Petite introduction à la géométrie algébrique et arithmétique

Diego Izquierdo

CMLS - École Polytechnique

Vendredi 17 mai 2024

Variétés algébriques

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

Variétés algébriques

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

$$f_1(x) = \cdots = f_m(x) = 0.$$

$\rightsquigarrow$ **Variété algébrique affine** sur K.

- L/K extension de corps :

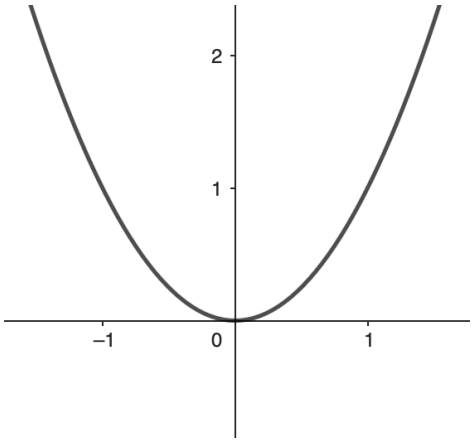
$$V(L) := \{\text{solutions du sytème } V \text{ dans } L^n\}.$$

$\rightsquigarrow$ **Points L-rationnels** de V. $\rightsquigarrow$ **Partie algébrique** de L^n.

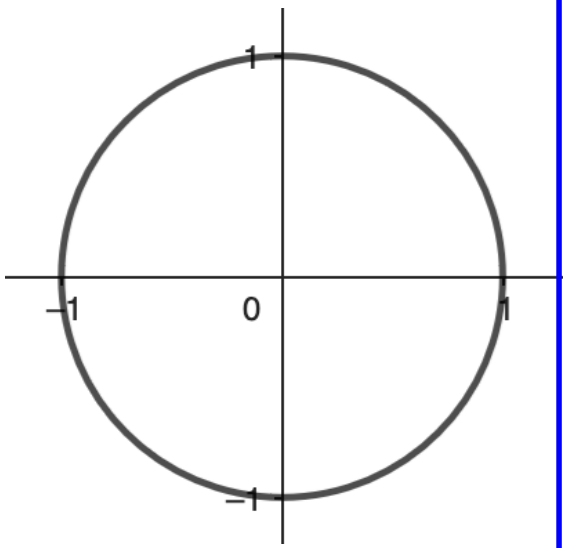
Variétés algébriques

Exemples :

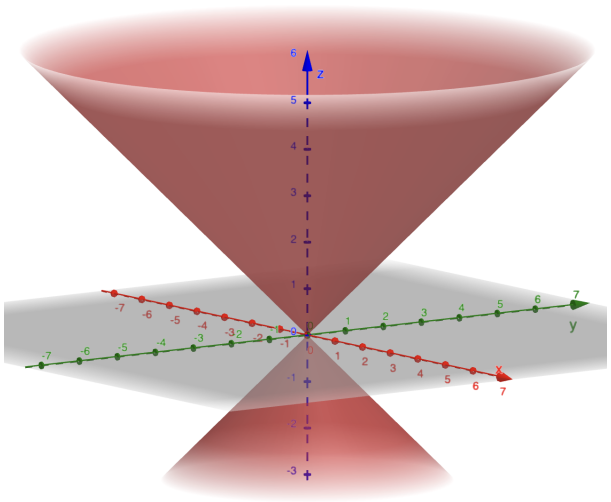
$V = V(Y - X^2)$



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



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



Variétés algébriques

- Espace projectif de dimension n :

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

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

$$(x_0 : \ldots : x_n) = (y_0 : \ldots : y_n) \Leftrightarrow$$
$$\exists \lambda \in K^\times, (x_0, \ldots, x_n) = \lambda(y_0 : \ldots : y_n).$$

Variétés algébriques

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

$$f_1(x) = \cdots = f_m(x) = 0.$$

$\rightsquigarrow$ **Variété algébrique projective** sur K.

- L/K extension de corps :

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

$\rightsquigarrow$ **Points L-rationnels** de V.
$\rightsquigarrow$ **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**...
  $\Rightarrow$ Notion de **schéma**.

Le problème des points rationnels

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

Cas géométrique : le corps K est algébriquement clos.

Théorème (Théorème des zéros de Hilbert, 1893)

- *K corps algébriquement clos.*
- $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$.
- $V := V(f_1, \ldots, f_m)$.

On a :

$$V(K) = \emptyset \Leftrightarrow \exists g_1, \ldots, g_m \in K[X_1, \ldots, X_n], \sum g_i f_i = 1$$
$$\Leftrightarrow (f_1, \ldots, f_m) = K[X_1, \ldots, X_n].$$

Le cas géométrique

$$V : \{\text{idéaux de } K[X_1, \ldots, X_n]\} \leftrightarrow \{\text{parties algébriques de } K^n\} : I$$

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

$$I(V) := \{f \in K[X_1, \ldots, X_n] : \quad \hookleftarrow V$$

$$\forall x \in V, f(x) = 0\}$$

$I(V)$ est un idéal **radical** :

$$\forall f \in K[X_1, \ldots, X_n], \forall m \geq 0, f^m \in I(V) \Rightarrow f \in I(V).$$

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 $K[X_1, \ldots, X_n]$.

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 indémendamment par **Artin** et **Grothendieck** d'un côté et **Dwork** de l'autre.
- 1974 : preuve complète par **Deligne**.

Le cas des corps finis

Hypthèse : $V = C$ est une courbe.

Fonction zêta associée à la courbe C :

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

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

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

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

Le cas des corps finis

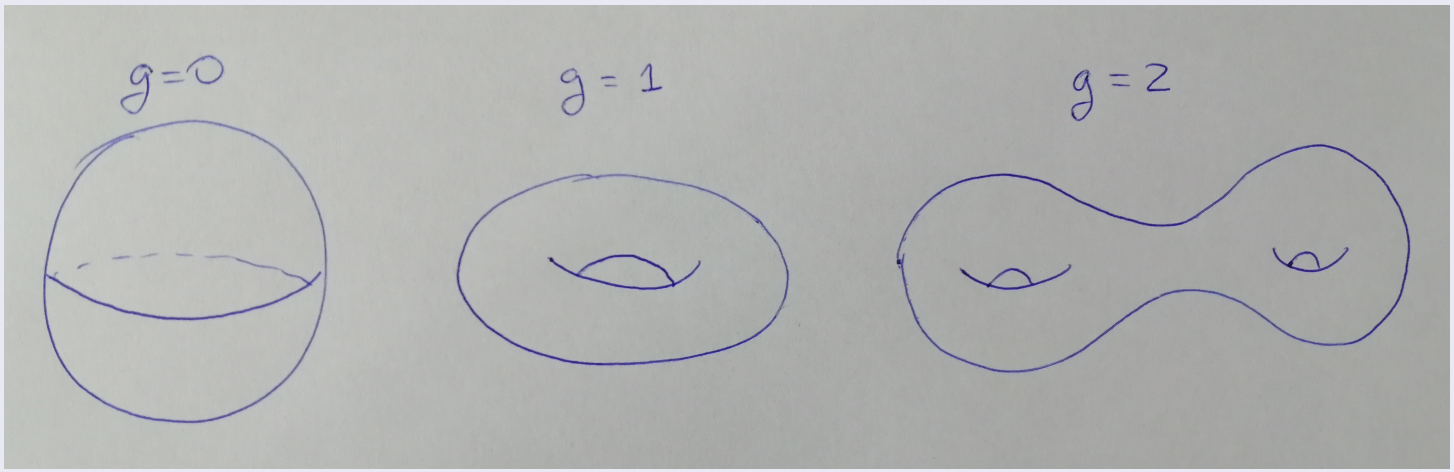
Théorème (Conjectures de Weil pour les courbes, Weil 1948)

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

1. *(Rationnalité) La fonction Z_C est une fraction rationnelle :*

$$Z_C(T) = \frac{\prod_{j=1}^{2g}(1-\alpha_j T)}{(1-T)(1-pT)},$$

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



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 :*

$$Z_C\left(\frac{1}{pT}\right) = \pm p^{\chi/2} T^{\chi} Z_C(T),$$

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

3. *(Hypothèse de Riemann) $|\alpha_j| = \sqrt{p}$ pour tout j.*

Corollaire

$$|C(\mathbb{F}_{p^m})| = 1 + p^m - \sum_j \alpha_j^m.$$

Le cas des corps finis

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

$$y^2z = (x - \lambda_1 z)(x - \lambda_2 z)(x - \lambda_3 z), \quad \lambda_i \text{ deux à deux distincts.}$$

Alors :

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

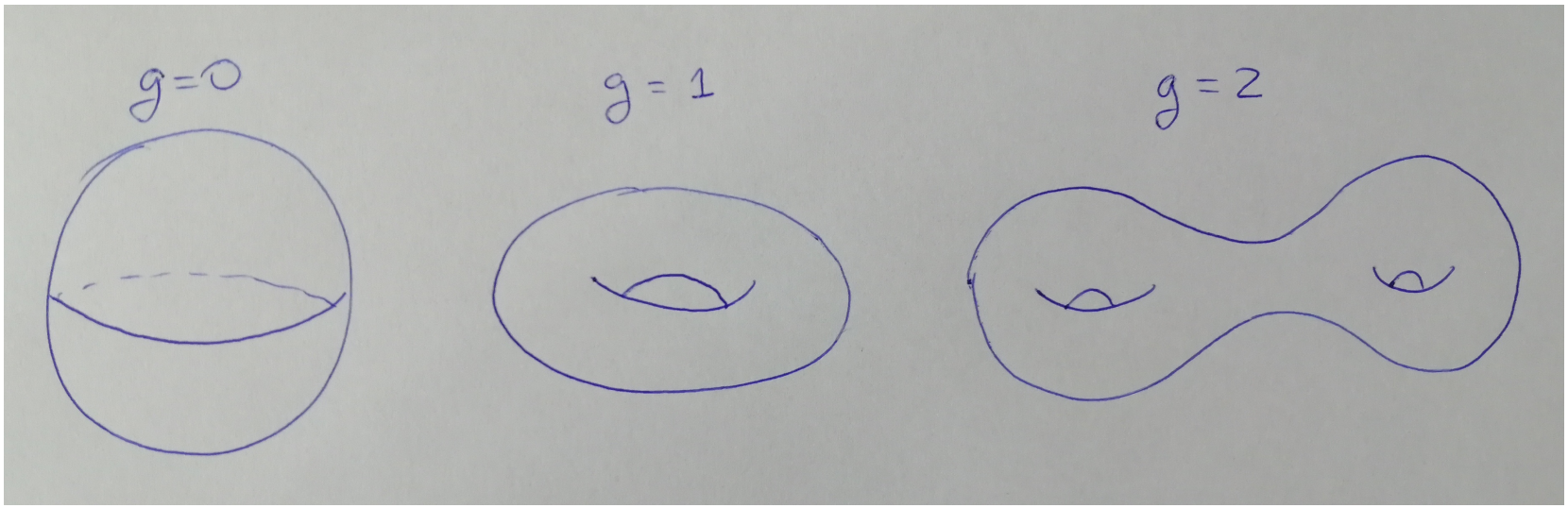
avec α, β deux nombres complexes conjugués avec $\alpha\beta = p$, et :

$$|C(\mathbb{F}_{p^m})| = 1 + p^m - \alpha^m - \beta^m.$$

Le cas du corps des nombres rationnels

Cas $K = \mathbb{Q}$:

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

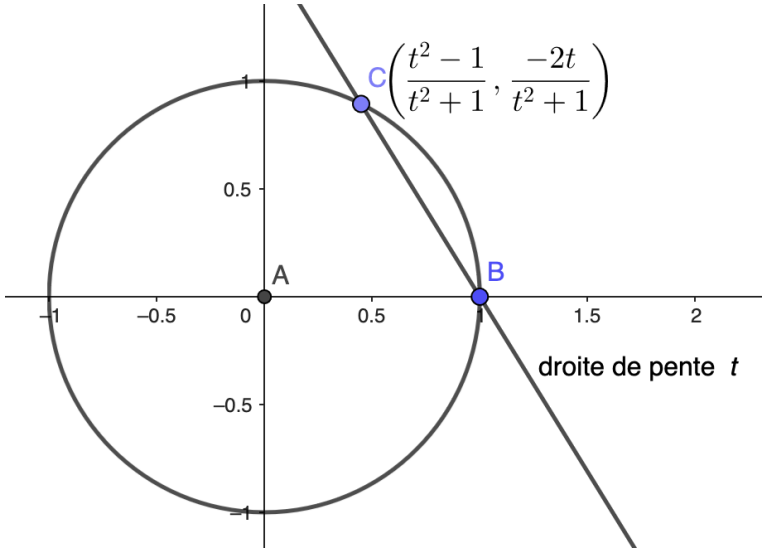


Le cas du corps des nombres rationnels

- 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 $C(K) \cong \mathbb{P}^1(K)$.

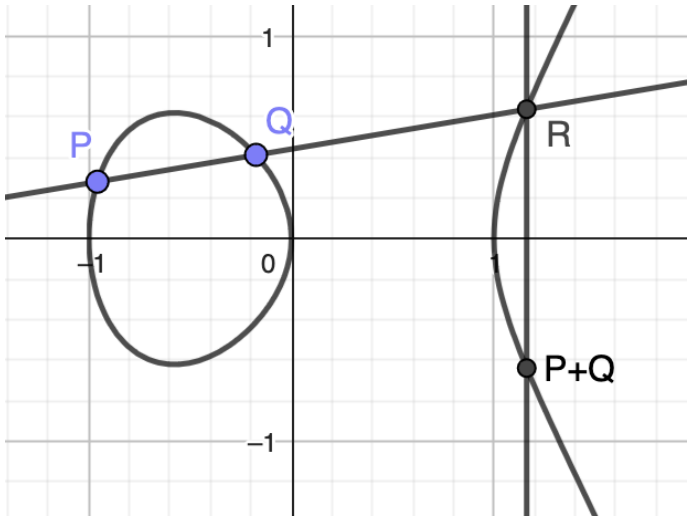


Le cas du corps des nombres rationnels

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

  $y^2 z = (x - \lambda_1 z)(x - \lambda_2 z)(x - \lambda_3 z), \quad \lambda_i$ 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 paramétrage rationnel	• **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. **Ex. :** $V_p(F) \subset \mathbb{P}^n$ avec $\deg F \leq n$. **Conjecture** (Colliot-Thélène, 1990) : contrôle des obstructions à l'existence de points rationnels sur les variétés rationnellement connexes. **Ex. avec** $(n, \deg F) \neq (3,3)$ **:** l'équation $F = 0$ devrait avoir des solutions non triviales dans $\mathbb{Q}$ ssi elle a des solutions modulo tout entier naturel.

Le cas du corps des nombres rationnels : conjectures

Courbes	dim > 1
$g = 1$: la courbe $C(\mathbb{C})$ admet une loi de groupe abélien définie 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'admet pas d'application holomorphe non constante $\mathbb{C} \to C(\mathbb{C})$	**Variétés hyperboliques** : $V(\mathbb{C})$ n'admet pas d'application holomorphe non constante $\mathbb{C} \to V(\mathbb{C})$. **Ex. :** une hypersurface *générale* $V_p(F) \subset \mathbb{P}^n$ 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 !