Introduction aux courbes elliptiques *

Olivier Ruatta †

30 Mars 1999

1 Intoduction

Les courbes elliptiques sont aux confluents de plusieurs disciplines traditionnelles mathématiques :

1. la géométrie algèbrique,
2. la théorie des groupes,
3. la théorie des nombres.

Plus récemment, la cryptologie a commencé à employer les propriétés de ces objets pour créer des protocoles basés sur le problème du logarithme discret. Ainsi leurs études, dans le cadre des applications à l'informatique ce sont elles beaucoup développée ces dernières années. J'ai choisi un exposé que j'espère compréhensible, ne suivant pas tout à fait l'ordre historique. Mais la théorie des courbes elliptiques est maintenant très vaste, et il existe de multiples façons de l'exposer. Historiquement, elles ont été introduites pour l'études des équations diophantiennes et des courbes algèbriques.
Personnellement, j'ai choisi un exposé qui permet d'introduire un minimum de matériel mathématique pour arriver aux courbes sur un corps fini, qui est le coeur de beaucoup de protocoles cryptographiques modernes, et qui me permettra d'expliquer les idées pour calculer le nombre de points sur une courbe elliptique sur un corps fini.

Dans tout cet exposé, tous les corps sont supposés commutatifs.

2 Espace projectif $P^2(k)$

Soit k un corps. On considère $E = k^2 - (0,0)$, et une relation d'équivalence $\Re$ sur E : $(x,y)\,\Re\,(x',y')$ si et seulement si il existe $\lambda \in k^*$ telle que $(x,y) = \lambda\,(x',y')$. On définit alors $P^1(k) = E/\Re$. $P^1(k)$ peut être

*Aspects arithmétiques et algorithmiques

†Ce travail est soutenu par moi-même au sein d'un projet très très local de mon organisation "qui laisse à désirer", dans le but de faire un exposé au niveau D.E.A. dans un groupe d'étude au sein de l'équipe D.S.A du C.M.I (Marseille).

vu comme l'ensemble des droites vectorielles k^2. On a un système de coordonnées sur $P^1(k)$, si $(x,y) \in E$, on note $[x:y]$ sa classe dans $P^1(k)$ et si $y \neq 0$, on a $[x:y] = [x/y:1]$. On définit une addition $[a:1]+[b:1] = [\frac{a+b}{2}:1]$. On remarque que toutes les droites sont représentées sauf la droite d'équation $y=0$, qui est représentées par $[1:0]$ qu'on appelle point à l'infini. On a $P^1(k) = k \sqcup \infty$. On réitère l'opération sur $k^3 - (0,0)$, on définit ainsi un ensemble $P^2(k)$ appelé plan projectif. On note $P_{z=0}$ le plan d'équation $z=0$. Toute droite non incluse dans $P_{z=0}$ a un representant de la forme $[a:b:1]$ qui est la classe du point d'intersection de cette droite avec le plan affine $P_{z=1} = \{(x,y,1) \in k^3 - \{(0,0,0)\}\}$. Dans $P^2(k)$ le projeté du plan $P_{z=0}$ est isormorphe à $P^1(k)$ et le projeté de $P_{z=1}$ est isomorphe à k^2. On a donc :

$$P^2(k) = k^2 \sqcup P^1(k)$$

Le projeté du plan $P_{z=0}$ est appelé droite à l'infini.

La géométrie projective est le cadre naturel de la géométrie algèbrique , dont je vais maintenant décrire quelques idées.

3 Géométrie projective - théorème de Bezout

3.1 Polynômes homogènes

Définition 1 *Soit k un corps, un polynôme $P \in k[x,y,z]$ est homogène de degré d si chacun de ses monômes est de degré d. On note $k[x,y,z]_d$ l'ensemble des polynômes homogènes de degré d.*

Proposition 1 *Soit k un corps, $P \in k[x,y,z]$ est homogène de degré d si et seulement si $P(tx,ty,tz) = t^d P(x,y,z)$.*

Preuve : Si $P \in k[x,y,z]_d$ alors $P(x,y,z) = \sum_{i+j+l=d} a_{i,j,l} x^i y^j z^l$ et donc $P(tx,ty,tz) = \sum_{i+j+l=d} a_{i,j,l} t^i x^i t^j y^j t^l z^l = t^d \sum_{i+j+l=d} a_{i,j,l} x^i y^j z^l$ et finalement $P(tx,ty,tz) = t^d P(x,y,z)$. Supposons que $P \in k[x,y,z]$ soit tel que $P(tx,ty,tz) = t^d P(x,y,z)$. On peut écrire P comme une somme de polynômes homogènes. Soit l le degré de P, alors $P = \sum_{i=0}^{l} P_i$ où $P_i \in k[x,y,z]_i$ est la somme des monômes de P de degré i. Alors $P(tx,ty,tz) = \sum_{i=0}^{l} P_i(tx,ty,tz) = \sum_{i=0}^{l} t^i P_i(x,y,z)$ et donc $P_i = 0$ sauf pour $i=d$. Donc $P = P_d$ est donc homogène de degré d. ♣

Corollaire 1 (Formule d'Euler) *Si P est un polynôme homogène de degré d sur k, alors :*

$$dP = x\frac{\partial P}{\partial x} + y\frac{\partial P}{\partial y} + z\frac{\partial P}{\partial z}.$$

Preuve : On a $P(tx, ty, tz) = t^d P(x, y, z)$, or $\frac{d}{dt}t^d P(x, y, z) = d * t^{d-1} P(x, y, z)$ et $\frac{d}{dt} P(tx, ty, tz) = x\frac{\partial}{\partial x} P(tx, ty, tz) + y\frac{\partial}{\partial y} P(tx, ty, tz) + z\frac{\partial}{\partial z} P(tx, ty, tz)$. On obtient la formule en posant $t = 1$. ♣

Définition 2 *On note $k[x, y, z]^l_{hom}$ l'ensemble des polynômes homogènes de degré inférieur à l, et $k[x, y, z]_{hom}$ celui des polynômes homogènes.*

Proposition 2 *$k[x, y, z]^l_{hom}$ est un k espace vectoriel et $k[x, y, z]_{hom}$ est une k-algèbre.*

Proposition 3 *Soit $P \in k[x, y, z]_{hom}$ alors si $P = RQ$ dans $k[x, y, z]$ alors R et $Q \in k[x, y, z]_{hom}$.*

3.2 Courbes algèbriques

Définition 3 *Soit $P \in k[x, y, z]_d$, on définit alors la courbe $C_k(P) = \{[x : y : z] \in P^2(k) : P(x, y, z) = 0$. On dit que la courbe est de degré d.*

Définition 4 *Une courbe $C_k(P)$ est dite irréductible si P est irréductible dans $k[x, y, z]_d / k^*$.*

Définition 5 *Si $P = P_1^{e_1} \dots P_l^{e_l}$ est la décomposition de P en facteurs irréductibles, alors $C_k(P_1), \dots, C_k(P_l)$ sont appelées les composantes irréductibles de $C_k(P)$.*

3.3 Résultants

Soient P de degré p et Q de degré q deux polynômes homogènes.

Définition 6 *On définit*

$$\Phi_{P,Q} : \left\{ \begin{array}{ccc} k[x, y, z]^q_{hom} \times k[x, y, z]^p_{hom} & \to & k[x, y, z]^{p+q}_{hom} \\ (U, V) & \longmapsto & UP + VQ \end{array} \right.$$

Proposition 4 *L'application $\Phi_{P,Q}$ est une application linéaire.*

Théorème 1 (Lemme de Bezout) $\ker \Phi_{P,Q} \neq 0$ *si et seulement si P et Q ont un facteur commun non constant.*

Preuve : Si $P = RP'$ et si $Q = RQ'$, avec R polynôme non constant. On pose alors $U = Q'$ et $V = -P'$, on a $\Phi_{P,Q}(U,V) = UP + VQ = Q'RP' - P'RQ' = 0$. Et alors $\ker \Phi_{P,Q} \neq 0$. Réciproquement, il existe U avec $deg(U) < deg(Q)$ et V avec $deg(V) < deg(P)$ tels que $UP + VQ = 0$. On décompose P en facteur premier, comme $deg(V) < deg(P)$, on a un facteur de P qui n'est pas un facteur de V et donc ce facteur divise Q et finalement les polynômes P et Q ont un facteur commun non constant. ♣

Définition 7 *On défini le résultant de deux polynômes P et Q, noté $Res(P,Q)$ ainsi :*

$$Res(P,Q) = \det(\Phi_{P,Q}).$$

Théorème 2 *Soient P et Q deux polynômes , alors P et Q ont un facteur commun si et seulement si $Res(P,Q) = 0$.*

3.4 Théorème de Bezout

Dans cette partie, le corps k est un corps infini et K est sa clotûre algèbrique.

Théorème 3 (Théorème de Bezout faible) *Soient $C_k(P)$ de degré p et $C_k(Q)$ de degré q, alors si $\#(C_k(P) \cap C_k(Q)) \geq pq + 1$, alors $C_k(P)$ et $C_k(Q)$ ont une composante irréductible en commun.*

Idée de la preuve : Si $\#(C_k(P) \cap C_k(Q)) \geq p + q + 1$, alors P et Q ont plus d'une racine commune. On considère $Res(x,y)$ en regardant le résultant comme un polynôme homogène, en effet :

$$P(x,y,z) = A_0(x,y)z^p + \ldots + A_p(x,y),$$

$$Q(x,y,z) = B_0(x,y)z^q + \ldots + B_q(x,y),$$

et comme les A_i et B_i sont des polynômes homogènes de degré i en x et y, $Res(P,Q)$ peut être vu comme un polynôme homogène en x et y de degré pq. Donc $Res(x,y)$ est un polynôme homogène de degré pq avec $pq + 1$ racines. Ainsi $Res(x,y) = 0$. La réciproque est facile. ♣

Définition 8 *La courbe $C_k(P)$ est dite absolument irréductible si P est irréductible dans $K[x,y,z]$.*

Propriété 1 *Soient P et Q deux polynômes homogènes et $[a:b:c] \in C_k(P) \cap C_k(Q)$ alors $[a:b:c]$ est un point singulier de $C_k(P,Q)$.*

Preuve :

$$\frac{\partial}{\partial x}(P,Q) = \frac{\partial Q}{\partial x}P + \frac{\partial P}{\partial x}Q$$

Or $P(a,b,c) = Q(a,b,c)$ et donc $\frac{\partial}{\partial x}(P,Q)|_{[a:b:c]} = 0$. On procède de même avec les variables y et z. ♣

Corollaire 2 *Si $C_K(P)$ est sans point singulier, alors $C_k(P)$ est absolument irréductible.*

4 Courbes elliptiques

Définition 9 *On dit qu'une cubique $C_k(P)$ de degré 3, définit une courbe elliptique si et seulement si $C_k(P)$ est sans point singulier et $C_k(P) \neq \emptyset$.*

4.1 Applications rationnelles

Définition 10 *Soient $C_k(P)$ et $C_k(Q)$ deux courbes définies sur k et soit trois polynômes de $k[x,y,z]$: $A(x,y,z)$,$B(x,y,z)$, $C(x,y,z)$. On dira que A, B et C définissent une application rationnelle $\phi : C_k(P) \to C_k(Q)$, définie sur k, si $\forall [a:b:c] \in C_K(P)$ alors $\phi(a,b,c) = [A(a,b,c), B(a,b,c), C(a,b,c)] \in C_K(Q)$.*

Définition 11 *Soient $C_k(P)$ et $C_k(Q)$ deux courbes et $\phi : C_k(P) \to C_k(Q)$ une application rationnelle sur k. On dira que ϕ est une application birationnelle s'il existe une application rationnelle $\psi : C_k(Q) \to C_k(P)$ telles que $\phi \circ \psi$ et $\psi \circ \phi$ soient des applications identités sauf pour un nombre fini de points.*

Définition 12 *Deux courbes elliptiques sont dites équivalentes si elles sont birationnellement équivalentes.*

4.2 Loi de groupe sur une courbe elliptique

On a vu qu'une courbe elliptique est donnée par une équation de degré 3 irréductible, et une droite est donné par un équation de degré 1, donc comme la droite ne peut pas être une composante irréductible de la courbe alors leur intersection est composée d'au plus trois points. Je vais juste développer quelques outils pour énoncer un théorème beaucoup plus précis, qui nous dira qu'en un certains sens, l'intersection d'une droite et d'une courbe elliptique est exactement un ensemble de trois points. Ceci nous permettra de definir une loi de groupe sur une courbe elliptique que nous décrirons d'abord d'un point de vu géométrique.

4.2.1 Multiplicité - théorème de Bezout

Soient P et $Q \in k[x,y,z]_{hom}$, on va définir la multiplicité d'un point d'intersection de $C_k(P)$ et $C_k(Q)$. On choisit un système de coordonnées homogène tel que $M \in C_k(P) \cap C_k(Q)$ ait pour coordonnées

$[0 : 0 : 1]$. Soit $P_b(x, y) = P(x, y, 1)$ et $Q_b(x, y) = Q(x, y, 1)$, et soit $O_M = \{\frac{U(x,y)}{V(x,y)} : U, V \in K[x, y]$ et $V(0, 0) \neq 0\}$ l'anneau local associé à P. Alors $dim_K \frac{O_M}{(P_b,Q_b)}$ ne dépend que de M et de P et Q.

Définition 13 *On appelle multiplicité de l'intersection de* $C_k(P)$ $C_k(Q)$ *en* M*, et on note* $I(M, C_k(P), C_k(Q)) = dim_K \frac{O_M}{(P_b,Q_b)}$.

Théorème 4 *Soient* $C_k(P)$ *et* $C_k(Q)$ *deux courbes de* $P^2(K)$ *de degré* p *et* q *respectivement, sans composante commune dans* $P^2(k)$*, alors on a :*

$$\sum_{M \in P^2(k)} I(M, C_k(P), C_k(Q)) = nm.$$

Pour le cas qui nous intéresse c'est-à-dire l'intersection d'une droite et d'une cubique irréductible, comme la droite ne peut pas partager de composante avec la cubique, deux cas peuvent se présenter :

1. Tous les points d'intersection sont simples (i.e. tous les points ont une multiplicité 1),
2. il y a un point d'intersection de multiplicité 2 et un de multiplicité 1.

C'est grâce à ce dernier résultat qu'on va pouvoir expliciter la structure de groupe sur les courbes elliptiques.

4.2.2 Groupe de Poincaré

Soit O un point quelconque de la courbe elliptique $C_k(P)$, et soient A et B dans $C_k(P)$, on note $< AB >$ la droite définie par A et B. Soit $R = C_k(P) \cap < AB >$ alors on définit $A \oplus_O B =< OR > \cap C_k(P)$ la somme relativement à O.

Théorème 5 1. *La loi d'addition attachée au choix de l'origine* O *est une loi de groupe abélien sur* $C_k(P)$.

2. *Si* O *et* O' *sont deux points de* $C_k(P)$*, et si* $\oplus_O$ *et* $\oplus'_O$ *sont les lois correspondantes, alors les groupes* $(C_k(P), \oplus_O)$ *et* $(C_k(P), \oplus'_O)$ *sont isomorphes dans un automorphisme birationnel défini sur* k.

4.2.3 Courbe donnée par une équation de Weierstrass

Il existe de multiples manières de se donner une courbe elliptique. La plus usitée est celle qui consiste à se donner l'équation de la courbe sous une forme bien particulière dite forme de Weierstrass.

Définition 14 *On appelle courbe de Weierstrass la donnée d'une équation :*

$$W : y^2 + a_1yx + a_3y - \left(x^3 + a_2x^2 + a_4x + a_6\right)$$

et d'un point $O = [0 : 1 : 0]$ correspondant à un point de la courbe associé à l'équation dite homogénéisé de W :

$$W_{\#} : y^2z + a_1yxz + a_3yz^2 - \left(x^3 + a_2x^2z + a_4xz^2 + a_6z^3\right)$$

.

Si la courbe $C_k\left(W_{\#}\right)$ est lisse on parle de cubique de Weierstrass. Dans ce cas on a des formules explicites pour calculer la somme de deux points de la courbe : Si $P \in P_{z=1}$, alors si $P = [x : y : 1]$, on a $-P = [x : -y - a_1x - a_3 : 1]$. Si $P_1 \oplus P_2 = P_3$ avec $P_i = [x_i : y_i : 1]$, on pose :

1. si $x_1 \neq x_2$: $\lambda = \frac{x_2-x_1}{y_2-y_1}$ et $\nu = \frac{y_1x_2-y_2x_1}{x_2-x_1}$,
2. si $x_1 = x_2$ et $P_1 = P_2 : \lambda = \frac{3x_1{}^2+a_2x_1+2a_4-a_1y_1}{2y_1+a_1x_1+a_3}$ et $\nu = \frac{-x_1{}^3+a_4x_1+2a_6-a_3-a_3y_1}{2y_1+a_1x_1+a_3}$.

Et ainsi on a :

$$\left\{ \begin{array}{l} x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ y_3 = -\left(\lambda + a_1\right)x_3 - \nu - a_3 \end{array} \right. .$$

4.3 Courbes elliptiques sur un corps fini

Considérons une cubique plane, lisse, rationnelle (sur Q), donnée par son équation de Weierstrass :

$$W_{\#} = y^2z + a_1yxz + a_3yz^2 - \left(x^3 + a_2x^2z + a_4xz^2 + a_6z^3\right) = 0$$

où $a_1, a_2, \ldots, a_6 \in Q$. Lorsqu'on effectue une transformation rationnelle du type :

$$x = \xi/\lambda^2, y = \mu/\lambda^3, z = \zeta$$

on trouve une équation qui est du même type mais où a_i est devenu $\lambda^i a_i$. En choisissant λ convenablement, on peut se ramener à une équation à coefficient entiers pas trop grands.

On considère maintenant un nombre premier quelconque p et l'équation réduite suivante :

$$\widehat{W_{\#}} = y^2z + \widehat{a_1}yxz + \widehat{a_3}yz^2 - \left(x^3 + \widehat{a_2}x^2z + \widehat{a_4}xz^2 + \widehat{a_6}z^3\right) \in F_p[x, y, z]_3,$$

notre but est d'étudier l'application de réduction :

$$\left\{ \begin{array}{ccc} P^2\left(Q\right) & \to & P^2\left(F_p\right) \\ [a : b : c] & \longmapsto & \left[\widehat{a}, \widehat{b}, \widehat{c}\right] \end{array} \right.$$

où a, b, c sont premier entre eux, et de voir qu'elle induit un homomorphisme de $C_Q(W_\#)$ dans $C_{F_p}\left(\widehat{W_\#}\right)$ lorsque $C_{F_p}\left(\widehat{W_\#}\right)$ est lisse.

Proposition 5 *Soit C une cubique lisse plane définie sur Q et D une droite de $P^2(Q)$, on suppose que $C \cap D = \{P_1, P_2, P_3\}$ où P_i est répété un nombre de fois égale à sa multiplicité d'intersection. On désigne par $\widehat{C}$, $\widehat{D}$ et $\widehat{P_i}$ les objets déduits de C, D et P_i par réduction. Alors si $\widehat{D}$ n'est pas une composante de $\widehat{C}$ on a :*

$$\widehat{C} \cap \widehat{D} = \{\widehat{P_1}, \widehat{P_2}, \widehat{P_3}\}$$

avec la même convention sur la répétition des points.

Théorème 6 *Soit C une cubique lisse de $P^2(Q)$ et soit $O \in C$. Soit $\widehat{C}$ la cubique réduite modulo p et $\widehat{O}$ la réduction de O.*

1. *Si la cubique $\widehat{C}$ est lisse, alors l'opération π de réduction induit un homomorphisme de C muni de l'addition d'origine O sur $\widehat{C}$ muni de l'addition d'origine $\widehat{O}$.*
2. *Si la cubique $\widehat{C}$ admet un point double S dans $P^2(F_p)$, on désigne pas C_O l'ensemble $C - \pi^{-1}(S)$.*

Alors si $O \in C_O$ l'ensemble des points de C_O forme un sous groupe de C et l'application de réduction modulo p induit un homomorphisme de ce sous-groupe sur l'ensemble des points non singuliers de $\widehat{C}$ muni de la loi d'addition d'origine $\widehat{O}$.