Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Gilles Christol

Généralités sur les courbes elliptiques

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 10, n° 2 (1968-1969), exp. n° G3, p. G1-G4

<http://www.numdam.org/item?id=SDPP_1968-1969__10_2_A10_0>

Groupe d'Etude de
THÉORIE DES NOMBRES
Année 1968/69, n° 3, 4 p.

6 janvier 1969

GÉNÉRALITÉS SUR LES COURBES ELLIPTIQUES

par Gilles CHRISTOL

Définitions.

On appelle courbes elliptiques, les variétés algébriques irréductibles, de dimension 1 (ou courbes), non singulières, de genre 1 .

Soit k un corps algébriquement clos. Nous appellerons espace projectif, à r dimensions, $P_r(k)$, l'ensemble $(k^{r+1} - 0)/k^*$, muni de la topologie de Zariski (pour laquelle les fermés sont les ensembles formés des zéros communs à une famille de polynômes de $k(X_0 , \dots , X_r)$ qui sont stables modulo k^*) et de son corps des fonctions : ensemble des R/S , où R et S sont des polynômes homogènes de même degré. On appelle anneau local en P , O_P (P étant un point de $P_r(k)$), le sous-anneau du corps des fonctions défini par la condition $S \neq 0$ en P .

Une variété projective sera un sous-ensemble fermé de $P_r(k)$, muni de la structure induite : topologie de Zariski induite et anneau $O_{P,X}$, induit par les fonctions de O_P (en tant que fonctions sur X). Elle sera dite irréductible, si elle n'est pas la réunion de deux fermés (ou variétés) de $P_r(k)$; pour une variété irréductible, tous les $O_{P,X}$ ont le même corps des quotients, noté $k(X)$.

La dimension de la variété est le degré de transcendance de $k(X)/k$; $k(X)$ sera donc, pour une courbe, une extension de type fini de k , et de degré de transcendance 1 ; on dira que deux telles courbes sont isomorphes, si elles ont le même corps des fonctions (cette définition n'est valable que pour les courbes). Les $O_{P,X}$ sont alors des anneaux noethériens d'idéal maximal les fonctions nulles en P , et ne possédant pas d'autre idéal premier (on a alors une courbe).

La courbe est non singulière, si les idéaux $O_{P,X}$ peuvent être engendrés par un seul élément : un tel élément est appelé uniformisante locale en P . Il s'en suit que les $O_{P,X}$ sont des anneaux de valuation discrète, valuation que l'on notera v_P (ce sont les seuls qui contiennent k , cette condition est équivalente à "variété projective" : c'est ce que l'on appelle variété complète).

On appelle diviseur, un élément du groupe abélien libre, de base les points de X . Si $D = \sum n_P.P$, alors $\deg(D) = \sum n_P$. On pose $D \geqslant 0$, si, $\forall P$, $n_P \geqslant 0$. A une fonction de X , $f \in k(X)^*$, on associe le diviseur $(f) = \sum v_P(f).P$. On vérifie alors que $\deg((f)) = 0$, les diviseurs qui sont de cette forme sont les diviseurs principaux.

L'ensemble des différentielles est universel pour les propriétés suivantes : D_X est un $k(X)$-espace, muni d'une application k-linéaire $k(X) \xrightarrow{d} D_X$ vérifiant $d(xy) = xdy + ydx$, et tel que les dx engendrent D_X .

Pour une courbe, D_X est de dimension 1 sur $k(X)$. Pour une étude locale, nous prenons alors une uniformisante locale t en P ; si $w \in D_X$, nous avons $w = fdt$, alors nous posons : $v_P(w) = v_P(f)$, et nous associons à w le diviseur $(w) = \sum v_P(w).P$. Une différentielle sera dite de première espèce, si $\deg(w) \geqslant 0$.

Le genre de la courbe sera la dimension sur k de l'espace des différentielles de première espèce : pour une courbe elliptique, il n'existe, à une constante près, qu'une seule telle forme, notée Π .

Quelques propriétés. - Soit alors $\ell(D)$ la dimension sur k de l'espace des fonctions vérifiant $(f) \geqslant -D$ (si $\deg(D) < 0$, $\ell(D) = 0$, et si $D = 0$, $\ell(D) = 1$), et soit K le diviseur d'une forme différentielle. On a alors

$$\ell(D) - \ell(K - D) = \deg(D) + 1 - g \qquad \text{(théorème de Riemann-Roch)} ,$$

où g est le genre de la courbe considérée. En particulier, en faisant $D = K$, on trouve $\deg(K) = 2g - 2$ (on a $\ell(K) = g$, par définition).

Nous choisissons alors un point o sur notre courbe elliptique ([1]). On vérifie immédiatement que : $\ell(0) = 1$; $\ell(o) = 1$, $\ell(2.o) = 2$; $\ell(3.o) = 3$ (il suffit de remarquer que si $\deg(D) \geqslant 1$, $\deg(K - D) < 0$, d'où $\ell(D) = \deg(D)$). Il s'en suit qu'il n'existe que les constantes qui ont un pôle simple au plus en o , qu'il existe une seule fonction x (resp. y) à une constante près (à une constante et à ax près) qui possède un pôle double (triple) en o .

Nous prenons une uniformisante locale t en o , définie par $\Pi = dt + \ldots$, puis x , défini par $x = t^2 + \ldots$, enfin $y = -t^3 + \ldots$; x et y sont alors liés par une relation du type :

$$(1) \qquad y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 .$$

On voit facilement que x et y engendrent alors $k(X)$, ce qui veut dire que notre courbe est isomorphe (au sens du début) à la courbe définie par les zéros de (1) dans $P_2(k)$; nous les confondrons dorénavant ; trois points seront alignés, s'ils sont les trois zéros de la fonction $(ax + by + c)$ (qui a trois zéros, puisque un pôle triple en o ; si le pôle n'est que double, on compte un zéro en o).

([1]) Ne pas confondre le diviseur 0 correspondant à $n_P = 0$, $\forall P$, et le diviseur o où le point o de X est compté une fois.

On peut alors munir notre courbe d'une loi de groupe (dont o est l'élément neutre) qui vérifie $M_1 + M_2 + M_3 = 0$ s'ils sont alignés (les courbes elliptiques sont les seules courbes pour lesquelles ceci est possible).

Après manipulation (on change Π en $u^{-1}\Pi$, x en $u^2 x + b$, et y en $u^3 y + ax + c$), on trouve, si k est de caractéristique différente de 2 ou 3, $y^2 = x^3 + a_4 x + a_6$; ce qui nous conduit à la forme de Weierstrass :

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

avec alors

$$\Pi = \frac{dX}{Y} = \frac{2dY}{12X^2 - g_2} \ ;$$

on vérifie en effet facilement que cette forme est de valuation nulle en tout P (en o, c'est évident), sauf si $\Delta = g_2^3 - 27g_3^2 = 0$, auquel cas la courbe n'est pas non singulière (comme on le voit si $k = R$, par exemple).

Δ dépendant de Π (si on change Π en $u\Pi$, Δ est changé en $u^{12}\Delta$), nous construisons $j = 1728 g_2^3/\Delta$ [2] ; alors deux courbes sont isomorphes si, et seulement si, elles ont le même j.

Cas complexe. - Une courbe elliptique est isomorphe au tore C/Γ, où Γ est un réseau (w_1 , w_2), muni du corps des fonctions méromorphes ; une fonction particulière étant

$$X = \wp(z) = 1/z^2 + \Sigma' \{ \frac{1}{(z + mw_1 + nw_2)^2} - \frac{1}{(mw_1 + nw_2)^2} \}$$

qui est doublement périodique ; si nous posons $\wp'(z) = Y$, on sait que

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

où on a

$$g_2 = \Sigma' 60(mw_1 + nw_2)^{-4} \qquad \text{et} \qquad g_3 = 140\ \Sigma'(mw_1 + nw_2)^{-6} \ .$$

On retrouve tout ce qui précède avec $\Pi = dz$ (z est bien une uniformisante locale en 0), la loi de groupe étant l'addition complexe.

j ne dépendant que de la courbe à un isomorphisme près, j sera invariant si (w_1 , w_2) et (w_1' , w_2') définissent le même réseau : si $w_1' = aw_1 + bw_2$ et

---

[2] 1728 pour des raisons de normalisation.

$w_2' = cw_1 + dw_2$, avec a , b , c , d entiers et vérifiant $ad - bc = \pm 1$ (pour pouvoir inverser la matrice). D'autre part, deux réseaux homothétiques définissent la même courbe (par $f(z) \to f(az)$), on peut donc se ramener à $w_1 = 1$ et (quitte à changer d'indice) $w_1/w_2 = t$ avec $\mathrm{Im}(t) > 0$, donc j ne dépend en fait que de $t \in H$ (demi-plan supérieur) ; on vérifie immédiatement alors que $j(t) = j\left(\frac{at + b}{ct + d}\right)$, si $ad - bc = 1$ et a , b , c , d entiers. On peut, en outre, vérifier que sur H modulo le groupe Γ qui laisse j invariant, j prend une fois, et une seule, toute valeur complexe (et donc ne peut vérifier d'autres relations), et enfin que toute fonction vérifiant une relation du même type que j est une fraction rationnelle en j . Une telle étude est le point de départ de la théorie des fonctions automorphes.

(Texte reçu le 9 octobre 1969)

Gilles CHRISTOL
Ass. Fac. Sc. Paris
27 rue Charles Fourier
75 - PARIS 13