COURBES ELLIPTIQUES : FORMULAIRE

d'après J. Tate
mis au goût du jour par P. Deligne

1. Formules générales.

Dans ce formulaire, on appellera courbe de genre 1 sur un schéma de base S un morphisme propre et plat de présentation finie

$$p : E \longrightarrow S \quad ,$$

muni d'une section e contenue dans l'ouvert de lissité, dont les fibres géométriques sont des courbes réduites irréductibles de genre arithmétique 1 . Les fibres géométriques de p sont donc soit :

a) une courbe elliptique, i.e. une courbe propre, lisse et connexe de genre 1 ,

b) une droite projective dont on a identifié deux points distincts (cubique dans P_2 à point double ordinaire),

c) une droite projective dont on a identifié deux points infiniment voisins (cubique dans P_2 à singularité cuspidale).

On dira dans le cas a) (resp. b), c)) que la fibre est de type elliptique (resp. multiplicatif, resp. additif).

Si E est une courbe de genre 1 sur S , on définit un faisceau inversible ω sur S par la formule

$$\omega = e^* \Omega^1_{E/S} \quad .$$

La section e est un diviseur de Cartier relatif de E sur S ;

de plus, on vérifie fibre par fibre que

$$R^1 p_* \mathcal{O}(ne) = 0 \quad \text{pour} \quad n > 0 \quad .$$

Il en résulte, par Riemann-Roch, que pour $n > 0$, le faisceau $p_* \mathcal{O}(ne)$ est localement libre de rang n, et que sa formation commute à tout changement de base. La suite exacte de cohomologie fournit de plus une suite exacte

$$0 \longrightarrow p_* \mathcal{O}(ne) \longrightarrow p_* \mathcal{O}((n+1)e) \longrightarrow \omega^{\otimes -(n+1)} \longrightarrow 0 \quad (n > 0) \; .$$

Par ailleurs, $\mathcal{O}(e)$ étant localement libre de rang 1, on vérifie fibre par fibre, compte tenu de (SGA 1 X 1.2), que

$$\mathcal{O}_S \xrightarrow{\sim} p_* \mathcal{O}_E \xrightarrow{\sim} p_* \mathcal{O}(e) \quad .$$

En d'autres termes, les $p_* \mathcal{O}(me)$ pour $1 \leq m \leq n$ définissent une filtration de $p_* \mathcal{O}(ne)$, de gradué associé

$$(1.1) \qquad \mathrm{Gr} \; p_* \mathcal{O}(ne) = \sum_{\substack{i=0 \\ i \neq 1}}^{n} \omega^{\otimes -i} \quad .$$

Le morphisme p est d'intersection complète relative ; il en résulte que $Rp^! \mathcal{O}_S \in D^+(E)$ a un seul groupe de cohomologie non nulle, $R^1 p^! \mathcal{O}_S$, et que ce dernier est un faisceau inversible sur E ; on l'appelle le faisceau des différentielles régulières sur E et on le désigne par $\Omega^{reg}_{E/S}$. Là où p est lisse, on a $\Omega^{reg}_{E/S} = \Omega^1_{E/S}$. La dualité montre que $R^1 p_* \Omega^{reg}_{E/S}$ est isomorphe à $\mathcal{O}$, $p_* \Omega^{reg}_{E/S}$ est donc localement libre, de formation compatible à tout changement de base et, raisonnant fibre par fibre, on en déduit que

$$p_* \Omega^{reg}_{E/S} \xrightarrow{\sim} e^* \Omega^1_{E/S} = \omega ,$$

et que pour la flèche adjointe à la flèche inverse

$$p^* \omega \xrightarrow{\sim} \Omega^{reg}_{E/S} .$$

Les sections de $\Omega^{reg}_{E/S}$ ainsi associées aux sections de ω s'appellent les différentielles invariantes.

Soit π une section inversible de ω ; il existe, localement pour la topologie de Zariski, une base $(y, x, 1)$ de $p_* \mathcal{O}(3e)$ telle que l'image de y dans $\omega^{\otimes -3}$ soit $- \pi^{\otimes -3}$, que x appartienne à $p_* \mathcal{O}(2e)$, et que son image dans $\omega^{\otimes -2}$ soit π^{-2} . Si π' est une autre section inversible de ω , les bases correspondantes s'écrivent toutes, sous forme implicite (pour r, s, t convenables)

$$(1.2) \qquad \begin{cases} x = u^2 x' + r \\ y = u^3 y' + s u^2 x' + t \\ \pi' = u \pi \end{cases} .$$

Le faisceau $\mathcal{O}(3e)$ est très ample et $(x, y, 1)$ sont les coordonnées projectives d'un plongement de E dans P_2/S .

La courbe image vérifiera une équation

$$(1.3) \qquad y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 .$$

Pour vérifier l'existence et l'unicité de cette équation, on utilise (1.1), en regardant les deux membres de (1.3) comme des sections de $p_* \mathcal{O}(6e)$: en effet, $y^2 - x^3$ est dans $p_* \mathcal{O}(5e)$, xy dans $p_* \mathcal{O}(5e)$, x^2 dans $p_* \mathcal{O}(4e)$, y dans $p_* \mathcal{O}(3e)$, x dans $p_* \mathcal{O}(2e)$ et 1 dans $p_* \mathcal{O}$.

Si on pose

$$F(x,y) = y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6$$

la forme différentielle invariante définie par π s'écrit

$$\pi = dx/F_y = - dy/F_x \qquad \text{soit}$$

$$\pi = \frac{dx}{2y+a_1x+a_3} = \frac{dy}{3x^2+2a_2x+a_4-a_1y} \quad .$$

Réciproquement toute équation (1.3) est l'équation non homogène d'une courbe de genre 1 plongée comme une cubique dans P_2 et présentant un point d'inflexion en $(0,1,0)$ avec la droite de l'infini pour tangente d'inflexion.

On pose alors

(1.4) $\quad b_2 = a_1^2 + 4a_2 \qquad b_4 = a_1a_3 + 2a_4 \qquad b_6 = a_3^2 + 4a_6$

$$-b_8 = a_1\, a_3\, a_4 + a_4^2 - a_1^2\, a_6 - a_2\, a_3^2 - 4a_2\, a_6$$

$$d_6 = b_2\, b_4 - 18b_6 \qquad d_8 = b_2^2\, b_4 - 2^4\, 3\, b_4^2 + 2\;\; 3^2\, b_2\, b_6$$

On a

$$-4b_8 = b_4^2 - b_2\, b_6$$

$$12\, d_6 = c_6 + b_2\, c_4 \qquad\qquad - 12\, d_8 = c_4^2 + b_2\, c_6$$

$$(1.5)\qquad c_4 = b_2^2 - 24\, b_4 \qquad\qquad -c_6 = b_2^3 - 36\, b_2\, b_4 + 216\, b_6$$

$$\Delta = -b_2^2\, b_8 - 8\, b_4^3 - 27\, b_6^2 + 9\, b_2\, b_4\, b_6$$

$$= b_4^3 - 27\, b_6^2 + b_8\,(36\, b_4 - b_2^2) \quad .$$

Soient maintenant (x', y', π') reliés à (x, y, π) par (1.2). On aura :

$$(1.6)\qquad u\, a_1' = a_1 + 2s$$

$$u^2\, a_2' = a_2 - sa_1 + 3r - s^2$$

$$u^3\, a_3' = a_3 + ra_1 + 2t = F_t(r,t)$$

$$u^4\, a_4' = a_4 - sa_3 + 2a_2 r - (t+rs)a_1 + 3r^2 - 2st = -F(r,t) - s\, F_t(r,t)$$

$$u^6\, a_6' = a_6 + ra_4 + r^2 a_2 + r^3 - ta_3 - t^2 - rta_1 = -F(r,t)$$

$$(1.7)\qquad u^2\, b_2' = b_2 + 12\, r$$

$$u^4\, b_4' = b_4 + rb_2 + 6r^2 \quad \text{(équ. de discr. } c_4\text{)}$$

$$u^6\, b_6' = b_6 + 2r\, b_4 + r^2\, b_2 + 4r^3 \quad \text{(équ. de discr. } 16\,\Delta\text{)}$$

$$u^8\, b_8' = b_8 + 3r\, b_6 + 3r^2\, b_4 + r^3\, b_2 + 3r^4$$

$$u^6\, d_6' = d_6 + c_4\, r \qquad\qquad u^8\, d_8' = d_8 - c_6\, r$$

(1.8) $\qquad u^4 c_4' = c_4 \qquad u^6 c_6' = c_6 \qquad u^{12} \Delta' = \Delta$.

Les formules (1.8) expriment que la section $c_4\, \pi^{\otimes 4}$ (resp. $c_6\, \pi^{\otimes 6}$, resp. $\Delta\, \pi^{\otimes 12}$) du fibré $\omega^{\otimes 4}$ (resp. $\omega^{\otimes 6}$, $\omega^{\otimes 12}$) ne dépend pas du choix arbitraire de π, x et y .

2. Cas où 2 et 3 sont inversibles.

Lorsque 2 et 3 sont inversibles, on peut d'une et d'une seule façon choisir x et y (π étant donné) de sorte que dans l'équation (1.3.) on ait $a_1 = a_2 = a_3 = 0$. On a alors

(2.1) $$y^2 = x^3 + a_4 x + a_6 \quad , \text{ avec } \pi = dx/2y \quad ,$$

(2.2) $$c_4 = -2^4.3a_4 \quad , \quad c_6 = -2^5.3^3\, a_6 \quad , \quad \Delta = 2^4(-4a_4^3 - 27\, a_6^2) \quad .$$

Posant $Y = 2y$, $X = x$, on retombe sur la forme de Weierstrass

(2.3) $$Y^2 = 4\,X^3 - g_2\, X - g_3 \quad , \quad \text{avec} \quad \pi = d\,X/Y \quad , \quad \text{et}$$

(2.4) $$g_2 = -4\, a_4 = \frac{1}{12}\, c_4 \qquad g_3 = -4\, a_6 = \frac{1}{216}\, c_6$$

$$\Delta = g_2^3 - 27\, g_3^2 \qquad .$$

Proposition 2.5. Au dessus de $\mathrm{Spec}(\mathbb{Z}[2^{-1}, 3^{-1}]$, il existe un schéma de modules pour les courbes de genre un munies d'une forme différentielle invariante inversible. Ce schéma est

$$\mathrm{Spec}(\mathbb{Z}[2^{-1}\ , 3^{-1}][g_2, g_3] \quad ,$$

avec pour courbe universelle (en coordonnées non homogènes)

$$Y^2 = 4X^3 - g_2 X - g_3$$

et pour différentielle invariante $\pi = dX/Y$.

De plus, lorsque 2 et 3 sont inversibles, la donnée d'une forme différentielle invariante suffit à rigidifier une courbe de genre 1.

Il résulte aussitôt de (2.2) qu'on a

$$c_4^3 - c_6^2 = 1728\,\Delta \tag{2.6}$$

et cette formule, se réduisant à une identité algébrique, est valable en toute caractéristique.

3. Cas où 2 et c_4 sont inversibles.

Supposons que E soit une courbe de genre un sur une base S où 2 soit inversible. La forme différentielle invariante π étant donnée, on peut choisir x et y tels que dans (1.3) on ait $a_1 = a_3 = 0$. Les changements de coordonnées respectant cette condition s'obtiennent en faisant $u = 1$, $s = t = 0$ dans (1.2) .

On a donc

$$y^2 = x^3 + a_2 x^2 + a_4 x + a_6 \tag{3.1}$$

$$b_2 = 4a_2 \quad b_4 = 2a_4 \quad b_6 = 4a_6 \quad d_6 = 8(a_2 a_4 - 9a_6)$$

$$c_4 = 2^4(a_2^2 - 3a_4) \quad -c_6 = 2^6 a_2^3 - 2^5 3^2 a_2 a_4 + 2^5 3^3 a_6 \quad \text{et} \tag{3.2}$$

$$\Delta = 2^4\,\delta \quad ,$$

où δ est le discriminant du second membre de (3.1). Le discriminant δ étant invariant par translation, il suffit de vérifier cette identité algébrique pour 3 inversible et $a_2 = 0$.

Lorsque c_4 est inversible, un et un seul choix de x et y donne $d_6 = 0$; i.e. $a_2 a_4 - 9 a_6 = 0$. On a, lorsque cette condition est remplie,

(3.3) $$- c_6 = 2^6(a_2^3 - 3^3 a_6) \qquad \Delta = 2^6(- a_2^3 a_6 - a_4^3 + 2.3^3 a_6^2)$$

et

(3.4)
$$a_2 c_4 = - 2^{-2} c_6$$

$$a_4 c_4^2 = - 2^2 3^2 \Delta$$

$$a_6 c_4^3 = c_6 \Delta \quad .$$

Il suffit de vérifier ces identités en caractéristique 0 , auquel cas la troisième est le produit des deux premières, puisque $d_6 = 0$.

Proposition 3.5. Au dessus de $\mathrm{Spec}(\mathbb{Z}[2^{-1}])$, il existe un schéma de module pour les courbes de genre un munies d'une forme différentielle invariante inversible et telles que c_4 soit inversible. Ce schéma est

$$\mathrm{Spec}(\mathbb{Z}[2^{-1}][a_2, a_4, a_6, (a_2^2 - 3 a_4)^{-1}]/(a_2 a_4 - 9 a_6))$$

avec pour courbe universelle (en coordonnées non homogène)

$$y^2 = x^3 + a_2 x^2 + a_4 x + a_6$$

et pour différentielle invariante $\pi = dx/2y$.

De plus, sous ces hypothèses, la donnée d'une forme différentielle invariante suffit à rigidifier une courbe.

4. Cas où 2 est nilpotent et c_4 inversible.

Lorsque $2 = 0$, la forme différentielle ne suffit plus jamais à rigidifier une courbe de genre un. Lorsque c_4 est inversible et 2 nilpotent, donc a_1 inversible, en changeant le choix de π, x, y on peut trouver une équation

$$(4.1) \qquad y^2 + xy = x^3 + a_2 x^2 + a_6 \qquad \pi = \frac{dx}{x + 2y} \quad .$$

Les autres choix de x et y donnant lieu à une telle équation s'obtiennent en faisant, dans (1.2)

$$(4.2) \qquad r = t = 0 \qquad u = 1 + 2s$$

et on aura

$$(4.3) \qquad \begin{aligned} u^2 a_2' &= a_2 - s - s^2 \\ u^6 a_6' &= a_6 \end{aligned}$$

et modulo 2

$$(4.4) \qquad c_4 = 1 \qquad c_6 = 1 \qquad \Delta = a_6 \quad .$$

5. Cas où $c_4 = 0$, $p = 2$ ou $p = 3$

a) $p = 3$

En caractéristique 3 , lorsque l'équation est mise sour forme

(3.1), $c_4 = 0$ si et seulement si $a_2^2 = 0$. Supposons qu'on ait même $a_2 = 0$

$$(5.1) \qquad y^2 = x^3 + a_4 x + a_6 \qquad \pi = a_4^{-1}\, dy = dx/2y$$

$$c_4 = c_6 = 0 \qquad \Delta = -a_4^3 \quad .$$

Les autres systèmes (π, x, y) donnant une équation de cette forme s'obtiennent en faisant $s = t = 0$ dans (1.2) et

$$(5.2) \qquad \begin{aligned} u^4 a'_4 &= a_4 \\ u^6 a'_6 &= a_6 + r a_4 + r^3 \end{aligned} \quad .$$

b) $p = 2$

En caractéristique 2, on a $c_4 = a_1^4$. Supposons qu'on ait $a_1 = 0$; π étant donnée, on peut alors choisir x et y tels que (1.3) soit

$$(5.3) \qquad y^2 + a_3 y = x^3 + a_4 x + a_6 \qquad \pi = \frac{dx}{a_3} = dy/_{x^2 + a_4}$$

$$b_2 = b_4 = 0 \qquad b_6 = a_3^2 \qquad b_8 = a_4^2 \qquad \Delta = a_3^4 \qquad c_4 = c_6 = 0 \; .$$

Les autres systèmes (π, x, y) donnant une équation de cette forme s'obtiennent en faisant $r = s^2$ dans (1.2) et

$$(5.4) \qquad \begin{aligned} u^3 a'_3 &= a_3 \\ u^4 a'_4 &= a_4 + s a_3 + s^4 \\ u^6 a'_6 &= a_6 + s^2 a_4 + t a_3 + s^6 + t^2 \end{aligned} \quad .$$

6. Applications.

Proposition 6.1. *Si E est une courbe de genre un sur un corps algébriquement clos, E est de type elliptique (resp. multiplicatif, resp. additif) si et seulement si $\Delta \neq 0$ (resp. $\Delta = 0$ et $c_4 \neq 0$, resp. $\Delta = c_4 = 0$).*

a) Lorsque la caractéristique $p \neq 2$, la première assertion résulte de la troisième formule (3.2). Lorsque $p = 2$ et $c_4 \neq 0$, on vérifie aussitôt que la différentielle de (4.1) ne s'annule qu'en $(0, 0)$, et Δ est elliptique si et seulement si $\Delta = a_6 \neq 0$. Pour $p = 2$ et $c_4 = 0$, on raisonne de même sur (6.2).

b) Lorsque $p \neq 2$, il résulte de (3.2) que $\Delta = c_4 = 0$ si et seulement si le deuxième membre de (3.1) a toutes ses racines égales, ce qui caractérise le cas additif.

c) Lorsque $p = 2$, $\Delta = 0$, $c_4 \neq 0$, la partie principale de (4.1) en $(0, 0)$ est $y^2 + xy + a_2x^2 = 0$, ce qui correspond à un point double à tangentes distinctes.

d) Lorsque $p = 2$, $\Delta = 0$, $c_4 = 0$, la partie principale de (6.2) en $(0, 0)$ est $y^2 + a_4x + a_6 = 0$, ce qui correspond à une singularité cuspidale.

Soit alors E une courbe de genre un sur une base S, sans fibre de type additif. Puisque Δ et c_4 ne sont jamais simultanément nuls, et sont respectivement des sections de $\omega^{\otimes 12}$ et $\omega^{\otimes 4}$, on définit une section j de P_1/S par la formule

(6.2) $$j = c_4^3 / \Delta = 1728 + c_6^2 / \Delta \ .$$

Proposition 6.3. *Soient* E *et* E' *deux courbes de genre un sur* S , *sans fibre additive* .

(I) *Isom*(E, E') *est représentable, fini et non ramifié sur* S

(II) *si* $j_E = j_F$, *la projection de* *Isom*(E, E') *sur* S *est surjective*

(III) *si* $j_E = j_F$ *ne prend pas les valeurs* 0 *et* 1728, *Isom*(E, E') *est un revêtement étale de rang* 2 *de* S .

Donnons-nous E et E' par des équations (1.3) et (1.3)'. Se donner un isomorphisme entre E et E' revient à se donner u, r, s et t, vérifiant les équations (1.6), donc aussi (1.7) et (1.8), u devant de plus être inversible. Par hypothèse, localement sur S, c_4 ou Δ est inversible (6.1), et de même c'_4 ou Δ' l'est. Localement sur S , les équations (1.8) sont donc des équations de dépendance intégrale pour u et u^{-1}, les équations $(1.7)_6$ ou $(1.7)_8$ des équations de dépendance intégrale pour r et enfin $(1.6)_6$ (resp. $(1.6)_2$) est une équation de dépendance intégrale pour t (resp. s). Ceci prouve que *Isom*(E, E') est représentable par un schéma affine fini sur S ; il est même non ramifié car les courbes considérées n'ont pas d'automorphismes infinitésimaux (respectant l'origine).

Lorsque 2 est inversible sur S , l'assertion (III) résulte de l'énoncé plus précis.

Proposition 6.4. *Soient* E *et* E' *deux courbes de genre un sur* S , sans fibre additive, munies de formes différentielles invariantes π et π', et de même invariant modulaire. On suppose que 2 , c_4 et c_6 sont inversibles, i.e. que 2^{-1} , $1/j$ et $1/j-1728$ sont des sections de S . Alors, le schéma Isom(E, F) s'identifie au schéma défini par l'équation

$$\lambda^2 = c_4 c_6'/c_6 c_4' \quad .$$

En vertu de (3.6), se donner (E, π) revient à se donner a_2 , a_4 et a_6 vérifiant $a_2 a_4 - 9 a_6 = 0$, et un isomorphisme de E sur E' est décrit par λ tel que (E π) soit isomorphe à (E',λ π'), i.e. par λ vérifiant

$$(6.4.1) \qquad a_2' = \lambda^2 a_2 \qquad a_4' = \lambda^4 a_4 \qquad a_6' = \lambda^6 a_6 \quad .$$

Par hypothèse, $j = j'$, de sorte que (c_4^3 , c_6^2 , Δ) est proportionnel à $(c_4'^3 , c_6'^2 , \Delta')$, et que $\mu = c_4 c_6'/c_6 c_4'$ vérifie

$$(6.4.2) \qquad c_4' = \mu^2 c_4 \qquad c_6' = \mu^3 c_6 \qquad \Delta' = \mu^6 \Delta \quad .$$

En vertu de (3.4), on a alors

$$a_2' = \mu a_2 \qquad a_4' = \mu^2 a_4 \qquad a_6' = \mu^3 a_6 \quad .$$

De plus, d'après (3.4) encore, localement, soit a_2 , soit a_4 et a_6 sont inversibles, de sorte que (6.4.1) équivaut à $\lambda^2 = \mu$.

Pour prouver (III) en général, on peut se ramener à supposer S noethérien, et supposer soit 2 inversible (cas traité en (6.4)), soit

2 nilpotent, ce qui permet de mettre la courbe sous la forme (4.1)

$$y^2 + xy = x^3 + a_2 x + a_6$$

et un isomorphisme d'une telle courbe sur une autre est décrit par s vérifiant (4.3) pour $u = 1 + 2s$. Lorsque $j = j'$, la première de ces équations

$$(1 + 2s)^2 a_2' = a_2 - s - s^2$$

définit un revêtement étale de degré deux, et elle implique la seconde ; pour le voir, on se ramène à supposer $a_2 = a_2'$ et on remarque que d'après (4.4)

$$1/j = a_6 + 2 R(a_2, a_6)$$

pour une fraction rationnelle R.

Pour vérifier (II) dans les cas non couverts par (III), on peut supposer que S est le spectre d'un corps algébriquement clos et que $c_4 = 0$ ou $c_6 = 0$, i.e. que $j = 0$ ou $j = 1728$. Soit p la caractéristique du corps,

a) $p \neq 2, 3$: on met la courbe sous la forme (2.1) ; si $c_4 = 0$ (resp. $c_6 = 0$) on aura $a_4 = 0$ (resp. $a_6 = 0$) et on peut par homothétie transformer la courbe en la courbe type

$$(6.5) \qquad y^2 = x^3 + 1 \qquad (\text{si } c_4 = 0)$$

$$(6.6) \qquad y^2 = x^3 - x \qquad (\text{si } c_6 = 0)$$

b) $p = 3$: on met la courbe sour la forme (6.1) ; résolvant (6.2) pour $a_4' = 1$ et $a_6' = 0$, on met la courbe sous la forme type

(6.7) $$y^2 = x^3 - x \qquad (\text{si } c_4 = c_6 = 0)$$

c) $p = 2$: ici, on met la courbe sour la forme (6.3) et on résoud (6.4) avec $a_3 = 1$, $a_4 = a_6 = 0$ pour obtenir la forme type

(6.8) $$y^2 + y = x^3 \qquad (\text{si } c_4 = c_6 = 0) .$$

Pour compléter le tableau, reste à décrire les automorphismes des courbes elliptiques.

Proposition 6.9. Soit E une courbe de genre un sur une base S, sans fibre additive

(I) Si c_4 et c_6 sont inversibles, les seuls automorphismes de E sont l'identité et la symétrie.

(II) Si 2 et 3 sont inversibles, l'application canonique

(6.6.) $$\underline{\mathrm{Aut}}(E) \longrightarrow G_m$$

donnée par l'action sur les différentielles invariantes, est une immersion fermée.

(III) Si 2 et 3 sont inversibles, et $c_4 = 0$ (resp. $c_6 = 0$) l'image de (6.6) est μ_6 (resp. μ_4).

Supposons maintenant que S soit le spectre d'un corps

(IV) Si $3 = c_4 = c_6 = 0$, $\mathrm{Aut}(E)$ est géométriquement isomorphe au produit semi-direct (non commutatif) de $\mathbb{Z}/(4)$ par $\mathbb{Z}/(3)$, et l'image de (6.6) est μ_4 .

(V) Si $2 = c_4 = c_6 = 0$, $\mathrm{Aut}(E)$ est géométriquement d'ordre 24, et l'image de (6.6) est μ_3.

<u>Preuve</u> : (I) D'après (6.3), il n'y a en effet pas plus de deux automorphismes.

(II) et (III) Lorsque les courbes sont mises sous la forme (2.1), il résulte de (2.5) que les automorphismes sont décrits parleur action sur π et que $\lambda \in G_m$ défini un automorphisme si et seulement si

$$c_4 = \lambda^4 c_4 \qquad \text{et} \qquad c_6 = \lambda^6 c_6 \quad ,$$

d'où les assertions.

(IV) Si la courbe est mise sous forme (6.1), les automorphismes sont donnés par (1.2) : $x' \rightsquigarrow x$, pour $s = t = 0$ et

$$\begin{cases} u^4 = 1 \\ r^3 + ra_4 + a_6(1 - u^2) = 0 \end{cases}$$

et la loi de composition par

$$(u', r') \quad (u, r) = (u\, u' \, , \, u'^2 r + r')$$

Lorsque la courbe est mise sous forme (6.7), ces équations se réduisent à $u \in \mu_4$ et $r \in F_3$.

(V) Si la courbe est mise sous forme (6.3), les automorphismes sont donnés par (1.2) : $x' \rightsquigarrow x$, pour $r = s^2$ et

$$\begin{cases} u^3 = 1 \\ s^4 + sa_3 + a_4(1 - u) = 0 \\ t^2 + ta_3 + s^6 + s^2 a_4 = 0 \end{cases}$$

et la loi de composition par

$$(u', s', t') \circ (u, s, t) = (u\,u', u's + t', u'^3 t + t' + u'^2 rs') .$$

Lorsque la courbe est mise sous forme (6.8), ces équations se réduisent à

$$u \in \mu_3 \qquad s \in \mathbb{F}_4 \qquad t^2 + t = s^3 \quad (= 0 \text{ ou } 1 \text{ selon que } s = 0 \text{ ou } s \neq 0) .$$

7. Anneau des formes modulaires entières.

On appelle forme modulaire entière de poids n une loi qui à chaque courbe de genre un sur une base S associe une section de $\omega^{\otimes n}$, et ce de façon compatible au changement de base. Il reviendrait au même de se limiter aux courbes sans fibres additives.

Proposition 7.1. *L'anneau des formes modulaires entières est engendré sur $\mathbb{Z}$ par c_4, c_6 et Δ soumis à la seule relation*

$$(7.2.) \qquad c_4^3 - c_6^2 = 1728\,\Delta \quad .$$

Appliquant la définition à la courbe (1.3), on voit qu'une forme modulaire entière de poids n s'exprime comme polynome de poids n en les a_i. Pour 2 et 3 inversibles, il résulte de 2.5 que ces formes sont les polynomes en c_4 et c_6, et en particulier que c_4, c_6 et Δ ne satisfont pas d'autres relations que (7.2). Reste à prouver que si un polynome en c_4, c_6 et Δ est identiquement nul en caractéristique 2 (resp. 3), alors il est divisible par 2 (resp.3) dans $\mathbb{Z}[c_4, c_6, \Delta]/c_4^3 - c_6^2 - 1728\,\Delta$, ce qui signifie qu'il est divisible par $c_4^3 - c_6^2$ dans $\mathbb{Z}/(2)[c_4, c_6, \Delta]$ (resp. $\mathbb{Z}/(3)[c_4, c_6, \Delta]$). Cela résulte de la structure de l'anneau des formes modulaires de caractéristique 2 (resp. 3).

<u>Proposition</u> 7.2. (I) <u>L'anneau des formes modulaires de caractéristique</u> 2 <u>est</u> $\mathbb{Z}/(2)[a_1, \Delta]$, <u>et</u> $c_4 = a_1^4$, $c_6 = a_1^6$

(II) <u>L'anneau des formes modulaires de caractéristique</u> 3 <u>est</u> $\mathbb{Z}/(3)[b_2, \Delta]$, et $c_4 = b_2^2$, $c_6 = - b_2^3$.

Tout d'abord, il résulte de $(1.6)_1$ et $(1.7)_2$ que a_1 (resp. b_2) est une forme modulaire de caractéristique 2 (resp. 3).

En caractéristique 2, cherchons tout d'abord les formes modulaires relatives aux seules courbes telles que a_1 soit inversible. Ces courbes se mettent sous forme (cf. (4.1))

$$y^2 + a_1 xy = x^3 + a_2 x^2 + a_6 \qquad \pi = \frac{dx}{a_1 x}$$

et, compte tenu de (4.3), on voit que ces formes s'écrivent

$$a_1^{-n} P(a_1, a_6) \qquad \text{pour } P \text{ isobare, ou encore}$$

$$a_1^{-m} Q(a_1, \Delta)$$

et cela garde un sens pour $a_1 = 0$, $\Delta \neq 0$ si et seulement si on avait en fait affaire à un polynome en a_1 et Δ.

En caractéristique 3, raisonnant de même d'abord sur les courbes telles que c_4 soit inversible, et remarquant que $d_6 = 0$ équivaut alors à $a_4 = 0$ dans (3.1), on voit que toute forme modulaire s'écrit

$$b_2^{-n} P(b_2 , \Delta) \quad \text{pour } P \text{ isobare} \quad ,$$

et que cette forme modulaire est définie aussi pour $j = 0$ si et seulement si elle s'écrit comme polynome en b_2 et Δ .