathbb{C})$. Les élements de $\Gamma\backslash\mathrm{P}_1(\mathbb{Q})$ ou leurs images par π sont appelés les pointes. Pour $l \in \mathrm{P}_1(\mathbb{Q})$, il existe $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ tel que $l = \gamma(\infty)$ (Bezout), ce qui permet de ramener l'étude au voisinage d'une pointe à celle de la pointe ∞. Un paramètre local en ∞ est q.

On a :

$$\gamma^*(f(z)dz) = (f_{|2}\gamma)(z)dz$$

Il résulte de cette identité qu'une forme de poids 2 peut s'interpréter comme une forme différentielle sur $X_*(N)$. On a ; $f(z)dz = 2\pi i\frac{dq}{q}g(q)$. Elle est donc holomorphe si f est cuspidale ; a des pôles d'ordre 1 aux pointes sinon.

Une surface de Riemann compacte et connexe X a une structure de courbe algébrique irréductible lisse. Son corps de fonctions sur $\mathbb{C}$ est le corps des fonctions méromorphes. ll est de degré de transcendance 1 sur $\mathbb{C}$. Ce n'est pas évident même qu'il existe une fonction méromorphe non constante : cela résulte du théorème de Riemann-Roch. Les sections de son faisceau structural sur $X - \{p_1, \ldots, p_r\}$ est l'anneau des fonctions méromorphes sur $X - \{p_1, \ldots, p_r\}$.

Pour $Y(1)$, la fonction j définit un isomorphisme de $X(1)$ sur $P_1(\mathbb{C})$. On définit la courbe elliptique sur $\mathbb{C}$: $E_z = \mathbb{C}/L_z$ (tore complexe). C'est aussi une surface de Riemann compacte. La structure algébrique sur E_z peut être explicitée. Pour L un réseau dans $\mathbb{C}$, on considère la fonction $\wp$ de Weierstrass :

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in L}{}' (\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2})$$

$\sum'$ désignant la somme sur les éléments non nuls et $z \in \mathbb{C}$. La convergence pour $z \notin L$ vient du fait que les termes de la somme sont $O(1/\omega)^3$ pour z variant dans un domaine borné.. Pour $k > 2$, k pair, posons $G_k(z) = \sum'_{c,d} \frac{1}{(cz+d)^k}$ et $g_2 = 60G_4$, $g_3 = 140G_6$. On prouve que la série d'Eisenstein G_k est une forme non parabolique de poids k. On a au voisinage de 0 :

$$\wp(z) = \frac{1}{z^2} + \sum_{n \geq 2, \text{pair}}^{\infty} (n+1)G_{n+2}(L)z^n$$

On a :

$$(\wp'(z))^2 = 4(\wp(z))^3 - g_2(L)\wp(z) - g_3(L).$$

On prouve que le discriminant $\delta = g_2^3 - 27g_3^2$ ne s'annule pas sur $\mathcal{H}$; on pose $\Delta = (2\pi)^{-12}(g_2^3 - 27g_3^2)$ (la normalisation est telle que $\Delta = q + \ldots$). Δ est une forme parabolique de poids 12. Il en résulte que la fonction $j = 1728\frac{(g_2)^3}{\delta}$ est une fonction méromorphe sur $X(1)$. On peut prouver que le corps des fonctions de $X(1)$ est $\mathbb{C}(j)$. De plus, l'ensemble $Y(1)(\mathbb{C})$, complémentaire de ∞ dans $X(1)(\mathbb{C})$, est en bijection avec les réseaux de $\mathbb{C}$ à homothéties près. ll est encore en bijection avec les classes d'isomorphies de courbes elliptiques. On dit que $Y(1)$ est un espace de modules (grossier) pour les courbes elliptiques.

Plus précisément, si k est un corps, une courbe elliptique sur k est une cubique non singulière dans $(\mathrm{P}_2)_k$ munie d'un point rationnel sur k, deux courbes elliptiques étant isomorphes si elles sont transformées l'une de l'autre par un élément de $\mathrm{PGL}_3(k)$. Si k est de caractéristique 0, toute courbe elliptique a une équation de Weierstrass du type $y^2 = x^3 - g_2x - g_3$, deux telles équations donnant des courbes isomorphes s'il existe $u \in k$ tel que $u^4g_2' = g_2$ et $u^6g_3' = g_3$. On a alors $u^{12}\Delta' = \Delta$ et $j' = j$.

Remarque. Si E est définies sur k, alors $j \in k$. Il n'est pas difficile de prouver que si $j \in k$, il existe une courbe elliptique définie sur k et d'invariant j. Par exemple sur le corps $\mathbb{Q}(j)$, la courbe elliptique $E_j : y^2 = 4x^3 - (\frac{27j}{j-1728})x - (\frac{27j}{j-1728})$ a pour invariant l'indéterminée j. La spécialisation en $j = 0$ ou 1728 n'est pas une courbe elliptique.

La courbe elliptique n'est pas unique en général. Pour $\pm n$ non carré dans $\mathbb{Q}$, les courbes elliptiques $y^2 = x^3 - x$ et $ny^2 = x^3 - x$ sont isomorphes sur $\mathbb{C}$ mais pas sur $\mathbb{Q}$. On a un espace de modules grossier (les objets qu'on classe ont des isomorphismes non triviaux donc il ne peut pas y avoir d'objet universel).

Soit $E = \mathbb{C}/L$ une courbe elliptique sur $\mathbb{C}$. Elle est naturellement munie d'une loi de groupe provenant de l'addition dans $\mathbb{C}$. On voit que $E(\mathbb{C})_N \simeq N^{-1}L/L \simeq L/NL$ est une groupe isomorphe à $(\mathbb{Z}/N\mathbb{Z})\omega_1 \oplus (\mathbb{Z}/N\mathbb{Z})\omega_2$.

Décrivons le corps des fonction de $X_*(N)$. Pour $\gamma \in \Gamma(1)$, on a $L_{\gamma(z)} = (cz+d)^{-1}L_z$ et la multiplication par $cz + d$ définit un isomorphisme de $L_{\gamma(z)}$ dans L_z qui envoie $\gamma(z)$ sur $az + b$ et 1 sur $cz + d$. On voit que si $\gamma \in \Gamma(N)$, l'isomorphisme i_{Nz} de L_z/NL_z sur $(\mathbb{Z}/N\mathbb{Z})\omega_1 \oplus (\mathbb{Z}/N\mathbb{Z})\omega_2$ qui envoie z sur ω_1 et 1 sur ω_2 ne dépend pas du choix de z dans son orbite sous

$\Gamma(N)$. Pour $\gamma \in \Gamma(1)$, on a $i_{N,\gamma(z)} = \gamma \circ i_{N,z}$. Il en résulte sur $E_N(\mathbb{C})$ un déterminant *i.e.* une forme simplectique non dégénérée, l'accouplement de Weil (plus précisément, l'accouplement de Weil est l'accouplement obtenu en composant avec $\exp(2\pi i * /N)$). On voit que les points de $Y_N(\mathbb{C})$ sont en bijection avec l'ensemble des classes d'isomorphie de couples (E, i) où E est une courbe elliptique sur $\mathbb{C}$ avec un isomorphisme i de $E_N(\mathbb{C})$ sur $(\mathbb{Z}/N\mathbb{Z})\omega_1 \oplus (\mathbb{Z}/N\mathbb{Z})\omega_2$ qui envoie l'accouplement de Weil sur l'accouplement qui vaut 1 sur (ω_1, ω_2). Attention : les couples (E, i) et $(E, -i)$ sont isomorphes (l'isomorphisme est donné par la multiplication par -1 sur E). On prouve que le corps des fonctions de $X(N)$ est engendré sur $\mathbb{C}(j)$ par les fonctions $f_{\bar{v}} := \frac{g_2(z)}{g_3(z)}\wp_z((\bar{c}z + \bar{d}/N)$, les $\bar{v} = (\bar{c}, \bar{d})$ décrivant les vecteurs non nuls de $(\mathbb{Z}/N\mathbb{Z})^2$ (remarquer que $f_{\bar{v}} = f_{-\bar{v}}$).

Le groupe de Galois de $\mathbb{C}(X_N)/\mathbb{C}(j)$ est $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm \mathrm{id}$. Les corps de fonction de $X_1(N)$ et de $X_0(N)$ sont les invariants par les images de $\Gamma_1(N)$ et de $\Gamma_0(N)$ dans $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm \mathrm{id}$. On obtient une extension à groupe de Galois $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ incluse dans une clôture algébrique $\overline{\mathbb{Q}(j)}$ en prenant le corps de rationalité $\mathbb{C}(j, E_{j,N})$ des points d'ordre N de E_j.

En fait, on a besoin d'une structure de $X_1(N)$ et de $X_0(N)$ sur $\mathbb{Q}$ i.e. de définir leurs corps de fonctions comme une extension transcendante pure de $\mathbb{Q}$. Le corps $\mathbb{Q}(j, E_{j,N})$ est une extension de $\mathbb{Q}(j)$ à groupe de Galois $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Le sous-corps correspondant à $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ est $\mathbb{Q}(j, \mu_N)$. Pour deux points P_1 et P_2 engendrant définissant une structure de niveau N, l'accouplement de Weil (P_1, P_2) est une racine primitive N-ième de l'unité.

Les corps de fonction de $X_1(N)$ et de $X_0(N)$ sont les corps fixes par les matrices de la forme $\pm \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ et les triangulaires supérieures dans $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

Remarque. Pour une courbe elliptiqe modulaire, on peut définir des points comme images de points de $X_0(N)$. Par exemple, la courbe $X_0(11)$ est isomorphe à la courbe elliptique $y^2 + y = x^3 - x^2 - 10x - 20$. Le point défini par $L = O_K$, $K = \mathbb{Q}(\sqrt{-2})$ et $1/(3 - \sqrt{-2})$ est défini sur K. C'est le point $(-3 + \sqrt{-2}, -4 - 3\sqrt{-2})$.

1.1. **Courbes lisses sur un corps.** On s'inspire de [6].

Soit k un corps parfait et soit $\bar{k}$ une clôture algébrique de k.

On suppose tout d'abord que $k = \bar{k}$.

Soit A une k-algèbre de type fini. On lui associe le schéma $V = \mathrm{spec}(A)$ (si A est réduit on parle d'ensemble algébrique). Si de plus, A est intègre autrement dit $A = k[T_1, \ldots, T_n]/I$ avec I premier, on parle alors de variété affine. Le corps des fonctions rationnelles $k(V)$ de V est le corps des fractions de A.

On définit de même un schéma projectif $V \subset (\mathrm{P}_n)_k$. Il est définie par un idéal homogène I de $k[T_0, \ldots, T_n]$ engendré par des polynômes homogènes f_j (on peut prendre les f_j dans un ensemble fini). Les points sont les points de l'espace projectif qui annulent les polynômes f_i ($f_i(P)$ n'a pas de sens,

sa nullité en a). Le schéma est obtenu en recollant les ensembles algébriques affines V_i, $0 = 1, \ldots, n$, V_i définie dans $k[T_0, \ldots, T_{i-1}, T_{i+1}, \ldots, T_n]$ en faisant dans les f_j $X_j = T_j$ pour $j \neq i$ et $X_i = 1$. Si V est $\subset (\mathrm{P}_n)_k$, $I(V)$ est l'idéal des polynômes homogènes qui s'annulent sur V (il est toujours différent de l'idéal $(X_0, \ldots, X_n)$). Si $I(V)$ est un idéal premier, on dit que V est irréductible et le corps des fractions rationnelles est le corps des f/g, f homogènes de même degré, $g \notin I(V)$ et : f/g et f'/g' sont équivalents si $fg' - f'g \in I(V)$.

Ne supposons plus necessairement k algébriquement clos. A une k-algèbre est associé une schéma affine. A un idéal premier homogène I de $k[T_0, \ldots, T_n]$ on peut associer par recollement un schéma V et une immersion fermée de V dans $(\mathrm{P}_n)_k$. On a alors en particulier les points à valeurs dans k' estension de k. Si A est intègre ou si I est premier, on a un corps des fonctions rationnelles $k(V)$. Si V n'est pas inclus dans l'hyperplan $X_i = 0$, c'est le corps des fonctions rationnelles de $\cap A_i$ (A_i est le complémentaire dans $(\mathrm{P}_n)_k$ de l'hyperplan $X_i = 0$).

Exercice. Prouver que si $A = k[T_1, \ldots, T_n]/I$ est une k-algèbre intègre, le corps des fractions de A est le quotient du localisé $k[T_1, \ldots, T_n]_I$ par son idéal maximal. Soit $V \subset (\mathrm{P}_n)_k$ et soit $S(V)$ la k-algèbre $k[T_0, \ldots, T_n]/I$. Pour une algèbre graduée, et $\wp$ un idéal premier homogène, on note $S_{(\wp)}$ la partie homogène de degré 0 de $S_\wp$. Prouver que le corps des fonctions rationnelles de V est $S_{((0))}$. Prouver que les fonctions partout définies sur V sont les constantes (on suppose $k = \bar{k}$).

Le 1) permet de voir que l'on ne rajoute pas de nilpotents en étendant les scalaires de k à $\bar{k}$ et que pour une courbe lisse sur k sur $\bar{k}$ donne une réunion disjointe de courbes lisses sur $\bar{k}$.

Proposition 1.1. *Soit k un corps parfait et K une extension de type fini de k.*

1) $\bar{k} \otimes_k K$ est un produit fini de corps : plus précisément, soit k' l'extension maximale algébrique de k contenue dans $\bar{k}$. Alors k' est une extension finie de k et $\bar{k} \otimes_k K$ est le produit de $[k' : k]$ corps.

2) Il existe $x_1, \ldots x_d$ algébriquement indépendants dans K tels que K soit une extension finie séparable de $k(x_1, \ldots x_d)$.

Indication sur une preuve. 1) C'est vrai si $K = k'$ donc par associativité du produit tensoriel, on peut supposer $k' = k$. Si $x_1, \ldots x_d$ sont comme dans 2), le produit tensoriel est $\bar{k}(x_1, \ldots, x_d) \otimes_{k(x_1, \ldots, x_d)} K$ et utiliser que K est séparable sur $k(x_1, \ldots, x_d)$ pour voir que c'est un produit de corps. Pour prouver que si $k = k'$ c'est absolument irréductible, voir que la plus grande sous-algèbre finie de $\bar{k} \otimes_k K$ est définie sur k (utiliser Hilbert 90 pour GL_n : $H^1(G_k, \mathrm{GL}_n(\bar{k})) = 1$, [7]).

Pour le 2), définir les différentielles de Kähler $\Omega_{B/A}$ (B module engendré par les $d(b)$, soumis aux relations $d(b + b') = d(b) + d(b')$, $d(bb') = bd(b') + b'd(b)$). et $d(a) = 0$ pour $a \in A$. On peut aussi définir $\Omega_{B/A}$ comme I/I^2

où I est le noyau de $B \otimes_A B \to B$ (dérivation : $d(b) = b \otimes 1 - 1 \otimes b$). Les A-dérivations de B à valeurs dans un B-module M sont $\mathrm{Hom}_B(\Omega_{B/A}, M)$.

On le fait dans le cas où le degré de transcendance d de K sur k est 1. Si K est obtenu à partir de $k(T)$ par succession d'extensions séparables et d'extensions radicielle, on prouve que $\Omega_{K'/k}$ est de dimension 1 sur L et que $[K : K^p] = p$. Si K'/K est radicielle $K' \otimes_k \Omega_{K/k} \to \Omega_{K'/k}$ nest pas injective.

On choisit $x_1, \ldots, x_d$ tels que $\Omega_{K/k}$ a pour base $d(x_1), \ldots, d(x_d)$. Alors K est une extension algébrique séparable de $k(x_1, \ldots, x_d)$.

Exemple $X^2 + Y^2$ est irréductible dans $\mathbb{R}[X, Y]$; réductible dans $\mathbb{C}[X, Y]$. Trouver un élément i du corps des fonctions de $\mathbb{R}[X, Y]/(X^2+Y^2)$ qui vérifie $i^2 + 1 = 0$.

On a la notion de dimension. C'est le degré de transcendance du corps du corps des fonctions, donc aussi la dimension de $\Omega_{K/k}$. Pour spec(A) avec A noethérien c'est aussi la dimension de Krull de A *i.e.* le plus grand entier d tel que l'on ait une chaîne d'idéaux premiers distincts $\wp_0 \subset \ldots \subset \wp_d$ (voir [8]). Cela résulte du lemme de normalisation (A est entier sur $C = A[X_1, \ldots, X_d]$)

Une courbe est V de dimension 1.

Exercice Qu'est ce que A intègre de dimension 0 ?

Définissons la lissité.

Soit $V \subset A_n$ une variété affine et $P \in V$. Notons $A = A(V)$. Soit $f_1, \ldots, f_r$ des générateurs de $I(V) \subset B = k[x_1, \ldots, x_n]$. Soit d la dimension de V.

Définition. Soit P un point de V. On dit que V est lisse en P si la matrice jacobienne $J(P)$ des $df_i/dx_j(P)$ a pour rang $n - d$.

Si C est une k-algèbre locale, on note $t^*(C) = \mathsf{m}_C/(\mathsf{m}_C)^2$ l'espace cotangent. Si C est noethérienne et que P est un point correspondant à l'idéal maximal m, on a $t^*(C_P) = \mathsf{m}/(\mathsf{m})^2$.

Soit θ l'applicaton $f \mapsto (df/dx_1(P), \ldots, df/dx_n(P))$. θ définit un isomorphisme de $t^*(B_P)$ avec k^n. Le rang $r(J)$ de J est la dimension de $\theta(I) = I + m_A^2/m_A^2$. On a $t^*(A_P) = \mathsf{m}_B/(\mathsf{m}_B)^2 + I$. On voit que $\dim(t^*(A_P)) + r(J) = n$. Or on a pour C anneau local noethérien $\dim(C) \leq \dim(t_C^*)$ avec égalité si l'anneau est par définition régulier (la dimension de C est égale à la dimension de de son complété qui est un quotient de $k[[x_1, \ldots, x_m]]$ avec m la dimension de $t^*(C_P)$).

On voit donc que la condition de lissité revient à dire que l'anneau local soit régulier.

Exercices Prouver que si C est une k-algèbre locale complète noetherienne régulière de corps résiduel k, alors k est isomorphe à un anneau de séries formelles $k[[x_1, \ldots, x_d]]$.

Prouver que $k \otimes_C \Omega_{C/k}$ est isomorphe à $t^*(C_P)$.

Remarques. On voit donc que la notion de lissité est intrinsèque : elle ne dépend pas du plongement affine.

Supposons $k = \mathbb{C}$. On a $r(J) \leq n - d$. Si V est lisse en P, au voisinage de P est $\leq n - d$. C'est donc qu'il est constant au voisinage de P. Le

théorème des fonctions implicites implique que V est au voisinage de P une variété différentielle complexe de dimension d. Si V est projective, $V(\mathbb{C})$ est compacte car $\mathrm{P}_n(\mathbb{C})$ l'est.

Supposons k algébriquement clos.

Soit V une courbe projective et lisse sur k.

On a le théorème suivant :

Theorem 1.2. *Soit A un anneau intègre local noethérien de dimension 1, avec m son idéal maximal. On a l'équivalence :*

1) A est un anneau de valuation discrète,

2) A est intégralement clos,

3) A est un anneau régulier,

4) m est principal.

Pour 2) implique 3) voir [1]. Les autres implications sont faciles (pour 3) implique 4) utiliser le lemme de Nakayama).

On voit donc que les anneaux locaux aux points de $C(k)$ sont des anneaux de valuation discrète dont la valuation s'annule sur k.

Si K/k est de dimension 1, on définit une courbe projective et lisse de la façon suivante. Soit $f \in K$, f non nulle et telle que K soit séparable sur $k(f)$. on définit C comme la clôture intégrale de $(\mathrm{P}_1)_k$ dans K. Il n'est pas difficile de prouver que C est définie de la manière suivante. Les points fermés sont en bijection avec les valuations discrètes triviales sur k et la topologie de Zariski a pour ouverts les complémentaires des parties finies et les fonctions sur les ouverts U sont les fonctions telles que $v(f) \geq 0$ pour $v \in U$. La courbe est bien projective. On a

Theorem 1.3. *Soit C une courbe lisse et $P \in C$. Soit $C - P \to Y$ un morphisme vers Y projective. Alors ce morphisme s'étend de manière unique à C.*

Pour prouver que C est projective, on la recouvre par U_1 et U_2 affines. Soient Y_1 et Y_2 les complétions projectives de U_1 et U_2. Par le théorème ci-dessus on a un morphisme de C vers $Y_1 \times Y_2$. On utilise Segre.

On prouve que si C_1 et C_2 sont deux courbes projectives et lisses de même corps des fonctions K, on a $C_1 = C_2$. Cela résulte du théorème ci-dessus.

Plus généralement un k-plongement (séparables ou non) $K_1 \hookrightarrow K_2$ définit un morphisme $C_2 \to C_1$.

Exercice Une fonction $f \in k(C)$ non constante définit un morphisme surjectif de C vers $\mathbb{P}_1$.

2. Théorème de Riemann-Roch.

On suppose k algébriquement clos.

Soit C une courbe projective et lisse sur k. Un diviseur D est une somme formelle $D = \sum n_P P$, la somme portant sur un ensemble fini de points P, et $n_P \in \mathbb{Z}$. Son degré est $\deg(D) = \sum n_P$. $D \geq D'$ si $n'_P \geq n_P$. D est effectif si il est ≥ 0.

Si $f \in k(C)$, $f \neq 0$, le diviseur de f est $\mathrm{div}(f) = \sum_{P \in C(k)} v_P(f)P$. On a $\deg(\mathrm{div}(f)) = 0$. On le vérifie en le vérifiant pour P_1.

Deux diviseurs D et D' sont linéairement équivalents si $D - D'$ est le diviseur d'une fonction.

Un faisceau inversible $\mathcal{L}$ sur C définit une classe d'équivalence linéaire de diviseurs. C'est la classe d'équivalence définie par les sections rationnelles non nulles de ce fibré. Réciproquement, une classe d'équivalence de diviseurs définit un faisceau inversible sur C. Si D est un diviseur de la classe, le fibré est défini par le fait que les sections de $\mathcal{L}$ qui sont définies en P sont les $f \in k(C)$ sont celles qui vérifient $v_P(f) \geq -n_P$.

On note $l(D)$ la dimension des sections $\Gamma(C, \mathcal{L}(D))$ (elle est finie). Ces sections s'identifient aux fonctions $f \in k(C)$ telles que $f = 0$ ou $\mathrm{div}(f) \geq -D$. Les diviseurs des sections de $\mathcal{L}$ sont les diviseurs effectifs linéairement équivalents à D. Ils sont en bijection avec l'espace projectif $(\Gamma(C, \mathcal{L}(D)) - \{0\})/k^*$ de dimension $l(D) - 1$. (si D est effectif $l(D) = 0$ sauf si $D = 0$ auquel cas $l(D) = 1$).

Exercice Soit $f \in k(C)$ non constante de diviseur $\sum n_P P$, les P étant distincts. Alors, le degré du morphisme vers $\mathbb{P}_1$ qu'elle définit est $\sum n_P$ pour les $n_P > 0$.

On note K le faisceau inversible $\Omega_{C/k}$. Le genre est $l(K)$: c'est la dimension des formes différentielles régulières. (Les diviseurs correspondants sont dits canoniques).

Exemple : Pour $\mathbb{P}_1$, $g = 0$ et $\deg(K) = -2$.

Theorem 2.1. *(Riemann-Roch)* $l(D) - l(K - D) = \deg(D) + 1 - g$.

Remarques

Il en résulte : $\deg(K) = 2g - 2$. Si $\deg(D) < 0$, $l(D) = 0$. En effet si $l(D) > 0$, D est linéairement équivalent à un diviseur effectif, donc est de degré ≥ 0. On voit donc que si $\deg(D) > 2g-2$, on a $l(D) = \deg(D)+1-g$.

Supposons $g = 0$. Soient P et Q deux points distincts de C. Appliquons Riemann-Roch à $D = P - Q$. On trouve $l(D) = 1$. D est donc linéairement équivalent à un diviseur effectif, de degré 0, donc nul. Donc D est le diviseur d'une fonction f. Cette fonction définit un morphisme $C \to \mathbb{P}_1$ de degré 1, donc C est isomorphe à $\mathbb{P}_1$.

Soit $f : C_1 \to C_2$ non constant.

Si $C_1 \to C_2$ est inséparable, C_1 et C_2 sont isomorphes et $g(C_1) = g(C_2)$.

Si f est séparable, on a la suite exacte :

$$0 \to f^*\Omega_{C_2} \to \Omega_{C_1} \to \Omega_{C_1/C_2} \to 0$$

L'exactitude à gauche résulte de la bijectivité aux points générique. Ω_{C_1/C_2} est nul en dehors des points de ramification. Si la ramification est modérée en $P \in C_2$, (l'indice de ramification e_P est premier à la caractéristique de k), la longueur de Ω_{C_1/C_2} est $e_P - 1$. En effet si P_1 s'envoie sur P_2, et si t_1 est une uniformisante de en P_1 et t_2 en P_2, et le polynôme minimal de t_1 est le polynôme d'Eisenstein $t_1^e + \sum_{i=0}^{e-1} a_i u^i$, l 'annulateur de $d(t_1)$ est

$eu^{e-1} + \sum_{i=0}^{e-1} ia_i u^{i-1}$. Si la caractéristique de k est nulle ou première à e, c'est de valuation $e-1$.

La suite exacte ci-dessus donne :

Theorem 2.2. *(Hurwirtz) Soit $f : C_1 \to C_2$ un morphisme séparable non constant. On a :*

$$2g(C_1) - 2 = \deg(f)(2g(C_2) - 2) + \deg(R)$$

avec $\deg(R) = \sum_{P \in C_1}(e_P - 1)$ *si la ramification est modérée.*

3. Courbes elliptiques

Une référence est [2].

Une courbe elliptique est une courbe projective lisse sur k (k algébriquement clos) de genre 1. Pour $P \in C$, on a $l(nP) = n$ pour $n \geq 1$. Soient $1, x$ une base de $\Gamma(C, \mathcal{L}(2P))$ et $1, x, y$ une base de $\Gamma(C, \mathcal{L}(3P))$. On a une relation linéaire entre $1, x, y, x^2, xy, y^2, x^3$ éléments de $\Gamma(C, \mathcal{L}(6P))$, qui, en regardant les valuations en P comporte vraiment des termes en y^2 et x^3, donc peut se mettre sous la forme (après changement de y en by) :

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

La fonction x définit un morphisme $C \to \mathbb{P}_1$ qui est de degré 2. On a $k(C) = k(x, y)$. En effet, sinon $y \in k(x)$, et y définirait un morphisme de C vers $\mathbb{P}_1$ de degré pair. Une cubique singulière est rationnelle (a son corps de fonctions de genre 0). Donc la cubique n'est pas singulière.

Si la caractéristique de k est différente de 2, le changement de variable $y' = y + \frac{1}{2}(a_1x + a_3)$ transforme l'équation de la cubique en : $y^2 = (x - a)(x-b)(x-c)$. La condition de non singularité est que a, b, c soient distincts, autrement dit que le discriminant de $P(x) = (x-a)(x-b)(x-c)$ soit non nul. Par un changement linéaire de la variable x, on se ramène à $y^2 = x(x-1)(x-\lambda)$ (Legendre). Si la caractéristique est de plus différente de 3, on se ramène à $y^2 = 4x^3 - g_2x - g_3$ (Weierstrass).

Pour une telle équation $y^2 = P(x)$ avec P de degré 3, la droite à l'infinie est tangente d'inflexion en le point d'intersection de C avec la droite de l'infini. La fonction x définit un morphisme de C sur $\mathbb{P}_1$ qui est de degré 2 et ramifié en l'infini et a, b, c.

Réciproquement, une cubique non singulière C a un point d'inflexion. Cela peut se voir de la manière suivante ([6] ex. 4 2.3.). Si O est un point de C qui n'est pas sur C ou sur une tangente d'inflexion ou une bitangente, et L une droite ne ne contenant pas P, la projection de centre O sur la droite L est ramifiée avec indice de ramification 2 exactement aux points P tels que la tangente en P contienne O. Par Hurwitz, passent par O 6 tangentes. Si maintenent L est une droite non tangente à C, on considère le morphisme qui à $P \in C$ associe l'intersection de la tangente en P avec L. Il est ramifié si $P \in L$ et si P est une inflexion. Par Hurwitz, on trouve 9 points d'inflexion.

En l'envoyant un point d'inflexion à $(0,1,0)$ et en envoyant la tangente en la droite à l'infini, on trouve une équation de la forme $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$..

La jacobienne $J(C)$ de C est une variété abélienne sur k (variété projective et lisse, munie d'une loi de groupe) tel que $J(C)(k) = \mathrm{Pic}^0(C)$. $\mathrm{Pic}(C)$ est le quotient du groupe des diviseurs de C par les diviseurs de fonctions ; $\mathrm{Pic}(C)^0$ est le quotient des diviseurs de degré 0 par les diviseurs des fonctions.

Si C est de genre 0, $J(C)$ est triviale. Si elle est de genre g, $J(C)$ est de dimension g.

Theorem 3.1. *Soit C une courbe elliptique et P_0 un point de C. Alors, le morphisme $P \mapsto P - P_0$ est un isomorphisme de C sur sa jacobienne.*

En particulier C est munie d'une loi de groupe d'élément neutre P_0.

Pour prouver le théorème, il suffit de prouver que tout diviseur D de degré 0 est linéairement équivalent à $P - P_0$ pour un point P de C. On applique Riemann-Roch à $D + P_0$. On trouve $l(D + P_0) = 1$. ll existe un unique diviseur effectif linéairement équivalent à $D + P_0$. Comme il est de degré 1, c'est un point P et D est linéairement équivalent à $P - P_0$.

En particulier, pour tout point P de C, il existe un automorphisme a de C tel que $a(P_0) = P$. Si π_0 et π_1 sont deux morphismes de C sur $\mathbb{P}_1$ définis par des fonctions sections de $\mathcal{L}(2P_0)$ et $\mathcal{L}(2P_1)$ qui n'ont pas des pôles d'ordre 1, il existe b automorphisme de $\mathbb{P}_1$ tel que $\pi_1 \circ a = b \circ \pi_0$. Ceci résulte du fait que $a^*(\mathcal{L}(2P_1)) = \mathcal{L}(2P_0)$.

Il en résulte que le birapport des 4 points de ramification est déterminé par C, modulo permutation de ces points. On voit donc que, si la caractéristique est différente de 2 et 3, les équations de Weierstrass de C sont définies modulo $u^4 g_2' = g_2$ et $u^6 g_3' = g_3$, u non nul (changement de variable $y = u^{-3}y'$ et $x = u^{-2}x'$) (pour avoir l'équation de Weierstrass, on a dû envoyer un point de ramification à l'infini ; il ne reste plus que des tranformations linéaires possibles). Le discriminant est $\Delta = g_2^3 - 27g_3^2$; l'invariant j est $1728\frac{g_2^3}{\Delta}$ ($j = 1/q + \ldots$. Le 1728 permet la définition en caractéristique 2. On a alors $u^{12}\Delta' = \Delta$ et $j' = j$. j est donc un invariant de la courbe elliptique et C et C' sont isomorphes si et seulement si $j(C) = j(C')$ (k algébriquement clos). Etant donné j, il existe une courbe elliptique d'invariant j : si la caractéristique n'est pas 2 ou 3, c'est clair avec l'équation de Weierstrass.

Exercice. Trois points sur la cubique sont alignés si et seulement si leur somme est nulle.

Passons à la théorie analytique.

Soit L un réseau de $\mathbb{C}$. Alors $S = \mathbb{C}/L$ est une surface de Riemann compacte. Elle est de genre 1 car dz est une forme différentielle de diviseur trivial, donc le degré du diviseur canonique est 0 et $2(g-2) = 0$. En particulier les formes différentielles régulières sur S sont $\mathbb{C}dz$. Le principe du maximum entraîne que les fonctions partout réfulières sont les constantes (c'est vrai pour toutes les surfaces de Riemann compactes).

Proposition 3.2. *Soit f une fonction méromorphe sur S (fontion elliptique : fonction méromorphe sur $\mathbb{C}$ et L-périodique) et $\sum_i n_i a_i$ son diviseur. Alors 1) $\sum_i \mathrm{res}_{a_i}(f) = 0$, 2) $\sum_i a_i = 0$ et 3) $\sum_i n_i a_i = 0$.*

La deuxième assertion est que $\deg(\mathrm{div}(f)) = 0$. Soit ω_1, ω_2 une base de L. Pour la première, on intègre $f(z)dz$ le long du bord d'un parallélogramme du type $a, a+\omega_1, a+\omega_2, a+\omega_1+\omega_2$ où l'on a choisit a de sorte à éviter les zéros et pôles. Pour 3), on intègre $zf'(z)/f(z)dz$. Remarquer que $\int_a^{a+\omega_1} f'(z)/f(z)dz = 2\pi i m$ où m est l'indice de 0 pour la courbe fermée du plan complexe $f([a, a+\omega_1])$.

Remarque. Le 3) dit que l'image du diviseur d'une fonction est nulle dans la jacobienne de S (que l'on peut identifier à S).

On considère la fonction $\wp$ de Weierstrass :

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in L}{}' \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$

$\sum'$ désignant la somme sur les éléments non nuls et $z \in \mathbb{C}$. La fonction $\wp$ est paire. Il est clair que $\wp'(z)$ est elliptique. On a donc pour $\omega \in L$: $\wp(z+\omega) = \wp(z) + c_\omega$. On trouve $c_\omega = 0$ en faisant $z = \omega/2$. On pose $G_{2k} = \sum' \omega^{-2k}$ pour pour $k \geq 2$. On obtient :

$$\wp(z) = \frac{1}{z^2} + \sum_{k \geq 1}^{\infty} (2k+1) G_{2k+2}(L) z^n$$

La fonction $\wp'$ a pour seul pôle (modulo L) 0 avec multiplicité 3. Comme elle est impaire, on en déduit que le diviseur de $\wp'$ est $-3(0) + (\omega_1/2) + (\omega_1/2)((\omega_1+\omega_2)/2)$. Le diviseur de $\wp - \wp(a)$ pour $a \neq 0$ est $-2(0)+(a)+(-a)$. Il en résulte que $\wp$ a deux zéros a et $-a$ (qui n'ont pas d'interprétation simple).

Proposition 3.3. *Posons $g_2 = 60G_4$, $g_3 = 140G_6$. On a :*

$$(\wp'(z))^2 = 4(\wp(z))^3 - g_2(L)\wp(z) - g_3(L).$$

Si $\Delta := g_2^3 - 27g_3^2 \neq 0$. Le corps des fonctions de S est celui de la courbe elliptique E $y^2 = 4x^3 - g_2(L)x - g_3(L)$.

On vérifie que $(\wp'(z))^2 - 4(\wp(z))^3 + g_2(L)\wp(z) + g_3(L)$ qui est elliptique et n'a que 0 comme pôle est $o(z^2)$. Elle est donc nulle.

Le corps des fonctions elliptiques est une extension quadratique de celui des fonctions elliptiques paires. Soit f une fonction elliptique paire. Si $2a \in L$, $z \mapsto f(z+a)$ est paire et donc $v_a(f)$ est pair. Soit $\sum_i n_i a_i$ le diviseur de f. On pose $g = \prod(\wp - \wp(a_i))^{a_i'}$ où le produit porte sur les orbites par ± 1 des a_i et si $2a_i \in L$, $a_i' = a_i/2$, $a_i' = a_i$ sinon. Alors f et g ont le même diviseur.

Il en résulte que $\mathbb{C}(S)$ est le corps de la cubique. Prouvons qu'elle est bien irréductible.

Soit $\omega_3 = \omega_1 + \omega_2$. Les 0 de $\wp'(z)$ sont les $\wp(\omega_i)$. On a en posant $e_i = \wp(\omega_i)$:

$$\wp'(z) = 4(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3).$$

On a $\mathrm{div}(\wp - e_i) = -2(0) + 2(\omega_i/2)$. Ils sont distincts, donc les e_i aussi.

Proposition 3.4. *L'application $z \mapsto (z^3\wp(z), z^3\wp'(z), z^3)$ définit un isomorphisme de surfaces de Riemann de $\mathbb{C}/L$ sur E.*

Comme $\wp$ prend toute valeur complexe en deux valeurs opposées de z (sauf pour $2z \in L$) ; $\wp'$ sépare ces deux points. Donc l'applicaton est bijective. Elle est un isomorphisme de surfaces de Riemann car $\wp(z)$ et $\wp''(z)$ ne s'annule pas simultanément c'est un isomorphisme local. On le vérifie aussi à l'infini.

4. Corps de fonctions modulaires

Soient $E = \mathbb{C}/L$ et $E = \mathbb{C}/L'$ deux courbes elliptiques. Soit $f : E \to E'$ un morphisme non constant de surfaces de Riemann. Soit $\tilde{f} : \mathbb{C} \to \mathbb{C}$ un relèvement. de f. Pour $\omega \in L$, on doit avoir $\tilde{f}(z + \omega) - \tilde{f}(z) \in L'$. Donc $\tilde{f}(z + \omega) - \tilde{f}(z)$ est constant. Par suite $\tilde{f}'$ doit être une fonction elliptique et $\tilde{f}'$ doit être constant. Par suite $\tilde{f} = az + b$. Si c'est un morphisme de groupes, on doit avoir $b = 0$ et $aL \subset L'$.

En particulier, E et E' sont isomorphes si L et L' sont homothétiques. On voit donc qu'on a une bijection des classes d'isomorphies de courbes elliptiques sur $\mathbb{C}$ avec les points de $\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}$.

Rappelons que pour une fonction modulaire de poids k (fonction méromorphe sur $\mathcal{H}$ et aux pointes) on a :

$$v_\infty(f) + 1/2v_i(f) + 1/3v_j(f) + \sum v_P(f) = k/12.$$

Theorem 4.1. *L'invariant modulaire $j = 1728g_2^3/\Delta$ définit un isomorphisme de surfaces de Riemann de $X(1)_{\mathbb{C}}$ avec $\mathrm{P}_1(\mathbb{C})$.*

La formule ci-dessus entrîne $v_\infty(\Delta) = 1$, donc $v_\infty(j) = -1$. Pour tout $\lambda \in \mathbb{C}$, $j(z) - \lambda = 0$ a une seule solution en z. Donc J est de degré 1 et est un isomorphisme de surfaces de Riemann compactes.

Soit, pour $\bar{v} \in (\mathbb{Z}/N\mathbb{Z})^2 \neq 0$, on definit :

$$f_{\bar{v}}(z) = \frac{g_2(z)}{g_3(z)}\wp_z(\frac{cz + d}{N})$$

pour c et d entiers tels $\bar{v}$ soit l'image de (c, d).

Rappelons que $\Gamma(N)$ est le sous-groupe de congruences $\ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))$ et que $X(N)$ est la courbe modulaire correspondante. Soit Ω une clôture algébrique du corps des fonctions méromorphes sur le demi-plan de Poincaré. Il contient le corps des fonctions modulaires $\mathbb{C}(X(N))$.

Rappelons que E_j est la courbe elliptique $y^2 = 4x^3 - (\frac{27j}{j-1728})x - (\frac{27j}{j-1728})$ définie sur $\mathrm{Spec}(\mathbb{Q}[j][1/j, 1/(j - 1728)]$.

Theorem 4.2. *1) Les fonctions $f_{\bar{v}}$ sont dans $\mathbb{C}(X(N))$ et $\mathbb{C}(X(N))$ est engendré par j et les $f_{\bar{v}}$. L'extension $\mathbb{C}(X(N))/\mathbb{C}(X(1))$ est galoisienne de groupe de Galois $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm\mathrm{id}$. 2) Le sous corps de Ω engendré par les $x(P)$ pour P point d'ordre N de E_j est $\mathbb{C}(X(N))$. 3) Le sous corps $\mathbb{C}(j, E_{j,N})$ de Ω engendré par les points d'ordre N de E_j est une extension de degré 2 de $\mathbb{C}(X(N))$ et $\mathbb{C}(j, E_{j,N})/\mathbb{C}(j)$ a pour groupe de Galois $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.*

Les fonctions $f_{\bar{v}}$ vérifie la condtion d'automorphie de poids 0 pour $\Gamma(N)$. On vérifie que les fonctions $f_{\bar{v}}(z)$ ont une limite finie lorsque z tend vers la pointe ∞. Le groupe $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm\mathrm{id}$ agit sur l'ensemble des $f_{\bar{v}}$ par la formule $f_{\bar{v}}(z) \mapsto f_{\bar{v}}(\gamma z)$ qui n'est autre que $f_{\bar{v}\gamma}(z)$. Cela montre l'holomorphie aux pointes. Par suite les $f_{\bar{v}}$ sont des éléments de $\mathbb{C}(X(N))$.

L'égalité $f_{\bar{v}} = f_{\bar{v}'}$ n'est possible que si $\bar{v} = \pm\bar{v}'$ (se rappeler que $\wp(z) = \wp(z')$ entraîne $z = \pm z'$ modulo L). Il en résulte que l'action de $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm$ id sur le corps $K = \mathbb{C}(j, f_{\bar{v}})$ est fidèle. On a vu que le corps des points fixes est $\mathbb{C}(j)$. Le corps $\mathbb{C}(X(N))$ est une extension de $\mathbb{C}(j)$ de groupe de Galois un quotient de $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm\mathrm{id}$. Il en résulte que $\mathbb{C}(X(N)) = K$ est que $K/\mathbb{C}(j)$ est galoisienne de groupe de Galois $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm\mathrm{id}$.

Il existe un polynôme P_N à coefficients dans $\mathbb{Q}(j)$ tel que $P_N(x) = 0$, si et seulement $[N](x, y) = 0$ dans E_j. Pour le voir, utiliser que $E_j/\pm\mathrm{id}$ est isomorphe à $(\mathbb{P}_1)_{\mathbb{Q}(j)}$ et en déduire que $[N]$ définit un endomorphisme de $(\mathbb{P}_1)_{\mathbb{Q}(j)}$.

Considérons la $\mathbb{C}$-algèbre engendrée par j et les $f_{\bar{v}}$. Pour toute valeur de z qui n'est pas elliptique et tel que $j(z)$ ne soit pas un pôle d'un des coefficients de P_N, on peut évaluer j les $f_{\bar{v}}$ et P_N. Pour ces évaluations, on a $P_N(f_{\bar{v}}(z)) = 0$. Comme c'est vrai pour presque tous les z, on voit que l'on a bien $P_N(f_{\bar{v}}) = 0$. Ceci prouve 2).

Pour le 3), le groupe de Galois est une sous-groupe $H \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. En fait, comme l'accouplement de Weil a une définition algébrique (voir paragraphe suivant), on voit que $H \subset \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Par 2), l'image de H dans $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm\mathrm{id}$ est surjective. Il en résulte que pour tout $g \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, on a $\pm g \in H$. En particulier, l'une des deux matrices $\pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ est dans H. Leurs carré est dans H, soit $-\mathrm{id}$.

Le corps $\mathbb{C}(X_1(N))$ est le corps fixe de $\mathbb{C}(X(N))$ par $\Gamma_1(N)$. Si $f_1 = f_{\bar{v}}$ pour $\bar{v} = (0, 1)$, on a $\mathbb{C}(X(N)) = \mathbb{C}(j, f_1)$.

Soit maintenant $\mathbb{Q}(j, E_{j,N})$ le sous-corps de Ω fixé par la représentation sur les points d'ordre N de E_j.

Theorem 4.3. *$\mathbb{Q}(j, E_{j,N})$ est une extension de $\mathbb{Q}(j)$ de groupe de Galois $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.*

Soit $H \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ le groupe de Galois. Il contient $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ par le théorème précédent. Le déterminant a pour image $(\mathbb{Z}/N\mathbb{Z})^*$ par l'accouplement de Weil.

Il en résulte un modèle sur $\mathbb{Q}$ de $X_1(N)$: son corps des fonctions est le corps des fixes de $\mathbb{Q}(j, E_{j,N})$ par $\begin{pmatrix} a & b \\ 0 & \pm 1 \end{pmatrix}$. De même pour $X_0(N)$. Pour $X(N)$ le modèle est défini sur $\mathbb{Q}(\mu_N)$.

Remarque Supposons $N \geq 5$. Alors un couple (E, P) formé d'une courbe elliptique sur un corps et d'un point P d'ordre 5 n'a pas d'automorphisme non trivial. On peut prolonger E_j sur $Y_1(N)$ en un schéma en courbes elliptiques munies d'un point d'odre 5 et même sur $\mathbb{Z}[1/N]$. On obtient la famille universelle de schéma en courbes elliptiques muni d'un point d'ordre N sur $\mathbb{Z}[1/N]$.

5. L'accouplement de Weil

Il s'agit d'un accouplement alterné et parfait $E_N \times E_N \to \mu_N$.

Analytiquemet il est défini comme suit. Pour $L \subset \mathbb{C}$ un réseau, on choisit une base ω_1, ω_2 avec $\omega_2/\omega_1 \in \mathcal{H}$. La base ω_1, ω_2 est définie modulo $\mathrm{SL}_2(\mathbb{Z})$. Cela fixe donc un déterminant, et d 'où un acouplement parfait et alterné $E_N \times E_N \to \mathbb{Z}/N\mathbb{Z}$. On le pousse par $\exp(2\pi i * /N)$.

Donnons en une définition algébrique. Soient P et Q deux points tués par N. Soit f une fonction de diviseur $N(Q) - N(0)$. Le diviseur de $f \circ [N]$ est $N(\sum_S (Q' + S) - (S))$, où Q' est tel que $[N](Q') = Q$ et S décrit $E[N]$. On a donc une fonction g telle que $f \circ [N] = g^N$. On voit que $g(X+P)/g(X) \in \mu_N$: on a $(P, Q) = g(X + P)/g(X)$.

6. Opérateurs de Hecke.

Faisons quelques rappels sur les jacobiennes.

Soit k un corps. Une variété abélienne A sur k est une variété absolument irréductible sur k, qui est projective et est une variété en groupes (on a un morphisme $A \times A \to A$ vérifiant les axiomes d'une loi de groupe). La loi de groupe est alors commutative.

Soit k un corps et C une courbe projective et lisse absolument irréductible de genre g. Il existe une variété abélienne $\mathrm{Jac}(C)$ sur k, de dimension g, qui représente en un sens à préciser le foncteur $S \to \mathrm{Pic}^0(C_S)$ pour S k-schéma. En particulier, ses points à valeurs dans une clôture algébrique $\bar{k}$ de k est le groupe quotient des diviseurs de $C_{\bar{k}}$ de degré 0 par le groupe des diviseurs de fonctions. Si P_0 est un point de $C(\bar{k})$, l'application $f_{P_0} : P \mapsto P - P_0$ définit un morphisme de C dans sa Jacobienne. Les formes différentielles invariantes sur A s'identifie à l'espace cotangent à l'origine de A. Si $P_0 \in C(k)$, par f_{P_0} elles s'identifent à $H^0(C, \Omega_C)$. Cette identification ne dépend pas du choix de P_0 ce qui entraîne qu'elle est définie sur k si k est parfait.

Soient C_1 et C_2 deux courbes comme ci-dessus, J_1 et J_2 leurs jacobiennes et π un morphisme non constant de C_1 dans C_2. Il définit un morphisme π_* de J_1 dans J_2 qui induit sur les points l'application qui provient sur les diviseurs de l'application $P \mapsto \pi(P)$. On a $\pi_*(\mathrm{div}(f)) = \mathrm{div}(N(f))$ où $N(f)$ est la norme de $f \in \bar{k}(C_1)^*$. π définit aussi un morphisme π^* de J_2 dans

J_1. Il induit sur les points l'application qui provient de $P \mapsto \sum e_{P'} P'$ où la somme est sur les points $P' \in C_1$ tels que $\pi(P') = P$ et où $e_{P'}$ est l'indice de ramification en P'. On a $\pi^*(\mathrm{div}(f)) = \mathrm{div}(f \circ \pi)$. On a : $\pi_* \circ \pi^* = [\deg(\pi)]_{C_2}$.

Soient C_1 et C_2 deux courbes comme ci-dessus. Nous appelerons correspondance la donnée d'une courbe C comme ci-dessus avec deux morphismes non constants $\pi_1 : C \to C_1$ et $\pi_2 : C \to C_2$. Une telle correspondance définit deux morphismes $J_1 \to J_2 : (\pi_2)_* \circ (\pi_1)^*$ et $J_2 \to J_1 : (\pi_1)_* \circ (\pi_2)^*$.

Considérons $X_1(N)$. Soit $\Gamma_1^0(N,p) = \Gamma_1(N) \cap \Gamma^0(p)$ avec $\Gamma^0(p)$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), b \equiv 0 \mathrm{mod}.p.$$

et soit $Y_1^0(N,p)$ la courbe modulaire correspondante avec sa compactification $X_1^0(N,p)$. Si $N \geq 5$, la courbe $Y_1(N)$ est un espace de module qui classifie les couples (E,P) formés d'une courbe elliptique E et d'un point P d'ordre N. Cela résulte de ce que $Y_1(N)$ ne contient pas de points elliptiques (une courbe elliptique avec un point d'ordre 5 n' a pas d'automorphisme non trivial, car 1 n'est pas racine modulo 5 des polynômes caractéristiques des éléments elliptiques). Sur $\mathbb{C}$, le couple (E,P) défini par $z \in \mathcal{H}$ est la courbe elliptique $E_z = \mathbb{C}/(\mathbb{Z} + \mathbb{Z}z)$ avec le point $P = 1/N$. La courbe $Y_1^0(N,p)$ classifie les triplets (E,P,C) où (E,P) est comme ci-dessus et C est un sous-groupe d'ordre p tel que $C \cap < P >= (0)$ où $< P >$ est le sous groupe de E engendré par $< P >$. Le point de $Y_1^0(N,p)$ défini par z est $(E_z, 1/N, < z/p >)$. On note π_1 le morphisme de $X_1^0(N,p)$ vers $X_1(N)$ dont la restriction à $Y_1^0(N,p)$ associe à (E,P,C) le couple (E,P). Il est défini par $z \mapsto z$. On note π_2 le morphisme de $X_1^0(N,p)$ vers $X_1(N)$ dont la restriction à $Y_1^0(N,p)$ associe à (E,P,C) le couple $(E/C, P/C)$. Il est défini par $z \mapsto z/p$. Les morphismes π_1 et π_2 sont définis sur $\mathbb{Q}$.

Soit $J_1(N)$ la Jacobienne de $X_1(N)$. Pour p premier, on note T_p l'endomorphisme de $J_1(N)$ défini par $(\pi_2)_* \circ (\pi_1)^*$. On en déduit une action de T_p sur les formes paraboliques $S_2(\Gamma_1(N))$. Pour d premier à N, on définit l'action de $< d >$ par $(E,P) \mapsto (E, dP)$. On note $\mathbb{T}_1(N)$ l'anneau des endomorphismes de $S_2(\Gamma_1(N)$ engendré par les T_p et les $< d >$: on l'appelle l'algèbre de Hecke. Elle est commutative. On définit les T_{p^r} par la formule : $T_{p^r} = T_p T_{p^{r-1}} - p^{k-1} < p > T_{p^{r-2}}$ si p ne divise pas N et $T_{p^r} = (T_p)^r$ si p divise N , et les T_n pour tout entier n par $T_{mn} = T_n T_m$ si m et n sont premiers entre eux.

Theorem 6.1. *Soit $f \in M_k(\Gamma_1(N), \eta)$, $f = \sum_{m=0}^{\infty} a_m(f) q^m$. Alors $T_n(f) = \sum_{m=0}^{\infty} b(m) q^m$. avec $b(m) = \sum_d d^{k-1} \eta(d) a_{mn/d^2}(f)$, la somme portant sur les d divisant (m,n).*

En particulier, si $m = 1$, on a : $b(1) = a(n)$. Si n est un premier p, $b(m) = a(pm)$ si p ne divise pas m et $a(pm) + p^{k-1} a(m/p) \eta(p)$ si p divise m. Si p divise N on a $\eta(p) = 0$. On voit que

$$T_p(\sum_{n=0}^{\infty} a(n)q^n) = \sum_{n=0}^{\infty} a(pn)q^n + \eta(p)p^{k-1}\sum_{n=0}^{\infty} a(n)q^{np}.$$

Notons $S_2(\Gamma_1(N))_{\mathbb{Q}}$ les formes paraboliques qui sont des formes différentielles qui sont définies sur $\mathbb{Q}$ (ce sont aussi les formes paraboliques dont le q-développement en la pointe ∞ est à coefficients $\in \mathbb{Q}$).

Proposition 6.2. *$S_2(\Gamma_1(N))_{\mathbb{Q}}$ et $\mathrm{Hom}_{\mathbb{Q}}(S_2(\Gamma_1(N))_{\mathbb{Q}}, \mathbb{Q})$ sont des $(\mathbb{T}_1(N))_{\mathbb{Q}}$-modules libres de rang 1.*

Preuve. L'accouplement :

$$S_2(\Gamma_1(N))_{\mathbb{Q}} \times (\mathbb{T}_1(N))_{\mathbb{Q}} \to \mathbb{Q}$$

qui à (f, T) associe $a(1)(T(f))$. Il est parfait. En effet, si $a(1)(T(f)) = (0)$ pour tout T, on a $a(1)(T_n(f)) = 0$ pour tout n et donc $a(n)(f) = 0$, ce qui entraîne $f = 0$. Si $a(1)(T(f)) = 0$ pour tout f, on a $a(1)(TT_n(f)) = 0$ pour tout f, n, donc comme l'algèbre de Hecke est commutative ($a(1)(T_nT(f)) = 0$, $a(n)(T(f)) = 0$ donc $T(f) = 0$ pour tout f et $T = 0$.

On en déduit que $S_2(\Gamma_1(N))_{\mathbb{Q}}$ est un $(\mathbb{T}_1(N))_{\mathbb{Q}}$-module libre de rang 1. Si $\epsilon = \exp(\frac{2\pi i}{N})$, w_ϵ est l'involution de $X_1(N)$ est l'involution définie par $(E, P) \mapsto (E/ < P >, P')$ avec $(P, P')_{\mathrm{Weil}} = \epsilon$. L'accouplement :

$$(f, g) \mapsto (f, \sigma \circ w_\epsilon(g))_{\mathrm{Petersson}}$$

est autoadjoint pour l'action de $(\mathbb{T}_1(N))_{\mathbb{Q}}$ et il permet d'identifier $S_2(\Gamma_1(N))_{\mathbb{Q}}$ et $\mathrm{Hom}_{\mathbb{Q}}(S_2(\Gamma_1(N))_{\mathbb{Q}}, \mathbb{Q})$ en tant que $(\mathbb{T}_1(N))_{\mathbb{Q}}$-modules.

Il en résulte que $H_1(J_1(N)_{\mathbb{Q}})$ est libre de rang 2 en tant que $(\mathbb{T}_1(N))_{\mathbb{Q}}$-module. Cela résulte de la décomposition de Hodge : $H_1(J) = H^0(X, \Omega_X) \oplus H^1(X, \mathcal{O}_X)$ pour X une courbe projective et lisse sur $\mathbb{C}$ et J sa jacobienne. De plus $H^0(X, \Omega_X)$ et $H^1(X, \mathcal{O}_X)$ sont duaux par la dualité de Serre. Il en résulte que $H_1(J_1(N))_{\mathbb{C}})$ est libre de rang 2 sur $(\mathbb{T}_1(N))_{\mathbb{C}}$ et par suite $H_1(J_1(N)_{\mathbb{Q}})$ est libre de rang 2 en tant que $(\mathbb{T}_1(N))_{\mathbb{Q}}$-module.

Soient d et M tels que dM divise N. Alors $f(z) \mapsto f(dz)$ definit une injection de $S_k(\Gamma_1(M))$ dans $S_k(\Gamma_1(N))$. Soit $S_k^{\mathrm{n}}(\Gamma_1(N))$ (n pour nouvelle) l'orthogonal, pour le produit de Petersson, de la somme des images de $S_k(\Gamma_1(M))$. Alors , par Atkin-Lehner, $S_k^{\mathrm{n}}(\Gamma_1(N))$ admet une base f_i de vecteurs propres pour $\mathbb{T}_1(N)$, chacune apparaissant avec multipkicité 1. Si λ_n est la valeur propre de T_n , on a $a(n)(f_i) = \lambda_n a(1)(f_i)$. Il en résulte que $a(1)(f_i) \neq 0$, et on peut normailser f_i de sorte que $a_1(f_i) = 1$. Les f_i sont les formes primitives. Si f est primitive, $a(n)(f) = \lambda_n$ engendre sur $\mathbb{Q}$ un corps de nombres E_f, le corps des coefficients de f. Les $a(n)(f)$ sont de entiers algébriques. Ceci résulte de l'action de $\mathbb{T}_1(N)$ sur $H_1(J_1(N), \mathbb{Z})$. Une forme primitive est propre pour les opérateurs $< d >$ donc a un Nebentypus η_f.

Soit f une forme primitive. Soit $\Lambda_f : (\mathbb{T}_1(N))_{\mathbb{Q}} \to E_f$ le morphisme de $\mathbb{Q}$-algèbre qui à T_n associe $a(n)(f)$ (et à $< d >$ associe $\eta_f(d)$). Appelons I_f le noyau de Λ_f. On définit J_j comme la variété abélienne quotient de $J_1(N)$ par $I_f J_1(N)$. Le module de Tate $V_p(J_f)$ est un $\mathbb{Q}_p \otimes E_f$-module libre l de

rang 2. L'action de T_n est par $a(n)(f)$. $V_p(J_f)$ défini une représentation p-adique $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Q}_p \otimes E_f)$.

Soit ℓ un premier ne divisant pas Np. On a prolongement projectif et lisse $X_1(N)_{\mathbb{Z}[1/N]}$ définit par le problème universel courbe elliiptique E et point d'ordre exactement N dans toutes les fibres géométriques. Il en résulte que la représentation p-adique n'est pas ramifiée en ℓ. Soit F le Frobenius ent ℓ. Il définit un endomorphisme de $V_p(J_f) = V_p((J_f)_{\mathbb{F}_\ell}$.

Theorem 6.3. *Le polynôme caractéristique de F agissant sur le $\mathbb{Q}_p \otimes E_f$ module libre de rang 2 $V_p(J_f)$ est $X^2 - a(\ell)(f)X + \ell\eta(\ell)$.*

Le théorème résulte du :

Theorem 6.4. *On a dans l'algèbre des endomorphismes de $J_1(N)_{\mathbb{F}_\ell}$ les identités : $T_\ell = F + <\ell> F^\wedge$ et $w_\epsilon F w_\epsilon = <\ell>^{-1} F$. ($F^\wedge$ est l'isogénie duale de F).*

Esquisse de la preuve

Esquissons la preuve de la première identité. Soit $r : J_1(N)(\overline{\mathbb{Z}_\ell}) \to J_1(N)(\overline{F_\ell})$ l'application de réduction. Il suffit prouver que pour un ensemble Zariski dense de points x de $J_1(N)(\overline{\mathbb{F}_\ell})$, de relèvements $\hat{x}$ dans $J_1(N)(\overline{\mathbb{Z}_\ell})$, la réduction de $T_\ell(\hat{x})$ est $(F + <\ell> F^\wedge)(x)$. On prend les $x = (E, P) - (E_0, P_0)$ avec E et E_0 ordinaires. En fait on montre l'identité pour (E, P). On relève la courbe elliptique E en $\hat{E}$ et le point P en $\hat{P}$. On a $T_\ell((\hat{E}, \hat{P})) = \sum_C (\hat{E}/C, \hat{P}/C)$ C décrivant les sous-groupes d'ordre ℓ de $\hat{E}$. Cette identité est entre points dans une extension finie K de $\mathbb{Q}_\ell$. Elle s'étend entre identité entre points à valeurs dans l'anneau des entiers de K. Pour cela, on étend C en un schéma en groupes sur l'anneau des entiers O de K en prenant l'adhérence schématique de C dans $\hat{E}$. Cela permet de considérer le quotient $\hat{E}/C$. Comme E est ordinaire, quite à remplacer K par une extension non ramifiée, on a une suite exacte :

$$0 \to \mu_\ell \to \hat{E}[\ell] \to \mathbb{Z}/\ell\mathbb{Z} \to 0.$$

La réduction de cette suite exacte est canoniquement scindée.

Si $C = \mu_\ell$ clairement il se réduit en μ_ℓ. On prouve que les ℓ autres C se réduisent en $\mathbb{Z}/\ell\mathbb{Z}$. Ceci résulte de ce que si $C \to \mathbb{Z}/\ell\mathbb{Z}$ est un morphisme de schémas en groupes de rang ℓ sur O qui est un isomorphisme sur la fibre générique est un isomorphisme ([10]). Comme $F : E \to E_\sigma$ est inséparable, c'est l'isogénie de de noyau μ_ℓ. La contribution de $C = \mu_\ell$ est donc $F(x)$. On a la suite exacte : $E_{\sigma^{-1}} \to E \to E_{\sigma^{-1}}$, E_σ et $E_{\sigma^{-1}}$ étant les courbes elliptiques obtenues par changement de base par le Frobenius et son inverse, la flêche de droite étant l'isogénie de noyau $\mathbb{Z}/\ell\mathbb{Z}$. Le composé est la mutiplication par ℓ. Il en résulte que l'isogénie de droite envoie P sur $\ell\sigma^{-1}(P)$ On trouve que la contribution des ℓ C qui ne sont pas μ_ℓ est $\ell <\ell> F^{-1}(E, P)$ soit $<\ell> F^\wedge(E, P)$.

References

[1] Atiyah Macdonald Introduction to commutative algebra
[2] Alain Robert Elliptic curves
[3] Fred Diamond and Jerry Shurman A first course in Modular Forms.
[4] Miyake Modular forms.
[5] Joseph H. Silverman The Arithmetic of Elliptic Curves
[6] Robin Hartshorne Algebraic Geometry
[7] Jean-Pierre Serre Corps locaux.
[8] Jean-Pierre Serre Algèbre Locale Multiplicités
[9] Jean-Marc Fontaine and Barry Mazur. Geometric Galois representations. In *Elliptic curves, modular forms, & Fermat's last theorem* (Hong Kong, 1993), Ser. Number Theory, I, pages 41–78. Internat. Press, Cambridge, MA, 1995.
[10] Michel Raynaud Schémas en groupes de type $(p, \dots, p)$ Bulletin de la Soc. Math. de France, 102, 1974.
[11] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. Ann. of Math. (2), 141(3), 553–572, 1995.
[12] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. Ann. of Math. (2), 141(3), 443–551, 1995.

E-mail address: wintenb@math.u-strasbg.fr

Université Louis Pasteur, Département de Mathématique, Membre de l'Institut Universitaire de France, 7, rue René Descartes, 67084, Strasbourg Cedex, France