

# COURS DE L'INSTITUT FOURIER

ARMAND BRUMER

## **I- Courbes elliptiques et courbes modulaires**

*Cours de l'institut Fourier*, tome 10 (1975), p. 1-51

[http://www.numdam.org/item?id=CIF\\_1975\\_\\_10\\_\\_A2\\_0](http://www.numdam.org/item?id=CIF_1975__10__A2_0)

© Institut Fourier – Université de Grenoble, 1975, tous droits réservés.

L'accès aux archives de la collection « Cours de l'institut Fourier » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques  
<http://www.numdam.org/>

# 1- courbes elliptiques et courbes modulaires

## 1. CLASSIFICATION DES COURBES ELLIPTIQUES

### 1.1. DEFINITIONS ET NOTATIONS.

Soient  $K$  un corps de caractéristique  $p$  (positive ou nulle),  $\bar{K}$  une clôture algébrique de  $K$ , et  $K_s$  la clôture séparable de  $K$  contenue dans  $\bar{K}$ .

On appelle courbe elliptique sur  $K$  toute variété abélienne définie sur  $K$  de dimension 1.

Cette définition équivaut à la suivante :

Une courbe elliptique sur  $K$  est une courbe algébrique  $E$  projective non-singulière de genre 1 définie sur  $K$  et munie d'un point  $O$  rationnel sur  $K$ .

En effet, nous allons voir ci-dessous comment on peut définir une structure de groupe sur une telle courbe  $E$ .

#### 1.1.1. PROPOSITION .

(i) La courbe  $E$  est isomorphe à une cubique plane d'équation affine :

$$(1) \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad \text{où les } a_i \text{ sont dans } K ;$$

(ii) On a alors  $K(E) = K(x, y) = K[X, Y] / (F(X, Y))$  avec

$$F(X, Y) = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6 .$$

■ (i) Appliquons le théorème de Riemann-Roch au diviseur  $nO$ , où  $n$  est un entier strictement positif. La dimension  $\ell(nO)$  de l'espace  $L(nO)$  des diviseurs de fonctions supérieurs ou égaux à  $(-nO)$  est donnée par :  $\ell(nO) = \deg(nO) - g + 1 = \deg(nO) = n$ . En particulier,  $L(O) = K$ ,  $L(2O)$  a une base de la forme  $\{1, x, y\}$ , où  $x$  (resp.  $y$ ) a un pôle d'ordre 2 (resp. 3) en  $O$ . Et  $L(6O)$  est de dimension 6 ; or il contient les 7 éléments  $\{1, x, y, x^2, xy, y^2, x^3\}$ , donc il y a une relation  $K$ -linéaire entre ces éléments. Si le coefficient de  $y^2$  (resp. de  $x^3$ ) était nul, la courbe  $E$  serait de genre nul; ainsi, on peut écrire l'équation de  $E$  sous la forme (1).

(ii) L'ordre en  $O$  des fonctions  $1, x, y, x^2, xy, y^2, x^3$ , étant respectivement :  $0, -2, -3, -4, -5, -6, -6$ , il ne peut pas y avoir entre eux de relation de degré strictement plus petit que 2 en  $y$ , ou que 3 en  $x$ . Donc  $F(X, Y)$  est irréductible dans  $K[X, Y]$ , et l'on a bien :  $K(E) = K[X, Y]/(F(X, Y)) = K(x, y)$ . ■

Remarque : le point  $O$  est l'unique point à l'infini sur la courbe d'équation (1).

Remarquons aussi que la fonction  $\ell x + m y + n$  ( $\ell, m, n \in K$ ) a un pôle triple en  $O$  et pas d'autre pôle : elle a donc 3 zéros  $P_1, P_2, P_3$ . On définit une loi de groupe sur  $E$  en posant :  $P_1 + P_2 + P_3 = 0$  (cf. [11], 5, 6) ; on utilise ici la non-singularité de  $E$ . Sur la cubique d'équation affine (1), cela signifie que le point à l'infini est l'origine pour la loi de groupe, et que la somme de 3 points est nulle si et seulement si ces 3 points sont alignés (cf [5], 7). Soient  $E$  et  $E'$  deux courbes elliptiques sur  $K$ , et  $L$  une extension de  $K$  contenue dans  $\bar{K}$ . Nous appellerons L-homomorphisme de  $E$  dans  $E'$  toute application rationnelle définie sur  $L$  de  $E$  dans  $E'$  qui soit un homomorphisme de groupes. En fait, toute application rationnelle de  $E$  dans  $E'$  définie sur  $L$  et transformant l'origine de  $E$  en l'origine de  $E'$  est un L-homomorphisme (cf [5]).

1.1.2. Réciproquement, une équation du type (1) définit une courbe  $E$  qui est elliptique si et seulement si elle n'a pas de points singuliers, ce qui équivaut à  $\Delta \neq 0$ , où  $\Delta$  est le discriminant défini par les formules ci-dessous, (cf [47]) :

$$(2) \quad b_2 = a_1^2 + 4a_2, \quad b_4 = a_1 a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6,$$

$$b_8 = b_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 = \frac{b_2 b_6 - b_4^2}{4}$$

$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2 b_4 - 216b_6,$$

$$\Delta = \frac{c_4^3 - c_6^2}{12^3} = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6.$$

Posons aussi :  $j = c_4^3 / \Delta$  ;  $j$  est appelé l'invariant de  $E$ .

1.1.3. Lorsque  $p \neq 2, 3$ , l'équation de  $E$  peut s'écrire sous la forme :

$$(3) \quad y^2 = 4x^3 - g_2 x - g_3,$$

dite "forme de Weierstrass" (cf.[5], 7). Dans ce cas,  $\Delta$  est le discriminant du polynôme cubique du second membre multiplié par 16.

La forme de Weierstrass d'une courbe elliptique n'est pas unique, mais  $g_2$  (resp.  $g_3, \Delta$ ) sont définis à un coefficient près dans  $K^{*4}$  (resp.  $K^{*6}, K^{*12}$ ), comme nous le voyons ci-dessous (1.2.1).

## 1.2. CLASSIFICATION A $\bar{K}$ ISOMORPHISME PRES.

1.2.1. PROPOSITION . L'application qui fait correspondre à toute courbe elliptique  $E$  son invariant  $j$  définit une bijection entre l'ensemble des classes de  $\bar{K}$ -isomorphisme de courbes elliptiques sur  $K$ , et l'espace affine  $A^1(K)$  de dimension 1 sur  $K$ .

■ Soient  $E, E'$ , 2 courbes elliptiques sur  $K$ , et  $f$  un  $\bar{K}$ -isomorphisme de  $E$  sur  $E'$ , donc  $f$  envoie  $O$  sur l'origine  $O'$  de  $E'$ . Ecrivons les équations de  $E$  et  $E'$  sous la forme (1), les coor-

données étant notées  $(x, y)$  pour  $E$ , et  $(x', y')$  pour  $E'$ , et considérons  $x, y$  (resp.  $x', y'$ ) comme fonctions rationnelles sur  $E$  (resp.  $E'$ ) ; alors  $x' \circ f$  (resp.  $y' \circ f$ ) est une fonction rationnelle sur  $E$  avec un pôle d'ordre 2 (resp. 3) en  $O$ , autrement dit c'est un élément de  $L(2O)$  (resp.  $L(3O)$ ), c'est-à-dire une combinaison  $\bar{K}$  linéaire de  $\{1, x\}$  (resp.  $\{1, x, y\}$ ). Mais les coefficients de  $y^2$  et  $x^3$  dans (1) sont égaux à 1, donc on a plus précisément :

$$(4) \quad x' \circ f = u^2 x + r, \quad y' \circ f = u^3 y + u^2 s x + t,$$

où  $u, r, s, t \in \bar{K}$ ,  $u \neq 0$ . Les calculs donnent :

$$c'_4 = u^4 c_4, \quad c'_6 = u^6 c_6, \quad \Delta' = u^{12} \Delta \quad \text{et} \quad j' = j.$$

(cf. [18], Appendix 1, §1).

D'autre part, si  $E$  et  $E'$  sont 2 courbes elliptiques sur  $K$ , de même invariant, on peut déterminer  $u, r, s, t \in \bar{K}$ ,  $u \neq 0$ , de telle sorte que les formules (4) définissent un  $\bar{K}$ -isomorphisme  $f$  de  $E$  sur  $E'$ . (cf. [18], Appendix 1, §2).

Enfin, pour tout  $j$  de  $K$ , il existe une courbe elliptique  $E$  sur  $K$  dont  $j$  soit l'invariant ; si  $j \neq 0, 12^3$ , on peut prendre la courbe d'équation :  $y^2 + xy = x^3 - \frac{36}{j-12^3} x - \frac{1}{j-12^3}$  ; si  $j = 0$  et  $p \neq 2, 3$ , la courbe d'équation :  $y^2 = x^3 - \frac{c_6}{864}$ , pour n'importe quelle valeur non nulle de  $c_6$  ; si  $j = 12^3$  et  $p \neq 2, 3$ , la courbe d'équation :  $y^2 = x^3 - \frac{c_4}{48} x$  pour n'importe quelle valeur non nulle de  $c_4$  ; si  $p = 2$  (resp.  $p = 3$ ) et  $j = 0 = 12^3$ , on peut prendre la courbe d'équation :  $y^2 + y = x^3$  (resp.  $y^2 = x^3 - x$ ). ■

### 1.2.2. Application : détermination de $\text{Aut}(E)$ .

Notons  $\text{Aut}(E)$  le groupe des  $\bar{K}$ -automorphismes de  $E$ , et  $\mu_n$  le groupe des racines  $n^{\text{èmes}}$  de l'unité.

*PROPOSITION* . Si  $j \neq 0, 12^3$  , alors  $\text{Aut}(E) = \{\pm 1\} = \mu_2$  ; si  $j = 0$  et  $p \neq 2, 3$  , alors  $\text{Aut}(E) = \mu_6$  ; si  $j = 12^3$  et  $p \neq 2, 3$  , alors  $\text{Aut}(E) = \mu_4$  .

■ Considérons un automorphisme de  $E$  défini à l'aide des formules (4) . Comme  $c'_4 = c_4$  et  $c'_6 = c_6$  , nous avons  $u^2 = 1$  si  $j \neq 0, 12^3$  ; si  $j = 0$  et  $p \neq 2, 3$  , nous avons seulement  $u^6 = 1$  car  $c_4 = c'_4 = 0$  ; si  $j = 12^3$  et  $p \neq 2, 3$  , nous avons seulement  $u^4 = 1$  car  $c_6 = c'_6 = 0$  . Or, le changement de variable défini par les formules (4) doit définir la même courbe  $E$  : cela implique  $r = s = t = 0$  . ■

1.2.3. Remarque : Si  $p = 2$  (resp.  $p = 3$ ) et  $j = 0 = 12^3$  , alors  $\text{Aut } E \simeq \text{SL}_2(\mathbb{F}_3)$  (resp.  $\text{Aut } E \simeq \sigma_3$ ) (cf. [47] , 2).

1.3. CLASSIFICATION A K-ISOMORPHISME PRES. (cf.[5] , théorème 9.1).

1.3.1. *PROPOSITION* . Soit  $j$  un élément de  $K$  . L'ensemble des classes de K-isomorphisme de courbes elliptiques sur  $K$  d'invariant  $j$  , est en bijection avec le groupe de cohomologie  $H^1(G_K, \text{Aut}(E))$  , où  $G_K$  est le groupe de Galois de  $\bar{K}_s/K$  et  $\text{Aut}(E)$  le groupe des  $\bar{K}$ -automorphismes de n'importe quelle courbe elliptique sur  $K$  d'invariant  $j$  .

Rappelons que les éléments de  $H^1(G_K, \text{Aut}(E))$  sont les classes des 1-cocycles continus, et qu'un 1-cocycle  $\lambda_\sigma$  ( $\sigma \in G_K$ ) est dit continu s'il existe une extension galoisienne finie  $L/K$  telle que  $\lambda_\sigma = \lambda_\tau$  dès que  $\sigma$  et  $\tau$  ont la même action sur  $L$  . Et remarquons que  $\text{Aut}(E)$  n'est pas toujours abélien (cf. 1.2.3).

■ Définissons d'abord une application de l'ensemble des courbes elliptiques sur  $K$  d'invariant  $j$  dans le groupe  $H^1(G_K, \text{Aut}(E))$  , de sorte que deux courbes elliptiques  $K$ -isomorphes aient même image.

Soient  $E$  et  $E_1$  deux courbes elliptiques sur  $K$  d'invariant  $j$  .

D'après la proposition (1.2.1), il existe un  $\bar{K}$ -isomorphisme  $\psi$  de  $E$  sur  $E_1$ . Ecrivons l'équation de  $E$  sous la forme (1), et considérons un élément  $\sigma$  de  $G_K$ . Notons  $E^\sigma$  la courbe obtenue en remplaçant les coefficients  $a_i$  par leur image  $a_i^\sigma$ ; ici  $a_i \in K$  donc  $a_i^\sigma = a_i$  et  $E^\sigma = E$ . Notons  $\sigma(\psi)$  le  $\bar{K}$ -isomorphisme de  $E^\sigma$  sur  $E_1^\sigma$  obtenu en appliquant  $\sigma$  aux coefficients de  $\psi$ . Ainsi, pour chaque  $\sigma \in G_K$ , nous déduisons de  $\psi$  un  $\bar{K}$ -isomorphisme  $\sigma(\psi)$  de  $E$  sur  $E_1$ . Définissons  $\phi : G_K \rightarrow \text{Aut}(E)$  par :  $\phi_\sigma = \psi^{-1} \circ \sigma(\psi)$  pour tout  $\sigma \in G_K$ . Alors  $\phi$  est un 1-cocycle de  $G_K$  dans  $\text{Aut}(E)$  car  $\phi_\rho \circ \rho(\phi_\sigma) = \psi^{-1} \circ \rho(\psi) \circ \rho(\psi^{-1}) \circ \rho\sigma(\psi) = \psi^{-1} \circ \rho\sigma(\psi) = \phi_{\rho\sigma}$  pour tous  $\rho, \sigma \in G_K$ . De plus  $\phi$  est continu : en effet  $\phi_\sigma = \phi_\tau$  dès que  $\sigma$  et  $\tau$  ont la même action sur l'extension galoisienne de  $K$  engendrée par les coefficients de la transformation birationnelle  $\psi$ . D'autre part, si 2 courbes elliptiques  $E_1$  et  $E_2$  sur  $K$  d'invariant  $j$  sont  $K$ -isomorphes, soient  $\psi_i$  un  $\bar{K}$ -isomorphisme de  $E$  sur  $E_i$  ( $i = 1, 2$ ),  $\lambda$  un  $K$ -isomorphisme de  $E_1$  sur  $E_2$ , et  $\mu = \psi_2^{-1} \circ \lambda \circ \psi_1 \in \text{Aut}(E)$ . Alors

$$\begin{array}{ccc} E & \xrightarrow{\psi_1} & E_1 \\ \downarrow \mu & & \downarrow \lambda \\ E & \xrightarrow{\psi_2} & E_2 \end{array}$$

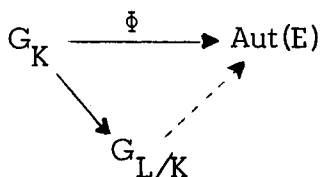
$$\begin{aligned} \phi_{1,\sigma} &= \psi_1^{-1} \circ \sigma(\psi_1) = \mu^{-1} \circ \psi_2^{-1} \circ \lambda \circ \sigma(\lambda^{-1}) \circ \sigma(\psi_2) \circ \sigma(\mu) \\ &= \mu^{-1} \circ \phi_{2,\sigma} \circ \sigma(\mu) \end{aligned}$$

pour tout  $\sigma \in G_K$ , donc les cocycles  $\phi_1$  et  $\phi_2$  sont cohomologues. Ceci s'applique en particulier

au cas  $E_1 = E_2$ ,  $\psi_1 \neq \psi_2$ .

En résumé, soit  $E$  une courbe elliptique sur  $K$  d'invariant  $j$ , et soit une  $K$ -classe de courbes elliptiques sur  $K$  d'invariant  $j$ . Considérons une courbe  $E'$  quelconque dans cette classe, un  $\bar{K}$ -isomorphisme quelconque  $\psi$  de  $E$  sur  $E'$ , et la classe de cohomologie du 1-cocycle continu de  $G_K$  à valeurs dans  $\text{Aut } E$  défini par :  $\phi_\sigma = \psi^{-1} \circ \sigma(\psi)$  pour tout  $\sigma \in G_K$ ; nous venons de montrer que ceci définit une application de l'ensemble des  $K$ -classes de courbes elliptiques sur  $K$  d'invariant  $j$ , dans  $H^1(G_K, \text{Aut}(E))$ . Nous allons voir que cette application est bijective. C'est une injection : si  $\psi_i : E \rightarrow E_i$  ( $i = 1, 2$ ) donnent des cocycles homologues, c'est-à-dire s'il existe  $\mu \in \text{Aut } E$  tel que pour tout  $\sigma \in G_K$ ,  $\psi_1^{-1} \circ \sigma(\psi_1) = \mu^{-1} \circ \psi_2^{-1} \circ \sigma(\psi_2) \circ \sigma(\mu)$ , alors l'isomorphisme  $\lambda = \psi_2 \circ \mu \circ \psi_1^{-1}$  de  $E_1$  sur  $E_2$  est invariant par  $\sigma$ , donc défini sur  $K$ .

C'est une surjection : soit  $\phi$  un 1-cocycle continu de  $G_K$  à valeurs dans  $\text{Aut}(E)$ , et  $L$  une extension galoisienne finie de  $K$  telle que  $\phi$  se factorise par le groupe de Galois  $G_{L/K}$  de  $L/K$ . Soit  $K(E)$



le corps des fonctions rationnelles de  $E$ , et  $L(E) = K(E) \otimes_K L$ . Le groupe  $G_{L/K}$  agit sur  $L$ ; comme  $L$  et  $K(E)$  sont 2 extensions linéairement disjointes sur  $K$ , on

peut prolonger l'action de  $G_{L/K}$  à  $L(E)$  de telle sorte que l'action sur  $K(E)$  soit triviale. Notons  $\sigma(f)$  l'image de  $f \in L(E)$  par  $\sigma \in G_{L/K}$ .

D'autre part, notons  $\tilde{\sigma}(f) = \sigma(f) \circ \phi_\sigma^{-1}$ ; cela définit une autre action de  $G_{L/K}$  sur  $L(E)$ , car  $\phi$  est un 1-cocycle :

$$\tilde{\rho\sigma}(f) = \rho\sigma(f) \circ [\phi_\rho \circ \rho(\phi_\sigma)]^{-1} = \tilde{\rho}\tilde{\sigma}(f)$$

si  $\sigma, \rho \in G_{L/K}$ ,  $f \in L(E)$ . Le corps des invariants de  $L(E)$  pour l'action "ordinaire" de  $G_{L/K}$  est  $K(E)$ . Notons  $L(E)^{\tilde{G}_{L/K}}$  le corps des invariants pour l'action "tordue" de  $G_{L/K}$ ; son corps des constantes est  $L^{\tilde{G}_{L/K}} = K$  et son degré de transcendance sur  $K$  est égal à 1. Donc  $L(E)^{\tilde{G}_{L/K}}$  est de la forme  $K(E')$  pour une courbe algébrique  $E'$  sur  $K$  telle que  $K(E') \cdot L = L(E)$ : donc  $E'$  est de genre 1, c'est une courbe elliptique sur  $K$ . Et il existe un  $L$ -isomorphisme  $\psi$  de  $E$  sur  $E'$  puisque  $L(E) = L(E')$ ; d'où un  $L$ -isomorphisme de  $K(E')$  sur  $K(E)$ , défini par :  $f \mapsto f \circ \psi$  et tel que :  $\sigma(f) \circ \psi = \tilde{\sigma}(f \circ \psi)$  c'est-à-dire  $(\sigma f) \circ \psi = \sigma(f \circ \psi) \circ \phi_\sigma^{-1} = \sigma(f) \circ \sigma(\psi) \circ \phi_\sigma^{-1}$  pour tout  $f \in L(E)$ , et tout  $\sigma \in G_{L/K}$  d'où :  $\phi_\sigma = \psi^{-1} \circ \sigma(\psi)$  pour tout  $\sigma \in G_K$ . ■

## 2. COURBES ELLIPTIQUES SUR $\mathbb{C}$

### 2.1. FONCTIONS DE WEIERSTRASS.

2.1.1. THEOREME . Toute surface de Riemann compacte de genre 1 sur  $\mathbb{C}$  est analytiquement isomorphe à une courbe elliptique sur  $\mathbb{C}$ .

■ Toute surface de Riemann compacte de genre 1 sur  $\mathbb{C}$  est un tore de la forme  $\mathbb{C}/L$  pour un réseau  $L$  de  $\mathbb{C}$ . Notons  $\mathfrak{H} = \{\tau \in \mathbb{C} / \text{Im}(\tau) > 0\}$  le demi-plan de Poincaré, et soit  $L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$  un réseau



de  $\mathbb{C}$  tel que  $\tau = \omega_1/\omega_2 \in \mathbb{H}$ . Définissons la fonction de Weierstrass de  $L$  par  $\wp(u;L) = \frac{1}{u^2} + \sum'_{\lambda \in L} \left( \frac{1}{(u-\lambda)^2} - \frac{1}{\lambda^2} \right)$  pour tout  $u \in \mathbb{C}$ ; ici  $\sum'$  signifie qu'on somme sur tous éléments non nuls de  $L$ . On montre (cf. [18], 1,3) que cette série converge sur tout compact de  $\mathbb{C}$  ne rencontrant pas  $L$ . De plus,  $\wp$  a un pôle double en  $O$  et est paire. Sa dérivée  $\wp'(u;L)$  est impaire et  $L$ -périodique, i.e.  $\wp'(u+\lambda;L) = \wp'(u;L)$  pour tout  $\lambda \in L$ . On en déduit que  $\wp$  et  $\wp'$  sont deux fonctions  $L$ -elliptiques, c'est-à-dire méromorphes sur  $\mathbb{C}$  et  $L$ -périodiques.

Montrons que  $\wp$  et  $\wp'$  sont liés par une relation algébrique : soit  $k$  un entier  $\geq 2$ , et  $G_{2k}(L)$  la série d'Eisenstein de poids  $2k$  associée à  $L$ , définie par :

$$G_{2k}(L) = \sum'_{\lambda \in L} \frac{1}{\lambda^{2k}} = \sum'_{(m,n) \in \mathbb{Z}^2} \frac{1}{(m\omega_1 + n\omega_2)^{2k}}$$

(le second  $\sum'$  signifie qu'on somme sur  $\mathbb{Z}^2 - \{(0,0)\}$ ). La série  $G_{2k}(L)$  est convergente, car la série  $\sum'_{\lambda \in L} \frac{1}{|\lambda|^\alpha}$  converge pour tout nombre réel  $\alpha > 2$  (cf. [18], 1,2). Alors, nous avons :

$$\wp(u;L) = \frac{1}{u^2} + \sum_{k \geq 1} (2k+1)u^{2k} G_{2k+2}(L)$$

et

$$\wp'(u;L) = \frac{-2}{u^3} + \sum_{k \geq 1} (2k+1)(2k)u^{2k-1} G_{2k+2}(L),$$

d'où  $\wp'^2 = 4\wp^3 - 60G_4\wp - 140G_6$ .

Posons  $g_4 = 60G_4$  et  $g_6 = 140G_6$ . La courbe  $E$  d'équation  $y^2 = 4x^3 - g_4x - g_6$  est une cubique du plan affine  $\mathbb{A}^2(\mathbb{C})$ . Les racines du trinôme  $4x^3 - g_4x - g_6$  sont les valeurs  $\wp(v_i;L)$  ( $i = 1, 2, 3$ ) où les nombres  $v_i$  sont les zéros de  $\wp'(u;L) \pmod{L}$ .

Comme la fonction  $\wp'$  est à la fois impaire et  $L$ -périodique, on a

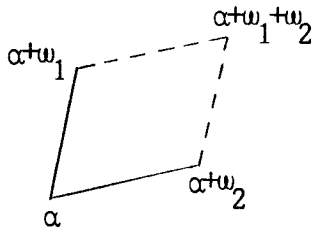
$$\wp'(-\omega_1/2) = -\wp'(\omega_1/2) = \wp'(\omega_1/2),$$

donc  $\omega_1/2$  est un zéro de  $\wp'$ ; de même  $\omega_2/2$  et  $(\omega_1 + \omega_2)/2$  sont des zéros de  $\wp'$ , donc les nombres  $v_1, v_2, v_3$  sont congrus modulo  $L$  à

$\omega_1/2$  ,  $\omega_2/2$  ,  $(\omega_1+\omega_2)/2$  (cf. [3]). La fonction  $\wp$  est paire, et  $v_i \equiv -v_i \pmod{L}$  , donc  $\wp$  prend la valeur  $\wp(v_i)$  avec une multiplicité paire ( $\geq 2$ ) . Or  $\wp$  a un seul pôle d'ordre 2 modulo  $L$  , et nous avons le lemme suivant :

2.1.2. LEMME . Soient  $f$  une fonction  $L$ -elliptique de points "singuliers" (zéros ou pôles)  $\{a_i\}$  dans  $\mathbb{C}/L$  , et  $m_i$  l'ordre de  $f$  en  $a_i$  . Alors  $\sum_i m_i = 0$  .

■ Soit  $R$  un domaine fondamental pour  $\mathbb{C}/L$  , défini par :



$R = \{z \in \mathbb{C} / z = \alpha + t_1\omega_1 + t_2\omega_2, 0 \leq t_i < 1\}$  , où  $\alpha$  est un complexe choisi de telle sorte que la frontière  $\partial R$  de  $R$  ne contienne aucun point singulier de  $f$  . Le théorème des résidus appliqué à la fonction  $L$ -elliptique  $f'/f$  et au contour  $\partial R$  donne  $\sum_i m_i = 0$  . ■

Terminons la démonstration du théorème : la fonction  $L$ -elliptique  $\wp - \wp(v_i)$  , ayant un seul pôle double modulo  $L$  ne peut avoir d'autre zéro que le zéro double  $v_i$  ; en particulier  $\wp(v_j) \neq \wp(v_i)$  dès que  $i \neq j$  . Ainsi les 3 racines du trinôme  $4x^3 - g_4x - g_6$  sont distinctes, le discriminant est non nul, et  $E$  est une courbe elliptique (cf. 1.1.3).

L'isomorphisme de  $\mathbb{C}/L$  sur  $E$  (considérée comme courbe projective) est donné par :  $u \longmapsto (u^3 \wp(u), u^3 \wp'(u), u^3)$  . ■

2.1.3. Loi de groupe.  $\mathbb{C}/L$  et  $E$  sont des groupes abéliens (la structure de  $\mathbb{C}/L$  étant induite par celle de  $\mathbb{C}$ ), et l'isomorphisme défini dans le théorème (2.1.1) est un isomorphisme de groupes. Autrement dit, si  $P_i = (\wp(u_i), \wp'(u_i))$  est le point de  $E$  correspondant à  $u_i \in \mathbb{C}/L$  ( $i=1,2$ ) , alors le point  $P_1+P_2$  correspond à  $u_1+u_2$  , i.e.  $P_1+P_2 = (\wp(u_1+u_2), \wp'(u_1+u_2))$  (cf. [18] , 1,3). La loi d'addition sur  $E$  étant définie par des propriétés d'alignement (cf. 1.1.1), un raisonnement de géométrie affine élémentaire nous donne les formules :

$$\wp(u_1+u_2) = -\wp(u_1) - \wp(u_2) + \frac{1}{4} \left( \frac{\wp'(u_1) - \wp'(u_2)}{\wp(u_1) - \wp(u_2)} \right)^2 \quad \text{si } u_1 \neq u_2 ,$$

$$\wp(2u) = -2\wp(u) + \frac{1}{4} \left( \frac{\wp''(u)}{\wp'(u)} \right)^2 \quad (\text{cf. [18] , 1,3}).$$

2.1.4. Corps de fonctions. D'après (1.1.1), le corps  $\mathbb{C}(E)$  est égal à  $\mathbb{C}(\wp, \wp')$ . De façon analogue,  $\mathbb{C}(\wp, \wp')$  est le corps des fonctions méromorphes sur  $\mathbb{C}/L$ , c'est-à-dire le corps des fonctions  $L$ -elliptiques (une autre démonstration est donnée dans [18] , 1,2). Ainsi, les fonctions algébriques sur  $E$  s'identifient aux fonctions analytiques sur  $\mathbb{C}/L$ .

2.1.5. Homomorphismes. Lorsqu'on identifie  $\mathbb{C}/L$  avec  $E$  (resp.  $\mathbb{C}/L'$  avec  $E'$ ) au moyen de l'isomorphisme précédent, les homomorphismes de  $E$  dans  $E'$  correspondent aux homomorphismes analytiques de  $\mathbb{C}/L$  dans  $\mathbb{C}/L'$ . C'est ce que nous entendrons désormais par "homomorphisme de  $\mathbb{C}/L$  dans  $\mathbb{C}/L'$ ".

PROPOSITION . Tout homomorphisme  $\psi$  de  $\mathbb{C}/L$  dans  $\mathbb{C}/L'$  est induit par la multiplication, dans  $\mathbb{C}$ , par un nombre complexe  $\alpha$  tel que  $\alpha L \subset L'$  ; et  $\psi$  est un isomorphisme si et seulement si  $\alpha L = L'$ .

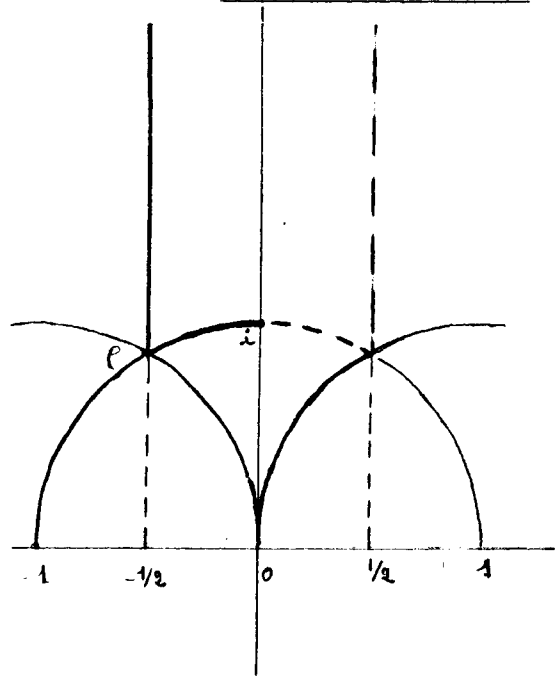
■ Au voisinage de  $0$ , nous avons  $\psi(z) = \sum_{n \geq 0} a_n z^n$ ,  $a_n \in \mathbb{C}$ , mais aussi  $\psi(z+z') = \psi(z) + \psi(z')$ , car la congruence modulo  $L'$  devient égalité. Ce n'est possible que si  $a_n = 0$  pour  $n \neq 1$  et  $a_1 = \alpha \in \mathbb{C}$ . Soit  $z$  un complexe quelconque; pour un entier  $n$  assez grand,  $z/n$  est assez proche de  $0$  pour que  $\psi(z/n) = \alpha \frac{z}{n}$ . Or  $\psi(z/n) = \frac{1}{n} \psi(z) \pmod{L'}$  d'où  $\psi(z) \equiv \alpha z \pmod{L'}$ . Et bien sûr  $\alpha L \subset L'$ , avec égalité si et seulement si  $\psi$  est un isomorphisme. ■

Remarque : Réciproquement, si  $\alpha \in \mathbb{C}$  est tel que  $\alpha L \subset L'$ , la multiplication par  $\alpha$  induit un homomorphisme de  $\mathbb{C}/L$  dans  $\mathbb{C}/L'$ .

2.1.6. Le groupe modulaire. Soit  $\Gamma = \text{SL}_2(\mathbb{Z}) = \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} / a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$  et  $\bar{\Gamma} = \text{PSL}_2(\mathbb{Z}) = \text{SL}_2(\mathbb{Z}) / \{\pm 1\}$ . Le groupe  $\Gamma$  agit sur  $\mathbb{H}$  par  $\gamma(\tau) = \frac{a\tau + b}{c\tau + d}$ , et cette expression ne dépend que de la classe de  $\gamma$  dans  $\bar{\Gamma}$ . Nous pouvons donc parler de l'action de  $\bar{\Gamma}$  sur  $\mathbb{H}$  et du quotient  $\bar{\Gamma} \backslash \mathbb{H}$ . Le groupe  $\bar{\Gamma}$  est appelé le groupe modulaire. Il est engendré

par  $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  et  $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ , (cf. [38], 7,1,2). On trouve dans ([38], 7,1,2), la détermination d'un domaine fondamental pour  $\overline{\Gamma} \backslash \mathbb{H}$ .

Plongeons  $\mathbb{C}$  dans la sphère de Riemann, par adjonction d'un point à l'infini (noté  $\infty$ ), (cf. [3]). L'ensemble  $\overline{\Gamma} \backslash \mathbb{H} \cup \{\infty\}$ , noté  $\widehat{\overline{\Gamma} \backslash \mathbb{H}}$ , a une structure de surface de Riemann compacte de genre 0.



Le revêtement  $\hat{\mathbb{H}} = \mathbb{H} \cup \{\infty\}$  de  $\widehat{\overline{\Gamma} \backslash \mathbb{H}}$  est non ramifié en dehors de  $\infty, i, \rho$ . L'indice de ramification est égal à 2 en  $i$ , à 3 en  $\rho$ , et il est infini en  $\infty$ . En effet, l'indice de ramification de la classe d'un point  $\tau$  de  $\widehat{\overline{\Gamma} \backslash \mathbb{H}}$  est égal à l'ordre du stabilisateur de  $\tau$  dans  $\overline{\Gamma}$ .

2.1.7. PROPOSITION. L'application :  $\tau \mapsto \mathbb{C}/\mathbb{Z}\tau \oplus \mathbb{Z}$  induit une bijection entre  $\overline{\Gamma} \backslash \mathbb{H}$  et l'ensemble des classes de  $\mathbb{C}$ -isomorphisme des courbes elliptiques de la forme  $\mathbb{C}/L$ .

■ Soit  $L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$  un réseau de  $\mathbb{C}$ , et  $\tau = \omega_1/\omega_2 \in \mathbb{H}$  ; Alors  $L = \omega_2(\mathbb{Z}\tau \oplus \mathbb{Z})$ , et d'après la proposition (2,1,5),  $\mathbb{C}/L$  et  $\mathbb{C}/\mathbb{Z}\tau \oplus \mathbb{Z}$  sont isomorphes. Il suffit donc de regarder les courbes de la forme  $\mathbb{C}/\mathbb{Z}\tau \oplus \mathbb{Z}$ . La même proposition (2.1.5) montre que deux telles courbes (correspondant à  $\tau$  et  $\tau'$ ) sont  $\mathbb{C}$ -isomorphes si et seulement si il existe un complexe  $\alpha$  tel que  $\alpha(\mathbb{Z}\tau' \oplus \mathbb{Z}) = \mathbb{Z}\tau \oplus \mathbb{Z}$ , c'est-à-dire tel que  $\{\alpha\tau', \alpha\}$  et  $\{\tau, 1\}$  forment deux bases du même réseau  $\mathbb{Z}\tau \oplus \mathbb{Z}$ . Or nous avons le lemme suivant :

2.1.8. LEMME. Soient  $\{\omega_1, \omega_2\}$  et  $\{\omega'_1, \omega'_2\}$  deux couples de complexes tels que  $\tau = \omega_1/\omega_2$  et  $\tau' = \omega'_1/\omega'_2$  soient dans  $\mathbb{H}$ . Les deux réseaux  $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$  et  $\mathbb{Z}\omega'_1 \oplus \mathbb{Z}\omega'_2$  sont identiques si et seulement si  $\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \gamma \begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix}$  pour une matrice  $\gamma$  de  $\Gamma$ .

■ En effet, nous devons avoir  $\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \gamma \begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix}$  pour une matrice  $\gamma$  de  $GL_2(\mathbb{Z}) = \{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} / a, b, c, d \in \mathbb{Z}, ad - bc = \pm 1 \}$ . Et comme  $Im(\gamma\tau) = \frac{Im(\tau)}{|c\tau+d|^2} \cdot \det \gamma$ , nous avons  $\det \gamma = +1$ . La réciproque est immédiate. ■

Revenons à la démonstration de la proposition :  $\mathbb{C}/\mathbb{Z}\tau \oplus \mathbb{Z}$  et  $\mathbb{C}/\mathbb{Z}\tau' \oplus \mathbb{Z}$  sont isomorphes si et seulement si  $\begin{pmatrix} \alpha\tau' \\ \alpha \end{pmatrix} = \gamma \begin{pmatrix} \tau \\ 1 \end{pmatrix}$  pour une matrice  $\gamma$  de  $\Gamma$ , ce qui équivaut à  $\tau' = \gamma(\tau)$ . ■

2.1.9. Invariant. Calculons l'invariant de  $\mathbb{C}/L = E$ . Pour tout  $\tau \in \mathfrak{H}$ , et tout entier  $k \geq 2$ , la série ci-dessous converge (cf. 2,1,1) :

$$G_{2k}(\tau) = \sum'_{(m,n) \in \mathbb{Z}^2} \frac{1}{(m\tau+n)^{2k}} = \omega_2^{2k} G_{2k}(L).$$

Posons :

$$E_{2k}(\tau) = 1 + (-1)^k \frac{4k}{B_k} \sum_{n \geq 1} \sigma_{2k-1}(n) q^n,$$

où  $q = e^{2\pi i \tau}$ ,  $\sigma_k(n) = \sum_{d|n} d^k$ , et où les  $B_k$  sont les nombres de Bernoulli, liés à la fonction zeta de Riemann par

$$\zeta(2k) = \frac{2^{2k-1}}{(2k)!} B_k \pi^{2k} \quad (k \text{ entier } > 0) \quad (\text{cf. [38] , 7,4,1}).$$

Par exemple,  $B_1 = 1/6$ ,  $B_2 = 1/30$ ,  $B_3 = 1/42$ , ... .

Les calculs (cf. [38] , 7,4,2) montrent que :

$$G_{2k}(\tau) = 2\zeta(2k) + 2 \frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{n \geq 1} \sigma_{2k-1}(n) q^n = 2\zeta(2k) E_{2k}(\tau).$$

Ceci prouve que la série  $E_{2k}(\tau)$  est convergente sur  $\mathfrak{H}$ , pour tout entier  $k \geq 2$ . Ainsi, on a :

$$c_4(L) = \frac{48}{4} g_4(L) = \left(\frac{2\pi}{\omega_2}\right)^4 E_4(\tau)$$

$$c_6(L) = \frac{864}{4} g_6(L) = \left(\frac{2\pi}{\omega_2}\right)^6 E_6(\tau)$$

$$\Delta(L) = \frac{c_4(L)^3 - c_6(L)^2}{12^3} = \left(\frac{2\pi}{\omega_2}\right)^{12} \frac{E_4(\tau)^3 - E_6(\tau)^2}{12^3}.$$

$$\text{Soit } \Delta(\tau) = \frac{E_4(\tau)^3 - E_6(\tau)^2}{12^3} = \frac{(1+240 \sum_{n \geq 1} \sigma_3(n)q^n)^3 - (1-540 \sum_{n \geq 1} \sigma_5(n)q^n)^2}{12^3} .$$

Le numérateur est congru à  $12^2(5 \sum_{n \geq 1} \sigma_3(n)q^n + 7 \sum_{n \geq 1} \sigma_5(n)q^n)$  modulo  $12^3$ , et la parenthèse est nulle modulo 12 car  $7 \equiv -5 \pmod{12}$  et  $d^3 \equiv d^5 \pmod{12}$  pour tout entier  $d$ . Ainsi, dans le développement  $\Delta(\tau) = \sum_{n \geq 1} \tau(n)q^n$ ,

l'application  $\tau$  est à valeurs entières, et  $\tau(1) = 1$  (l'application  $\tau$  est appelée la fonction de Ramanujan, et n'a bien sûr rien à voir avec la varia-

ble  $\tau \in \mathbb{H}$ ). Enfin,  $j(\tau) = j(L) = \frac{c_4(L)^3}{\Delta(L)} = \frac{1}{q} + 744 + \sum_{n \geq 1} c(n)q^n$  où les coefficients  $c(n)$  sont entiers.

## 2.2. FORMES MODULAIRES.

2.2.1. Soit  $G$  un sous-groupe d'indice fini de  $\Gamma$ , et soit  $\bar{G} = G/G \cap \{\pm 1\}$ ;  $\bar{G}$  agit sur  $\mathbb{H}$ . L'image, par un élément de  $\bar{\Gamma}$ , de  $\infty$  est  $\infty$  ou un point rationnel. L'action de  $\bar{G}$  décompose  $\bar{\Gamma} \cdot \infty$  en  $\bar{G}$ -orbites, dites pointes de  $\widehat{\bar{G} \backslash \mathbb{H}}$ ; en particulier,  $\infty$  est la pointe unique de  $\bar{\Gamma} \backslash \mathbb{H}$ . La réunion de  $\bar{G} \backslash \mathbb{H}$  et de ses pointes est notée  $\widehat{\bar{G} \backslash \mathbb{H}}$ ; c'est une surface de Riemann compacte, formant un revêtement de  $\bar{\Gamma} \backslash \mathbb{H}$  de degré égal à l'indice  $[\bar{\Gamma} : \bar{G}]$ .

D'autre part, soient  $f$  une fonction définie sur  $\mathbb{H}$ ,  $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  un élément de  $GL_2^+(\mathbb{R}) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc > 0, a, b, c, d \in \mathbb{R} \}$ , et  $k$  un entier. Posons, par définition :

$$(f|_k \gamma)(\tau) = (ad-bc)^{k/2} (c\tau+d)^{-k} f\left(\frac{a\tau+b}{c\tau+d}\right)$$

pour tout  $\tau$  dans  $\mathbb{H}$ . Alors  $(\gamma, f) \longmapsto f|_k \gamma$  définit une action de  $GL_2^+(\mathbb{R})$  sur l'ensemble des fonctions définies sur  $\mathbb{H}$  à valeurs dans  $\mathbb{C}$ . Cette action de  $GL_2^+(\mathbb{R})$  a les propriétés suivantes :

$$f|_k 1 = f, \quad f|_k \gamma\gamma' = (f|_k \gamma)|_k \gamma', \quad f|_k \lambda\gamma = f|_k \gamma$$

pour tous  $\gamma, \gamma' \in GL_2^+(\mathbb{R})$  et  $\lambda \in \mathbb{R}^*$ .

2.2.2. Nous pouvons maintenant définir une forme modulaire de poids  $k$  pour  $G$  : c'est une fonction  $f$ , holomorphe dans  $\mathfrak{H}$ , telle que  $f|_k \gamma = f$  pour tout  $\gamma$  de  $G$ , et holomorphe aux pointes de  $\overline{G} \backslash \mathfrak{H}$ . Cette dernière condition a la signification suivante : soit  $n_0$  le plus petit entier tel que  $n_0 T = \begin{pmatrix} 1 & n_0 \\ 0 & 1 \end{pmatrix} \in G$  ; or  $(f|_k n_0 T)(\tau) = f(\tau + n_0)$  ; donc  $f$  est (par abus de langage) fonction de  $q^{1/n_0}$ , holomorphe dans  $\{q \in \mathbb{C} / 0 < |q| < 1\}$  ;  $f$  est dite holomorphe à la pointe  $\infty$  si  $f$  se prolonge en une fonction holomorphe en  $q = 0$  ; et  $f$  est dite holomorphe à la pointe  $P = \gamma_0(\infty)$  (où  $\gamma_0 \in \Gamma$ ) si  $f|_k \gamma_0$  est holomorphe à l'infini.

Lorsque, de plus,  $f$  s'annule aux pointes,  $f$  est dite forme parabolique de poids  $k$  pour  $G$ . Si on remplace l'hypothèse "f holomorphe" ou l'hypothèse plus faible "f méromorphe",  $f$  est dite fonction modulaire.

2.2.3. Formes modulaires pour  $\Gamma$  (cf. [38], 7,3). Notons  $M_{2k}$  (resp.  $M_{2k}^0$ ) le  $\mathbb{C}$ -espace vectoriel des formes modulaires (resp. paraboliques) de poids  $2k$  pour  $\Gamma$ . Par exemple,  $E_{2k} \in M_{2k}$ ,  $\Delta \in M_{12}^0$ ,  $j \in M_0$ .

*PROPOSITION*. La dimension de  $M_{2k}$  est égale à :

$$\begin{aligned} 0 & \quad \text{si } k < 0 \\ [k/6] & \quad \text{si } k \equiv 1 \pmod{6} \text{ et } k \geq 0 \\ [k/6] + 1 & \quad \text{si } k \not\equiv 1 \pmod{6} \text{ et } k \geq 0. \end{aligned}$$

De plus, si  $\dim M_{2k} \neq 0$ , on a :  $\dim M_{2k}^0 = \dim M_{2k} - 1$ .

■ Pour  $k \geq 0$ , on montre d'abord la proposition pour  $k < 6$ , en prouvant :  $M_0 = \mathbb{C}$ ,  $M_2 = 0$ ,  $M_{2k} = \mathbb{C}G_{2k}$  si  $k = 3, 4, 5$ , et  $M_{2k}^0 = 0$ . Puis on montre que la multiplication par  $\Delta$  définit un isomorphisme de  $M_{k-6}$  sur  $M_k^0$ . La démonstration se trouve dans ([38], 7,3,2) ; elle s'appuie sur le lemme suivant (2.2.4). ■ En particulier,  $M_{12}^0 = \mathbb{C} \cdot \Delta$ .

2.2.4. *LEMME*. Soit  $f$  une fonction modulaire de poids  $2k$  pour  $\Gamma$ , non identiquement nulle. Alors on a :

$$v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_\rho(f) + \sum_{P \in \Gamma \backslash \mathfrak{H}} v_P(f) = \frac{k}{6}.$$

Dans cet énoncé,  $v_p(f)$  est l'ordre de la fonction méromorphe  $f$  en  $P$ , et le signe  $\sum'$  indique que l'on somme sur les points de  $\bar{\Gamma} \setminus \mathbb{H}$  distincts de  $i$  et  $\rho$ .

■ Pour démontrer ce lemme, on peut intégrer la fonction  $\frac{1}{2i\pi} \frac{df}{f}$  sur le bord d'un domaine fondamental pour  $\Gamma$  (cf. [38], 7,3,1), ou calculer le degré de la forme différentielle  $f(\tau)(d\tau)^k$  et utiliser la formule de Riemann-Roch. ■

2.2.5. *THEOREME*. Toute courbe elliptique  $E$  sur  $\mathbb{C}$  est de la forme  $\mathbb{C}/L$  pour un réseau  $L$  de  $\mathbb{C}$ .

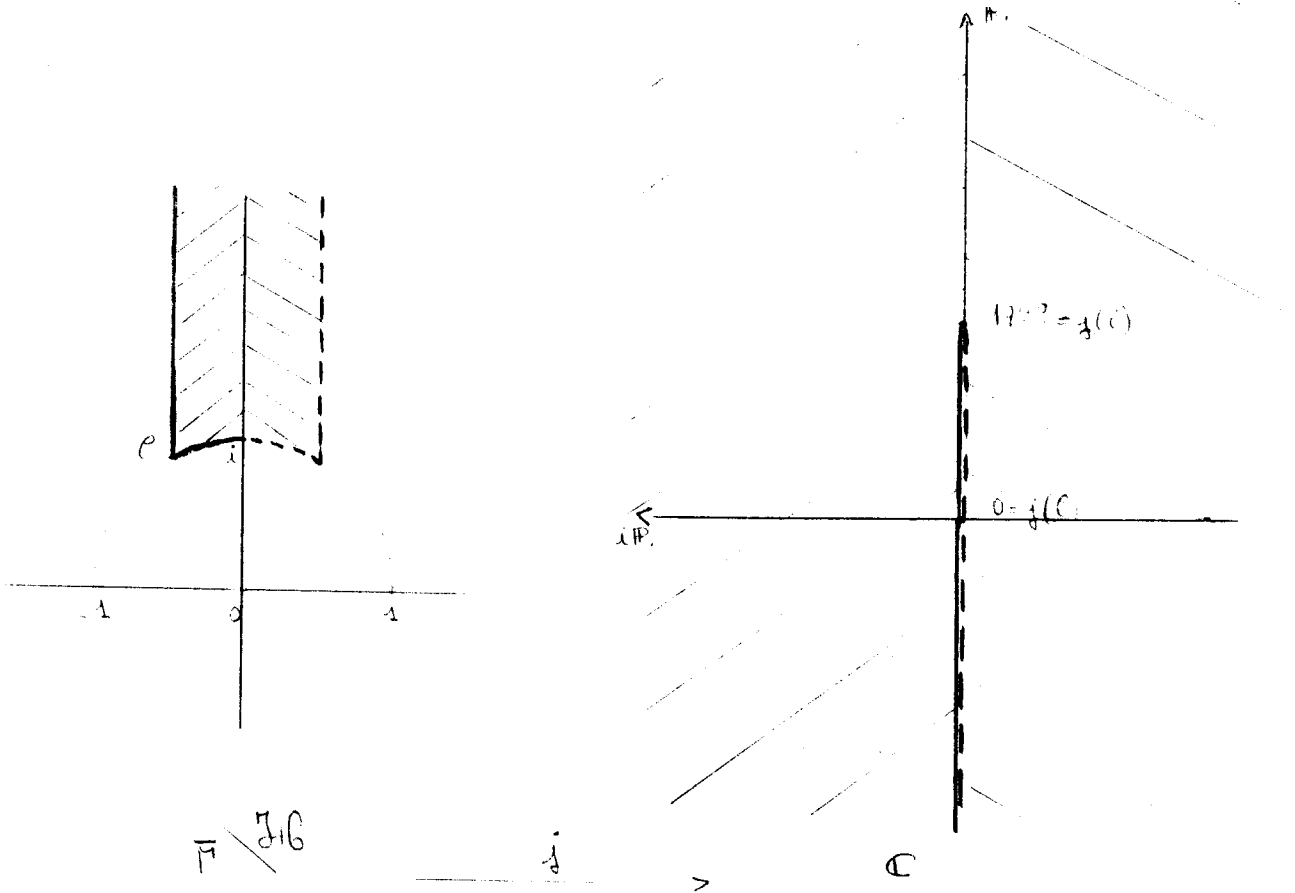
C'est la réciproque du théorème (2.1.1).

■ Soit  $E$  une courbe elliptique sur  $\mathbb{C}$ , d'équation  $y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}$ , de discriminant  $\Delta = \frac{c_4^3 - c_6^2}{12^3}$  non nul et d'invariant  $j = \frac{c_4^3}{\Delta}$  (cf. 1.1.3).

Nous allons montrer que  $j$  est l'invariant d'une courbe elliptique de la forme  $\mathbb{C}/L$  : en effet, la fonction  $j(\tau) = \frac{c_4(\tau)^3}{\Delta(\tau)}$  définie en (2.1.9) induit une bijection de  $\bar{\Gamma} \setminus \mathbb{H}$  sur  $\mathbb{C}$  ; pour le voir, il suffit d'appliquer le lemme (2.2.4) à la forme modulaire  $f_\lambda(\tau) = c_4(\tau)^3 - \lambda\Delta$  pour tout complexe  $\lambda$  ;  $f_\lambda$  est de poids 12 ; donc  $k/6 = 1$ , et on a une égalité de la forme  $1 = n + n'/2 + n''/3$ , avec  $n, n', n'' \in \mathbb{N}$ , ce qui n'est possible que pour  $(n, n', n'') = (1, 0, 0)$  ou  $(0, 2, 0)$  ou  $(0, 0, 3)$ , et prouve que  $f_\lambda$  s'annule en un point  $\tau$  et un seul de  $\bar{\Gamma} \setminus \mathbb{H}$ . (cf. [38], 7,3,3). Ainsi les courbes elliptiques  $E$  et  $\mathbb{C}/\mathbb{Z}\tau \oplus \mathbb{Z}$  ont même invariant et sont  $\mathbb{C}$ -isomorphes. En fait,  $E$  est l'image par l'isomorphisme du théorème (2.1.1) de  $\mathbb{C}/L$  où  $L = u(\mathbb{Z}\tau \oplus \mathbb{Z})$ ,  $u$  étant l'un des nombres complexes définis par :  $g_4(\tau) = u^4 \cdot c_4/48$ ,  $g_6(\tau) = u^6 \cdot c_6/864$ . Dans le cas général, cela détermine  $u^2$  ( $\text{Aut}(E) \simeq \mu_2$ ) ; si  $c_4 = 0$  (i.e.  $j = 0$ ,  $\tau = \rho$  et  $\text{Aut}(E) \simeq \mu_6$ ) cela détermine  $u^6$  ; et si  $c_6 = 0$  (i.e.  $j = 12^3$ ,  $\tau = i$  et  $\text{Aut}(E) \simeq \mu_4$ ) cela détermine  $u^4$ . Dans tous les cas,  $L$  est bien déterminé. ■



Remarque : L'application  $\tau \longmapsto j(\tau)$  est une représentation conforme du domaine fondamental pour  $\overline{\Gamma} \backslash \mathbb{H}$  sur  $\mathbb{C}$  :



2.2.6. COROLLAIRE . L'ensemble des classes de  $\mathbb{C}$ -isomorphisme de courbes elliptiques sur  $E$  est en bijection avec  $\overline{\Gamma} \backslash \mathbb{H}$  .

■ C'est la proposition (2.1.7) associée au théorème (2.2.5) ■

2.3. LA FORMULE  $\Delta(q) = q \prod_{n \geq 1} (1 - q^n)^{24}$  (cf. [45] , [18] ).

2.3.1. La formule sommatoire de Poisson. Soit  $\varphi$  une fonction de  $\mathbb{R}$  dans  $\mathbb{C}$  , indéfiniment dérivable, qui tende "rapidement" vers 0 à l'infini ainsi que toutes ses dérivées, au sens suivant : pour tous  $n$  ,  $m \in \mathbb{N}$  , la fonction  $x \longmapsto |x|^m \varphi^{(n)}(x)$  est bornée. Sa transformée de Fourier est la fonction de  $\mathbb{R}$  dans  $\mathbb{C}$  définie par :  $\hat{\varphi}(y) = \int_{-\infty}^{+\infty} \varphi(x) e^{-2\pi i x y} dx$  ; elle vérifie les mêmes propriétés que  $\varphi$  .

**THEOREME** . Si  $\varphi$  est une telle fonction, alors, pour tout réel  $t$ , nous avons :  $\sum_{n \in \mathbb{Z}} \varphi(t+n) = \sum_{n \in \mathbb{Z}} \hat{\varphi}(n) e^{2\pi i n t}$ , et en particulier  $\sum_{n \in \mathbb{Z}} \varphi(n) = \sum_{n \in \mathbb{Z}} \hat{\varphi}(n)$ .

■ Soit  $\Phi(t) = \sum_{n \in \mathbb{Z}} \varphi(t+n)$ ; alors  $\Phi$  est périodique de période 1, et  $\Phi'(t) = \sum_{n \in \mathbb{Z}} \varphi'(t+n)$  est continue; donc  $\Phi$  est égale à sa série de Fourier :  
 $\Phi(t) = \sum_{n \in \mathbb{Z}} a_n e^{2\pi i n t}$ , où  $a_n = \int_0^1 e^{-2\pi i n u} \Phi(u) du = \sum_{m \in \mathbb{Z}} \int_0^1 e^{-2\pi i n u} \varphi(u+m) du = \hat{\varphi}(n)$ . ■

2.3.2. **Exemple : la fonction thêta.** Posons  $\theta(\tau) = \sum_{n \in \mathbb{Z}} e^{\pi i n^2 \tau}$ , ( $\tau \in \mathbb{H}$ ).

**PROPOSITION** . Nous avons  $\theta^4 \Big|_2 S = -\theta^4$  et  $\theta^4 \Big|_2 T^2 = \theta^4$  si  
 $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  et  $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ .

Rappelons que le groupe  $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm 1\}$  est engendré par  $S$  et  $T$  (cf.2.1.6). Si  $z \in \mathbb{C}^*$ , choisissons son argument de sorte que  $-\pi < \text{Arg}(z) \leq +\pi$ , et posons  $\sqrt{z} = \sqrt{|z|} e^{i/2 \text{Arg}(z)}$ .

■ Nous allons montrer que  $\theta(\tau) \sqrt{\tau/i} = \theta(-1/\tau)$  et  $\theta(\tau+2) = \theta(\tau)$ . La seconde égalité est évidente; pour la première, appliquons la formule sommatoire de Poisson à  $\varphi_\tau(t) = e^{\pi i t^2 \tau}$ :

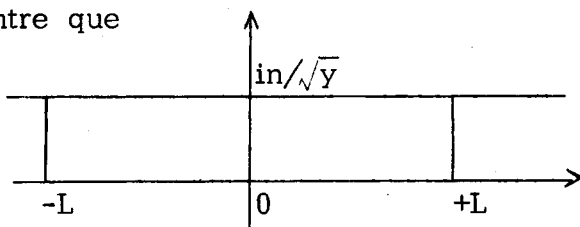
$$\theta(\tau) = \sum_{n \in \mathbb{Z}} \varphi_\tau(n) = \sum_{n \in \mathbb{Z}} \hat{\varphi}_\tau(n) \quad \text{où} \quad \hat{\varphi}_\tau(n) = \int_{-\infty}^{+\infty} e^{-2\pi i n u} e^{\pi i u^2 \tau} du.$$

Lorsque  $\tau$  est sur le demi-axe imaginaire positif; c'est-à-dire  $\tau = iy$ ,  $y \in \mathbb{R}$ ,  $y > 0$ , cela donne :

$$\hat{\varphi}_{iy}(n) = \int_{-\infty}^{+\infty} e^{-2\pi i n u - \pi u^2 y} du = \frac{1}{\sqrt{y}} \int_{-\infty + \frac{in}{\sqrt{y}}}^{+\infty + \frac{in}{\sqrt{y}}} e^{-(\pi n^2/y) - \pi v^2} dv$$

où  $v = \sqrt{y} \cdot u + \frac{in}{\sqrt{y}}$ . Or le théorème de Cauchy, appliqué au rectangle ci-contre lorsque  $L$  tend vers l'infini, montre que

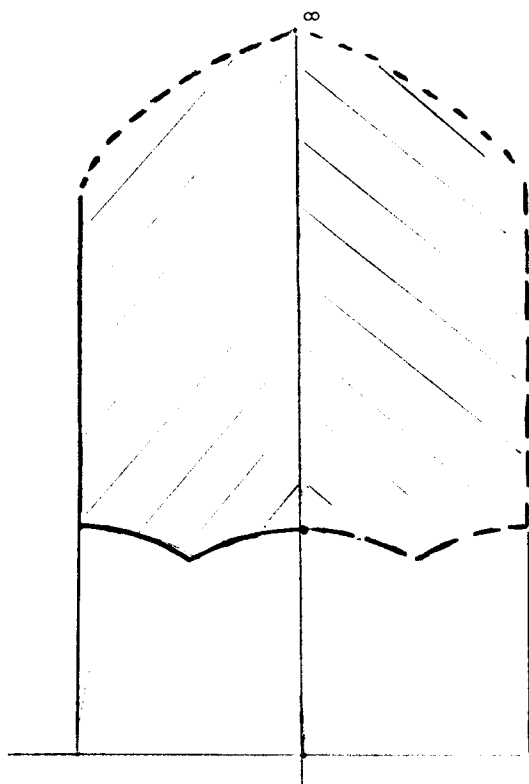
$$\int_{-\infty + \frac{in}{\sqrt{y}}}^{+\infty + \frac{in}{\sqrt{y}}} e^{-\pi v^2} dv = \int_{-\infty}^{+\infty} e^{-\pi v^2} dv = 1$$



d'où :  $\hat{\varphi}_{iy}(n) = \frac{1}{\sqrt{y}} e^{-\pi n^2/y}$  et  $\theta(iy) \sqrt{iy/i} = \theta(-1/iy)$ ; par prolongement

analytique, on obtient l'égalité cherchée. ■

Cette proposition montre que  $\theta^4$  est "presque" une forme modulaire de poids 2 pour le sous-groupe  $\Gamma_\theta = \langle S, T^2 \rangle$  de  $\Gamma$ .  $\Gamma_\theta$  est d'indice 2 dans  $\Gamma$ ; voici ci-contre un domaine fondamental de  $\Gamma_\theta$  dans  $\mathfrak{H}$ , formé de la réunion de 2 domaines fondamentaux de  $\Gamma$  (cf. 2.1.6). On voit que  $\widehat{\Gamma_\theta \backslash \mathfrak{H}}$  est une surface de Riemann compacte de genre 1 avec une seule pointe, à l'infini. L'indice de ramification de la pointe  $\infty$  dans le revêtement  $\widehat{\Gamma_\theta \backslash \mathfrak{H}} \rightarrow \widehat{\Gamma \backslash \mathfrak{H}}$  est égal à 2.



2.3.3. La fonction  $\eta$  de Dedekind. Posons  $\eta(\tau) = e^{2\pi i \tau / 24} \prod_{n \geq 1} (1 - e^{2\pi i n \tau})$  pour tout  $\tau$  de  $\mathfrak{H}$ . Pour tout réseau  $L$  de  $\mathbb{C}$  et tout complexe  $s$  tel que  $\text{Re}(s) > 1$ , posons  $\phi_L(s) = (\text{vol.}L)^s \sum'_{\lambda \in L} \frac{1}{|\lambda|^{2s}}$ . Si  $L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ , avec  $\omega_1/\omega_2 = \tau = x + iy \in \mathfrak{H}$ , posons  $L_1 = \mathbb{Z}\tau \oplus \mathbb{Z}$ ; le volume de  $L$ , c'est-à-dire l'aire du parallélogramme de sommets  $0, \omega_1, \omega_2, \omega_1 + \omega_2$  dans le plan complexe, est égal à  $|\omega_2|^2 \times \text{vol.}L_1 = |\omega_2|^2 \cdot y$ , donc  $\phi_L(s) = \phi_{L_1}(s) = \sum'_{m, n \in \mathbb{Z}} \frac{y^s}{|n\tau + m|^{2s}}$  (en fait, pour tout  $s$  tel que  $\text{Re}(s) > 1$ , la fonction  $L \mapsto \phi_L(s)$  est une fonction de réseau de poids 0, c'est-à-dire une fonction telle que  $\phi_{\gamma L}(s) = \phi_L(s)$  pour tout  $\gamma \in \Gamma$ , (cf. [38] 7,2). Etudions le comportement de  $\phi_L(s)$  lorsque  $s$  tend vers 1.

PROPOSITION. Première formule limite de Kronecker : soit  $\gamma$  la constante d'Euler ; alors  $\phi_L(s) = \frac{\pi}{s-1} + 2\pi[\gamma - \log 2 - \log(\sqrt{y} |\eta(\tau)|^2)] + O(s-1)$ .

■ En effet,

$$\hat{\phi}_L(s) = \sum'_{n, m \in \mathbb{Z}} \frac{y^s}{|n\tau + m|^{2s}} = 2y^s \sum_{m \geq 1} \frac{1}{m^{2s}} + 2y^s \sum_{n \geq 1} \sum_{m \in \mathbb{Z}} \frac{1}{((nx+m)^2 + n^2 y^2)^s};$$

Or  $\zeta(2s) = \sum_{m \geq 1} \frac{1}{m^{2s}}$ , et la formule sommatoire de Poisson, appliquée à

$$\varphi(t) = \frac{1}{(t^2 + n^2 y^2)^s} \text{ donne : } \sum_{m \in \mathbb{Z}} \varphi(nx+m) = \sum_{m \in \mathbb{Z}} e^{2\pi i m n x} \hat{\varphi}(m), \text{ où}$$

$$\hat{\varphi}(m) = \int_{-\infty}^{+\infty} \frac{e^{-2\pi i m u}}{(u^2 + n^2 y^2)^s} du = (ny)^{1-2s} \int_{-\infty}^{+\infty} \frac{e^{-2\pi i m n y v}}{(v^2 + 1)^s} dv \text{ (pour } v = u/ny \text{)}.$$

Remarquons que  $\hat{\varphi}(-m) = \hat{\varphi}(m)$ , et posons  $\hat{\phi}_L = \hat{\phi}_1 + \hat{\phi}_2 + \hat{\phi}_3$  où

$$\hat{\phi}_1(s) = 2y^s \zeta(2s)$$

$$\hat{\phi}_2(s) = 2y^{1-s} \zeta(2s-1) \int_{-\infty}^{+\infty} \frac{dv}{(v^2 + 1)^s}$$

$$\hat{\phi}_3(s) = 2y^s \sum_{n \geq 1} \sum_{\substack{m \in \mathbb{Z} \\ m \neq 0}} \frac{e^{2\pi i m n x}}{(ny)^{2s-1}} \int_{-\infty}^{+\infty} \frac{e^{2\pi i |m| n y v}}{(v^2 + 1)^s} dv.$$

Etudions chacune de ces 3 fonctions lorsque  $s$  tend vers 1 :

a)  $\hat{\phi}_1$  est continue en  $s = 1$ , et  $\hat{\phi}_1(1) = 2y\zeta(2) = -2\pi\left(\frac{2\pi i \tau}{24} + \frac{2\pi i \bar{\tau}}{24}\right)$ .

b)  $\zeta(2s-1) = \frac{1}{2(s-1)} + \gamma + O(s-1)$ ,

$$y^{1-s} = 1 - (s-1) \log y + O((s-1)^2),$$

$$\int_{-\infty}^{+\infty} \frac{du}{(u^2 + 1)^s} = \left(\int_{-\infty}^{+\infty} \frac{du}{u^2 + 1}\right)(1 - (s-1) \log 4 + O((s-1)^2)).$$

De ces 3 développements limités, le 1er est connu, le 2e est évident et le 3e expliqué ci-dessous :

Soit  $f(s) = \int_{-\infty}^{+\infty} \frac{du}{(u^2 + 1)^s}$ ; nous voulons calculer  $f'(1) = -\int_{-\infty}^{+\infty} \frac{\log(u^2 + 1)}{(u^2 + 1)} du$ .

Utilisons la méthode de Lang [18]. Soit  $g(x) = \int_0^{+\infty} \frac{\log(u^2 x^2 + 1)}{u^2 + 1} du$ : alors

$g(0) = 0$ ,  $g(1) = -\frac{1}{2}f'(1)$ , et  $g'(x) = \frac{\pi}{1+x}$ . D'où :

$$f'(1) = -2 \int_0^1 \frac{\pi}{1+x} dx = -\pi \log 4.$$

Or  $\int_{-\infty}^{+\infty} \frac{du}{u^2+1} = \pi$  .

Ainsi, en multipliant les développements ,

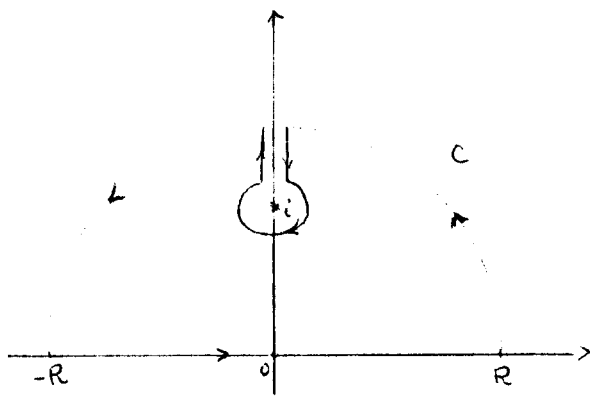
$$\phi_2(s) = \frac{\pi}{s-1} + \pi(2\gamma - \log 4y) + O(s-1) .$$

c) Calculons d'abord  $I_a(s) = \int_{-\infty}^{+\infty} \frac{e^{2\pi i a u}}{(u^2+1)^s} du$  ( $a > 0$ ) par la méthode

des résidus, appliquée au contour  $C$  ci-contre, qui est contenu dans un domaine de  $\mathbb{C}$  où l'on peut définir

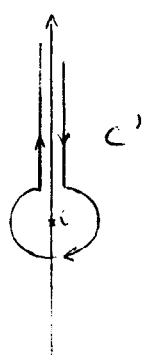
$(u^2+1)^s = e^{s \log(u^2+1)}$  . Nous obtenons

$\oint_C \frac{e^{2\pi i a u}}{(u^2+1)^s} du = 0$  . Si  $s$  est dans un compact du demi-plan  $\text{Re}(s) > 0$  , l'intégrale de  $\frac{e^{2\pi i a u}}{(u^2+1)^s}$  sur les 2 quarts de



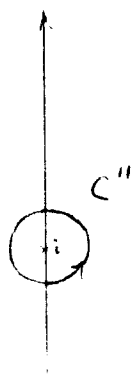
cercle de rayon  $R$  tend uniformément vers 0 lorsque  $R$  tend vers l'infini, et l'intégrale sur le contour  $C'$  est uniformément bornée, donc

$I_a(s)$  est holomorphe sur tout compact de  $\{\text{Re}(s) > 0\}$  et en particulier,  $I_a(1) = \lim_{s \rightarrow 1} I_a(s)$  . Mais alors les intégrales sur les parties verticales de  $C'$  s'annulent, et il reste :



$$\int_{-\infty}^{+\infty} \frac{e^{2\pi i a u}}{u^2+1} du = \oint_{C''} \frac{e^{2\pi i a u}}{u^2+1} du = \pi \cdot e^{-2\pi a}$$

puisque le résidu en  $i$  vaut  $e^{-2\pi a} / 2i$  . D'où



$$\phi_3(1) = \lim_{s \rightarrow 1} \phi_3(s)$$

$$= 2\pi \sum_{n \geq 1} \sum_{\substack{m \in \mathbb{Z} \\ m \neq 0}} \frac{1}{n} e^{2\pi i m n x - 2\pi |m| n y}$$

$$= 2\pi \sum_{m \geq 1} \sum_{n \geq 1} \frac{1}{n} (e^{2\pi i m n \tau} + e^{-2\pi i m n \bar{\tau}}) = -2\pi \log \left( \prod_{m \geq 1} (1 - e^{2\pi i m \tau})(1 - e^{\overline{2\pi i m \tau}}) \right) .$$

d) Regroupons ces résultats :  $\phi_1(1) + \phi_3(1) = -2\pi \log |\eta(\tau)|^2$  , d'où

$$\phi_L(s) = \frac{\pi}{s-1} + 2\pi(\gamma - \log 2 - \log(\sqrt{y} |\eta(\tau)|^2)) + O(s-1) .$$

2.3.4. COROLLAIRE 1 .  $\eta(-1/\tau) = \sqrt{\tau/i} \eta(\tau)$  pour tout  $\tau$  dans  $\mathbb{H}$  .

■ Soient  $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$  ;  $L$  un réseau de base  $\{\omega_1, \omega_2\}$  ;  $\gamma L$  le réseau de base  $\{a\omega_1 + b\omega_2, c\omega_1 + d\omega_2\}$  ;  $\tau = \omega_1/\omega_2$  et

$$\gamma(\tau) = \frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2} = \frac{a\tau + b}{c\tau + d} . \text{ Alors } \operatorname{Im} \gamma(\tau) = \frac{\operatorname{Im} \tau}{|c\tau + d|^2} , \text{ et la propriété :}$$

$\phi_L(s) = \phi_{\gamma L}(s)$  se traduit, grâce à la proposition (2.3.3), par :

$$\sqrt{\operatorname{Im} \tau} |\eta(\tau)|^2 = \sqrt{\operatorname{Im} \gamma(\tau)} |\eta(\gamma(\tau))|^2 , \text{ c'est-à-dire } \left| \frac{\eta(\gamma\tau)}{\sqrt{|c\tau + d|} \eta(\tau)} \right| = 1 .$$

La fonction  $\tau \longmapsto \eta(\gamma\tau)/\sqrt{|c\tau + d|} \eta(\tau)$  est analytique dans  $\mathbb{H}$  , de module 1 . Elle est donc constante ; soit  $\epsilon(\gamma)$  sa valeur. Notons que  $\epsilon(-\gamma) = \epsilon(\gamma)$  et que  $\epsilon$  est multiplicatif, c'est-à-dire  $\epsilon(\gamma\gamma') = \epsilon(\gamma)\epsilon(\gamma')$  . Calculons  $\epsilon(T)$  et  $\epsilon(S)$  :  $\eta(\tau+1) = e^{2\pi i/24} \eta(\tau)$  , donc  $\epsilon(T) = e^{2\pi i/24} \in \mu_{24}$  ; on doit avoir  $\eta(-1/i) = \epsilon(S) \sqrt{i} \eta(i)$  , mais  $-1/i = i$  , et  $\eta(i)$  est non nul, donc  $\epsilon(S) = 1/\sqrt{i}$  . Cela prouve que  $\eta(-1/\tau) = \sqrt{\tau/i} \eta(\tau)$  , et d'autre part, puisque  $S$  et  $T$  engendrent  $\operatorname{PSL}_2(\mathbb{Z})$  , que  $\epsilon(\gamma) \in \mu_{24}$  pour tout  $\gamma$  de  $\operatorname{SL}_2(\mathbb{Z})$  .

2.3.5. COROLLAIRE 2 .  $\Delta(q) = q \prod_{n \geq 1} (1 - q^n)^{24}$  .

■ La fonction  $\eta^{24}$  est une forme modulaire de poids 12 pour  $\Gamma$  , d'après ce qui précède. Comme elle est nulle à l'infini, elle doit être proportionnelle à  $\Delta$  d'après (2.2.3) . Le coefficient de  $q$  étant le même, on a  $\Delta = \eta^{24}$  . ■

2.3.6. Par analogie avec la définition des séries  $E_{2k}(\tau)$  et  $G_{2k}(\tau)$  (pour  $k \geq 2$ ) (cf. 2.1.9), on appelle  $E_2(\tau)$  et  $G_2(\tau)$  les séries divergentes ci-dessous :

$$\begin{cases} E_2(\tau) = 1 + (-1)^k \sum_{n \geq 1} \sigma_1(n) q^n ; \\ G_2(\tau) = \sum_{(m,n) \in \mathbb{Z}^2} \frac{1}{(m\tau + n)^2} . \end{cases}$$

On a alors les résultats suivants :

*COROLLAIRE 3* .  $E_2\left(\frac{a\tau+b}{c\tau+d}\right) \cdot (c\tau+d)^{-2} = E_2(\tau) + \frac{12}{2\pi i} \frac{c}{c\tau+d}$  si  
 $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$  .

■ Nous avons :  $\frac{24}{2\pi i} \frac{d(\log \eta(\tau))}{d\tau} = 1 - 24 \sum_{n \geq 1} \frac{nq^n}{1-q^n} = 1 - 24 \sum_{n \geq 1} \sigma_1(n)q^n = E_2(\tau)$

et de même  $E_2(\gamma\tau) = \frac{24}{2\pi i} \cdot \frac{d(\log \eta(\gamma\tau))}{d\tau} \cdot (c\tau+d)^2$  . Mais nous venons de voir que  $\eta(\gamma\tau) = \epsilon(\gamma)\sqrt{c\tau+d} \cdot \eta(\tau)$  , d'où

$$\frac{d(\log \eta(\gamma\tau))}{d\tau} = \frac{c}{2(c\tau+d)} + \frac{d(\log \eta(\tau))}{d\tau} \quad \blacksquare$$

Ainsi,  $E_2$  "ressemble" à une forme modulaire de poids 2 , et en particulier :  $E_2(-1/\tau) \cdot \tau^{-2} = E_2(\tau) + 12/2\pi i \tau$  .

*COROLLAIRE 4* .  $1/3(4E_2(2\tau) - E_2(\tau/2))$  est une série convergente, de somme  $\theta^4(\tau)$  .

■ Soient  $H = \theta^4$  ,  $G(\tau) = 1/3(4E_2(2\tau) - E_2(\tau/2))$  , et  $f = H - G$  .

Montrons que la série  $G(\tau)$  est convergente sur  $\mathbb{H}$  : par définition,  $E_2(\tau)$  est proportionnel à  $\sum'_{\lambda \in \mathbb{Z}\tau \oplus \mathbb{Z}} 1/\lambda^2 = \sum'_{(n,m) \in \mathbb{Z}^2} 1/(n\tau+m)^2$  (cf. 2.1.9) ; donc  $G(\tau)$  est proportionnel à

$$\frac{1}{(\tau/2)^2} + \frac{1}{\tau^2} + \frac{1}{(3\tau/2)^2} + \sum'_{(n,m) \in \mathbb{Z}^2} a_{n,m} \frac{1}{(4n\tau/2 + m)^2} ,$$

où

$$a_{n,m} = 3 - \frac{1}{\left(1 + \frac{\tau/2}{4n\tau/2 + m}\right)^2} - \frac{1}{\left(1 + \frac{2\tau/2}{4n\tau/2 + m}\right)^2} - \frac{1}{\left(1 + \frac{3\tau/2}{4n\tau/2 + m}\right)^2} ;$$

ainsi,  $|a_{n,m}|$  est équivalent à  $\frac{12}{|4n\tau/2 + m|}$  lorsque  $|4n\tau/2 + m|$  tend vers l'infini. Or, nous savons que la série  $\sum'_{\lambda \in \mathbb{Z}2\tau \oplus \mathbb{Z}} 1/|\lambda|^\alpha$  converge pour tout réel  $\alpha > 2$  (cf. [18], 1,2) ; donc  $\sum'_{(n,m) \in \mathbb{Z}^2} 1/|2n\tau + m|^3$

converge, et  $G(\tau)$  est convergente sur  $\mathbb{H}$  .

La fonction  $f$  s'annule à l'infini, car les développements :

$$H(q) = \left(\sum q^{n^2/2}\right)^4 \quad (2.3.2)$$

et

$$G(q) = \frac{1}{3} (4-1-4.24 \sum_{n \geq 1} \sigma_1(n)q^{2n} + 24 \sum_{n \geq 1} \sigma_1(n)q^{n/2}) \quad (2.1.6)$$

commencent tous les deux par 1 ;  $f|_2 S = -f$  et  $f|_2 T^2 = f$  car on a vu les formules analogues pour  $H$  (2.3.2) et pour  $G$  (appliquer le corollaire 3 ci-dessus en remplaçant  $\tau$  par  $\tau/2$  puis par  $2\tau$ ). Donc  $f^2$  est une forme parabolique de poids 4 sur  $\widehat{\Gamma_\theta} \backslash \mathbb{H}$  (où  $\Gamma_\theta$  est le sous-groupe de  $\Gamma$  engendré par  $S$  et  $T^2$ , cf. 2.3.2) avec un zéro d'ordre au moins égal à 2 à l'infini, et  $f^6/\Delta$  est une fonction sur  $\widehat{\Gamma_\theta} \backslash \mathbb{H}$ . Si elle n'est pas nulle, le degré de son diviseur des zéros doit être égal au degré de son diviseur des pôles ;  $f$  et  $\Delta$  étant holomorphes, cela signifie :  $3 \times \deg(f^2) = \deg(\Delta)$ . Considéré comme forme modulaire sur  $\widehat{\Gamma} \backslash \mathbb{H}$ ,  $\Delta$  a un seul zéro, à l'infini, et c'est un zéro simple. Comme l'infini est ramifié dans le revêtement  $\widehat{\Gamma_\theta} \backslash \mathbb{H} \rightarrow \widehat{\Gamma} \backslash \mathbb{H}$ , l'infini est le seul zéro de  $\Delta$  dans  $\widehat{\Gamma_\theta} \backslash \mathbb{H}$ , et c'est un zéro double (cf. 2.3.2). Ainsi, le degré du diviseur de  $\Delta$  dans  $\widehat{\Gamma_\theta} \backslash \mathbb{H}$  est égal à 2.

En particulier, il n'est pas divisible par 3 ; donc  $f$  est identiquement nulle. ■

APPLICATION : Le nombre de manières d'écrire un entier positif  $n$  comme somme de au plus 4 carrés d'entiers de signe quelconque est égal à

$$8 \sum_{\substack{d|n \\ 4 \nmid d}} d .$$

■ Par définition,  $\theta(\tau) = \sum_{n \in \mathbb{Z}} q^{n^2/2}$  si  $q = e^{2\pi 2\tau}$  (2.3.2)

donc  $\theta^4(\tau) = \sum_{n \geq 0} a_n q^{n/2}$  si  $a_n$  est le nombre de manières d'écrire  $n$  comme somme de 4 carrés d'éléments de  $\mathbb{Z}$ . Or

$$E_2(\tau) = 1 - 24 \sum_{n \geq 1} \sigma_1(n)q^n$$

donc

$$G(\tau) = 1 - 8 \sum_{n \geq 1} (4\sigma_1(n/4) - \sigma_1(n))q^{n/2} ,$$

en posant  $\sigma_1(x) = 0$  si  $x \notin \mathbb{N}$ . D'après le corollaire 4, nous avons  $G = \theta^4$  donc  $a_n = 8 (\sigma_1(n) - 4\sigma_1(n/4))$ . Or  $\sigma_1(n) = \sum_{d|n} d$  ; et  $d'$



divise  $n/4$  si et seulement si  $d'$  est de la forme  $d/4$  où  $d$  divise  $n$  et  $4$  divise  $d$ , donc  $\sigma_1(n/4) = 1/4 \sum_{\substack{d|n \\ 4|d}} d$ ; et enfin

$$\sigma_1(n) - 4\sigma_1(n/4) = \sum_{\substack{d|n \\ 4 \nmid d}} d \quad . \quad \blacksquare$$

2.4. THEOREME D'ABEL JACOBI (cf.[18] par exemple).

2.4.1. Condition d'Abel.

*THEOREME* . Soit  $L$  un réseau de  $\mathbb{C}$ , et  $D = \sum_{P \in \mathbb{C}/L} n_P \cdot (P)$  un diviseur donné sur  $\mathbb{C}/L$ . Il existe une fonction  $L$ -elliptique de diviseur  $D$  si et seulement si  $\deg(D) = 0$  et  $\sum n_P P \in L$ , et alors cette fonction est unique à une constante multiplicative non nulle près.

■ La condition est nécessaire : appliquons le théorème des résidus aux fonctions méromorphes  $\frac{f'(z)}{f(z)}$  et  $z \frac{f'(z)}{f(z)}$  sur le bord  $\partial R$  d'un domaine fondamental  $R$  pour  $L$  (cf. 2.1.2) choisi de sorte que  $\partial R$  ne passe par aucun point singulier de ces deux fonctions. Puisque le diviseur de  $f$  est

$D = \sum_{P \in \mathbb{C}/L} n_P \cdot (P)$ , les points singuliers de  $f$  sont les représentants de ces points  $P$  contenus dans  $R$ , avec l'ordre  $n_P$ . D'où :

$$\int_{\partial R} \frac{f'(z)}{f(z)} dz = 2\pi i \sum_P n_P$$

et

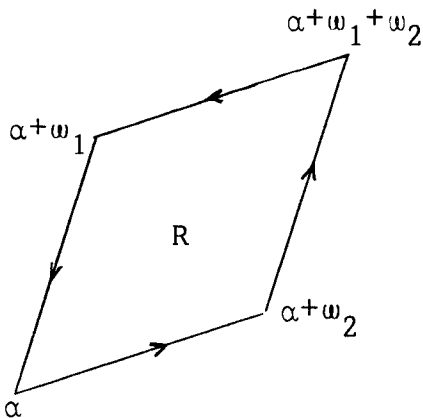
$$\int_{\partial R} z \frac{f'(z)}{f(z)} dz = 2\pi i \sum_P n_P \cdot P .$$

D'autre part,  $\frac{f'(z)}{f(z)}$  est  $L$ -elliptique, donc

$$\int_{\partial R} \frac{f'(z)}{f(z)} dz = 0 \quad (\text{c'est le lemme 2.1.2}), \text{ et}$$

$$\int_{\partial R} z \frac{f'(z)}{f(z)} dz = -\omega_2 \int_{\alpha}^{\alpha+\omega_1} \frac{f'(t)}{f(t)} dt + \omega_1 \int_{\alpha}^{\alpha+\omega_2} \frac{f'(t)}{f(t)} dt$$

$$= 2\pi i (k_1 \omega_1 + k_2 \omega_2) \quad \text{avec } k_1, k_2 \in \mathbb{Z} .$$



Réciproquement, pour tout  $\tau \in \mathfrak{H}$ , définissons une fonction thêta méromorphe sur  $\mathbb{C}$  par :

$$\theta(u) = \theta(z) = \prod_{n \geq 0} (1 - q^n z) \prod_{n \geq 1} (1 - q^n z^{-1}),$$

où  $q = e^{2\pi i \tau}$ ,  $z = e^{2\pi i u}$ . Le produit infini est convergent car  $|q| < 1$  lorsque  $\tau \in \mathfrak{H}$ . Cette fonction vérifie les propriétés suivantes, dont la vérification est immédiate :  $\theta(u+1) = \theta(u)$  et  $\theta(u+\tau) = -e^{-2\pi i u} \theta(u)$ , c'est-à-dire  $\theta(e^{2\pi i} z) = \theta(z)$  et  $\theta(qz) = -z^{-1} \theta(z)$ ;  $\theta$  est holomorphe sur  $\mathbb{C}$ , ses zéros sont simples et leur ensemble est le réseau  $L = \mathbb{Z}\tau \oplus \mathbb{Z}$ .

Soient  $R$  un parallélogramme fondamental pour  $L$ , et  $D = \sum_{P \in R} n_P(P)$  un diviseur sur  $\mathbb{C}/L$ . Posons  $\theta_D(u) = \prod_{P \in R} (\theta(u-P))^{n_P}$  c'est-à-dire

$$\theta_D(z) = \prod_{P \in R} (\theta(z/a_P))^{n_P} \quad \text{où } a_P = e^{2\pi i P}.$$

La fonction  $\theta_D$  vérifie les propriétés suivantes : elle est méromorphe sur  $\mathbb{C}$ ,  $\theta_D(u+1) = \theta_D(u)$  et

$$\theta_D(u+\tau) = (-z^{-1})^{\deg(D)} \cdot e^{2\pi i (\sum_{P \in R} n_P \cdot P)} \theta_D(u),$$

comme on le vérifie aisément.

Si, de plus,  $\deg(D) = 0$  et  $\sum_{P \in R} n_P \cdot P = s\tau + r$  ( $r, s \in \mathbb{Z}$ ), nous obtenons :

$$\theta_D(u+\tau) = q^s \theta_D(u).$$

Ainsi, la fonction :  $u \mapsto e^{-2\pi i s u} \theta_D(u)$  est  $L$ -elliptique de diviseur  $D$ .

Enfin, deux fonctions méromorphes sur  $\mathbb{C}$  de même diviseur sont proportionnelles, d'après le théorème de Liouville appliqué à leur quotient. ■

2.4.2. COROLLAIRE. Soit  $\mathcal{D}(E)$  (resp.  $\mathcal{D}_0(E)$ , resp.  $\mathcal{D}_\ell(E)$ ) le groupe des diviseurs (resp. des diviseurs de degré 0, resp. des diviseurs de fonctions) sur  $E = \mathbb{C}/L$ . L'application qui fait correspondre au diviseur  $\sum_{P \in \mathbb{C}/L} n_P(P) \in \mathcal{D}(E)$  le point  $\sum n_P P \in E$  induit un isomorphisme de groupes de  $\mathcal{D}_0(E)/\mathcal{D}_\ell(E)$  sur  $E$ .

■ Le théorème montre que  $\mathcal{D}_\ell(E)$  est un sous-groupe  $\mathcal{D}_0(E)$  et est le noyau de l'application de  $\mathcal{D}(E)$  dans  $E$  définie ci-dessus ; d'autre part, cette application est un homomorphisme de groupes ; et enfin, tout point  $P$  de  $\mathbb{C}$  est l'image du diviseur  $(P) - (0) \in \mathcal{D}_0(E)$ . ■

2.5. EQUATION DE TATE.

2.5.1. Le calcul des coefficients de Fourier des fonctions L-elliptiques  $\wp$  et  $\wp'$  donne le résultat suivant (cf [18] ,4,2 et 15,1) où  $q = e^{2\pi i\tau}$  ,  $z = e^{2\pi iu/\omega_2}$  :

$$\wp(u;L) = \left(\frac{2\pi i}{\omega_2}\right)^2 \left(\frac{1}{12} + \sum_{n \in \mathbb{Z}} \frac{q^n z}{(1-q^n z)^2} - 2 \sum_{n \geq 1} \frac{nq^n}{1-q^n}\right)$$

$$\wp'(u;L) = \left(\frac{2\pi i}{\omega_2}\right)^3 \sum_{n \in \mathbb{Z}} \frac{q^n z(1+q^n z)}{(1-q^n z)^3} .$$

Posons  $X(u) = (\omega_2/2\pi i)^2 \wp(u;L) - 1/12$  et  $Y(u) = 1/2[(\omega_2/2\pi i)^3 \wp'(u;L) + X(u)]$  c'est-à-dire :

$$X(u) = \sum_{n \in \mathbb{Z}} \frac{q^n z}{(1-q^n z)^2} - 2 \sum_{n \geq 1} \frac{nq^n}{1-q^n} ,$$

et

$$Y(u) = \sum_{n \in \mathbb{Z}} \frac{q^n z}{(1-q^n z)^3} - \sum_{n \geq 1} \frac{nq^n}{1-q^n}$$

(la formule (1γ) de [18] ,15,1 contient une erreur).

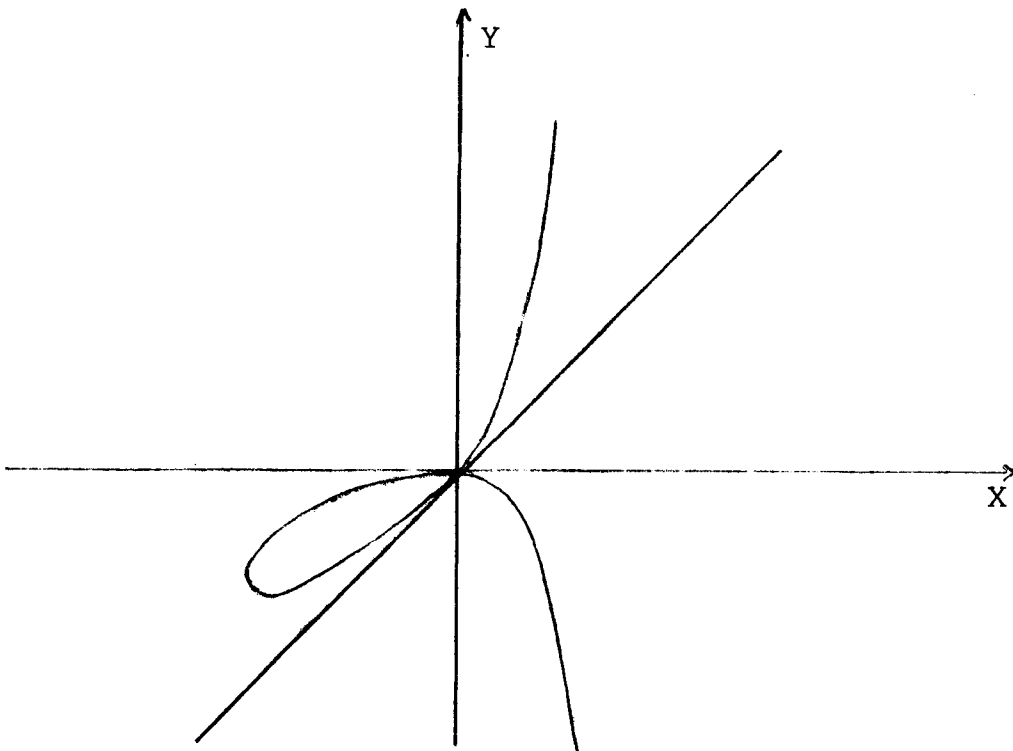
Alors l'équation de Weierstrass qui liait  $\wp$  et  $\wp'$  se transforme en l'équation de Tate :  $Y^2 - XY = X^3 - h_2 X - h_3$  , où  $h_2 = 5 \sum_{n \geq 1} n^3 \frac{q^n}{1-q^n}$  et  $h_3 = \sum_{n \geq 1} \frac{5n^3 + 7n^5}{12} \frac{q^n}{1-q^n}$  .

Les coefficients  $5n^3$  et  $\frac{5n^3 + 7n^5}{12}$  sont entiers (cf. 2.1.9) et  $|q| < 1$  , donc les séries définissant  $h_2$  et  $h_3$  convergent. De plus, les coefficients sont définis en toute caractéristique, et nous utiliserons au paragraphe 3 cette équation pour définir les courbes de Tate sur des corps locaux.

2.5.2. Soient  $\tau \in \mathbb{H}$  ,  $L = 2\pi i(\tau\mathbb{Z} \oplus \mathbb{Z})$  , et  $q = e^{2\pi i\tau}$  . Alors l'application  $u \longmapsto q^u$  de  $\mathbb{C}$  dans  $\mathbb{C}^*$  induit un isomorphisme de  $\mathbb{C}/L$  sur  $\mathbb{C}^*/q^{\mathbb{Z}}$  , dans lequel les fonctions L-elliptiques sont transformée en les fonctions méromorphes sur  $\mathbb{C}^*/q^{\mathbb{Z}}$  , i.e. méromorphes sur  $\mathbb{C}^*$  de période multiplicative  $q$  :  $f(qz) = f(z)$  pour tout  $z$  dans  $\mathbb{C}^*$  .

En résumé, le groupe  $\mathbb{C}^*/q^{\mathbb{Z}}$  peut être muni d'une structure de courbe elliptique  $E$  sur  $\mathbb{C}$ , de corps de fonctions  $\mathbb{C}(E)$  égal au corps des fonctions méromorphes sur  $\mathbb{C}^*/q^{\mathbb{Z}}$ . Et toute courbe elliptique sur  $\mathbb{C}$  est  $\mathbb{C}$ -isomorphe à une courbe de cette forme (pour  $q = e^{2\pi i \omega_1/\omega_2}$ ).

2.5.3. Nous avons vu (cf.1.2.1) que l'invariant  $j$  définit une bijection entre les classes de  $\mathbb{C}$ -isomorphisme de courbes elliptiques sur  $\mathbb{C}$  et l'espace affine  $A^1(\mathbb{C})$ . Nous pouvons plonger  $A^1(\mathbb{C})$  dans  $\mathbb{P}^1(\mathbb{C})$  et étudier ce qui se passe lorsque  $j$  tend vers l'infini grâce à ce qui précède : dans chaque classe de  $\mathbb{C}$ -isomorphisme, choisissons pour représentant une courbe  $\mathbb{C}^*/q^{\mathbb{Z}}$ , d'équation  $Y^2 - XY = X^3 - h_2X - h_3$ . Lorsque  $q$  tend vers 0,  $h_2$  et  $h_3$  tendent vers 0, et l'équation devient :  $Y^2 - XY = X^3$ . C'est l'équation d'une cubique dégénérée à l'origine, avec deux tangentes distinctes, de pentes 0 et 1.



### 3. COURBES ELLIPTIQUES SUR UN CORPS LOCAL (cf.[32])

#### 3.1. DEFINITIONS.

3.1.1. Fonctions holomorphes et méromorphes. Soit  $K$  un corps muni d'une valuation discrète  $v$  ; la valeur absolue définie par  $|x| = e^{-v(x)}$  est une valeur absolue non archimédienne sur  $K$  . Si  $K$  est complet pour cette valeurs absolue, nous appellerons  $K$  un corps local. La valeur absolue de  $K$  se prolonge de manière unique à  $\bar{K}$  , mais en général  $\bar{K}$  n'est pas complet.

Par analogie avec le cas complexe, posons les définitions suivantes :

Une fonction K-holomorphe sur  $\bar{K}^*$  est une fonction  $f$  de  $\bar{K}^*$  dans  $\bar{K}$  définie par  $f(z) = \sum_{n \gg -\infty} a_n z^n$  , où la série de Laurent  $\sum_{n \gg -\infty} a_n X^n$  est à coefficients dans  $K$  et converge en tout point  $z$  de  $\bar{K}^*$  . L'ensemble des fonctions K-holomorphes sur  $\bar{K}^*$  forme un anneau intègre. Les éléments du corps des fractions sont les fonctions K-méromorphes sur  $\bar{K}^*$  . Nous appellerons désormais ces fonctions des fonctions holomorphes ou méromorphes (sans référence à  $K$  ).

3.1.2. Diviseurs. Nous appelons diviseur (défini sur  $K$ ) tout ensemble d'entiers de la forme  $\{n_a, a \in \bar{K}^*\}$  , vérifiant les deux conditions suivantes :

- (i) Si  $r$  et  $r'$  sont deux réels tels que  $0 < r < r'$  , le nombre d'éléments  $a$  de  $\bar{K}^*$  , tels que  $r \leq |a| \leq r'$  et  $n_a \neq 0$  , est fini ;
- (ii) Si  $a$  et  $b$  sont conjugués sur  $K$  , alors  $n_a = n_b$  .

D'autre part, si  $f$  est une fonction holomorphe, non nulle, et si  $a$  est un élément de  $\bar{K}^*$  de polynôme minimal  $\varphi_a(X)$  sur  $K$  , nous avons le lemme suivant :

LEMME . La fonction  $f$  s'écrit de manière unique sous la forme :  
 $f(X) = \varphi_a(X)^m g(X)$  , où  $m \in \mathbb{Z}$  et où  $g$  est une fonction holomorphe, non nulle en  $a$  .

■ La démonstration de ce lemme repose sur le lemme de Hensel. ■

L'entier  $m$  est appelé l'ordre de  $f$  en  $a$  et noté  $w_a(f)$ . L'application  $w_a$  ainsi définie se prolonge de façon unique en une valuation sur le corps des fonctions méromorphes.

L'ensemble  $\{w_a(f), a \in \bar{K}^*\}$ , pour toute fonction méromorphe  $f$  non nulle, est un diviseur. Nous l'appelons le diviseur de  $f$  et le notons  $(f)$ .

### 3.1.3. Fonctions de même diviseur.

LEMME. Deux fonctions méromorphes  $f$  et  $g$  ont même diviseur si et seulement si il existe un entier  $d$  et un élément  $\alpha$  de  $K^*$  tels que  $g(X) = \alpha X^d f(X)$ .

■ Dire que  $f$  et  $g$  ont le même diviseur équivaut à dire que leur quotient n'a ni zéro ni pôle dans  $\bar{K}^*$ . Or les fonctions méromorphes vérifiant cette condition sont les fonction définies par une série de la forme  $\alpha X^d$ , car la valeur absolue de  $K$  est non-archimédienne (c'est faux sur  $\mathbb{C}$  : par exemple la fonction définie par  $e^{\alpha X^2 + \beta X + \gamma}$  a un diviseur nul) : cette propriété est démontrée dans [13]. ■

3.1.4. Diviseurs  $q$ -périodiques. Soit  $q \in K$ ,  $0 < |q| < 1$  ; un diviseur  $\{n_a, a \in \bar{K}^*\}$  est dit  $q$ -périodique si  $n_a = n_b$  dès que  $a$  et  $b$  sont congrus modulo  $q^{\mathbb{Z}}$ .

Soit  $f$  une fonction méromorphe ; supposons que le diviseur  $D$  de  $f$  est  $q$ -périodique. Alors la fonction  $f(q^{-1}X)$  a le même diviseur, et d'après le lemme (3.1.3), il existe un entier  $d$  et un élément  $\alpha$  de  $K^*$  tels que  $f(q^{-1}X) = \alpha^{-1}(-X)^d f(X)$ . En fait, l'entier  $d$  et la classe de  $\alpha$  modulo  $q^{\mathbb{Z}}$  ne dépendent que du diviseur  $D$  de  $f$  ; on appelle  $d$  le degré de  $D$ , on le note  $\deg(D)$  ; on note  $\mathfrak{J}(D)$  la classe de  $\alpha$  dans  $K^*/q^{\mathbb{Z}}$  et on l'appelle l'image de Jacobi de  $D$ .

3.1.5. Fonctions q-périodiques. Une fonction méromorphe  $f$  telle que  $f(q^{-1}X) = f(X)$  est dite q-périodique. Son diviseur  $(f)$  est alors q-périodique.

*PROPOSITION .* Si un diviseur q-périodique  $D$  est un diviseur de fonction, alors c'est le diviseur d'une fonction q-périodique si et seulement si  $\deg(D) = 0$  et  $\phi(D) = 1$ . Cette fonction est unique à un facteur dans  $K^*$  près.

■ Par hypothèse,  $D = (f)$ , et  $f(q^{-1}X) = \alpha^{-1}(-X)^d f(X)$  d'après (3.1.4). Si  $f$  est q-périodique,  $\alpha = 1$  et  $d = 0$ , d'où :  $\deg(D) = 0$  et  $\phi(D) = 1$ . Réciproquement si  $\deg(D) = 0$  et  $\phi(D) = 1$ , cela signifie :  $d = 0$  et  $\alpha = q^s$  pour un entier  $s$ . Mais alors la fonction  $g$  définie par  $g(X) = X^s f(X)$  est q-périodique de diviseur  $D$ .

Enfin, si  $f$  et  $g$  sont 2 fonctions q-périodiques de diviseur  $D$ , d'après le lemme (3.1.3) on a  $g(X) = \alpha' X^{d'} f(X)$ , et la q-périodicité impose  $d' = 0$ . ■

### 3.2. THEOREME D'ABEL-JACOBI.

3.2.1. *THEOREME .* Un diviseur q-périodique est le diviseur d'une fonction q-périodique si et seulement si son degré est nul et son image de Jacobi égale à 1. Dans ce cas, la fonction correspondante est unique à un facteur dans  $K^*$  près.

■ Vu la proposition (3.1.5), il suffit de montrer que tout diviseur q-périodique est un diviseur de fonction. Pour cela, nous allons considérer la fonction thêta, définie formellement en (2.4.1), comme une fonction de  $\bar{K}^*$  à valeurs dans  $\bar{K}$  :  $\theta(z) = \prod_{n \geq 0} (1 - q^n z) \prod_{n \geq 1} (1 - q^n z^{-1})$ . Le produit infini converge car  $|q| < 1$ ,  $\theta$  est holomorphe sur  $\bar{K}^*$ , ses zéros sont simples, leur ensemble est  $q^{\mathbb{Z}}$ , et enfin  $\theta(q^{-1}z) = -z \theta(z)$ . Soit  $D = \{n_a, a \in \bar{K}^*\}$ , un diviseur q-périodique, et posons

$$\Theta_D(z) = \prod_{|q| < |a| \leq 1} (\Theta(a^{-1}z))^{n_a e_a}$$

où  $e_a$  est le degré d'inséparabilité de  $K(a)/K$ . Alors la fonction  $\Theta_D$  est méromorphe et de diviseur  $D$ , d'où le théorème. ■

### 3.2.2. Expression du degré et de l'image de Jacobi.

*PROPOSITION.* Si  $D$  est un diviseur  $q$ -périodique,  $D = \{n_a, a \in \overline{K^*}\}$ , alors :  $\deg(D) = \sum_{|q| < |a| \leq 1} [K(a):K] \cdot n_a$  et  $\phi(D) \equiv \prod_{|q| < |a| \leq 1} N_{K(a)/K}(a)^{n_a} \pmod{q^{\mathbb{Z}}}$ .

L'accent indique que  $a$  parcourt un système de représentants de classes de  $K$ -conjugaison. En remarquant que deux éléments  $K$ -conjugés ont même valeur absolue, on voit que ces formules s'écrivent aussi ;

$$\deg(D) = \sum_{|q| < |a| \leq 1} e_a n_a \quad \text{et} \quad \phi(D) \equiv \prod_{|q| < |a| \leq 1} a^{e_a n_a} \pmod{q^{\mathbb{Z}}}.$$

■ Pour les démontrer, utilisons à nouveau la fonction  $\Theta_D$  définie en (3.2.1) :  $\Theta_D$  a pour diviseur  $D$ , donc  $\Theta_D(q^{-1}z) = \alpha^{-1}(-z)^d \Theta_D(z)$  avec  $d = \deg(D)$  et  $\alpha \equiv \phi(D) \pmod{q^{\mathbb{Z}}}$ . Mais d'autre part, la formule  $\Theta(q^{-1}z) = -z \Theta(z)$  implique :

$$\Theta_D(q^{-1}z) = \prod_{|q| < |a| \leq 1} a^{-e_a n_a} (-z)^{\sum_{|q| < |a| \leq 1} e_a n_a} \Theta_D(z),$$

d'où la proposition. ■

3.2.3. Notons  $\mathcal{D}(K^*/q^{\mathbb{Z}})$  (resp.  $\mathcal{D}_0(K^*/q^{\mathbb{Z}})$ ,  $\mathcal{D}_\ell(K^*/q^{\mathbb{Z}})$ ) le groupe des diviseurs  $q$ -périodiques définis sur  $K$  (resp. le sous-groupe des diviseurs de degré 0, des diviseurs de fonctions). Nous avons alors l'analogie du corollaire (2.4.2) :

*COROLLAIRE.* L'application qui fait correspondre au diviseur  $q$ -périodique  $\{n_a, a \in \overline{K^*}\}$  le point  $\prod_{|q| < |a| \leq 1} a^{n_a}$  induit un isomorphisme de groupes de  $\mathcal{D}_0(K^*/q^{\mathbb{Z}})/\mathcal{D}_\ell(K^*/q^{\mathbb{Z}})$  sur  $K^*/q^{\mathbb{Z}}$ .



### 3.3. COURBES DE TATE.

3.3.1. *THEOREME*. Soit  $q \in K^*$  tel que  $|q| < 1$ . Il existe une courbe elliptique  $E(q)$  sur  $K$  d'équation  $Y^2 - XY = X^3 - h_2X - h_3$ , où

$$h_2 = 5 \sum_{n \geq 1} n^3 \frac{q^n}{1-q^n} \quad \text{et} \quad h_3 = \sum_{n \geq 1} \frac{5n^3 + 7n^5}{12} \cdot \frac{q^n}{1-q^n}.$$

L'invariant de  $E(q)$  est  $j(q) = \frac{1}{q} + 744 + \sum c(n)q^n$  où  $c(n) \in \mathbb{Z}$ . Réciproquement, si  $j \in K^*$  est tel que  $|j| > 1$ , il existe une courbe  $E(q)$  d'invariant  $j$ , unique à  $\bar{K}$ -isomorphisme près;  $E(q)$  est isomorphe à  $K^*/q^{\mathbb{Z}}$  et a pour discriminant  $\Delta(q) = \sum_{n \geq 1} \tau(n)q^n = q \prod_{n \geq 1} (1-q^n)^{24}$ , où la fonction  $\tau$  est la fonction de Ramanujan définie en (2.1.9).

La dernière assertion signifie que les groupes  $E(q)$  et  $K^*/q^{\mathbb{Z}}$  sont isomorphes, et que le corps des fonctions de  $E(q)$  sur  $K$  est isomorphe au corps des fonctions  $K$ -méromorphes  $q$ -périodiques.

Ce théorème est analogue aux théorèmes (2.1.1 et 2.2.6) sur  $\mathbb{C}$ ; ne pouvant pas définir la notion de réseau de  $K$ , on utilise la remarque (2.5.2) :  $\mathbb{C}/L \simeq \mathbb{C}^*/q^{\mathbb{Z}}$  si  $L = \omega_2(\mathbb{Z}\tau \oplus \mathbb{Z})$  et  $q = e^{2\pi i\tau}$ . La principale différence entre ces 2 cas est qu'on obtient toutes les classes de courbes elliptiques sur  $\mathbb{C}$ , alors que sur  $K$  on n'obtient que les classes de courbes telles que  $|j| > 1$ .

Remarquons que les coefficients  $5n^3$  et  $\frac{5n^3 + 7n^5}{12}$  qui interviennent dans la définition de  $h_2$  et  $h_3$  sont entiers (2.5.1), donc définis en caractéristique quelconque et de valeur absolue  $\leq 1$ ; ainsi les séries définissant  $h_2$  et  $h_3$  convergent dans  $K$  pour  $|q| < 1$ .

■ Pour montrer que l'équation de Tate définit une courbe elliptique sur  $K$ , il suffit de vérifier que la cubique d'équation  $Y^2 - XY = X^3 - h_2X - h_3$  a un discriminant non nul. Or les formules (2) de (1.1.2) donnent ici

$$\Delta(q) = h_3 + h_2^2 + 72h_2h_3 - 432h_3^2 + 64h_2^3, \quad \text{et nous retrouvons ainsi}$$

$$\Delta(q) = \sum_{n \geq 1} \tau(n)q^n \quad \text{et} \quad j(q) = \frac{(1+48h_2)^3}{\Delta(q)} = \frac{1}{q} + 744 + \sum_{n \geq 1} c(n)q^n, \quad \text{où} \quad \tau(n)$$

et  $c(n)$  sont entiers,  $\tau(1) = 1$  (cf.2.1.9) . La formule

$$\sum_{n \geq 1} \tau(n)q^n = q \prod_{n \geq 1} (1-q^n)^{24}$$

démontrée sur  $\mathbb{C}$  en (2.3) ne fait intervenir que des coefficients entiers, elle est donc valable formellement (i.e. en remplaçant  $q$  par un indéterminée  $X$ ) en caractéristique quelconque. En particulier sur  $K$ , si  $|q| < 1$  les deux membres convergent et on a encore  $\Delta(q) = q \cdot \prod_{n \geq 1} (1-q^n)^{24}$ . Ainsi,  $|\Delta| = |q| < 1$ , donc  $\Delta \neq 0$  et  $E(q)$  est bien une courbe elliptique sur  $K$ ; et  $|j(q)| = \frac{1}{|q|} > 1$ .

Réciproquement, soit  $j \in K^*$ ,  $|j| > 1$ . La série formelle

$$\frac{1}{j} = \frac{q}{1 + 744q + \sum_{n \geq 1} c(n)q^{n+1}} = q - 744q^2 + \dots$$

est à coefficients entiers. La série formelle réciproque est donc aussi à coefficients entiers (cf.[3] prop.7.1 et formule 7.5). Donc elle est convergente dans le domaine  $|\frac{1}{j}| < 1$  et les fonctions :  $q \mapsto \frac{1}{j(q)}$ , et  $q \mapsto j(q)$ , admettent des fonctions réciproques dans le domaine  $|j| > 1$ . Enfin, l'application de  $K^*$  dans  $\mathbb{P}^2(K)$  définie par :  $\omega \mapsto (\omega^3 X(\omega), \omega^3 Y(\omega), \omega^3)$  où

$$X(\omega) = \sum_{n \in \mathbb{Z}} \frac{q^n \omega}{(1-q^n \omega)^2} - 2 \sum_{n \geq 1} \frac{nq^n}{1-q^n}$$

$$Y(\omega) = \sum_{n \in \mathbb{Z}} \frac{(q^n \omega)}{(1-q^n \omega)^3} - \sum_{n \geq 1} \frac{nq^n}{1-q^n} \quad (\text{cf. (2.5.1) et [18], 15.1})$$

induit un isomorphisme de  $K^*/q^{\mathbb{Z}}$  sur  $E(q)$ . ■

**3.3.2. COROLLAIRE.** L'ensemble des classes de  $\bar{K}$ -isomorphisme de courbes elliptiques sur  $K$  d'invariant  $j$  tel que  $|j| > 1$  est en bijection avec l'ensemble des éléments  $q$  de  $K^*$  tels que  $|q| < 1$ .

■ C'est le théorème (3.3.1) joint au théorème (1.2.1). ■

**3.3.3. Réduction de la courbe de Tate.** L'équation de  $E(q)$  étant à coefficients entiers sur  $K$ , on peut considérer l'équation obtenue en ré-

duisant les coefficients modulo l'idéal maximal  $\mathfrak{p} = \{z \in K / |z| < 1\}$  de  $K$ . Comme  $q \in \mathfrak{p}$ , cela revient à remplacer  $q$  par  $0$ . Ainsi, quelle que soit la caractéristique de  $K$ , la courbe obtenue est la cubique dégénérée d'équation  $Y^2 - XY = X^3$  (cf. 2.5.3).

Les calculs de (2.5.3) sont valables et montrent que la cubique a un point double en  $(0,0)$  à tangentes distinctes rationnelles sur  $K$ . On dit que  $E(q)$  est à réduction multiplicative (mod.  $\mathfrak{p}$ ) (cf. III, 1).

#### 4. POINTS D'ORDRE FINI ET ISOGENIES

##### 4.1. POINTS D'ORDRE FINI.

Soient  $K$  un corps de caractéristique  $p$ ,  $E$  une courbe elliptique sur  $K$ ,  $N$  un entier strictement positif,  $E_N = \{P \in E(\bar{K}) / N.P = 0\}$  le groupe des points de  $E$  définis sur  $K$  dont l'ordre divise  $N$ .

4.1. PROPOSITION. Si  $p = 0$  ou si  $p$  ne divise pas  $N$ , alors  $E_N \simeq (\mathbb{Z}/N\mathbb{Z})^2$ . Si  $p | N$ , il existe une injection de  $E_N$  dans  $(\mathbb{Z}/N\mathbb{Z})^2$ .

Nous démontrons cette proposition lorsque  $p = 0$ . Pour  $p > 0$ , nous donnons une idée de la démonstration en (4.3.2), et renvoyons le lecteur à ([31], 3, 4 ou [5], 7).

■ Si  $K/\mathbb{Q}$  est fini, on peut plonger  $K$  et  $\bar{K}$  dans  $\mathbb{C}$ , et alors  $E_N$  est un sous-groupe de  $E_N(\mathbb{C})$  (on note  $E_N(\mathbb{C})$  le groupe des points de  $E$ , définis sur  $\mathbb{C}$ , dont l'ordre divise  $N$ ). Comme  $E(\mathbb{C}) = \mathbb{C}/L$  pour un réseau  $L$ ,  $E_N(\mathbb{C}) = N^{-1}L/L$  est isomorphe à  $(\mathbb{Z}/N\mathbb{Z})^2$ . Or  $E_N(\mathbb{C})$  est stable par tout  $K$ -automorphisme de  $\mathbb{C}$ ; ainsi, un point quelconque de  $E_N(\mathbb{C})$  n'a qu'un nombre fini de conjugués sur  $K$ , donc ce point est algébrique sur  $K$ . En conclusion, tout point de  $E_N(\mathbb{C})$  est dans  $E(\bar{K})$ ,

donc  $E_N = E_N(\mathbb{C}) \simeq (\mathbb{Z}/N\mathbb{Z})^2$ .

Si  $K/\mathbb{Q}$  n'est pas fini, on ne peut pas toujours plonger  $K$  dans  $\mathbb{C}$ . Soient :  $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + y$  l'équation de  $E$ ;  $P$  un point de  $E_N$ ;  $(x_p, y_p)$  les coordonnées de  $P$ . Notons  $K'$  le corps  $\mathbb{Q}(a_1, a_2, a_3, a_4, a_6, x_p, y_p)$  : c'est une extension finie de  $\mathbb{Q}$  et  $P \in E(K')$ . Ainsi, d'après ce qui précède,  $P$  est dans  $E_N(\mathbb{C})$ . Là encore,  $E_N \simeq E_N(\mathbb{C}) \simeq (\mathbb{Z}/N\mathbb{Z})^2$ . ■

4.1.2. Sous-groupes cycliques d'ordre fini. Soit  $C$  un sous-groupe fini cyclique d'ordre  $N$  de  $E$ . Nous dirons que  $C$  est défini sur  $K$  s'il est globalement invariant par tout automorphisme de  $\bar{K}/K$ .

4.1.3. Problèmes. Etant donné  $K$ , pour quelles valeurs de  $N$  existe-t-il une courbe elliptique  $E$  sur  $K$  contenant un point  $P$  (resp. un sous-groupe cyclique  $C$ ) d'ordre  $N$  défini sur  $K$ ? Nous étudierons surtout le second de ces problèmes. Deux couples  $(E, C)$  et  $(E', C')$  définis sur  $K$  sont dits  $\bar{K}$ -isomorphes s'il existe un  $\bar{K}$  isomorphisme  $\psi$  de  $E$  sur  $E'$  tel que  $\psi(C) = C'$ . L'ensemble des classes de  $\bar{K}$ -isomorphisme de couples  $(E, C)$  définis sur  $K$  est noté  $Y_0(N)(K)$ .

4.2. EXEMPLE  $K = \mathbb{C}$ .

Alors  $E$  s'identifie à  $\mathbb{C}/L$ , et il est possible de choisir une base  $\{\omega_1, \omega_2\}$  de  $L$  telle que  $C = \frac{1}{N} \cdot \mathbb{Z}\omega_2/L$ . De même,  $E' = \mathbb{C}/L'$  où  $L' = \mathbb{Z}\omega'_1 \oplus \mathbb{Z}\omega'_2$  et  $C' = \frac{1}{N} \mathbb{Z}\omega'_2/L'$ .

4.2.1. PROPOSITION. Soit  $\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma / c \equiv 0 \pmod{N} \right\}$ . Alors  $Y_0(N)(\mathbb{C}) \simeq \bar{\Gamma}_0(N) \backslash \mathfrak{H}$ .

■ Les courbes  $E$  et  $E'$  sont  $\mathbb{C}$  isomorphes si et seulement si il existe un complexe  $\alpha$  tel que  $\alpha L = L'$ . Mais alors  $\{\alpha\omega_1, \alpha\omega_2\}$  et  $\{\omega'_1, \omega'_2\}$  sont deux bases de  $L'$ , donc (cf. lemme 2.1.8) il existe une matrice  $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$  telle que  $\begin{pmatrix} \alpha \omega_1 \\ \alpha \omega_2 \end{pmatrix} = \gamma \begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix}$ . Ceci étant réalisé,

l'image de  $C$  est égale à  $C'$ , si et seulement si les sous-groupes de  $E'$  engendrés par  $\alpha \frac{\omega_2}{N} = \frac{c\omega_1' + d\omega_2'}{N}$  et  $\frac{\omega_2'}{N}$  sont les mêmes. Ceci équivaut à :  $c \equiv 0 \pmod{N}$ . ■

4.2.2. Posons  $X_0(N)(\mathbb{C}) = \widehat{\Gamma_0(N) \backslash \mathbb{H}}$ ; autrement dit (cf. 2.2.1)  $X_0(N)(\mathbb{C})$  est la réunion de  $Y_0(N)(\mathbb{C})$  et des pointes; c'est une surface de Riemann compacte, et le revêtement  $X_0(N)(\mathbb{C}) \longrightarrow \widehat{\Gamma \backslash \mathbb{H}}$  est de degré  $[\overline{\Gamma} : \overline{\Gamma_0(N)}]$ . La formule de Riemann-Hurwitz permet de calculer le genre  $g_0(N)$  de  $X_0(N)(\mathbb{C})$ , sachant que le genre de  $\widehat{\Gamma \backslash \mathbb{H}}$  est nul.

*PROPOSITION.* Le genre de  $X_0(N)(\mathbb{C})$  est égal à :

$$g_0(N) = 1 + \mu/12 - \mu_2/4 - \mu_3/3 - \sigma_0/2,$$

$$\text{où } \mu = N \prod_{p|N} \left(1 + \frac{1}{p}\right); \quad \mu_2 = \begin{cases} \prod_{p|N} (1 + \frac{-1}{p}) & \text{si } 4 \nmid N \\ 0 & \text{sinon} \end{cases};$$

$$\mu_3 = \begin{cases} \prod_{p|N} (1 + \frac{-3}{p}) & \text{si } 9 \nmid N \\ 0 & \text{sinon} \end{cases}; \quad \sigma_0 = \sum_{d|N} \varphi\left(d, \frac{N}{d}\right).$$

Dans cet énoncé,  $p$  désigne un nombre premier,  $\varphi$  la fonction indicatrice d'Euler, et  $\left(\frac{\cdot}{p}\right)$  le symbole de Legendre; on trouve dans [33], par exemple, la définition et le calcul de ces expressions. En particulier, on a :  $\left(\frac{-1}{p}\right) = 0$  si  $p=2$ ,  $\left(\frac{-1}{p}\right) = 1$  si  $p \equiv 1 \pmod{4}$ ,  $\left(\frac{-1}{p}\right) = -1$  si  $p \equiv 3 \pmod{4}$ ; et  $\left(\frac{-3}{p}\right) = 0$  si  $p=3$ ,  $\left(\frac{-3}{p}\right) = 1$  si  $p \equiv 1 \pmod{3}$ ,  $\left(\frac{-3}{p}\right) = -1$  si  $p \equiv 2 \pmod{3}$ .

■ La proposition se démontre en 2 temps :

D'abord, si  $G$  est un sous-groupe de  $\Gamma$  d'indice fini, notons  $\mu$  l'indice de  $\overline{G}$  dans  $\overline{\Gamma}$ ,  $\mu_2$  (resp.  $\mu_3$ ) le nombre de points au-dessus de  $i$  (resp. de  $\rho$ ) dans le revêtement  $\widehat{G \backslash \mathbb{H}} \longrightarrow \widehat{\Gamma \backslash \mathbb{H}}$ , et  $\sigma_0$  le nombre des pointes de  $\widehat{G \backslash \mathbb{H}}$ . La formule de Riemann-Hurwitz donne alors le genre  $g$

de  $\widehat{G \backslash \mathbb{H}}$  par :  $g = 1 + \mu/12 - \mu_2/4 - \mu_3/3 - \sigma_0/2$  .

Ensuite, on calcule  $\mu$  ,  $\mu_2$  ,  $\mu_3$  ,  $\sigma_0$  , lorsque  $G = \Gamma_0(N)$  .  
 Pour une démonstration détaillée, voir ([43] , propositions 1.40 et 1.43). ■

4.2.3. Lorsque  $N$  est premier, la formule donnant  $g_0(N)$  est particulièrement simple.

*COROLLAIRE.* Si  $N$  est premier, le genre de  $X_0(N)(\mathbb{C})$  est égal à :

$$g_0(N) = \begin{cases} \left[ \frac{N+1}{12} \right] & \text{si } 12 \nmid N-1 \\ \left[ \frac{N+1}{12} \right] - 1 = \frac{N-1}{12} - 1 & \text{si } 12 \mid N-1 . \end{cases}$$

■ En effet,  $\mu = N+1$  et  $\sigma_0 = 2$  , d'où

$$g_0(N) = \frac{N+1}{12} - \frac{\mu_2}{4} - \frac{\mu_3}{4} ;$$

on vérifie que  $g_0(2) = g_0(3) = 0$  , puis on suppose  $N \neq 2, 3$  ; alors  $\mu_2$  et  $\mu_3$  ne peuvent prendre que les valeurs 0 ou 2 , ce qui donne pour  $g_0(N)$  les valeurs :  $\frac{N+1}{12}$  ,  $\frac{N+1}{12} - \frac{1}{3}$  ,  $\frac{N+1}{12} - \frac{1}{2}$  ,  $\frac{N+1}{12}$  . Or  $g_0(N)$  est entier, et les 3 premières valeurs, lorsqu'elles sont entières, valent  $\left[ \frac{N+1}{12} \right]$  .  
 Enfin la quatrième valeur correspond à  $\mu_2 = \mu_3 = 2$  c'est-à-dire

$N-1 \equiv 0 \pmod{3 \text{ et } 4}$  , et alors  $\left[ \frac{N+1}{12} \right] = \frac{N-1}{12}$  alors que  $\frac{N+1}{12} - \frac{7}{6} = \frac{N-1}{12} - 1$ . ■

### 4.3. ISOGENIES.

Soient  $E$  et  $E'$  deux courbes elliptiques sur  $K$  ,  $\lambda$  un homomorphisme de  $E$  dans  $E'$  .

4.3.1. *PROPOSITION.* Les trois propriétés suivantes sont équivalentes :

- (I)  $\lambda \neq 0$  ;
- (II)  $\text{Ker } \lambda$  est fini ;
- (III)  $\lambda$  est surjectif.

Un homomorphisme  $\lambda$  vérifiant ces trois propriétés est appelé une isogénie de  $E$  dans  $E'$  .

■ La proposition vient du fait que toute courbe elliptique est une variété abélienne de dimension 1. ■

Soient un homomorphisme de  $E$  dans  $E'$  ,  $K(E)$  (resp.  $K(E')$ ) les corps de fonctions de  $E$  (resp.  $E'$ ) . Alors  $f$  induit un homomorphisme  $f^*$  de  $K(E')$  dans  $K(E)$  . Appelons degré de  $f$  le degré de l'extension  $K(E)/f^*(K(E'))$  , et disons que  $f$  est séparable (resp. inséparable) si cette extension est séparable (resp. inséparable). Définissons de même les degrés de séparabilité et d'inséparabilité de  $f$  , notés respectivement  $(\deg f)_i$  et  $(\deg f)_s$  et égaux respectivement au degré de séparabilité et d'inséparabilité de  $K(E)/f^*(K(E'))$  . Alors , l'image réciproque par  $f$  de chaque point de  $E'$  contient  $(\deg f)_s$  points , chacun étant affecté d'une multiplicité égale à  $(\deg f)_i$  (la structure de groupe de  $E'$  empêche qu'il y ait des points de ramification). En particulier , l'ordre de  $\text{Ker } f$  est égal à  $(\deg f)_s$  .

4.3.2. Exemples : Multiplication par  $N$  . Notons  $N$  l'endomorphisme "multiplication par  $N$ " sur  $E$  .

*PROPOSITION.* La multiplication par  $N$  est une isogénie de  $E$  de degré  $N^2$  .

■ Si  $E$  est définie sur un corps  $K$  de caractéristique nulle , nous avons vu en (4.1.1) que  $E_N$  (c'est-à-dire le noyau de  $N$ ) est isomorphe à  $(\mathbb{Z}/N\mathbb{Z})^2$  ; donc  $N$  est de degré  $N^2$  .

Si  $E$  est définie sur un corps  $K$  de caractéristique  $p$  non nulle , il faut écrire explicitement les formules de multiplication par  $N$  en caractéristique nulle , voir qu'elles se réduisent bien (modulo  $p$ ) et calculer le degré de l'extension  $K(E)/N^*(K(E))$  (cf.[31] 3.4 et [4]) . ■

*COROLLAIRE.* (On retrouve la proposition (4.1.1)). Si  $p \nmid N$  , le groupe  $E_N$  est isomorphe à  $(\mathbb{Z}/N\mathbb{Z})^2$  ; si  $p \mid N$  , c'est un sous-groupe de  $(\mathbb{Z}/N\mathbb{Z})^2$  .

- En effet,  $E_N = \text{Ker}(N)$ , et l'ordre de  $E_N$  est égal à  $(\deg N)_s$ . ■

### 4.3.3. Isogénies et sous-groupes.

*PROPOSITION.* Soient  $E, E'$ , deux courbes elliptiques sur  $K$ . Il y a une bijection entre les isogénies  $\lambda$  de  $E$  dans  $E'$  définies sur  $K$  séparables de degré  $m$ , et les sous-groupes  $F$  de  $E$ , rationnels sur  $K$  d'ordre  $m$ , cette bijection étant définie par :  $F = \text{Ker } \lambda$ .

■ Soit  $\lambda : E \rightarrow E'$  une isogénie définie sur  $K$  (cela signifie que  $E, E'$  et  $\lambda$ , sont définis sur  $K$ ). Supposons  $\lambda$  séparable. Alors  $\text{Ker } \lambda$  est un sous-groupe de  $E$  d'ordre  $\deg \lambda$ . Le groupe de Galois de  $\bar{K}/K$  agit sur  $\lambda(E)$  par :  $(\lambda(p))^\sigma = \lambda^\sigma(p^\sigma)$ . Mais  $\lambda^\sigma = \lambda$  puisque  $\lambda$  est défini sur  $K$ , donc  $(\text{Ker } \lambda)^\sigma = \text{Ker } \lambda$  est un sous-groupe de  $E$  rationnel sur  $K$ .

Réciproquement, soit  $F$  un sous-groupe de  $E$  rationnel sur  $K$ . Montrons qu'alors  $E' = E/F$  est une courbe elliptique sur  $K$ , et que la projection canonique  $\lambda : E \rightarrow E'$  est une isogénie définie sur  $K$  de noyau  $F$ . Le sous-groupe  $F$  de  $E$  agit sur  $\bar{K}(E)$  par translation : si  $a \in F$ ,  $f \in \bar{K}(E)$ , posons  $af(x) = f(x-a)$  pour tout  $x \in E$ . Définissons les fonctions  $X$  et  $Y$  de  $\bar{K}(E)$  par :  $X(M) = \sum_{a \in F} x(M-a)$ ,  $Y(M) = \sum_{a \in F} y(M-a)$ , pour tout  $M \in E$ . En fait,  $X$  et  $Y$  sont dans  $\bar{K}(E)^F$ , et  $X$  (resp.  $Y$ ) a un pôle d'ordre 2 (resp. 3) en tout point de  $F$ , donc  $\deg(X) = 2d$  et  $\deg(Y) = 3d$ , si  $d = \#F$ ; on en déduit :  $[\bar{K}(E) : \bar{K}(X)] = 2d$ ,  $[\bar{K}(E) : \bar{K}(Y)] = 3d$ ,  $[\bar{K}(E) : \bar{K}(X, Y)] = d$ . Or  $[\bar{K}(E) : \bar{K}(E)^F] = \#F = d$ , d'où  $\bar{K}(E)^F = \bar{K}(X, Y)$ .

On peut montrer que  $\bar{K}(E)^F$  est un corps de fonctions algébriques sur  $\bar{K}$  de genre 1, et que l'équation liant  $X$  et  $Y$  est celle d'une courbe elliptique (cf. [49] et [50]). ■

*COROLLAIRE.* L'ensemble  $Y_0(N)(K)$  peut être considéré comme l'ensemble des classes de  $\bar{K}$ -isomorphisme de triplets  $(E, E', \lambda : E \rightarrow E')$  d'isogénies définies sur  $K$  à noyau cyclique d'ordre  $N$ .



#### 4.4. ACCOUPLEMENT DE WEIL.

Soit  $K$  un corps égal à  $\mathbb{C}$  ou à un corps local. Supposons  $N$  premier à la caractéristique de  $K$ .

4.4.1. THEOREME. Il existe une fonction  $e_N : E_N \times E_N \longrightarrow \mu_N$  vérifiant les propriétés suivantes :

- (i)  $e_N$  est bilinéaire ;
- (ii)  $e_N$  est alternée, c'est-à-dire  $e_N(s, t) = e_N(t, s)^{-1}$  ;
- (iii)  $e_N$  établit une dualité, c'est-à-dire  $e_N(s, t) = 1$  pour tout  $s$  si et seulement si  $t = 0$  ;
- (iv)  $e_N(s, t)^\sigma = e_N(s^\sigma, t^\sigma)$  pour tout  $\sigma \in \text{Gal}(\bar{K}/K)$  .

(cf. [43] , proposition 4.2).

■ Définissons  $e_N$  : soient  $t \in E_N$  et  $t' \in E_{N^2}$  tel que  $Nt' = t$  (la multiplication par  $N$  est surjective), et soient les diviseurs  $D = N(t) - N(0)$  et  $D' = \sum_{u \in E_N} (t'+u) - \sum_{u \in E_N} (u)$ . D'après le critère d'Abel (2.4 et 3.2) il existe deux fonctions  $f_t$  et  $g_t$  dans  $K(E)$  de diviseurs  $(f_t) = D$  et  $(g_t) = D'$ . La fonction  $f_t \circ N$  définie par  $f_t \circ N(x) = f_t(Nx)$  a pour zéros les points  $x$  tels que  $Nx = t$  et pour pôles les points  $x$  tels que  $Nx = 0$ , ces zéros et pôles étant d'ordre  $N$ , donc son diviseur est  $(f_t \circ N) = N \sum_{u \in E_N} (t'+u) - N \sum_{u \in E_N} u = ND' = (g_t^N)$ . Quitte à multiplier  $g_t$  par une constante, nous obtenons :  $f_t(Nx) = g_t(x)^N$  pour tout  $x$  de  $E$ . Soit  $s \in E_N$  ; alors  $g_t(x+s)^N = f_t(N(x+s)) = f_t(Nx) = g_t(x)^N$ , donc il existe  $e_N(s, t) \in \mu_N$  tel que  $g_t(x+s) = e_N(s, t)g_t(x)$  quel que soit  $x \in E$ .

Montrons que  $e_N$  vérifie les propriétés du théorème :

(i)  $g_t(x+s_1+s_2) = e_N(s_1+s_2, t)g_t(x) = e_N(s_2, t)g_t(x+s_1) = e_N(s_2, t)e_N(s_1, t)g_t(x)$  pour tout  $x$ , donc  $e_N$  est linéaire par rapport à la 1ère variable.

$$\begin{aligned} (f_{t_1+t_2}) &= N(t_1+t_2) - N(0) \\ &= (N(t_1)-N(0)) + (N(t_2)-N(0)) + N((t_1+t_2)-(t_1)-(t_2)+(0)) \\ &= (f_{t_1}) + (f_{t_2}) + N(h) \end{aligned}$$

d'après le critère d'Abel, donc, quitte à multiplier  $h$  par une constante, nous avons  $f_{t_1+t_2} = f_{t_1} \cdot f_{t_2} \cdot h^N$ , d'où  $g_{t_1+t_2}(x)^N = g_{t_1}(x)^N \cdot g_{t_2}(x)^N \cdot h(Nx)^N$ . Appliquant ceci à  $x+s$ , comme  $h(N(x+s)) = h(Nx)$ , nous voyons que  $e_N(s, t_1+t_2) = e_N(s, t_1) + e_N(s, t_2)$ . Ainsi  $e_N$  est bilinéaire.

(ii) Comme  $e_N$  est bilinéaire, il suffit de montrer que  $e_N(t, t) = 1$  pour tout  $t \in E_N$  et d'utiliser :  $e_N(s+t, s+t) = e_N(s, s) \cdot e_N(t, t) \cdot e_N(s, t) \cdot e_N(t, s)$  pour montrer (ii). Considérons la fonction :

$$y \longmapsto f_t(y) \cdot f_t(y-t) \dots f_t(y-(N-1)t) .$$

Elle a pour diviseur  $N((t)-(0) + (2t) - (t) + \dots + (Nt) - ((N-1)t)) = 0$ , donc elle est constante. Posons  $t = Nt'$ ,  $y = Nx$ , et considérons la racine  $N^{\text{ème}}$  de la fonction, en utilisant :  $g_t(x)^N = f_t(y)$  : la fonction continue  $x \longmapsto g_t(x) \cdot g_t(x-t') \dots g_t(x-(N-1)t')$  est constante. En particulier, elle a la même valeur en  $x$  et en  $x-t'$ , ce qui mène à :  $g_t(x) = g_t(x-Nt') = g_t(x-t)$  c'est-à-dire  $e_N(t, t) = 1$ .

(iii) Si  $e_N(s, t) = 1$  pour tout  $s$ , c'est-à-dire  $g_t(x+s) = g_t(x)$  cela signifie que  $g_t \in K(E)^{E_N} = K(E/E_N) = K(NE)$  (cf. 4.3.3). Autrement dit, il existe  $h \in K(E)$  tel que  $g_t(x) = h(Nx)$ , d'où  $f_t(Nx) = h(Nx)^N$ , et le diviseur de  $h$  est donné par :  $(h) = \frac{1}{N}(f_t) = (t) - (0)$ , ce qui n'est possible que si  $t = 0$  (critère d'Abel).

(iv) provient de la définition de  $e_N$  et de la propriété :

$$(g_t(x))^\sigma = g_{t^\sigma}(x^\sigma) . \quad \blacksquare$$

4.4.2. COROLLAIRE. Le corps  $K(\mu_N)$  est contenu dans  $K(E_N)$ , et le diagramme suivant est commutatif :

$$\begin{array}{ccc} \text{Gal}(K(E_N)/K) & \xrightarrow{\text{restriction}} & \text{Gal}(K(\mu_N)/K) \\ \downarrow & & \downarrow \\ \text{Aut}(E_N) & \xrightarrow{\text{déterminant}} & (\mathbb{Z}/N\mathbb{Z})^* \end{array} .$$

■ L'application  $e_N$  est surjective, d'après (iii) ; or  $e_N(s,t)^\sigma = e_N(s,t)$  si  $\sigma \in \text{Gal}(\bar{K}/K(E_N))$  ; ainsi  $\mu_N \subset K(E_N)$  . En fait,  $e_N$  définit un isomorphisme de  $\Lambda^2 E_N$  sur  $\mu_N$  , donc  $e_N$  correspond au déterminant. ■

#### 4.4.3. Application.

PROPOSITION. Le groupe des points de torsion définis sur  $\mathbb{Q}$  une courbe elliptique sur  $\mathbb{Q}$  est ou bien cyclique, ou bien égal au produit de  $\mathbb{Z}/2\mathbb{Z}$  par un groupe cyclique.

■ En effet, le groupe de torsion de  $E(K)$  est égal à :  
 $E(K)^{\text{tor}} = \prod_p E(K)_p$  où  $p$  parcourt l'ensemble des nombres premiers ; et d'autre part  $E(\mathbb{Q})_p \subset E(\bar{\mathbb{Q}})_p \simeq (\mathbb{Z}/p\mathbb{Z})^2$  . Supposons que  $E(\mathbb{Q})_p \simeq E(\bar{\mathbb{Q}})_p$  . D'après le corollaire (4.4.2),  $\mathbb{Q}(\mu_p) \subset \mathbb{Q}(E_p)$  ; or  $E_p = E(\bar{\mathbb{Q}})_p$  par définition, donc notre hypothèse implique :  $\mathbb{Q}(\mu_p) \subset \mathbb{Q}(E(\mathbb{Q})_p)$  c'est-à-dire  $\mathbb{Q}(\mu_p) \subset \mathbb{Q}$  : ce n'est possible que si  $p=2$  . Ainsi  $E(\mathbb{Q})_p$  est trivial ou isomorphe à  $\mathbb{Z}/p\mathbb{Z}$  si  $p \neq 2$  , et peut être isomorphe à  $(\mathbb{Z}/2\mathbb{Z})^2$  si  $p=2$  . ■

## 5. COURBES MODULAIRES

### 5.1. $X_0(N)$ ET $X(N)$ .

5.1.1. Rappelons que  $Y_0(N)(K)$  est l'ensemble des classes de  $\bar{K}$ -isomorphisme de couples  $(E,C)$  où  $E$  est une courbe elliptique sur  $K$  et  $C$  un sous-groupe cyclique d'ordre  $N$  de  $E$  défini sur  $K$  .

Si  $\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid c \equiv 0 \pmod{N} \right\}$  nous avons vu que

$Y_0(N)(\mathbb{C}) \simeq \overline{\Gamma_0(N)} \backslash \mathbb{H}$  , et qu'en ajoutant les pointes nous obtenons une surface de Riemann compacte  $\widehat{\Gamma_0(N)} \backslash \mathbb{H}$  notée  $X_0(N)(\mathbb{C})$  .

5.1.2. Fixons une racine  $N^{\text{ème}}$  de l'unité  $\zeta_N$  dans  $K(\mu_N)$ . Définissons  $Y(N)(K)$  comme l'ensemble des triplets  $(E, P, Q)$  où  $E$  est une courbe elliptique sur  $K$ ,  $P$  et  $Q$  deux points de  $E$  tels que  $Q \in E(K)$ ,  $P \in E(K(\mu_N))$  et  $e_N(P, Q) = \zeta_N$ .

Soit  $\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma / \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv 1 \pmod{N} \right\}$  (où  $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$  est l'identité dans  $\Gamma$ ). Il est facile de vérifier (comme en (4.2.2)) que  $Y(N)(\mathbb{C}) \sim \overline{\Gamma(N)} \backslash \mathbb{H}$ , et de même  $\widehat{\overline{\Gamma(N)} \backslash \mathbb{H}}$  est une surface de Riemann compacte, notée  $X(N)(\mathbb{C})$ .

## 5.2. FONCTIONS DE WEBER (cf. [43], 4.5).

5.2.1. *DEFINITION*. Soient  $K$  un corps de caractéristique  $p$  différente de 2 ou 3,  $N$  un entier  $\geq 2$  et premier à  $p$ ,  $E$  une courbe elliptique sur  $K$  donnée par son équation de Weierstrass :

$$y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864} \quad (\text{cf. 1.1.3}).$$

Rappelons que le discriminant de  $E$  est  $\Delta = \frac{c_4^3 - c_6^2}{12^3} \neq 0$  et que l'invariant de  $E$  est  $j = \frac{c_4^3}{\Delta}$ . Enfin, la proposition (1.2.2) détermine  $\text{Aut}(E)$  : nous avons  $\text{Aut}(E) \simeq \mu_{2i}$  où  $i = 1$  si  $j \neq 0, 12^3$ ,  $i = 2$  si  $j = 12^3$ ,  $i = 3$  si  $j = 0$ . Posons, pour tout  $P$  de  $E$  :

$$f^{(1)}(P) = \frac{x(P)c_4c_6}{\Delta}, \quad f^{(2)}(P) = \frac{x(P)^2c_4^2}{\Delta}$$

$$f^{(3)}(P) = \frac{x(P)^3c_6}{\Delta}.$$

La fonction  $f^{(i)}$  appartient à  $K(E)$ . On l'appelle la  $i^{\text{ème}}$  fonction de Weber de  $E$ , et on la note parfois  $f_E^{(i)}$ . Elle est paire car  $x$  est paire.

### 5.2.2. Propriétés.

(i) Lorsque  $\text{Aut}(E) \simeq \mu_{2i}$ , on a  $f^{(i)}(P) = f^{(i)}(P')$  si et seulement si  $P = \alpha P'$  pour un  $\alpha \in \text{Aut}(E)$ .

■ Notons  $x, y, x', y'$  les coordonnées  $x(P)$ ,  $y(P)$ ,  $x(P')$ ,  $y(P')$ , de  $P$  et  $P'$ , qui sont liées par :

$$\begin{cases} y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864} \\ y'^2 = x'^3 - \frac{c_4}{48}x' - \frac{c_6}{864} \end{cases} .$$

Alors  $f^{(i)}(P) = f^{(i)}(P')$  si et seulement si  $x^i = x'^i$ , ce qui donne :

$$\begin{cases} x = x' \\ y^2 = y'^2 \end{cases} \text{ si } i = 1, \quad \begin{cases} x^2 = x'^2 \\ y^4 = y'^4 \end{cases} \text{ si } i = 2, \quad \begin{cases} x^3 = x'^3 \\ y^2 = y'^2 \end{cases} \text{ si } i = 3 . \quad \blacksquare$$

(ii) Soient  $E$  et  $E'$  deux courbes elliptiques sur  $K$ , et  $\lambda$  un  $\bar{K}$ -isomorphisme de  $E$  sur  $E'$ . Alors  $f_{E'}^{(i)} \circ \lambda = f_E^{(i)}$  pour  $i = 1, 2, 3$ .

■ Soit  $y^2 = x^3 - \frac{c_4'}{48}x - \frac{c_6'}{864}$  l'équation de  $E'$ . D'après (1.2.1) l'isomorphisme  $\lambda$  est de la forme :  $\lambda(x) = u^2x$ ,  $\lambda(y) = u^3y$ , pour un  $u$  dans  $\bar{K}^*$  (les nombres  $r, s, t$  de la formule (4) sont nuls puisque les 2 courbes sont définies par leur équation de Weierstrass). Alors  $c_4' = u^4c_4$ ,  $c_6' = u^6c_6$ ,  $\Delta' = u^{12}\Delta$ , et la propriété (ii) se déduit de la définition des  $f^{(i)}$ . ■

### 5.3. INTERPRETATION GEOMETRIQUE.

5.3.1. *DEFINITION.* Jusqu'à la fin de ce paragraphe,  $N$  est un entier  $\geq 2$ ,  $K$  est égal à  $\mathbb{C}$  et  $E$  à  $\mathbb{C}/L$ , où  $L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$  et  $\tau = \omega_1/\omega_2 \in \mathbb{H}$ ; ainsi  $L = \{a\omega_1 + b\omega_2 \mid (a, b) \in \mathbb{Z}\}$ ,  $NL = \{a\omega_1 + b\omega_2 \mid (a, b) \in N\mathbb{Z}^2\}$ , et  $E_N \simeq L/NL \simeq (\mathbb{Z}/N\mathbb{Z})^2$ .

Pour tout  $(a, b) \in \{0, 1, \dots, N-1\}^2 - \{(0, 0)\}$ , posons

$$f_{(a, b)}^{(i)}(\tau) = f^{(i)}\left(\frac{a\omega_1 + b\omega_2}{N}\right) \quad (i = 1, 2, 3) ;$$

$f_{(a, b)}^{(i)}$  est bien fonction de  $\tau$ , grâce aux propriétés d'homogénéité des  $f^{(i)}$ . Elle vérifie les propriétés suivantes :

(i)  $f_{(a,b)}^{(i)} \Big|_{\gamma} = f_{(a,b)\gamma}^{(i)}$  pour tout  $\gamma \in \Gamma$  si  $(a,b)\gamma$  désigne le produit matriciel de  $(a,b)$  par  $\gamma$ .

(ii)  $f_{(a,b)}^{(i)} = f_{(a',b')}^{(i)}$  si  $(a,b) \equiv \pm(a',b') \pmod{N\mathbb{Z}^2}$ .

5.3.2. *PROPOSITION.* La fonction  $f_{(a,b)}^{(i)}$  est une fonction modulaire de poids zéro pour le groupe  $\Gamma(N)$ , et son développement de Fourier est à coefficients dans  $\mathbb{Q}(\zeta_N)$ .

■ C'est une fonction holomorphe dans  $\mathfrak{H}$  d'après sa définition (rappelons que  $\Delta \neq 0$  dans  $\mathfrak{H}$ ). Si  $\gamma \in \Gamma(N)$ , i.e.  $\gamma \in \Gamma$  et  $\gamma \equiv \pm 1 \pmod{N}$  (cf. 5.1.2), on a  $f_{(a,b)}^{(i)} \Big|_{\gamma} = f_{(a,b)\gamma}^{(i)}$  et  $(a,b)\gamma \equiv \pm(a,b) \pmod{N\mathbb{Z}^2}$ , donc  $f_{(a,b)}^{(i)} \Big|_{\gamma} = f_{(a,b)}^{(i)}$ . Enfin, le développement de Fourier de  $x = \rho$  (cf. 2.5.1) donne celui de  $f_{(a,b)}^{(i)}$ . Par exemple pour  $i = 1$ :

$$f_{(a,b)}^{(1)}(\tau) = \rho\left(\frac{a\tau+b}{N}; \mathbb{Z}\tau \oplus \mathbb{Z}\right) \cdot \frac{E_4(\tau) \cdot E_6(\tau)}{\Delta(\tau)}$$

$$= \left[ \frac{1}{12} + \frac{q}{(1-q)^2} + \sum_{n,m \geq 1} nq^{mn} (\zeta_N^{nb} q^{na/N} + \zeta_N^{-nb} q^{-na/N} - 2) \right] \frac{1}{q} + R(q)$$

où  $R(q) \in \mathbb{Z}[q]$  et  $a < N$ . Donc  $f_{(a,b)}^{(1)}(\tau) \in \mathbb{Q}(\zeta_N)((q^{1/N}))$ . Or la variable locale en  $\infty$  pour  $\widehat{\Gamma(N)} \backslash \mathfrak{H}$  est  $q^{1/m}$  où  $m$  est l'indice de ramification de  $\widehat{\Gamma(N)} \backslash \mathfrak{H}$  sur  $\widehat{\Gamma} \backslash \mathfrak{H}$  en  $\infty$ , c'est-à-dire le plus petit entier tel que  $\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \in \Gamma(N)$ : donc  $m = N$  et  $f_{(a,b)}^{(1)}$  est méromorphe à l'infini; par conjugaison, et d'après la formule (i)  $f_{(a,b)}^{(1)}$  est méromorphe aux autres pointes de  $\widehat{\Gamma(N)} \backslash \mathfrak{H}$ . Un raisonnement analogue permet de conclure pour  $i = 2$  et  $3$ . ■

Remarque: le développement de Fourier de  $\frac{f_{(a,b)}^{(i)}(\tau)}{j(\tau)}$  est dans  $\mathbb{Q}(\zeta_N)[[q^{1/N}]]$ .

5.3.3. *DEFINITION.* Cherchons des fonctions analogues pour  $\Gamma_o(N) : (a,b)$  et  $(a',b')$  étant dits équivalents si les sous-groupes

$$\left\langle \frac{aw_1 + bw_2}{N} \right\rangle \quad \text{et} \quad \left\langle \frac{a'w_1 + b'w_2}{N} \right\rangle$$

d'ordre  $N$  de  $E$  sont égaux, notons  $g_k^{(i)}$  les fonctions symétriques élémentaires des  $f_{(a,b)}^{(i)}$  regroupées selon les classes d'équivalence de  $(a,b)$ .

L'indice  $k$  parcourt un certain ensemble  $\mathcal{K}$  lorsque  $(a,b)$  parcourt un système de représentation de  $\mathbb{Z}^2/N\mathbb{Z}^2$ .

5.3.4. *PROPOSITION.* La fonction  $g_k^{(i)}$  est une fonction modulaire de poids zéro pour le groupe  $\Gamma_0(N)$ , et son développement de Fourier est à coefficients dans  $\mathbb{Q}$

■ C'est une conséquence de la proposition analogue pour les  $f_{(a,b)}^{(i)}$  (cf. 5.3.3) et de la définition des  $g_k^{(i)}$ . ■

5.3.5. Nous pouvons maintenant définir deux applications :  $\phi$  de  $\overline{\Gamma}(N)\backslash\mathbb{H}$  dans  $\mathbb{C}^{M+1}$  telle que  $\phi(\tau) = (j(\tau), f_{(a,b)}^{(i)}(\tau))$ ,  $i \in \{1, 2, 3\}$ ,  $(a,b) \in \{0, 1, \dots, N-1\}^2 - \{(0,0)\}$ ; et  $\psi$  de  $\overline{\Gamma}_0(N)\backslash\mathbb{H}$  dans  $\mathbb{C}^{M'+1}$  telle que  $\psi(\tau) = (j(\tau), g_k^{(i)}(\tau))$ ,  $i \in \{1, 2, 3\}$ ,  $k \in \mathcal{K}$  ( $M$  et  $M'$  étant 2 entiers convenables).

Aux pointes, posons  $\phi(\tau) = (1, \frac{f_{(a,b)}^{(i)}(\tau)}{j(\tau)})$ , et  $\psi(\tau) = (1, \frac{g_k^{(i)}(\tau)}{j(\tau)})$  (en remplaçant les fonctions par leurs développements de Fourier). Cela permet de prolonger  $\phi$  (resp.  $\psi$ ) en une fonction de  $\widehat{\overline{\Gamma}(N)\backslash\mathbb{H}}$  (resp.  $\widehat{\overline{\Gamma}_0(N)\backslash\mathbb{H}}$ ) dans  $\mathbb{P}^M$  (resp.  $\mathbb{P}^{M'}$ ) (espaces projectifs sur  $\mathbb{C}$ ).

5.3.6. *PROPOSITION.*  $\phi$  (resp.  $\psi$ ) est un plongement biholomorphe de la surface de Riemann  $\widehat{\overline{\Gamma}(N)\backslash\mathbb{H}}$  (resp.  $\widehat{\overline{\Gamma}_0(N)\backslash\mathbb{H}}$ ) dans l'espace projectif  $\mathbb{P}^M$  (resp.  $\mathbb{P}^{M'}$ ).

■ D'après ce qui précède,  $\phi$  et  $\psi$  sont holomorphes, y compris aux pointes.

Injectivité de  $\phi$  : soient  $\tau$  et  $\tau'$  dans  $\mathbb{H}$  tels que leurs classes modulo  $\overline{\Gamma_0(N)}$  aient la même image par  $\phi$ ; cela signifie :  $j(\tau) = j(\tau')$ , et  $f_{(a,b)}^{(i)}(\tau) = f_{(a,b)}^{(i)}(\tau')$  pour tous  $i, a, b$ . Supposons d'abord que  $j(\tau) \in \mathbb{C}^M$ , c'est-à-dire que  $\tau$  et  $\tau'$  ne sont pas des pointes. D'après (2.1.8), il existe une matrice  $\gamma \in \Gamma$  telle que  $\gamma\tau = \tau'$ , d'où  $f_{(a,b)}^{(i)}(\tau') = f_{(a,b)\gamma}^{(i)}(\tau)$  (cf. 5.2.1). Ainsi  $f_{(\frac{a\tau+b}{N})}^{(i)} = f_{(\frac{a'\tau+b'}{N})}^{(i)}$  si  $(a', b') = (a, b)\gamma$ ; d'après (5.1.2(i)), il existe un automorphisme  $\alpha_{a,b}$  de  $E = \mathbb{C}/\mathbb{Z}\tau + \mathbb{Z}$  tel que  $(a, b) = (a', b')\alpha_{a,b}$  (écriture matricielle). Montrons que  $\alpha_{a,b}$  est en fait

indépendant de  $(a,b)$ . Soient les couples  $(a,b)$ ,  $(a',b')$  et  $(a'',b'') = (a,b) + (a',b')$ . Nous devons avoir les égalités de matrices suivantes :

$$(a''b'') = \alpha_{a'',b''}(a''b'')\gamma = [\alpha_{a,b}(ab) + \alpha_{a',b'}(a'b')] \gamma$$

c'est-à-dire :  $\alpha_{a'',b''}(a''b'') = \alpha_{a,b}(ab) + \alpha_{a',b'}(a'b')$  ou encore :

$$(\alpha_{a'',b''} - \alpha_{a,b})(a''b'') = (\alpha_{a',b'} - \alpha_{a,b})(a'b')$$

Lorsque  $\text{Aut } E \simeq \mu_2$  ( $\tau \neq i, \rho$ ), la différence entre 2 automorphismes de  $E$  ne peut prendre que les valeurs  $\pm 2$  ou  $0$ . Donc, ou bien  $\alpha_{a,b} = \alpha_{a',b'} = \alpha_{a'',b''}$ , ou bien  $(a''b'') = \pm(a'b')$  et le nombre des couples  $(a,b)$  est égal à 2. Or le nombre des couples  $(a,b)$  est égal au cardinal de  $(\mathbb{Z}/N\mathbb{Z})^2 - \{(0,0)\}$ , c'est-à-dire à  $N^2 - 1$  et ce nombre est  $\geq 3$  dès que  $N \geq 2$ . Donc  $\alpha_{a,b} = \alpha$  est indépendant de  $(a,b)$ . Lorsque  $\text{Aut } E \simeq \mu_4$  ou  $\mu_6$ , la démonstration est plus lourde mais le résultat est encore vrai. Alors, l'égalité  $(ab) = (ab)\gamma\alpha$ , valable pour tout  $(a,b)$ , donne  $\gamma\alpha = 1$ ; ainsi  $\gamma$  est dans  $\text{Aut } E$ , qui est isomorphe au groupe d'isotropie de  $\tau$  dans  $\widehat{\Gamma \backslash \mathbb{H}}$ : donc  $\tau' = \gamma\tau = \tau$ .

Supposons maintenant que  $j(\tau)$  est infini, c'est-à-dire que  $\tau$  et  $\tau'$  sont des pointes. Le développement de Fourier donne

$$\frac{f^{(i)}(a,b)(\tau)}{j(\tau)} = \frac{1}{12} + \frac{q^{a/N} \zeta_N^b}{(1 - q^{a/N} \zeta_N^b)^2} + O(q^{2/N}) \equiv \begin{cases} \frac{1}{12} + \frac{\zeta_N^b}{(1 - \zeta_N^b)^2} & \text{si } a=0 \\ \frac{1}{12} & \text{si } a \neq 0 \end{cases} \pmod{q^{2/N}}.$$

Ainsi, les différentes valeurs de  $(a,b)$  telles que  $a=0$  correspondent

à des valeurs distinctes de  $\frac{f^{(i)}(a,b)(\tau)}{j(\tau)}$ . Par conjugaison, il en est de même pour toutes les valeurs de  $(a,b)$ . Ainsi  $\phi$  est injectif; la démonstration est analogue pour  $\psi$ .

Enfin, on vérifie que  $\phi$  et  $\psi$  sont biholomorphes. ■

Remarque : Cette proposition généralise ce qu'on a vu en (2.2) :

il existe une représentation conforme de  $\overline{\Gamma \backslash \mathbb{H}}$  sur  $\mathbb{C}$ , définie par  $\tau \mapsto j(\tau)$ , qui est prolongée par :  $\infty \mapsto \infty$  en une bijection biholomorphe de  $\widehat{\Gamma \backslash \mathbb{H}}$  sur  $\mathbb{P}$ .

.../...



#### 5.4. COURBES MODULAIRES.

5.4.1. *THEOREME.* ( $N \geq 1$ ) Sur  $\widehat{\Gamma(N) \backslash \mathbb{H}}$  (resp.  $\widehat{\Gamma_0(N) \backslash \mathbb{H}}$ ) existe une structure de courbe algébrique non singulière définie sur  $\mathbb{Q}(\zeta_N)$  (resp. sur  $\mathbb{Q}$ ) et "compatible" avec la notion de triplet (resp. de paire).

Cette courbe algébrique  $X(N)(\mathbb{C})$  (resp.  $X_0(N)(\mathbb{C})$ ) est appelée une courbe modulaire.

La 2e assertion signifie : si  $K$  est un sous-corps de  $\mathbb{C}$ , alors la classe de  $K$ -isomorphisme de  $(E, C)$  (resp. de  $(E, P, Q)$ ) contient un couple (resp. un triplet) défini sur  $K$  si et seulement si son image par  $\psi$  (resp. par  $\phi$ ) est dans  $K^M$ .

Démontrons d'abord un lemme :

5.4.2. Soit  $\Omega$  un corps algébriquement clos, contenant  $K$ , de degré de transcendance infini sur  $K$  (par exemple,  $\Omega = \mathbb{C}$  si  $K = \mathbb{Q}$  ou  $\mathbb{Q}(\zeta_N)$ ).

*LEMME.* Soient  $f_1, f_2, \dots, f_r$  des séries formelles à coefficients dans  $K$ , et  $I$  l'idéal des polynômes  $F$  de  $\Omega[X_1, X_2, \dots, X_r]$  tels que  $F(f_1, f_2, \dots, f_r) = 0$ . Alors  $I$  a un système générateur dans  $K[X_1, X_2, \dots, X_r]$ .

■ Soit  $\{c_i\}_i$  une base de  $\Omega$  sur  $K$ ; alors  $F = \sum_i c_i F_i$  où  $F_i \in K[X_1, X_2, \dots, X_r]$  et  $F_i(f_1, f_2, \dots, f_r) = 0$  pour tout  $i$ . Il suffit donc de considérer les composantes d'un système générateur de  $I$  dans  $\Omega[X_1, X_2, \dots, X_r]$  pour obtenir un système générateur de  $I$  dans  $K[X_1, X_2, \dots, X_r]$ . ■

5.4.3. Démonstration du théorème : ■ Comme  $j$  et  $f_{(a,b)}^{(i)}$  (resp.  $j$  et  $g_k^{(i)}$ ) sont développables en série entière de  $q^{1/N}$  à coefficients dans  $\mathbb{Q}(\zeta_N)$  (resp. dans  $\mathbb{Q}$ ), le plongement dans un espace projectif, joint au lemme (5.4.2) ci-dessus, montre la 1ère assertion.

Si  $(E, C)$  (resp.  $(E, P, Q)$ ) est défini sur  $K$ , alors  $\psi((E, C))$

.../...

(resp.  $\mathfrak{f}(E,P,Q)$ ) est dans  $K^m$ . Montrons la réciproque pour  $\psi$  (la démonstration pour  $\mathfrak{f}$  est analogue). Supposons que  $\psi((E,C)) \in K^M$ , et soit  $\sigma$  un  $K$ -automorphisme de  $\mathbb{C}$ . Alors  $\psi((E,C))^\sigma = \psi((E,C))$ ; or  $\psi$  est défini sur  $K$ , comme  $j$  et les  $g_k^{(i)}$ , donc  $\psi((E,C))^\sigma = \psi((E,C)^\sigma)$ . L'injectivité de  $\psi$  prouve alors que  $(E,C)$  et  $(E,C)^\sigma$  sont isomorphes sur  $\mathbb{C}$ . Notons  $\varphi_\sigma$  ce  $\mathbb{C}$ -isomorphisme de  $E$  sur  $E^\sigma$  tel que  $\varphi_\sigma(C) = \sigma(C)$ . Montrons que l'on peut supposer  $E$ , puis  $C$ , définis sur  $K$ .

Pour  $E$ : par hypothèse,  $j(E) \in K$ . Donc il existe une courbe  $E'$  définie sur  $K$  telle que  $j(E) = j(E')$ ; soit  $\psi_1$  le  $\mathbb{C}$ -isomorphisme qui existe alors de  $E$  sur  $E'$ , et  $C' = \psi_1(C)$ . Ainsi, quitte à remplacer  $(E,C)$  et  $(E^\sigma, \sigma(C))$  par  $(E',C')$  et  $(E',\sigma(C'))$ , on peut supposer  $E$  défini sur  $K$  et  $\varphi_\sigma \in \text{Aut}(E)$ .

Pour  $C$ , c'est une conséquence du lemme (5.4.4) ci-dessous. Enfin,  $X(N)$  (resp.  $X_0(N)$ ) étant muni d'une structure de groupe, si un point était singulier, tous les points le seraient, ce qui est impossible. ■

5.4.4. *LEMME.* (Serre) Soit  $K$  un corps de caractéristique quelconque. Tout élément de  $X(N)(K)$  (resp. de  $X_0(N)(K)$ ) possède un représentant  $(E,P,Q)$  (resp.  $(E,C)$ ) défini sur  $K$ .

Montrons le lemme pour  $X_0(N)$ .

■ Si  $j \neq 0$ ,  $12^3$ ,  $\text{Aut}(E) \simeq \mu_2$ , donc  $\mathfrak{f}_\sigma = \pm 1$ , et  $\sigma(C) = \pm C = C$ .

Si  $j = 0$  (resp.  $12^3$ ),  $\text{Aut}(E) \simeq \mu_{2i}$ , où  $i = 3$  (resp.  $i = 2$ ).

Montrons que  $\varphi : \sigma \mapsto \varphi_\sigma$  définit, par passage au quotient, un 1-cocycle de  $\text{Gal}(\bar{K}/K)$  à coefficients dans  $\text{Aut}(E)/\text{Aut}((E,C))$ : en effet,

$\varphi_{\rho_\sigma}(C) = \rho_\sigma(C) = (\rho\varphi_\sigma)(\rho C) = (\rho\varphi_\sigma)(\varphi_\rho(C))$  donc  $\varphi_{\rho_\sigma}^{-1}(\rho\varphi_\sigma)\varphi_\rho \in \text{Aut}((E,C))$ . Or

$\text{Aut}(E) \simeq \mu_{2i}$ , et  $\text{Aut}((E,C))$  contient  $\mu_2$ . Donc ou bien  $\text{Aut}((E,C)) = \text{Aut}(E)$

et  $C$  est invariant par tout  $\sigma$  de  $\text{Aut}(E)$ , ou bien  $\text{Aut}((E,C)) \simeq \mu_2$ ,

et alors  $\varphi$  se remonte en un 1-cocycle de  $\text{Gal}(\bar{K}/K)$  à coefficients dans

$\text{Aut}(E)$  grâce à la surjection:  $H^1(G, \mu_{2i}) \rightarrow H^1(G, \mu_{2i}/\mu_2) \rightarrow 0$  qui est en

réalité la surjection canonique:  $K^*/K^{*2i} \rightarrow K^*/K^{*i} \rightarrow 1$ . Mais d'après (1.3),

$H^1(G, \text{Aut}(E))$  classifie les courbes elliptiques sur  $K$ ,  $K$ -isomorphes à  $E$ , à  $K$ -isomorphisme près. Donc il existe une courbe elliptique  $E'$  sur  $K$ , et un  $K$ -isomorphisme de  $E$  sur  $E'$  tel que  $\varphi_\sigma = \sigma(f)^{-1}f$ . Alors le couple  $(E', f(C))$  est  $K$ -isomorphe à  $(E, C)$  et défini sur  $K$ , puisque  $\sigma(f(C)) = \sigma(f)(\sigma(C)) = \sigma(f)\varphi_\sigma(C) = f(C)$ . ■

5.4.5. La courbe modulaire  $X_1(N)$ . Notons  $\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$ . La surface de Riemann  $\widehat{\Gamma}_1(N) \backslash \mathbb{H}$ , notée  $Y_1(N)$ , classifie les classes de  $\mathbb{C}$ -isomorphisme de couples  $(E, \pm P)$ , où  $E$  est une courbe elliptique sur  $\mathbb{C}$ , et  $P$  un point d'ordre  $N$  de  $E$ . La compactifiée  $X_1(N) = \widehat{\Gamma}_1(N) \backslash \mathbb{H}$  de  $Y_1(N)$  peut être munie d'une structure de courbe algébrique non singulière définie sur  $\mathbb{Q}$ , et "compatible" avec la notion de couple  $(E, P)$ .

Ces propriétés se démontrent de manière analogue aux cas de  $X(N)$  et de  $X_0(N)$ . Correspondant aux inclusions :  $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \Gamma$ , nous avons les revêtements :

$$\widehat{\mathbb{H}} \longrightarrow X(N) \longrightarrow X_1(N) \longrightarrow X_0(N) \longrightarrow \widehat{\Gamma} \backslash \mathbb{H} = \mathbb{P}^1(\mathbb{C}).$$

5.4.6. Interprétation des pointes. Nous avons vu en (2.5.3) que les courbes de Tate  $E(q) = \mathbb{C}^*/q^{\mathbb{Z}}$  (pour  $|q| < 1$ ) permettent d'étudier la pointe  $\infty$  de  $\widehat{\Gamma} \backslash \mathbb{H}$ , en faisant tendre  $q$  vers 0.

De même, les courbes de Tate permettent d'étudier les pointes de  $X_0(N) = \widehat{\Gamma}_0(N) \backslash \mathbb{H}$  et de  $X_1(N) = \widehat{\Gamma}_1(N) \backslash \mathbb{H}$ . Nous supposons maintenant  $N$  premier pour simplifier cette étude.

Fixons dans  $\mathbb{C}$  une racine primitive  $N^{\text{ème}}$  de l'unité, notée  $\zeta$ , et une racine  $N^{\text{ème}}$  de  $q$ , notée  $q^{1/N}$ . Les  $N^2$  points d'ordre  $N$  de  $E(q) = \mathbb{C}^*/q^{\mathbb{Z}}$  sont alors les images (mod.  $q^{\mathbb{Z}}$ ) des points  $\zeta^a q^{b/N}$ , pour  $(a, b) \in (\mathbb{Z}/N\mathbb{Z})^2$ ; et les  $(N+1)$  sous-groupes cycliques d'ordre  $N$  de  $E(q)$  sont les groupes  $\mu_N = \langle \zeta \rangle$  et  $\langle \zeta^a q^{1/N} \rangle / q^{\mathbb{Z}}$ , pour  $a \in \mathbb{Z}/N\mathbb{Z}$ .

Lorsque  $q$  tend vers 0, la courbe de Tate  $E(q)$  "tend vers" la cubique dégénérée d'équation  $Y^2 - XY = X^3 - h_2X - h_3$  (cf. 2.6.3);

cette cubique a seulement  $N$  points d'ordre  $N$ , correspondant aux "limites" des points  $\zeta^a$  ( $a \in \mathbb{Z}/N\mathbb{Z}$ ), et un sous-groupe d'ordre  $N$ , correspondant à la "limite" de  $\mu_N$  : ceci permet d'étudier la pointe  $\infty$  de  $X_0(N)$ , et les pointes de  $X_1(N)$  dont l'image dans le revêtement  $X_0(N) \longrightarrow X_1(N)$  est la pointe  $\infty$ .

En faisant agir l'involution  $W_N$ , qui sera définie en (II.3.2), et qui transforme  $\infty$  en  $0$  sur  $X_0(N)$ , on est amené à étudier : la courbe de Tate  $E(q^N)$ , le sous-groupe d'ordre  $N$  :  $\langle q \rangle / q^{N\mathbb{Z}}$ , et les  $N$  points d'ordre  $N$  de la forme :  $q^a \pmod{q^{N\mathbb{Z}}}$ .