Courbes et Jacobiennes

Fabien Pazuki

Novembre 2006

Version β

Table des matières

Introduction

Nous présentons dans ces notes une introduction partielle et partiale à l'étude des courbes algébriques. C'est un domaine très riche et par voie de fait assez compliqué, la visée ici est principalement l'étude des problèmes diophantiens liés à ces courbes.

1 Courbes

1.1 La notion de dimension

Soit X un espace topologique. La dimension de X est la borne supérieure des longueurs de chaînes de parties fermées irreductibles de X. Elle peut être finie ou infinie ; lorsqu'elle est finie c'est un entier positif ou nul.

<u>Remarque</u> : cette notion est inutile si la topologie est séparée, car alors $\dim(X) = 0$ pour toute variété X. En effet si $Y \subsetneq X$ est un fermé non vide d'un espace topologique séparé X, soit $y \in Y$ et $x \in X$: on prend O_x et O_y deux voisinages ouverts disjoints de x et y respectivement et on considère l'égalité $Y = (\overline{O_y} \cap Y) \cup (\overline{O}_x \cup \complement_Y O_y)$: ceci montre que Y ne peut être irreductible lorsque la topologie est séparée.

Il existe d'autres approches de la notion de dimension d'une variété algébrique. On peut par exemple partir de la dimension de Krull d'un anneau A, définie comme la borne supérieure des longueurs de chaînes d'idéaux premiers de A. Si X est une variété algébrique affine définie sur le corps k, on considère l'anneau des fonctions sur X :

$$\Gamma(X) = k[X_1, ..., X_n]/I(X).$$

On a alors l'égalité $\dim(X) = \dim_{\text{Krull}}(\Gamma(X))$. De plus, si B est une algèbre de type finie et intègre, en notant $K = \text{Fr}(B)$ le corps des fractions de B, alors on a l'égalité $\dim_{\text{Krull}}(B) = \deg_{\text{Tr}}(K)$ (ou $\deg_{\text{Tr}}$ est le degré de transcendance du corps K sur k).

Ces relations donnent en fait une méthode de calcul de la dimension d'une variété algébrique générale : soit en effet X une variété algébrique. On peut décomposer X en une union finie de Zariski-fermés irréductibles. On se ramène ainsi à X irréductible. Si à présent on prend un ouvert U de X, on peut montrer que $\dim(X) = \dim(U)$. On se ramène donc à X affine irréductible, on peut alors utiliser le degré de transcendant de $K(X)$.

Définition : une courbe est une varité algébrique de dimension 1.

1.2 La notion de degré

Soit C une courbe projective irreductible dans $\mathbb{P}^N$. Le nombre d de points d'intersection (comptés avec multiplicité) de C avec un hyperplan H ne contenant pas C est appelé le degré de C, et noté $\deg(C)$. Ce nombre ne dépend pas de l'hyperplan choisi mais dépend du plongement projectif. On reviendra sur cette notion dans la suite.

1.3 La notion de genre

Pour classer les courbes on va chercher un invariant ne dépendant pas du plongement. On utilise un nombre particulier appelé le genre de la courbe. Il y a plusieurs possibilités pour se familiariser avec cette notion, on trouve en général les trois approches suivantes : soit C une courbe algébrique. On peut définir le genre $g(C)$ de C de plusieurs manières, on verra qu'elles sont cohérentes par la suite :

- $g(C)$ = le nombre de 'trous' de la surface de Riemann $C(\mathbb{C})$.
- $g(C)$ = dim{formes différentielles holomorphes sur C}.
- $g(C)$ = (nombre de zéros de ω)-(nombre de pôles de ω) pour ω une forme différentielle sur C.

Nous allons donner une définition plus poussée du genre de C en énonçant le théorème de Riemman-Roch. Nous avons besoin pour cela de la notion de diviseur.

Définition : un diviseur D sur une courbe algébrique C est une combinaison formelle finie à coefficients entiers de points de C, qu'on notera : $D = \sum_{P \in C} n_P(P)$. Le degré de D est alors la somme finie $\sum_P n_P$. C'est un entier (le diviseur est ici défini sur le même corps que la courbe.).

Le diviseur d'une fonction $f \in k(C)$ est donné comme suit : soit $\mathcal{Z}$ l'ensemble des zéros de f et $\mathcal{P}$ l'ensemble de ses pôles. Alors on définit :

$$\operatorname{div}(f) = \sum_{P \in \mathcal{Z}} (P) - \sum_{Q \in \mathcal{P}} (Q).$$

On remarque qu'on a donc toujours $\deg(\mathrm{div}(f)) = 0$.

Soit K_C un diviseur canonique de la courbe C, i.e. le diviseur d'une forme différentielle sur C.

On pose :

$$L(D) := \{f \in k(C) \mid \mathrm{div}(f) + D \geq 0\}.$$

L'ensemble $L(D) \cup \{0\}$ est un espace vectoriel de dimension finie $l(D)$.

Théorème 1. *(Riemann-Roch)*
Soit C une courbe projective lisse définie sur un corps k. Alors il existe un entier g, appelé genre de la courbe, tel que pour tout diviseur D sur C on a :

$$l(D) - l(K_C - D) = \deg(D) - g + 1.$$

Nous allons étudier quelques cas particuliers de ce théorème : tout d'abord si on choisit $D = 0$, le diviseur nul, on obtient : $l(D) = l(0) = 1$ car les seules fonctions régulières sur une variété projective sont les constantes. Comme le degré du diviseur nul est égal à zéro, le théorème donne l'égalité : $l(K_C) = g$. Si on particularise la courbe C à présent, en prenant $C = \mathbb{P}^1$, on obtient $l(K_{\mathbb{P}^1}) = 0$ car il n'y a pas de forme différentielle régulière sur tout $\mathbb{P}^1$, donc on conclut que $g(\mathbb{P}^1) = 0$.

Fort de cela, si on prend ensuite $D = K_C$, le théorème donne l'égalité $\deg K_C = 2g - 2$.

Ces deux particularisations du théorème de Riemann-Roch redonnent donc les interprétations du genre énoncées en début de partie.

Nous allons nous munir d'un outil supplémentaire pour l'étude du genre, outil donné par le théorème de Riemann-Hurwitz :

Théorème 2. *(Riemann-Hurwitz)*
Soient C et C' deux courbes définies sur le corps k, de genre respectivement g et g'. Soit $f : C \longrightarrow C'$ un morphisme fini, séparable de degré $d \geq 1$. On note e_P l'indice de ramification de f au point $P \in C$. On suppose enfin que la caractéristique de k est nulle, ou bien qu'elle ne divise aucun e_P. Alors on a :

$$2g - 2 = d(2g' - 2) + \sum_{P \in C} (e_P - 1).$$

Remarque : le fait d'avoir calculé le genre de $\mathbb{P}^1$ permet donc en utilisant cette égalité de Riemann-Hurwitz de calculer le genre d'une autre courbe, pour peu qu'il soit possible de mettre en évidence un morphisme entre la courbe et $\mathbb{P}^1$. On verra un exemple détaillé dans la suite.

2 Les questions qu'on se pose

1. Quels couples (degré, genre) existent dans la nature ?
2. Quelles informations peut-on obtenir sur les points rationnels d'une courbe algébrique ?

Nous allons répondre partiellement à ces questions, en nous concentrant sur les courbes planes dans un premier temps. Voyons tout d'abord comment les notions de genre et de degré sont liées, puis nous nous intéresserons à l'utilisation du genre comme critère dans l'étude de la rationalité des points sur une courbe algébrique.

3 Courbes planes

3.1 Un lien entre degré et genre

Lorsqu'on se concentre sur les courbes planes, i.e. les courbes lisses projectives pouvant être plongées dans $\mathbb{P}^2$, on peut énoncer le résultat suivant :

Théorème 3. *Soit C une courbe lisse projective et plane de degré n. Alors le genre de C est donné par :*

$$g(C) = \frac{(n-1)(n-2)}{2}.$$

La première remarque est la suivante : les hyperplans de $\mathbb{P}^2$ sont des droites, donc les zéros d'un polynôme $P \in k[X,Y,Z]$ homogène dont le degré est n forment une courbe de degré n. Ceci signifie qu'il existe des courbes algébriques planes de tout degré.

Partant de là, la formule exclut l'existence de courbes planes lisses projectives de certains genres, par exemple il n'existe pas de courbes plane lisse projective de genre 2...

Nous allons traiter un exemple de calcul de genre :

Soit la courbe affine plane donnée par l'équation

$$y^2 = x^6 - x.$$

Lorsqu'on veut calculer le genre de cette courbe, il faut tout d'abord regarder sa projectivisation :

$$C \;:\; Z^4Y^2 = X^6 - Z^5X.$$

C'est un polynôme homogène de degré 6 mais, méfiance, cette courbe n'est pas lisse en l'infini (au point $(0:1:0)$) ! On ne peut donc pas appliquer la formule du genre en fonction du degré... Nous allons donc considérer l'application suivante :

$$\begin{aligned} C &\longrightarrow \mathbb{P}^1 \\ (X:Y:Z) &\longmapsto (X:Z). \end{aligned}$$

Cette application est rationnelle, de degré 2 et ramifie en les six 'points de Weierstrass', i.e. les racines de $x^6 - x$, avec indice de ramification égal à 2. On va alors appliquer le théorème de Riemann-Hurwitz, on note $\mathcal{W}$ l'ensemble des points de ramification :

$$2g(C) - 2 = d(2g(\mathbb{P}^1) - 2) + \sum_{P \in \mathcal{W}} (e_P - 1),$$

ce qui implique avec les données précédentes :

$$2g(C) - 2 = -4 + \sum_{i=1}^{6} (2-1),$$

d'où on tire finalement :

$$g(C) = 2.$$

(Ceci est cohérent avec le fait qu'une courbe de genre 2 n'admet pas de modèle plan, projectif et lisse.)

3.1.1 Le genre 0

Si $g(C) = 0$, on obtient alors qu'une courbe plane lisse projective de genre 0 est soit de degré 1, i.e. une copie de $\mathbb{P}^1$, soit de degré 2, i.e. une conique dans $\mathbb{P}^2_{|k}$. Si $P_0 \in C(k)$, alors l'application :

$$\begin{aligned} \Phi : C &\longrightarrow \mathbb{P}^1 \\ P_0 &\longmapsto \overrightarrow{T}_{P_0} \\ P &\longmapsto (\overrightarrow{PP_0}) \end{aligned}$$

est une bijection. On peut donc conclure que la seule courbe plane lisse projective de genre 0 admettant un point rationnel est la droite projective $\mathbb{P}^1$.

3.1.2 Le genre 1

Soit C une courbe définie sur le corps k, projective lisse de genre 1 admettant un point rationnel sur k. Cet objet est appelé courbe elliptique. Nous allons lui appliquer le théorème de Riemann-Roch. Commençons par calculer, pour un diviseur $D \in \mathrm{Div}(C)$ et $f \in L(D)$:

$$0 = \deg \mathrm{div}(f) \geq \deg(-D) = -\deg(D),$$

ceci impose donc $\deg(D) \geq 0$. Or $\deg(K_C) = 2g - 2$, donc si $\deg(D) > 2g - 2$, il ne peut exister de fonction $f \in L(K_C - D)$, donc $l(K_C - D) = 0$.

Dans le cas particulier ou $g = 1$, on sait tout d'abord que $K_C = 0$. On déduit donc que $l(D) = \deg(D)$. Or on a supposé qu'il existe un point $P_0 \in C(k)$. Choisissons alors $D = D_n = n(P_0)$, pour $n \in \mathbb{N}$, et notons $L_n = L(n(P_0))$. On sait donc que $\dim(L_n) = \deg D_n = n$. On obtient alors :

$$\begin{aligned}
L_1 &= k, \\
L_2 &= k \oplus kx, \\
L_3 &= k \oplus kx \oplus ky, \\
L_4 &= k \oplus kx \oplus ky \oplus kx^2, \\
L_5 &= k \oplus kx \oplus ky \oplus kx^2 \oplus kxy, \\
L_6 &\supseteq \mathrm{Vect_k}\{1, x, x^2, x^3, y, xy, y^6\},
\end{aligned}$$

où x est une fonction n'ayant qu'un pôle d'ordre 2 en P_0 et y est une fonction n'ayant qu'un pôle d'ordre 3 en P_0. Le fait que L_6 contienne sept fonctions et soit de dimension 6 nous permet d'affirmer que ces sept fonctions sont liées par une relation du type :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

avec les a_i des coefficients dans k.

Cette relation est appelée le modèle de Weierstrass (forme longue) de la courbe elliptique C. C'est donc une courbe plane. Son degré est 3, il peut éventuellement être égal à 4 si l'on procède à un changement de carte déplaçant le point à l'infini.

Les courbes elliptiques sur un corps de nombres ont une structure très spéciale, décrite par le théorème suivant :

Théorème 4. *(Mordell-Weil)*
Soit E une courbe elliptique définie sur un corps de nombres k. Alors les points $k-$rationnels de E forment un groupe abélien de type fini, i.e. il existe un entier naturel r tel que :

$$E(k) \simeq \mathbb{Z}^r \oplus E(k)_{\mathrm{tors}}.$$

On comprend donc qu'il est possible d'avoir soit une infinité de points rationnels sur la courbe, auquel cas le rang r est strictement positif, soit un nombre fini de points rationnels, auquel cas $r = 0$. Un exemple en rang 0 :

$$E_0 \,:\, y^2 = x^3 - x,$$

alors :

$$E_0(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Un exemple en rang 1 :

$$E_1 \,:\, y^2 = x^3 - 5^2 x,$$

alors :

$$E_1(\mathbb{Q}) \simeq \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

3.1.3 En genre g $\geq$ 2

Lorsque le genre est supérieur ou égal à 2, les courbes ne sont plus nécessairement planes, cependant on verra dans la partie suivante qu'on connaît tout de même beaucoup de choses sur ces objets...

4 Courbes générales

4.1 Vivre dans $\mathbb{P}^3$

On se contentera ici de montrer qu'une courbe projective peut toujours être vue comme une courbe dans $\mathbb{P}^3$. Considérons en effet une courbe C dans $\mathbb{P}^N$. Soit P un point de C et H un hyperplan de $\mathbb{P}^N$. On peut alors considérer la projection π de centre P sur H, on note alors C' l'image de C. Cette opération permet de ramener C dans $H \simeq \mathbb{P}^{N-1}$. Pour que C et C' soient isomorphes il faut cependant que π soit injective sur C, donc le point P ne doit être sur aucune droite sécante à C. Or la réunion des sécantes de C est une sous-variété de dimension 3 de $\mathbb{P}^N$, cette construction n'est donc possible que si $N \geq 3$.

On voit donc que toute courbe projective est isomorphe à une courbe de $\mathbb{P}^3$, et que toute courbe lisse projective peut donc être plongée dans $\mathbb{P}^3$.

Cela réduit donc le problème posé par la question 1, mais l'étude reste cependant encore ouverte dans ce cadre...

4.2 Retour sur le genre $g \geq 2$

Si l'on s'intéresse à la question 2, nous allons découvrir que lorsque le genre est $g \geq 2$ la situation se simplifie radicalement par rapport au genre 1, comme en témoigne le théorème suivant, anciennement conjecture de Mordell :

Théorème 5. *(Faltings)*
Soit C une courbe de genre $g(C) \geq 2$, définie sur un corps de nombres k. Alors les points rationnels de C sur le corps k sont en nombre fini.

Ce théorème, dont la première preuve a été donnée par G.Faltings en 1986, permet en particulier de traiter l'exemple suivant :

Soit la courbe de $\mathbb{P}^2$ définie sur $\mathbb{Q}$ par le polynôme homogène de degré $n \geq 4$:

$$x^n + y^n = z^n.$$

On vérifie aisément que cette courbe plane est lisse. On peut donc affirmer que son genre est égal à $(n-1)(n-2)/2 \geq 3$. Il s'ensuit que le nombre de points rationnels est nécessairement fini... on sait depuis la publication des travaux d'A.Wiles qu'il n'y a en fait aucun point $\mathbb{Q}$-rationnel sur cette courbe ('dernier théorème de Fermat').

5 Une utilisation de la jacobienne

5.1 Définition

Soit C une courbe algébrique. On dit que deux diviseurs D et D' sur C sont linéairement équivalents s'il existe une fonction rationnelle f sur C telle que : $D = D' + \mathrm{div}(f)$. On notera $D \sim D'$.

On définit l'ensemble $\mathrm{Pic}(C)$ comme étant l'ensemble des classes de diviseurs sur C modulo équivalence linéaire.

L'application 'degré' qui a un diviseur associe son degré passe au quotient car le diviseur d'une fonction rationnelle est de degré zéro. On obtient donc une application :

$$\begin{aligned} \deg\ :\ \mathrm{Pic}(C) &\longrightarrow \mathbb{Z} \\ \mathrm{cl}(\sum_i n_i P_i) &\longmapsto \sum_i n_i. \end{aligned}$$

On peut alors définir la jacobienne de la courbe C, notée $\mathrm{Jac}(C)$, par :

$$\mathrm{Jac}(C) := \mathrm{Ker}\,[\deg\ :\ \mathrm{Pic}(C) \longrightarrow \mathbb{Z}].$$

5.2 Le cas particulier du genre 1

Nous allons voir que les courbes elliptiques sont en fait isomorphes à leurs jacobiennes. En effet soit E/k une courbe elliptique et $O \in E(k)$. Regardons l'application :

$$\begin{aligned} E &\longrightarrow \mathrm{Jac}(E) \\ P &\longmapsto \mathrm{cl}((P) - (O)). \end{aligned}$$

Le théorème de Riemann-Roch donne l'égalité $l(D) = \deg(D)$ pour tout diviseur sur la courbe E. Soit D_0 un représentant d'une classe de $\mathrm{Jac}(C)$, en appliquant le théorème de Riemann-Roch au diviseur $D_0 + (O)$ on obtient donc $\dim L(D_0 + (O)) = \deg(D_0 + (O)) = 1$, donc on sait qu'il existe une fonction f non nulle telle que $\mathrm{div}(f) \geq -D_0 - (O)$; or $\deg \mathrm{div}(f) = 0$ donc on sait qu'il existe $P \in E(k)$ tel que $\mathrm{div}(f) = -D_0 - (O) + (P)$, ce qui signifie exactement que $D_0 \sim (P) - (O)$. L'application est donc surjective.

De plus si $(P) \sim (P')$, on sait qu'il existe une fonction sur E telle que $\mathrm{div}(f) = (P) - (P')$, donc par définition il vient $f \in L((P'))$. Or par Riemann-Roch, $\dim(L((P'))) = \deg((P')) = 1$, comme les fonctions constantes forment un sous-espace de dimension 1, on a automatiquement que f est en fait une constante (non nulle) : mais alors elle n'admet ni zéro ni pôle, c'est donc que $P = P'$. Donc l'application est injective.

5.3 Propriétés de la jacobienne

5.3.1 Structure de groupe

L'un des aspects essentiels de la jacobienne d'une courbe algébrique est qu'elle est naturellement munie d'une structure de groupe abélien. On admettra qu'elle est en fait une variété abélienne dans laquelle la courbe d'origine peut être plongée. La dimension de cette variété est donné par le genre de C : $\dim(\mathrm{Jac}(C)) = g(C)$. Les courbes elliptiques sont des variétés abéliennes de dimension 1 ; ce sont en fait les seules, et elles héritent de la structure de groupe de leur jacobienne.

5.3.2 Hauteur de Néron-Tate

Nous allons utiliser le fait qu'on dispose d'une structure de groupe pour construire une hauteur vérifiant de bonnes propriétés sur la jacobienne. On se donne une courbe C sur un corps de nombres k et on note $A = \mathrm{Jac}(C)$ sa jacobienne.

1. La variété A est projective ; on choisit un plongement $\Phi : A \hookrightarrow \mathbb{P}^N$. On note M_k l'ensemble des places du corps k et on pose pour $P \in A(k)$:

$$h_{A,\Phi}(P) = \sum_{v \in M_k} \frac{[k_v : k]}{[\mathbb{Q}_v : \mathbb{Q}]} \log \max_{i=0..N} |\Phi(P)_i|_v.$$

   On appelle cette fonction hauteur de Weil, ou encore hauteur naïve.

2. On vérifie qu'on a, pour P et Q des points de A et en utilisant la structure de groupe pour sommer les points :

$$h_{A,\Phi}(P+Q) + h_{A,\Phi}(P-Q) = 2h_{A,\Phi}(P) + 2h_{A,\Phi}(Q) + O(1).$$

3. On pose alors :

$$\hat{h}_{A,\Phi}(P) = \lim_{n \to +\infty} \frac{1}{4^n} h_{A,\Phi}([2^n]P).$$

4. On obtient alors l'identité du parallèlogramme :

$$\hat{h}_{A,\Phi}(P+Q) + \hat{h}_{A,\Phi}(P-Q) = 2\hat{h}_{A,\Phi}(P) + 2\hat{h}_{A,\Phi}(Q).$$

5. Ceci démontre que $\hat{h}_{A,\Phi}$ est une forme quadratique sur A. On va donc pouvoir utiliser la structure euclidienne qu'elle induit.

5.3.3 Points rationnels d'une courbe de genre $g \geq 2$

Nous allons à présent utiliser les objets introduits jusqu'ici pour donner une méthode pour borner le nombre (fini) de points rationnels d'une courbe de genre $g \geq 2$ sur un corps de nombres. On va se concentrer sur le théorème suivant :

Théorème 6. *Soit C/k une courbe sur un corps de nombres. On suppose que $g(C) \geq 2$. Soit J la jacobienne de C. Alors il existe des constantes γ_1 et γ_2 telles que :*

$$\mathrm{Card}(C(k)) \leq \mathrm{Card}(J(k)_{\mathrm{tors}}) \left(1 + \frac{2\gamma_1}{\delta}\right)^r + \gamma_2 7^r,$$

où on a noté : $r =$ rang de $J(k)$, et :

$$\delta = \min_{P \in J(k)/J(k)_{\mathrm{tors}}} (\hat{h}(P))^{\frac{1}{2}}.$$

Preuve :

La preuve de ce théorème distingue deux 'types' de points sur la courbe algébrique : les 'grands' points pour lesquels on utilise les inégalités de Mumford et Vojta et les 'petits' points. Dans les deux cas on utilise la structure euclidienne mise en évidence plus haut.

Notons $|P| = (\hat{h}(P))^{\frac{1}{2}}$, norme euclidienne sur $J(k) \otimes \mathbb{R}$.

Pour ce qui est des 'grands' points, on utilise le résultat suivant : il existe deux constantes γ_1 et γ_2 telles que :

$$\mathrm{Card}\{P \in C(k) | \, |P| > \gamma_1\} \leq \gamma_2 7^r.$$

Insistons sur le fait que ce sont des points de la courbe, vus comme points de la jacobienne. Si l'on remplace $C(k)$ par $J(k)$ dans l'ensemble considéré, ce dernier devient évidemment infini... Ce résultat a été difficile à obtenir et provient des travaux de P.Vojta qui a donné une preuve différente de celle de G.Faltings de la conjecture de Mordell.

Nous allons majorer le nombre de 'petits' points de la manière suivante :

$$\begin{array}{lll} \mathrm{Card}\{P \in C(k) | \, |P| < \gamma_1\} & \leq & \mathrm{Card}\{P \in J(k) | \, |P| < \gamma_1\} \\ & \leq & \mathrm{Card}\{P \in J(k)/J(k)_{\mathrm{tors}} | \, |P| < \gamma_1\} \, \mathrm{Card}(J(k)_{\mathrm{tors}}) \quad \mathrm{lll} \\ & \leq & \left(1 + \frac{2\gamma_1}{\delta}\right)^r \mathrm{Card}(J(k)_{\mathrm{tors}}), \end{array}$$

où la dernière inégalité est un fait général. En effet, dans un réseau Λ d'un espace euclidien $(E, |.|)$ de dimension r :

$$\mathrm{Card}\{P \in \Lambda |\, |P| < X\} \,\mathrm{vol}(B(0, \frac{\delta}{2})) = \mathrm{vol}(\bigcup_{|P|<X} B(P, \frac{\delta}{2})) \leq \mathrm{vol}(B(0, X + \frac{\delta}{2})),$$

d'où :

$$\mathrm{Card}\{P \in \Lambda |\, |P| < X\} \leq \left(\frac{2X + \delta}{\delta}\right)^r .$$

En réunissant les deux analyses, on obtient donc la borne annoncée sur le cardinal des points d'une courbe algébrique de genre supérieur ou égal à deux. La jacobienne est ici l'outil crucial qui permet d'utiliser à la fois la structure de groupe et la structure euclidienne.

Références

[1] T.De Diego. Points rationnels sur les familles de courbes de genre au moins 2. *J. Number Theory* **67** (1997), no.1, p.85-114.

[2] R.Hartshorne. Algebraic geometry, *Springer-Verlag* **52** (1977).

[3] M.Hindry et J.Silverman. Diophantine geometry : an introduction, *Springer-Verlag* **201** (2000).

[4] D.Mumford. Curves and their jacobians, *Ann Arbor, the University of Michigan Press* (1975).

[5] D.Perrin. Géométrie algébrique, *CNRS Editions* (2001).

[6] J.H.Silverman. The Arithmetic of Elliptic Curves, *Springer-Verlag* **106** (1986).

[7] J.H.Silverman. Advanced topics in the arithmetic of elliptic curves, *Springer-Verlag* **151** (1994).