Chercher des points rationnels

Variétés algébriques et calcul dans les corps finis

Erwan Biland

Séminaire d'algèbre et géométrie de premier cycle
Université Laval

Jeudi 10 février 2011

Objectifs

1 - Un peu de géométrie

- Rappels sur le spectre d'un anneau
- Degré d'un point, diviseurs
- Courbe projective plane sur un corps k

2 - Un peu d'arithmétique

- Rappels sur la fonction zeta de Riemann
- Fonction zeta d'une courbe projective lisse sur un corps fini
- Théorème de Riemann-Roch et applications

3 - Un peu d'algorithmique

- Rappels sur les nombres algébriques
- Division euclidienne des polynômes et calcul dans les corps finis
- Chercher des points de degré donné sur une courbe

Rappels sur le spectre d'un anneau

Ensemble des points :

$$\mathrm{Spec}(A) = \Big\{\text{idéaux premiers de } A\Big\}$$

Ensemble des points *fermés* :

$$\mathrm{Spec}_{\mathrm{max}}(A) = \Big\{\text{idéaux maximaux de } A\Big\}$$

Exemple 1. $A = \mathbb{C}[X]$ anneau principal

$$\mathrm{Spec}_{\mathrm{max}}(\mathbb{C}[X]) = \Big\{\langle X - \alpha\rangle \ ; \ \alpha \in \mathbb{C}\Big\} \simeq \mathbb{C}$$

Exemple 2. $A = \mathbb{R}[X]$ anneau principal

$$\mathrm{Spec}_{\mathrm{max}}(\mathbb{R}[X]) = \Big\{\langle X - \alpha\rangle \ ; \ \alpha \in \mathbb{R}\Big\}$$
$$\cup\Big\{\langle X^2 + \beta X + \gamma\rangle \ ; \ \Delta = \beta^2 - 4\gamma < 0\Big\}$$

La droite algébrique affine sur le corps $\mathbb{R}$

Exemple 2. $A = \mathbb{R}[X]$ anneau principal

$$\mathrm{Spec}_{\max}(\mathbb{R}[X]) = \left\{ \langle X - \alpha \rangle \ ; \ \alpha \in \mathbb{R} \right\} \cup \left\{ \left\langle X^2 + \beta X + \gamma \right\rangle \ ; \ \Delta = \beta^2 - 4\gamma < 0 \right\}$$

Les points fermés de la droite algébrique affine $\mathbb{A}^1_{\mathbb{R}}$:

- les points $\langle X - \alpha \rangle$ sont dits de degré 1 ;
  ils correspondent à un point "naïf" $\alpha \in \mathbb{R}$;
  on remarque que $\mathbb{R}[X]/\langle X - \alpha \rangle \simeq \mathbb{R}$.
- les points $\left\langle X^2 + \beta X + \gamma \right\rangle$ sont dits de degré 2 ;
  ils correspondent à **deux** points $z, \bar{z} \in \mathbb{C} \setminus \mathbb{R}$;
  on remarque que $\mathbb{R}[X]/\left\langle X^2 + \beta X + \gamma \right\rangle \simeq \mathbb{C}$, avec $\dim_{\mathbb{R}} \mathbb{C} = 2$.

Une conique un peu spéciale

Exemple 3. $A = \mathbb{R}[X, Y]/\langle X^2 + Y^2 + 1\rangle$

Spec(A) est la courbe d'équation $x^2 + y^2 + 1 = 0$ dans le plan affine $\mathbb{A}^2_{\mathbb{R}}$.

- Il n'y a aucun point "rationnel" (de degré 1) ! ! !
  La courbe d'équation $x^2 + y^2 + 1 = 0$ n'a pas de point dans $\mathbb{R}^2$.
- On cherche les points de degré 2 :
  $\hookrightarrow$ **deux** points conjugués sur la courbe $x^2 + y^2 + 1 = 0$ dans $\mathbb{C}^2$

  $\left\{(i, 0); (-i, 0)\right\} \quad \rightsquigarrow \quad$ l'idéal $P = \langle Y, X^2 + 1\rangle$;

  $\left\{(\frac{i}{\sqrt{2}}, \frac{i}{\sqrt{2}}); (-\frac{i}{\sqrt{2}}, -\frac{i}{\sqrt{2}})\right\} \quad \rightsquigarrow \quad$ l'idéal $Q = \langle X - Y, 2X^2 + 1\rangle$;

Plan projectif sur un corps k

Le plan projectif sur k est l'ensemble des droites passant par l'origine dans k^3 :

$$\mathrm{P}^2_k = \Big\{ [x:y:z]\,;\ (x,y,z) \neq (0,0,0) \Big\}$$

$$\text{avec } [x:y:z] = [x':y':z'] \quad \Leftrightarrow \quad \frac{x}{x'} = \frac{y}{y'} = \frac{z}{z'}$$

On peut le voir comme la réunion du plan affine :

$$\mathrm{A}^2_k = \Big\{ [x:y:z]\,;\ z \neq 0 \Big\} = \Big\{ [x:y:1]\,;\ x,y \in k \Big\}$$

avec un ensemble de "points à l'infini" :

$$\mathrm{P}^1_k = \Big\{ [x:y:0]\,;\ (x,y) \neq (0,0) \Big\}$$

$$\text{avec } [x:y:0] = [x':y':0] \quad \Leftrightarrow \quad \frac{x}{x'} = \frac{y}{y'}$$

Courbe dans le plan algébrique projectif

On notera $\mathbb{P}^2_k$ le plan algébrique projectif, ce qui signifie qu'on s'autorise à chercher des points de degré plus grand que 1.

Pour définir une courbe dans le plan projectif, il faut se donner une équation homogène.

Exemple 3 bis. Soit la courbe $\mathcal{C}$ d'équation $x^2 + y^2 + z^2 = 0$

- On a déjà trouvé les points pour $z \neq 0$.
- On cherche les points à l'infini $(z = 0)$:

  $\hookrightarrow$ l'équation devient $x^2 + y^2 = 0$, $(x, y) \neq (0, 0)$

  aucun point de degré 1

  un seul point de degré 2 : $\left\{[1 : i : 0] \ ; \ [1 : -i : 0]\right\} \rightsquigarrow I$

Rappels sur les corps finis

Soit k un corps fini ; il existe un nombre premier p, la *caractéristique* de k, et un entier d tel que $|k| = p^d$.

A isomorphisme près, il existe un unique corps fini de cardinal p^d, noté $\mathbb{F}_{p^d}$.

En particulier, $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$.

Le corps $\mathbb{F}_{p^d}$ est une extension de degré d de $\mathbb{F}_p$: $\dim_{\mathbb{F}_p}(\mathbb{F}_{p^d}) = d$.

Exemple 4. $\mathcal{C}$ la courbe projective d'équation $x^2 + y^2 + z^2 = 0$ sur $\mathbb{F}_3$

- On note $\mathcal{C}(\mathbb{F}_3)$ les solutions de l'équation sur $\mathbb{F}_3$.
- On note $\mathcal{C}(\mathbb{F}_{3^d})$ les solutions de l'équation sur $\mathbb{F}_{3^d}$.
- d points "conjugués" de $\mathcal{C}(\mathbb{F}_{3^d})$ $\rightsquigarrow$ un point de $\mathcal{C}$ de degré d.

Si P est un point de $\mathcal{C}$ de degré d, on note $k(P) = \mathbb{F}_{3^d}$ son *corps résiduel*.

Degré d'un diviseur

Un *diviseur* sur la courbe $\mathcal{C}$ est un ensemble de points, auquels on donne des multiplicités entières (penser à l'ensemble des pôles et racines d'une fraction rationnelle).

On dit que le diviseur est *effectif* si toutes les multiplicités sont positives (penser à l'ensemble des racines d'un polynôme).

Le degré du diviseur est la somme pondérée des degrés de ses points.

Exemple 3 ter. Diviseur sur la courbe projective $\mathcal{C}$:

- $D = P + Q - 2I$
- $\deg D = \deg P + \deg Q - 2 \deg I$

$\deg : \mathrm{Div}(\mathcal{C}) \to \mathbb{Z}$ est un morphisme de groupes.

Il peut être surjectif (exemple 2) ou non (exemple 3)...

$\hookrightarrow \delta = \mathrm{pgcd}\Big\{\deg D \ ; \ D \in \mathrm{Div}(\mathcal{C})\Big\}$

Fonction zeta de Riemann

La fonction zeta renferme beaucoup d'information sur la distribution des nombres premiers.

$$\zeta(s) = \sum_{n \geqslant 1} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots$$

On peut transformer la somme en produit *eulérien* :

$$\zeta(s) = \prod_{p \text{ premier}} \frac{1}{1 - \frac{1}{p^s}} = \frac{1}{1 - \frac{1}{2^s}} \cdot \frac{1}{1 - \frac{1}{3^s}} \cdot \frac{1}{1 - \frac{1}{5^s}} \cdots$$

On a une équation fonctionnelle :

$$\zeta(1-s) = 2^{1-s} \pi^{-s} \sin \frac{\pi(1-s)}{2} \Gamma(s) \zeta(s)$$

Hypothèse de Riemann :

$$\text{en dehors des zéros "triviaux", } \quad \zeta(s) = 0 \ \Rightarrow \ \Re e(s) = \frac{1}{2}.$$

Fonction zeta d'une courbe

Soit $\mathcal{C}$ une courbe projective plane sur le corps $\mathbb{F}_p$.

$$\zeta_{\mathcal{C}}(s) = \sum_{D \text{ diviseur effectif}} \frac{1}{p^{s \deg(D)}} = 1 + \frac{N_1}{p^s} + \frac{N_2}{p^{2s}} + \frac{N_3}{p^{3s}} + \dots$$

où N_d est le nombre de diviseurs effectifs de degré d.

On peut transformer la somme en produit *eulérien* :

$$\zeta(s) = \prod_{P \text{ point}} \frac{1}{1 - \frac{1}{p^{s \deg(P)}}}$$

On voit que la fonction zeta de $\mathcal{C}$ permet de compter les points de degré d de $\mathcal{C}$, et donc de compter les points de la courbe $\mathcal{C}(\mathbb{F}_{p^d})$.

Fonction Z d'une courbe

En pratique, on définit une fonction Z en posant $T = p^{-s}$:

$$Z_{\mathcal{C}}(T) = \sum_{D \text{ diviseur effectif}} T^{\deg(D)} = 1 + N_1 T + N_2 T^2 + N_3 T^3 + \dots$$

où N_d est le nombre de diviseurs effectifs de degré d.

Conjectures de Weil (démontrées depuis) pour une courbe projective lisse :

- La fonction $Z_{\mathcal{C}}$ est une fraction rationnelle.
- On a une relation simple entre $Z_{\mathcal{C}}(\frac{1}{pT})$ et $Z_{\mathcal{C}}(T)$,

  c'est-à-dire entre $\zeta_{\mathcal{C}}(1-s)$ et $\zeta_{\mathcal{C}}(s)$.
- Pour toute racine α de $Z_{\mathcal{C}}$, on a $|\alpha| = \frac{1}{\sqrt{p}}$,

  c'est-à-dire $\zeta_{\mathcal{C}}(s) = 0 \ \Rightarrow \ \Re e(s) = \frac{1}{2}$.

Théorème de Riemann-Roch

Soit $\mathcal{C}$ une courbe projective lisse sur le corps fini $\mathbb{F}_p$.

Théorème (Riemann-Roch). Soit D un diviseur de $\mathcal{C}$. Le nombre de diviseurs effectifs rationnellement équivalents à D est $\frac{p^{h(D)}-1}{p-1}$, où $h(D)$ est un entier positif ou nul tel que :

$$h(D) - h(K - D) = \deg D + 1 - g$$

avec g un entier indépendant de D, appelé le genre de la courbe $\mathcal{C}$, et K un diviseur de $\mathcal{C}$, indépendant de D et de degré $2g - 2$.

Conséquence. Notons $\delta = \operatorname{pgcd}\Big\{\deg D \ ; \ D \in \operatorname{Div}(\mathcal{C})\Big\}$. Il existe une constante a, indépendante de d telle que

$$\text{pour } d \geqslant 2g-1, \quad N_d = \begin{cases} a\frac{p^{d+1-g}-1}{p-1} & \text{si } \delta \text{ divise } d \\ 0 & \text{sinon} \end{cases}$$

Application au calcul de la fonction Z

Grâce au théorème de Riemann-Roch, on obtient :

$$Z_{\mathcal{C}}(T) = \frac{a}{p-1}\Big[(p^{1-g}-1) + (p^{\delta+1-g}-1)\,T^{\delta} + (p^{2\delta+1-g}-1)\,T^{2\delta} + \dots\Big]$$
$$- (\textit{termes correctifs de degré } \leqslant 2g-2)$$
$$= \frac{a}{p-1}\left[\frac{p^{1-g}}{1-p^{\delta}\,T^{\delta}} - \frac{1}{1-T^{\delta}}\right]$$
$$- (\textit{termes correctifs de degré } \leqslant 2g-2)$$
$$= \frac{P(T)}{(1-p^{\delta}\,T^{\delta})(1-T^{\delta})}$$

Théorème. Grâce à une relation fonctionnelle entre la fonction $Z_{\mathcal{C}}$ et la fonction Z de $\mathcal{C}$ sur $\mathbb{F}_{p^{\delta}}$, on prouve que $\delta = 1$.

Il existe donc dans $\mathcal{C}$ une famille de points dont les degrés sont premiers entre eux dans leur ensemble (ce qui est faux pour une courbe sur $\mathbb{R}$).

Illustration

Exemple 5. $\mathcal{C}$ la courbe projective d'équation $x^4 + y^4 + z^4 = 0$ sur $\mathbb{F}_5$.

Il est clair que $\mathcal{C}$ n'a pas de point de degré 1.

Avec un logiciel de calcul formel comme Maple (voir la feuille de calcul jointe), on montre que :

- Il existe dans $\mathcal{C}$ des points de degré 2.
- Il existe dans $\mathcal{C}$ des points de degré 3.
- Il existe dans $\mathcal{C}$ des points de degré 5.
- ... ?

Ceci suffit en tout cas à vérifier qu'il existe des points dont les degrés sont premiers entre eux.