

Petite introduction à la géométrie algébrique et arithmétique

Diego Izquierdo

CMLS - École Polytechnique

Vendredi 17 mai 2024

Géométrie algébrique : étude des systèmes d'équations polynomiales à coefficients dans un corps (voire dans un anneau).

Variétés algébriques

- K corps.
- $f_1, \dots, f_m \in K[X_1, \dots, X_n]$.
- $V := V(f_1, \dots, f_m)$: le système d'équations

$$f_1(x) = \dots = f_m(x) = 0:$$

Variété algébrique affine sur K .

- $L=K$ extension de corps :

$V(L) := \{ \text{solutions du système } V \text{ dans } L^n \}$:

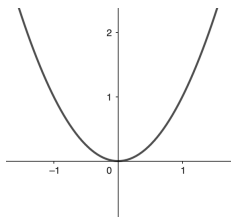
Points L -rationnels de V .

Partie algébrique de L^n .

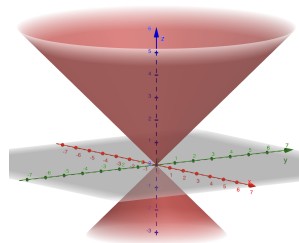
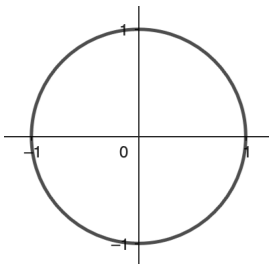
Variétés algébriques

Exemples :

$$V = V(Y - X^2)$$



$$V = V(X^2 + Y^2 - 1) \quad V = V(X^2 + Y^2 - Z^2)$$



- Espace projectif de dimension n :

$$\mathbb{P}^n(K) = \text{droites dans } K^{n+1} \setminus \{0\} / \sim \text{homothétie}$$

- $p \in \mathbb{P}^n(K) : (x_0 : \dots : x_n)$ les coordonnées d'un relèvement de p dans $K^{n+1} \setminus \{0\}$.

-

$$(x_0 : \dots : x_n) = (y_0 : \dots : y_n) ,$$

$$\exists \lambda \in K \setminus \{0\} ; (x_0 : \dots : x_n) = (\lambda y_0 : \dots : \lambda y_n) :$$

Variétés algébriques

- $f_1; \dots; f_m \in K[X_0; \dots; X_n]$ homogènes.
- $V := V_p(f_1; \dots; f_m)$: le système d'équations

$$f_1(x) = \dots = f_m(x) = 0:$$

Variété algébrique projective sur K .

- $L=K$ extension de corps :

$$V(L) := \{ \text{solutions du système } V \text{ dans } \mathbb{P}^n(L) \}$$

Points L -rationnels de V .

Partie algébrique de $\mathbb{P}^n(L)$.

Un peu d'histoire

- Objets anciens : mathématiques grecques, arabes...
- *Géométrie* de Descartes (1637) : géométrie des courbes algébriques par méthodes analytiques.
- XIXème et XXème siècle :
 - 1 Preuve du théorème des zéros de Hilbert.
 - 2 Géométrie projective de l'école italienne (Enriques, Castelnuovo, Segre...).

Un peu d'histoire

- **Années 1930 : formalisation et développement d'outils plus algébriques (théorie des anneaux, algèbre commutative) :**
 - ① école française : Weil, Chevalley, Picard...
 - ② école allemande : Noether, Brauer...
 - ③ école américaine : Zariski, Mumford...
- **Années 50 et 60 : développement de la géométrie algébrique moderne par l'école française : Samuel, Cartan, Serre, Grothendieck...**
 -) Notion de schéma.

Question

Soit V une variété algébrique (affine ou projective) sur un corps K . Peut-on décrire l'ensemble de ses points rationnels $V(K)$? Par exemple, est-il vide? Est-il fini?

Le cas géométrique

V : fidéaux de $K[X_1; \dots; X_n]$ $\$$ f parties algébriques de K^n : I

$$I \nabla V(I) := \{f \in K^n : f(x) = 0\}$$

$$\{f \in K^n : f(x) = 0\}$$

$$I(V) := \{f \in K[X_1; \dots; X_n] : f(x) = 0 \forall x \in V\}$$

$$\{f \in K[X_1; \dots; X_n] : f(x) = 0 \forall x \in V\}$$

$I(V)$ est un idéal radical :

$$\{f \in K[X_1; \dots; X_n] : f^m \in I(V) \implies f \in I(V)\}$$

Corollaire

Si K est algébriquement clos, les applications V et I induisent des bijections réciproques l'une de l'autre entre les parties algébriques de K^n et les idéaux radicaux de $K[X_1; \dots; X_n]$.

Le cas des corps finis

Cas des corps finis : $K = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

V variété algébrique projective lisse sur \mathbb{F}_p .

Question : Peut-on calculer le nombre d'éléments de $V(\mathbb{F}_{p^m})$ pour tout $m \geq 1$?

Conjectures de Weil :

- 1924 : énoncées pour les courbes par Artin.
- 1948 : démontrées pour les courbes par Weil.
- 1949 : énoncées pour les variétés de dimension supérieure par Weil.
- 1964 : une partie des conjectures démontrée indépendamment par Artin et Grothendieck d'un côté et Dwork de l'autre.
- 1974 : preuve complète par Deligne.

Le cas des corps finis

Hypothèse : $V = C$ est une courbe.

Fonction zêta associée à la courbe C :

$$Z_C(T) := \exp \left(\sum_{m=1}^{\infty} \frac{jC(\mathbb{F}_{p^m})}{m} T^m \right) \in \mathbb{Q}[[T]]:$$

Exemple : $C = \mathbb{P}_{\mathbb{F}_p}^1$.

Alors $jC(\mathbb{F}_{p^m}) = 1 + p^m$, donc :

$$Z_C(T) = \frac{1}{(1-T)(1-pT)}:$$

Théorème (Conjectures de Weil pour les courbes, Weil 1948)

Soit \mathcal{C} une courbe lisse sur \mathbb{Q} qui relève C .

1. (Rationalité) La fonction $Z_{\mathcal{C}}$ est une fraction rationnelle :

$$Z_{\mathcal{C}}(T) = \frac{\prod_{j=1}^{2g} (1 - \alpha_j T)}{(1 - T)(1 - pT)}$$

où g est le genre de la courbe complexe $\mathcal{C}(\mathbb{C})$.

Le cas des corps finis

Théorème (Conjectures de Weil pour les courbes, Weil 1948)

2. (Equation fonctionnelle) La fonction Z_C vérifie une équation fonctionnelle :

$$Z_C \left(\frac{1}{pT} \right) = p^{x/2} T^x Z_C(T);$$

où $x = 2 - 2g$ est la caractéristique d'Euler-Poincaré de $\mathcal{C}(\mathbb{C})$.

3. (Hypothèse de Riemann) $\rho_j = \bar{\rho}_j$ pour tout j .

Corollaire

$$|jC(\mathbb{F}_{p^m})j| = 1 + p^m \prod_j \rho_j^m$$

Le cas des corps finis

Exemple : C est une courbe elliptique (genre 1) :

$$y^2z = (x - x_1z)(x - x_2z)(x - x_3z); \quad x_i \text{ deux à deux distincts.}$$

Alors :

$$Z_C(T) = \frac{(1 - \alpha T)(1 - \beta T)}{(1 - T)(1 - qT)}$$

avec α, β ; deux nombres complexes conjugués avec $|\alpha| = |\beta| = \rho$, et :

$$|j_C(F_{p^m})| = 1 + p^m - \alpha^m - \beta^m.$$

Le cas du corps des nombres rationnels

Cas $K = \mathbb{Q}$:

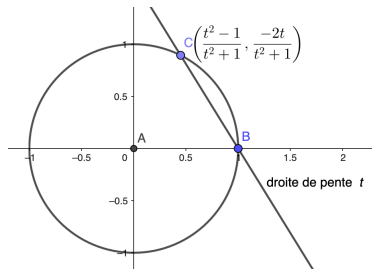
- C courbe projective lisse sur \mathbb{Q} .
- g genre de la courbe complexe $C(\mathbb{C})$.

Le cas du corps des nombres rationnels

- Si $g = 0$, alors C est une conique :

$$q(x_0; x_1; x_2) = 0$$

avec q forme quadratique. Si $C(\mathbb{Q}) \neq \emptyset$, alors C admet un paramétrage rationnel : pour tout corps K de caractéristique 0, on a $C(K) = \mathbb{P}^1(K)$.

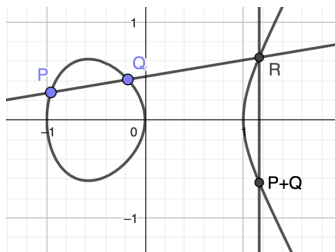


Le cas du corps des nombres rationnels

- Si $g = 1$, alors C est une courbe elliptique :

$$y^2z = (x - x_1z)(x - x_2z)(x - x_3z); \quad x_i \text{ deux à deux distincts:}$$

On a alors une loi de groupe abélien sur $C(\mathbb{Q})$:



Théorème (Théorème de Mordell, 1922)

Le groupe $C(\mathbb{Q})$ est de type fini.

Le cas du corps des nombres rationnels

- Si $g \geq 2$, on a le théorème suivant, conjecturé par Mordell en 1922 et démontré par Faltings en 1983 :

Théorème (Théorème de Faltings, 1983)

Si $g \geq 2$, l'ensemble $C(\mathbb{Q})$ est fini.

Et en dimension supérieure ?

Le cas du corps des nombres rationnels : conjectures

Courbes	dim > 1
$g = 0$: la courbe $C(\mathbb{C})$ admet un para- métrage rationnel	<ul style="list-style-type: none"> • Variétés rationnelles : $V(\mathbb{C})$ admet un paramétrage rationnel. • Variétés rationnellement connexes (Kollár, Miyaoka, Mori, 1990) : par deux points de $V(\mathbb{C})$ passe une courbe rationnelle. <p>Ex. : $V_p(F) \subset \mathbb{P}^n$ avec $\deg F = n$.</p> <p>Conjecture (Colliot-Thélène, 1990) : contrôle des obstructions à l'existence de points rationnels sur les variétés rationnellement connexes.</p> <p>Ex. avec $(n; \deg F) \notin (3; 3)$: l'équation $F = 0$ devrait avoir des solutions non triviales dans \mathbb{Q} ssi elle a des solutions modulo tout entier naturel.</p>

Le cas du corps des nombres rationnels : conjectures

Courbes	dim > 1
$g = 1$: la courbe $C(\mathbb{C})$ ad- met une loi de groupe abélien dé- finie par des fractions rationnelles	Variétés abéliennes : $V(\mathbb{C})$ admet une loi de groupe abélien définie par des fractions rationnelles. Théorème (Mordell-Weil, 1929) : le groupe $V(\mathbb{C})$ est de type fini. Conjecture de Birch et Swinnerton-Dyer (années 1960) : formule pour le rang de $V(\mathbb{C})$ en termes de fonction L .

Le cas du corps des nombres rationnels : conjectures

Courbes	dim > 1
$g \geq 2$: la courbe $C(\mathbb{C})$ n'ad- met pas d'applica- tion holo- morphe non constante $\mathbb{C} \not\rightarrow C(\mathbb{C})$	Variétés hyperboliques : $V(\mathbb{C})$ n'admet pas d'application holomorphe non constante $\mathbb{C} \rightarrow V(\mathbb{C})$. Ex. : une hypersurface <i>générale</i> $V_p(F) \subset \mathbb{P}^n$ avec $\deg F$ suffisamment grande par rapport à n (Brotbek, 2017). Conjecture de Lang (1974) : finitude du nombre de points rationnels.

Merci !

Merci pour votre attention !