

# SÉMINAIRE DELANGE-PISOT-POITOU. THÉORIE DES NOMBRES

GILLES CHRISTOL

## **Introduction aux formes modulaires. Formes modulaires $p$ -adiques**

*Séminaire Delange-Pisot-Poitou. Théorie des nombres*, tome 14, n° 2 (1972-1973),  
exp. n° G4 et G8, p. G1-G7

[http://www.numdam.org/item?id=SDPP\\_1972-1973\\_\\_14\\_2\\_A15\\_0](http://www.numdam.org/item?id=SDPP_1972-1973__14_2_A15_0)

© Séminaire Delange-Pisot-Poitou. Théorie des nombres  
(Secrétariat mathématique, Paris), 1972-1973, tous droits réservés.

L'accès aux archives de la collection « Séminaire Delange-Pisot-Poitou. Théorie des nombres » 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/>

INTRODUCTION AUX FORMES MODULAIRES .

FORMES MODULAIRES p-ADIQUES

par Gilles CHRISTOL

1° Modèle de Weierstrass des courbes elliptiques sur  $\mathbb{C}$  : Si  $\omega_1$  et  $\omega_2$  sont deux nombres complexes tels que  $\text{Im}(\omega_1/\omega_2) > 0$ , le corps des fonctions méromorphes de période  $\omega_1$  et  $\omega_2$  est engendré par  $X = \wp(u)$  et  $Y = \wp'(u)$ ,  $X$  et  $Y$  étant liés par la relation

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

avec

$$\begin{aligned} \wp(u) &= u^{-2} + \Sigma' [(u - n\omega_1 - m\omega_2)^{-2} - (n\omega_1 + m\omega_2)^{-2}] \\ &= u^{-2} + \sum_{k=2}^{\infty} (2k-1) G_{2k} u^{2k-2} \\ G_{2k} &= \Sigma' (n\omega_1 + m\omega_2)^{-2k} \end{aligned}$$

$g_2 = 60 G_4$   $g_3 = 140 G_6$ , les  $\Sigma'$  indiquant une sommation sur tous les couples d'entiers  $(m, n) \neq (0, 0)$ . Le groupe  $\mathbb{C}/\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$  se trouve ainsi muni d'une structure algébrique (liée à sa structure analytique de surface de Riemann). Nous noterons  $E(\omega_1, \omega_2)$  un tel groupe, et l'appellerons courbe elliptique. Ce sont les seules surfaces de Riemann ayant une structure de groupe.

2°  $\omega = dX/Y = du$  est, à constante multiplicative près, l'unique forme différentielle holomorphe sur  $E(\omega_1, \omega_2)$ . L'unicité et l'existence d'une telle forme équivalent à  $E$  de genre 1.

3°  $(\omega_1, \omega_2)$  et  $(\omega'_1, \omega'_2)$  définissent la même courbe elliptique si, et seulement si,  $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$  et  $\mathbb{Z}\omega'_1 + \mathbb{Z}\omega'_2$  sont identiques, c'est-à-dire si

$$\begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \text{ avec } a, b, c, d \in \mathbb{Z} \text{ et } ad - bc = 1 ,$$

l'ensemble des matrices  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ , vérifiant ces propriétés, forme le groupe

$$\text{SL}(2, \mathbb{Z})/\{\pm 1\}$$

(le  $\pm 1$  venant de la conservation de l'orientation).

4° Si  $\lambda \in \mathbb{C}$ , la transformation (holomorphe)  $u \rightarrow \lambda u$  définit, par passage au quotient, un isomorphisme de  $E(\omega_1, \omega_2)$  et  $E(\lambda\omega_1, \lambda\omega_2)$ . On vérifie que ce sont les seuls isomorphismes analytiques entre deux courbes elliptiques.  $E(\omega_1, \omega_2)$  est donc ainsi toujours en bijection avec un  $E(z, 1)$  avec  $z \in \mathbb{H}$ ,  $\mathbb{H}$  étant le

demi-plan de Poincaré  $\text{Im}(z) > 0$ . D'après 3°,  $E(z', 1)$  et  $E(z, 1)$  seront isomorphes si, et seulement si,  $z' = (az + b)/(cz + d)$  pour  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma = \text{SL}(2, \mathbb{Z})$ . On a donc une bijection :

$$H/\Gamma \leftrightarrow \{\text{courbes elliptiques à isomorphisme près}\}.$$

5° Dans l'isomorphisme défini en 4°, les éléments liés à  $E$  se transforment comme suit :

$$\begin{aligned} \omega & \rightarrow \lambda \omega \\ g_2 & \rightarrow \lambda^{-4} g_2 \\ g_3 & \rightarrow \lambda^{-6} g_3 \end{aligned}$$

Il en résulte que  $j = ((12)^3 g_2^3)/(g_2^3 - 27g_3^2)$  est un invariant dans les isomorphismes de courbes elliptiques.  $j$  définit même une bijection :

$$\mathbb{C} \xleftrightarrow{j} \{\text{courbes elliptiques à isomorphisme près}\}.$$

Remarque. - On peut vérifier que  $g_2^3 \neq 27g_3^2$  pour une courbe elliptique (sinon la courbe a un point double, et est de genre 0).

6°  $H/\Gamma$  n'est pas compact, on le compactifie en ajoutant un point "à l'infini", noté  $\{i\infty\}$ . Une fonction modulaire est une application des courbes elliptiques (à isomorphisme près) dans les complexes qui devient méromorphe sur le compactifié de  $H/\Gamma$  par la bijection du 4°. C'est donc une fonction méromorphe sur  $H \cup \{i\infty\}$  (pour la méromorphie en  $\{i\infty\}$  voir 8°) vérifiant :

$$f\left(\frac{az + b}{cz + d}\right) = f(z) \quad \text{pour tout } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z})$$

le compactifié de  $H/\Gamma$  est une surface de Riemann de genre 0, le corps des fonctions modulaires est donc  $\mathbb{C}(j)$ .

7° Une forme modulaire de poids  $k$  est une application de l'ensemble des couples  $(E, \omega)$  formé d'une courbe elliptique et d'une forme différentielle holomorphe associée (voir 2°) dans les complexes, homogène de poids  $-k$  en  $\lambda$  (de sorte que  $f(E, \omega) \omega^k$  soit un invariant de  $E$ ), holomorphe si on la considère comme fonction sur  $H \cup \{i\infty\}$  (c'est-à-dire si on se restreint aux courbes  $E(z, 1)$ ). En tant que fonction sur  $H$ , une forme modulaire vérifie la condition :

$$f\left(\frac{az + b}{cz + d}\right) = (cz + d)^{-k} f(z).$$

Les formes modulaires sont les polynômes en  $g_2$  et  $g_3$ , homogènes pour le poids (poids de  $g_2 = 4$ , poids de  $g_3 = 6$ ).

8° Les formes ou fonctions modulaires, considérées comme fonctions sur  $H$ , sont périodiques, de période 1 (en prenant  $a = b = d = 1$ ,  $c = 0$ ), elles se développent donc en série de Fourier, c'est-à-dire en série de Laurent en  $q = \exp 2i\pi z$ ,

$q$  est l'uniformisante locale en  $\{i \infty\}$  ; être méromorphe en  $\{i \infty\}$  signifiera n'avoir qu'un nombre fini de termes d'exposant négatif dans son développement ; être holomorphe signifiera n'avoir aucun terme d'exposant négatif dans ce développement. On a, par exemple,

$$j = \frac{1}{q} + 744 + \sum c(n) q^n ,$$

$$\Delta = (2\pi)^{12} (g_2^3 - 27g_3^2) = q \prod_1^\infty (1 - q^n)^{24} = \sum \tau(n) q^n ,$$

$$G_{2k} = 2\zeta(k) E_{2k} ,$$

$$E_k = 1 - \frac{2k}{b_k} \sum_n \sigma_{k-1}(n) q^n , \quad \sigma_k(n) = \sum_{d|n} d^k ,$$

où  $b_k$  est le  $k$ -ième nombre de Bernoulli :

$$\zeta(1 - k) = \frac{-b_k}{k} = \frac{2\zeta(k)(k-1)!}{(2\pi i)^k} .$$

9° Opérateurs de Hecke :  $E$  définit un recouvrement d'ordre  $p$  de  $E_p$  si le réseau, qui définit  $E_p$ , contient celui qui définit  $E$  comme sous-réseau d'ordre  $p$ . Si  $p$  est un nombre premier, on trouve qu'il n'y a que  $p+1$  courbes  $E_p$  dont  $E$  soit un recouvrement d'ordre  $p$ .  $f$  étant alors une forme modulaire, on définit l'opérateur  $T_p$  par

$$T_p(f)(E, \omega) = \frac{1}{p} \sum f(E_p, \omega) ,$$

où la forme différentielle  $\omega$  est définie sur  $E_p$  par restriction à partir de  $E$ .  $T_p(f)$  est alors une forme de même poids que  $f$ .

Si on part de la courbe  $E(z, 1)$ , les  $E_p$  sont les courbes  $E(z, 1/p)$ ,  $E(\frac{z+i}{p}, 1)$  pour  $0 \leq i < p$ . En considérant alors  $f$  comme une fonction de  $z$ , on trouve

$$p T_p(f)(z) = \sum_{i=0}^{p-1} f\left(\frac{z+i}{p}\right) + p^k f(pz) ,$$

par suite, en notant  $a(n)$  les coefficients de Fourier de  $f$ , et  $b(n)$  ceux de  $T_p(f)$ , on trouve

$$b(n) = a(np) + p^{k-1} a(n/p) \quad (a(s) = 0 \text{ si } s \notin \mathbb{Z}) .$$

10° D'après ce qui précède, si une forme est vecteur propre de tous les  $T_p$ , les valeurs propres associées sont les  $a(p)$ . On remarque que les  $E_k$  sont effectivement vecteurs propres de tous les  $T_p$ , de plus, PETERSSON, en munissant d'un produit scalaire les formes de poids  $k$  nulles à l'infini, a montré que l'on peut trouver une base de l'espace des formes de poids  $k$  (espace de dimension finie) formée de vecteurs propres pour tous les  $T_p$ .

11° Si on fait la transformation "naïve"

$$\sum_{n=0}^{\infty} a(n) q^n \leftrightarrow \sum_{n=1}^{\infty} a(n)/n^s ,$$

un vecteur propre de tous les  $T_p$  devient une série de Dirichlet, munie d'un pro-

duit d'Euler

$$\sum_{n=1}^{\infty} a(n) n^{-s} = \prod_p \frac{1}{1 - a(p) p^{-s} + p^{k-1-2s}} .$$

Supposons donnés une suite de  $a(n) = O(n^c)$  pour un  $c > 0$  (ce qui est le cas si les  $a(n)$  sont les coefficients de Fourier d'une forme modulaire), et un nombre  $k > 0$  ; posons

$$\begin{aligned} \varphi(s) &= \sum_{n=1}^{\infty} a(n) n^{-s} , \\ \Phi(s) &= (2\pi)^{-s} \Gamma(s) \varphi(s) , \\ f(z) &= \sum_{n=0}^{\infty} a(n) \exp 2\pi inz , \end{aligned}$$

alors les conditions (A) et (B) suivantes sont équivalentes :

(A)  $\Phi(s) + \frac{a(0)}{s} + \frac{\pm a(0)}{k-s}$  se prolonge en une fonction entière bornée sur toute bande verticale, et satisfait

$$\Phi(k-s) = \pm \Phi(s) .$$

(B)  $f(-1/z) = \pm (z/i)^k f(z)$  .

Ce théorème peut se résumer en disant qu'à une forme modulaire on associe une fonction vérifiant une certaine équation fonctionnelle.

Par exemple, à  $G_k$  correspond  $\zeta(s) \zeta(s+1-k)$  .

12° Sous-groupe de congruence : le sous-groupe de  $E(\omega_1, \omega_2)$  des points d'ordre  $p$  est formé des points  $(r\omega_1 + s\omega_2)/p$  pour  $0 \leq r < p$  ,  $0 \leq s < p$  .

On définit ainsi un isomorphisme de ce groupe dans  $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$  . Cet isomorphisme n'est pas indépendant du choix du couple  $(\omega_1, \omega_2)$  qui représente la courbe elliptique, il est cependant conservé dans l'isomorphisme défini au 4°. On peut alors considérer des formes plus générales, qui sont des fonctions sur les courbes elliptiques, munies d'un isomorphisme du groupe de leurs points d'ordre  $p$  dans  $(\mathbb{Z}/p\mathbb{Z})^2$  . En se ramenant à la variable  $z = \omega_1/\omega_2$  , on trouve que de telles formes vérifient

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{-k} f(z) ,$$

pour  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z})$  et  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{p}$  (le groupe de telles matrices se note  $\Gamma(p)$  ).

Parmi ces formes, il est intéressant de considérer celles qui ne dépendent que du choix d'une des deux projections des points d'ordre  $p$  sur  $\mathbb{Z}/p\mathbb{Z}$  , c'est-à-dire qui sont des fonctions sur les courbes elliptiques munies d'un sous-groupe d'ordre  $p$  du groupe des points d'ordre  $p$  (noyau de la projection ci-dessus).

Pour la variable  $z$  et le sous-groupe engendré par  $\frac{\omega_2}{p}$  , on trouve ainsi les formes qui sont conservées par  $\Gamma_0(p)$  c'est-à-dire par les matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z})$$

telles que  $c = 0 \pmod{p}$ . En particulier, l'ensemble des fonctions (formes de poids 0) invariantes par  $\Gamma_0(p)$  est le corps  $C(j, j')$  avec  $j(z) = j(pz)$ .

13° Formes modulaires p-adiques : Avec les notations du 8°, l'équation du modèle de Weierstrass de la courbe devient

$$Y^2 = 4X^3 - \frac{(2\pi)^4}{12} E_4 X - \frac{(2\pi)^6}{216} E_6,$$

$$E_4 = 1 + 240 \sum \sigma_3(n) q^n,$$

$$E_6 = 1 - 504 \sum \sigma_5(n) q^n.$$

$E_4$  et  $E_6$  sont donc à coefficients entiers. On peut alors "améliorer" le résultat du 7° :  $p$  étant un nombre premier différent de 2 et 3, un nombre est dit  $p$ -entier s'il est dans  $\mathbb{Q}$ , et si son dénominateur n'est pas divisible par  $p$ .

Une forme modulaire a des coefficients de Fourier  $p$ -entiers si, et seulement si, c'est un polynôme (isobare) à coefficients  $p$ -entiers en  $E_4$  et  $E_6$ . En particulier, la forme  $E_{p-1}$  de poids  $p-1$  s'exprime comme un polynôme  $A(E_4, E_6)$ .

SWINNERTON-DYER, d'autre part, a prouvé qu'un polynôme à coefficients  $p$ -entiers, en  $E_4$  et  $E_6$ , représente une forme modulaire à coefficients de Fourier nuls, modulo  $p$ , si, et seulement si, il est divisible, modulo  $p$ , par le polynôme  $A-1$ . Comme conséquence de ce résultat, on peut démontrer que deux formes modulaires, à coefficients de Fourier  $p$ -entiers, égales modulo  $p$ , ont des poids égaux modulo  $p^{\alpha-1}(p-1)$ . (On commence par montrer que si  $f = g \pmod{p}$ , alors  $f = gA^h$ , puis on vérifie que  $h$  doit être divisible par  $p^{\alpha-1}$ ).

On dira qu'une série  $f = \sum_{n=0}^{\infty} a_n q^n$ , à coefficients  $a_n$  dans  $\mathbb{Z}_p$ , est une forme modulaire  $p$ -adique si, pour tout  $\alpha$ , il existe une forme modulaire  $f_\alpha$  de poids  $k_\alpha$  à coefficients  $p$ -entiers, telle que  $f = f_\alpha$  modulo  $p$ ; le poids de  $f$  sera un élément de

$$\lim_{\alpha \rightarrow \infty} \mathbb{Z}/(p-1)p^\alpha \mathbb{Z} = \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p,$$

défini par la limite de  $k_\alpha$ .

14° Si  $f$  est une forme modulaire de poids  $k$  pour le groupe  $\Gamma_0(p)$ , à coefficients  $p$ -entiers,  $f$  est une forme modulaire  $p$ -adique de poids l'image de  $k$  dans le groupe  $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$ . Pour démontrer cela, on pose

$$\text{Tr}(f) = \sum_{\gamma} 1(\cdot z + \cdot)^{-k} f(\gamma z),$$

où  $\gamma$  parcourt un système de représentants de  $\Gamma_0(p) \backslash \text{SL}(2, \mathbb{Z})$ ; on peut vérifier que  $\text{Tr}(f)$  est une forme pour  $\text{SL}_2$ ; d'autre part, on note

$$E_{p-1}^*(z) = E_{p-1}(z) - p^{p-2} E_{p-1}(pz),$$

il est facile de vérifier que  $E_{p-1}^*$  est une forme pour  $\Gamma_0(p)$ , et est congrue à 1 modulo  $p$ . La suite  $\text{Tr}(f E_{p-1}^* p^\alpha)$  fournit alors une suite de formes de poids  $k + p^\alpha(p-1)$  qui tend  $p$ -adiquement vers  $f$ .

15° Si  $K$  est un corps quelconque, un point  $(x, y, z)$  de l'espace projectif à deux dimensions sur  $K$  appartient à la courbe elliptique  $E(K, g_2, g_3)$  (ou plus simplement  $E(K)$ ),  $g_2$  et  $g_3$  appartenant à  $K$ ,  $g_2 \neq 27g_3$ , si

$$y^2 z = 4x^3 - g_2 xz^2 - g_3 z^3 .$$

On peut munir l'ensemble des points de  $E(K)$  d'une loi de groupe abélien d'élément neutre le point  $(0, 1, 0)$ , appelé point à l'infini (on définit cette loi par : Trois points ont une somme nulle s'ils sont alignés).

Si  $K$  est algébriquement clos, de caractéristique 0., le sous-groupe de  $E(K)$ , des points d'ordre  $p$ , est d'ordre  $p^2$ .

$K$  sera un corps valué (valuation réelle), d'anneau de valuation  $\mathfrak{A}$ , d'idéal de valuation  $\mathfrak{M}$ , de corps des restes  $k$  que l'on suppose de caractéristique  $p$  ( $\geq 5$ ), on note  $\bar{a}$  l'image d'un élément  $a$  de  $\mathfrak{A}$  dans  $k$ . On appellera réduite de  $E(K, g_2, g_3)$ , la courbe  $E(k, \bar{g}_2, \bar{g}_3)$ . Si la courbe obtenue est de genre 0 ( $g_2 - 27g_3$  dans  $\mathfrak{M}$ ), on dit qu'il y a mauvaise réduction ; si elle est de genre 1, il y a bonne réduction.

Un point de  $E(K)$  ayant toujours une représentation  $(x, y, z)$  avec  $x, y, z$  dans  $\mathfrak{A}$ , et non tous dans  $\mathfrak{M}$ , se réduit en  $(\bar{x}, \bar{y}, \bar{z})$ .

16° Considérons le sous-groupe  $M$  de  $E(K)$  des points donnant par réduction le point à l'infini de  $E(k)$ , ce sont ceux tels que  $v(y) < \inf(v(x), v(z))$  ; pour ces points, la fonction sur  $E(K)$ ,  $t = x/y$ , prend des valeurs dans  $\mathfrak{M}$  ; inversement, pour tout  $t$  de  $\mathfrak{M}$ , il existe un point, et un seul,  $(x, y, z)$  dans  $M$  tel que  $t = x/y$ .

Si  $P$  et  $Q$  sont des points de  $M$ , on a donc

$$t(P + Q) = F(t(P), t(Q)) = \sum a_{n,m} t(P)^n t(Q)^m$$

On montre que les  $a_{n,m}$  sont dans  $A$ , et que la série formelle  $F(X, Y)$  vérifie

$$(a) \quad F(X, Y) = X + Y + \text{termes de degré } \geq 2 \text{ en } X \text{ et } Y$$

$$(b) \quad F(X, F(Y, Z)) = F(F(X, Y), Z),$$

qui traduit l'associativité du groupe.

$$(c) \quad F(X, Y) = F(Y, X),$$

qui traduit la commutativité.

Une série formelle à 2 variables, vérifiant (a), (b), (c), est appelée groupe formel à coefficients dans  $\mathfrak{A}$ .

17° A partir d'un groupe formel, on définit par récurrence les séries formelles (à une variable) à coefficients dans  $A$  :

$$[n]_{\mathbb{F}} = F(X, [n-1]_{\mathbb{F}} X) \quad [1] X = X ;$$

en particulier, si  $P$  est dans  $M$ , il est clair que

$$[n]_{\mathbb{F}} t(P) = t(nP)$$

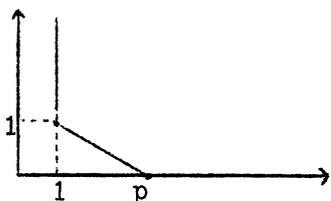
(avec des notations évidentes).

Il est clair que la série formelle

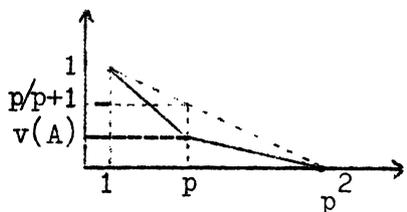
$$\overline{F}(X, Y) = \sum \overline{a}_{n,m} X^n Y^m$$

définit un groupe formel, à coefficients dans  $k$  ; or on sait que pour un tel groupe formel,  $[p]_{\mathbb{F}} X$  est une série en  $X^p$ , commençant, pour un certain  $h$ , appelé hauteur, par un terme en  $X^{p^h}$ . Il en résulte que  $[p]_{\mathbb{F}} = AX^p + \dots$  modulo  $\mathfrak{M}$ ,  $A$  est appelé invariant de Hasse de la courbe  $E(K)$ .

18° Nous supposons maintenant que  $K$  est algébriquement clos, et de caractéristique  $0$ . Les points d'ordre  $p$  de  $E(K)$ , qui sont dans  $M$ , correspondent (d'après (d'après 15° et 16°) aux racines de l'équation  $[p]_{\mathbb{F}} X$  qui sont dans  $\mathfrak{M}$ . Nous allons donc tracer le polygone de Newton de cette série (dont le premier terme est  $px$ ), deux cas se présentent :



Si  $v(A) = 0$ , on voit que la série  $[p]_{\mathbb{F}} X$  a  $p$  racines de valuation positive. Ces  $p$  points (dont le point à l'infini correspondant à  $t = 0$ ) forment un sous-groupe canonique des points d'ordre  $p$  de  $E(K)$ . La courbe  $E(k)$  a alors  $p$  points d'ordre  $p$ .



Si  $v(A) > 0$ ,  $E(K)$  ayant  $p^2$  point d'ordre  $p$ , le groupe formel  $F$  ne peut être que de hauteur  $2$  (et donc  $E(k)$  n'a que l'origine comme point d'ordre  $p$ ). On peut tout de même vérifier que  $E(K)$  conserve un sous-groupe "canonique" si  $v(A) < p/(p+1)$ , cette

limite est d'ailleurs "non améliorable".

19° On peut montrer que  $A$  est le coefficient de  $x^{p-1}$  dans le polynôme

$$(4x^3 - g_2 x - g_3)^{(p-1)/2}.$$

Si on considère la courbe  $E(\mathbb{Q}[[q]])$ ,  $E_4/12$ ,  $E_6/216$ , il est facile de voir que  $A$  est une forme modulaire (c'est-à-dire un polynôme à coefficients entiers en  $E_4$  et  $E_6$ ), de poids  $p-1$  ; on peut voir que  $A = 1$  modulo  $p$ , et par conséquent (miracle des notations) que l'invariant de Hasse  $A$  est le polynôme  $A$  du 13°, c'est-à-dire  $E_{p-1} \pmod{p}$ . Dans ce cas,  $A$  est bien inversible, et la courbe est munie d'un sous-groupe canonique ; les fonctions sur  $(E, \omega)$  sont donc aussi des fonctions sur  $(E, \omega, \text{ sous-groupe de point d'ordre } p)$ , ce qui explique les résultats du 14°.