

Cours 1 : Introduction

Bertrand Toën

Lundi 2 Mars 2020

1 Solutions de systèmes polynomiaux

On se fixe un système d'équations polynomiales

$$X : \begin{cases} F_1(X_1, \dots, X_n) = 0 \\ F_2(X_1, \dots, X_n) = 0 \\ \vdots \\ F_p(X_1, \dots, X_n) = 0 \end{cases}$$

Ici, les F_i sont des polynômes à n variables à coefficients dans un anneau commutatif A

$$F_i \in A[X_1, \dots, X_n].$$

De manière naïve, une *solution du système* X est la donnée de $(x_1, \dots, x_n) \in A^n$ tel que l'on ait

$$F_i(x_1, \dots, x_n) = 0 \forall i = 1, \dots, p.$$

Ces solutions forment un sous-ensemble $X(A) \subset A^n$. Cependant, le système X peut avoir très peu, voire pas du tout, de solutions dans A . On est donc amenés à poser la définition suivante.

Définition 1.1 Une solution du système X à valeurs dans un anneau (commutatif) B est un couple $(u, (x_1, \dots, x_n))$ avec

1. $u : A \longrightarrow B$ un morphisme d'anneaux

2. $(x_1, \dots, x_n) \in B^n$

et tels que

$$u(F_i)(x_1, \dots, x_n) = 0 \forall i = 1, \dots, p.$$

L'ensemble des solutions de X à valeurs dans B est un sous-ensemble de B^n noté $X(B)$.

Étudier un système X c'est étudier ses solutions à valeurs dans des anneaux variés B .

Exemples.

1. $A = \mathbb{Z}$ et $F_1(X) = X^2 + 1$ ($n = p = 1$). Alors

$$X(\mathbb{R}) = \emptyset \quad X(\mathbb{C}) = \{i, -i\}.$$

2. $A = \mathbb{Q}(T)$ et $F_1(X_1, X_2) = X_1 - X_2$. Alors

$$X(\mathbb{Q}(T)) \simeq \mathbb{Q}(T) \quad X(\mathbb{Q}) = \emptyset.$$

3. $A = \mathbb{Z}$ et $F_1(X_1, X_2)$ non constant. Alors $X(\mathbb{C})$ est infini et $X(\mathbb{F}_q)$ est toujours fini.

Dans ce cours nous allons nous intéresser aux interactions entre solutions à valeurs complexes et solutions à valeurs dans des corps finis.

2 Solutions à l'infini et espaces projectifs

Pour un système

$$X : \begin{cases} F_1(X_1, \dots, X_n) = 0 \\ F_2(X_1, \dots, X_n) = 0 \\ \vdots \\ F_p(X_1, \dots, X_n) = 0 \end{cases}$$

les ensembles de solutions $X(B)$ ne voient pas les *solutions situées à l'infini*.

Exemple. $F_1(X_1, X_2) = X_1 X_2 - 1$ et $B = \mathbb{R}$. Il existe de manière évidente des points à l'infini, deux en l'occurrence.

Pour chaque F_i on définit $\tilde{F}_i(X_0, \dots, X_n)$ l'unique polynôme homogène de même degré que F_i et tel que

$$\tilde{F}_i(1, X_1, \dots, X_n) = F_i(X_1, \dots, X_n).$$

Pour un corps K on a l'espace projectif de dimension n

$$\mathbb{P}^n(K) = (K^{n+1} - \{0\})/K^*.$$

Il contient K^n par l'inclusion canonique

$$K^n \hookrightarrow \mathbb{P}^n(K)$$

qui envoie $(x_1, \dots, x_n)$ sur $(1, x_1, \dots, x_n) \in K^{n+1} - \{0\}$.

Définition 2.1 Une solution complète du système X à valeurs dans un corps K est un couple $(u, (x_0, x_1, \dots, x_n))$ avec

1. $u : A \longrightarrow K$ un morphisme d'anneaux

2. $(x_0, \dots, x_n) \in \mathbb{P}^n(K)$

et tels que

$$u(\tilde{F}_i)(x_0, \dots, x_n) = 0 \forall i = 1, \dots, p.$$

L'ensemble des solutions complètes de X à valeurs dans K est un sous-ensemble de $\mathbb{P}^n(K)$ noté $\bar{X}(K)$.

Les éléments de $\bar{X}(K)$ qui ne sont pas dans $X(K) \subset \bar{X}(K)$ sont, par définition, les solutions à l'infini de X .

Exemple. $F_1(X_1, X_2) = X_1X_2 - 1$ et $\widetilde{F_1}(X_0, X_1, X_2) = X_1X_2 - X_0^2$. L'ensemble des solutions $X(K)$ est en bijection avec K^* , par la bijection $\lambda \mapsto (\lambda, \lambda^{-1}) \in X(K)$. L'ensemble $\bar{X}(K)$ possède deux points supplémentaires $(0, 1, 0)$ et $(0, 0, 1)$. L'ensemble $\bar{X}(K)$ est donc en bijection avec $K \cup \{\infty\} \simeq \mathbb{P}^1(K)$.

3 Solutions dans un corps fini

Soit un système polynômial

$$X : \begin{cases} F_1(X_1, \dots, X_n) = 0 \\ F_2(X_1, \dots, X_n) = 0 \\ \vdots \\ F_p(X_1, \dots, X_n) = 0 \end{cases}$$

avec $F_i \in \mathbb{Z}[X_1, \dots, X_n]$, et $q = p^m$ avec p un nombre premier. Il existe un unique morphisme d'anneaux $\mathbb{Z} \longrightarrow \mathbb{F}_q$, et l'on peut donc considérer les F_i , de manière non ambiguë, comme des polynômes à coefficients dans le corps fini $\mathbb{F}_q$ (réduction des coefficients mod p).

Ainsi, on dispose d'un ensemble fini de solutions complètes dans $\mathbb{F}_q$ $\bar{X}(\mathbb{F}_q) \subset \mathbb{P}^n(\mathbb{F}_q)$ et donc d'un nombre entier naturel

$$N(\bar{X}, q) := |\bar{X}(\mathbb{F}_q)| \in \mathbb{N}.$$

Lorsque q varie, la familles de nombres $N(\bar{X}, q)$ décrit la répartition des solutions de X dans les corps finis.

4 Solutions complexes

Soit de nouveau un système polynômial homogène

$$X : \begin{cases} F_1(X_1, \dots, X_n) = 0 \\ F_2(X_1, \dots, X_n) = 0 \\ \vdots \\ F_p(X_1, \dots, X_n) = 0 \end{cases}$$

avec $F_i \in \mathbb{Z}[X_1, \dots, X_n]$. Il existe un unique morphisme d'anneaux $\mathbb{Z} \longrightarrow \mathbb{C}$ et l'on peut donc considérer les F_i , de manière non ambiguë, comme des polynômes à coefficients complexes. L'ensemble des solutions complètes $\bar{X}(\mathbb{C})$ est alors un sous-ensemble de l'espace projectif $\mathbb{P}^n(\mathbb{C})$. Il s'agit généralement d'un ensemble infini non dénombrable. On le munit donc de la topologie induite par la topologie usuelle sur $\mathbb{C}^n$. C'est un espace topologique compact (car $\mathbb{P}^n(\mathbb{C})$ est un espace compact).

L'espace topologique $\bar{X}(\mathbb{C})$ possède des *invariants homologiques* (voir cours 2) : une caractéristique d'Euler $\chi(\bar{X}(\mathbb{C})) \in \mathbb{Z}$ et des nombres de Betti $b_i(\bar{X}(\mathbb{C})) \in \mathbb{N}$. Ils sont reliés par la formule

$$\chi(\bar{X}(\mathbb{C})) = \sum_i (-1)^i b_i(\bar{X}(\mathbb{C})).$$

Ces invariants seront définis lors du cours 2.

L'espace projectif $\mathbb{P}(\mathbb{C})$ est naturellement une variété complexe, et si le système $\bar{X}$ vérifie le critère jacobien en chacun de ses points le sous-espace $\bar{X}(\mathbb{C}) \subset \mathbb{P}^n(\mathbb{C})$ est un sous-variété complexe de l'espace projectif.

5 Une version des conjectures de Weil

Le but du cours est d'expliquer le théorème suivant.

Théorème 5.1 *Soit X un système d'équation polynômial*

$$X : \begin{cases} F_1(X_1, \dots, X_n) = 0 \\ F_2(X_1, \dots, X_n) = 0 \\ \vdots \\ F_p(X_1, \dots, X_n) = 0 \end{cases}$$

On suppose que $\bar{X}(\mathbb{C}) \subset \mathbb{P}^n(\mathbb{C})$ est une sous-variété. Alors, la famille de nombres $N(\bar{X}, q)$ (pour q variable) détermine les nombres $b_i(\bar{X}(\mathbb{C}))$ (et donc aussi $\chi(\bar{X}(\mathbb{C}))$).

Nous donnerons l'énoncé précis dans les cours suivants, mais signalons qu'il existe une formule explicite qui donne les b_i en termes des $N(\bar{X}, q)$.

6 Un exemple : espaces projectifs

Exemple fondamental : $F_i = 0$ et donc $\bar{X}(\mathbb{C}) = \mathbb{P}^n(\mathbb{C})$ et $\bar{X}(\mathbb{F}_q) = \mathbb{P}^n(\mathbb{F}_q)$.

Ensemblistement on a

$$\mathbb{P}^n(K) \simeq K^n \coprod \mathbb{P}^{n-1}(K)$$

En particulier

$$N(\bar{X}, q) = \sum_{i=0, \dots, n} q^i.$$

L'espace topologique $\mathbb{P}^n(\mathbb{C})$ est obtenu par un rajout de cellules

$$\mathbb{P}^n(\mathbb{C}) \simeq \mathbb{P}^{n-1}(\mathbb{C}) \cup_{S^{2n-1}} B^{2n}.$$

Ici

$$S^{2n-1} \hookrightarrow \mathbb{C}^n - 0 \longrightarrow \mathbb{P}^{n-1}(\mathbb{C})$$

est la *fibration de Hopf*. On a donc $n+1$ cellules, et une cellule en chaque dimension paire entre 0 et $2n$.

$$q^i \longleftrightarrow \{\text{Cellules de dimension } 2i\}$$

En particulier jolie formule

$$\lim_{q \rightarrow 1} N(\bar{X}, q) = \chi(\bar{X}(\mathbb{C})).$$