Géométrie algébrique 2016/17

§2. L'algèbre commutative

Soit $\mathbb{K}$ un corps (par exemple le corps $\mathbf{R}$ des réels, ou $\mathbf{C}$ les complexes). On considère des polynômes $f(x_1, \ldots, x_n)$ en n variables avec coefficients dans $\mathbb{K}$. Un tel polynôme est une somme de termes du type $ax_1^{\alpha_1} \cdots x_n^{\alpha_n}$, où $a \in k$; on l'appelle un *monôme*. On écrit $\mathbb{K}[x_1, \ldots, x_n]$ pour l'espace de tous les polynômes en n variables avec coefficients dans $\mathbb{K}$. Muni des opérations de addition et de multiplication, l'ensemble $\mathbb{K}[x_1, \ldots, x_n]$ est un *anneau commutatif.* En plus $\mathbb{K}[x_1, \ldots, x_n]$ est un espace vectoriel sur $\mathbb{K}$ muni de la base de tous les monômes : $\{x_1^{\alpha_1} \cdots x_n^{\alpha_n} : \alpha_j \in \mathbf{N}, j = 1, \ldots, n\}$.

Pour chaque entier positif n on définit *l'espace affine* de dimension n :

$$\mathbb{K}^n = \{(a_1, \ldots, a_n) : a_j \in \mathbb{K}, j = 1, \ldots, n\} .$$

Un polynôme $f \in \mathbb{K}[x_1, \ldots, x_n]$ détermine une fonction $\mathbb{K}^n \to \mathbb{K}$ par

$$(a_1, \ldots, a_n) \mapsto f(a_1, \ldots, a_n) ;$$

on l'appelle *évalutation.* On a donc deux façons de voir un polynôme : comme un élément de l'anneau $\mathbb{K}[x_1, \ldots, x_n]$ ou comme une fonction $\mathbb{K}^n \to \mathbb{K}$.

Pour $f \in \mathbb{K}[x_1, \ldots, x_n]$ on définit $V(f)$ comme l'ensemble des solutions à l'équation $f = 0$:

$$V(f) = \{(a_1, \ldots, a_n) \in \mathbb{K}^n : f(a_1, \ldots, a_n) = 0\} \subset \mathbb{K}^n ;$$

on l'appelle la *variété (algébrique) définie par f.*

Plus généralement, données $f_1, \ldots f_k \in \mathbb{K}[x_1, \ldots, x_n]$, la variété $V(f_1, \ldots, f_k)$ est définie comme l'ensemble de toutes les équations $f_1 = 0, \ldots, f_k = 0$:

$$V(f_1, \ldots, f_k) = \{(a_1, \ldots, a_n) \in \mathbb{K}^n : f_j(a_1, \ldots, a_n) = 0, j = 1, \ldots k\} = \cap_{j=1}^k V(f_j) .$$

Par exemple, la variété $V(x^2 + y^2 + z^2 - 1, x^2 + y^2 - z^2 - 1)$ est l'intersection d'une sphère et d'un hyperboloïde dans l'espace à trois dimensions. Plus géneral encore, pour $S \subset \mathbb{K}[x_1, \ldots, x_n]$, on définit

$$V(S) = \{(a_1, \ldots, a_n) \in \mathbb{K}^n : f(a_1, \ldots, a_n) = 0 \ \forall f \in S\} .$$

C'est *l'ensemble algébrique défini par S.*

Une façon de mieux comprendre l'ensemble des solutions à un système d'équations polynomiales est de trouver une meilleure représentation. Pour ça on considére l'idéal engendré par des polynômes.

Soient $f_1, \ldots f_k \in \mathbb{K}[x_1, \ldots, x_n]$. Alors, *l'idéal engendré par $f_1, \ldots, f_k$* est le sous-ensemble de $\mathbb{K}[x_1, \ldots, x_n]$ donné par

$$(f_1, \ldots, f_k) = \left\{ \sum_{j=1}^k u_j f_j : u_j \in \mathbb{K}[x_1, \ldots, x_n], j = 1, \ldots, k \right\} .$$

On voit que $I = (f_1, \dots, f_k)$ est bien un idéal ; en effet, si $f, g \in I$ il en est de même pour $f + g$ et si $f \in I$ et $h \in \mathbb{K}[x_1, \dots, x_n]$ et quelconque, alors $hf \in I$ (c'est la définition d'idéal). L'ensemble $\{f_1, \dots, f_k\}$ s'appelle un *ensemble générateur* pour I. On laisse la preuve du lemme suivant comme un exercice.

Lemma 0.1. *$V(I) = V(f_1, \dots, f_k)$; donc la variété est déterminée par l'idéal plutôt que par un ensemble générateur.*

Par exemple, dans $\mathbb{K}[x, y]$, on a $(x + y, x) = (x, y) = (x + xy, x^2, y^2, y + xy)$.

Exercises :

• Soit $\{I_\alpha\}$ une famille d'idéaux. Montrer que $V(\cup_\alpha I_\alpha) = \cap_\alpha V(I_\alpha)$, donc l'intersection d'une famille d'ensembles algébriques est algébrique.

• Si $I \subset J$ (I, J des idéaux), montrer que $V(I) \supset V(J)$.

• Pour des polynômes f et g montrer que $V(fg) = V(f) \cup V(g)$.

• Montrer que $V(I) \cup V(J) = V\{fg : f \in I, \ g \in J\}$; en particulier, toute réunion finie d'ensembles algébriques est aussi algébrique.

• Montrer que $V(0) = \mathbb{K}^n$ et que $V(1) = \emptyset$.

• Montrer que l'ensemble $\{(t, t^2, t^3) \in \mathbb{K}^3 : t \in \mathbb{K}\}$ est algébrique.

Maintenant, on change de perspective. On considère un ensemble de points $V \subset \mathbb{K}^n$. Soit $I(V)$ l'idéal dans $\mathbb{K}[x_1, \dots, x_n]$ défini par

$$I(V) = \{f \in \mathbb{K}[x_1, \dots, x_n] : f(a_1, \dots, a_n) = 0, \ \forall (a_1, \dots, a_n) \in V\} .$$

Vérifier que $I(V)$ est bien un idéal. Si V est définie par un ensemble de polynômes $f_1 = 0, \dots, f_k = 0$, quelle est la relation entre $I(V)$ et l'idéal $(f_1, \dots, f_k)$? Est-ce-que $V(I(V) = V$? Afin de répondre à ces questions on doit établir deux théorèmes fondamentaux : *le théorème de la base de Hilbert et le théorème de zéros de Hilbert : le Nullstellensatz.*

Theorem 0.2. Théorème de la base de Hilbert) *Dans l'anneau $\mathbb{K}[x_1, \dots, x_n]$ les deux propriétés suivantes sont vérifiées :*

(i) Soit $I \subset \mathbb{K}[x_1, \dots, x_n]$ in idéal, alors il existent polynômes $f_1, \dots, f_k \in \mathbb{K}[x_1, \dots, x_n]$ tels que $I = (f_1, \dots, f_k)$.

(ii) Soit $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ une chaîne croissante d'idéaux dans $\mathbb{K}[x_1, \dots, x_n]$, alors il existe N tel que $I_N = I_{N+1} = I_{N+2} = \cdots$.

Dans un anneau quelconque, un idéal qui vérifie la condition (i) s'appelle un *idéal finiment engendré.* La condition (ii) s'appelle *la condition à chaînes croissante sur idéaux.* Un anneau commutatif qui vérifie à cette condition s'appelle un *anneau noethérien.* D'abord on montre que les deux conditions sont équivalentes.

Lemma 0.3. *Dans un anneau commutatif R quelconque, les conditions (i) et (ii) du Théorème 0.2 sont équivalentes.*

Preuve : Supposons d'abord (i) et soit

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

une suite croissante d'idéaux de R. On considère $I = \cup_{n=1}^{\infty} I_n$. Puisque la suite est croissante, on voit facilement que I est un idéal dans R. Par la condition (i) on a $I = (f_1, \ldots, f_k)$ pour des éléments $f_1, \ldots, f_k \in R$. Alors, pour $j = 1, \ldots, k$ on a $f_j \in I$ et donc il existe N_j tel que $f_j \in I_{N_j}$. Soit $N = \max_{1 \leq j \leq k} N_j$; alors f_j est dans I_N pour tout $j = 1, \ldots, k$ et donc $I \subseteq I_N$. Il s'ensuit que $I = I_N$ et la condition (ii) est vérifiée.

Reciproquement, supposons qu'il existe un idéal I qui n'est pas engendré par un nombre fini d'éléments de R. Soit $f_1 \in I$. Alors il existe $f_2 \in I$ avec $f_2 \notin (f_1)$. Donc on a $(f_1) \subset (f_1, f_2)$ avec l'inclusion stricte. On continue afin de construire une chaîne strictement croissante d'idéaux ; ce qui contredit la condition (ii). q.e.d.

On démontre une version plus générale du théorème de la base de hilbert.

Theorem 0.4. *Si R est un anneau noethérien, il en est de même pour $R[x_1, \ldots, x_n]$.*

Preuve : Puisque $R[x_1, \ldots, x_n]$ est isomorphe à $R[x_1, \ldots, x_{n-1}][x_n]$, le théorème suivra par récurrence si on peut démontrer que $R[x]$ est noethérien lorsque R est noethérien. Soit I un idéal dans $R[x]$. On doit trouver un ensemble fini de générateurs pour I.

Soit $f = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 + a_0 \in R[x]$ avec $a_d \neq 0$; on appelle a_d le coefficient principal de f. soit J l'ensemble des coefficients principaux de tous les polynômes dans I. Alors J est un idéal dans R donc il existent des polynômes $f_1, \ldots, f_k \in I$ dont les coefficients principaux engendrent J. On prend un entier N plus grand que le degré de chaque f_j. Pour chaque $m \leq N$, soit J_m l'idéal de R qui consiste de tous les coefficients principaux de tous les polynômes $f \in I$ dont le degré est $\leq m$. Soit $\{f_{mj}\}$ un ensemble fini de polynômes dans I de degré $\leq m$ dont les coefficients principaux engendrent J_m. Soit I' l'idéal engendré par les f_i et les f_{mj}. Il suffit de démontrer que $I = I'$.

Supposons que $I' \subset I$ avec l'inclusion stricte ; soit $g \in I$ un élément de plus bas degré qui n'est pas dans I'. Si le degré de g est $> N$ on peut trouver des polynômes q_j tels que $\sum q_j f_j$ et g ont les mêmes termes principaux. Mais dans ce cas le degré de $g - \sum q_j f_j$ est inférieur au degré de g, d'où $g - \sum q_j f_j \in I'$, d'où $g \in I'$. De même si le degré m de g est $\leq N$, on peut diminuer le degré en considérant $g - \sum q_j f_{mj}$ pour des polynômes q_j. Ce qui démontre le théorème. q.e.d.

Puisque tout corps $\mathbb{K}$ est trivialement noethérien, on a le corollaire :

Corollary 0.5. $\mathbb{K}[x_1, \ldots, x_n]$ *est noethérien pour tout corps* $\mathbb{K}$.

Exemple : Soit V l'ensemble $V = \{(0,0), (0,1), (1,0)\} \subset \mathbf{R}^2$. On veut trouver un ensemble générateur de l'idéal $I(V) \subset \mathbf{R}[x, y]$. On voit que $x(x-1)$ et $y(y-1)$ sont dans $I(V)$, Mais

$V(x(x-1)) \cap V(y(y-1)) = \{(0,0),(0,1),(1,0),(1,1)\}$. Il faut alors ajouter le polynôme xy, et on voit que $I(V) = (x(x-1), xy, y(y-1))$.

Un *ensemble algébrique* dans $\mathbb{K}^n$ est un ensemble du type

$$V(S) = \{x \in \mathbb{K}^n : f(x) = 0 \text{ pour tout } f \in S\}$$

où $S \subset \mathbb{K}[x_1, \ldots, x_n]$. On a vu une corréspondance :

$$\left\{ \begin{array}{c} \text{ensembles algebriques} \\ \text{dans } \mathbb{K}^n \end{array} \right\} \begin{array}{c} I \\ \to \\ \leftarrow \\ V \end{array} \left\{ \begin{array}{c} \text{ideaux dans} \\ \mathbb{K}[x_1, \ldots, x_n] \end{array} \right\}$$

On veut étudier cette corréspondance en plus de détail.

On utilise la notation $I \lhd R$ pour indiquer que I est un idéal dans R. Un idéal propre I dans un anneau R est *maximal* s'il n'y a pas d'autre idéal propre J qui contient strictement I. C'est à dire, si $I \subseteq J \lhd R$ avec $J \neq R$ alors $I = J$. Donné un anneau commutatif R et un idéal $I \lhd R$ on définit le *quotient* R/I comme l'ensemble de classes d'équivalences $[a] = a + I := \{a + r : r \in I\}$, autrement $a \sim b \leftrightarrow a - b \in I$. Le quotient R/I est aussi un anneau commutatif.

Exercice : Montrer qu'un idéal est maximal si et seulement si R/I est un corps. Remarquer qu'on a un homomorphisme canonique $\pi : R \to R/I$ donné par $\pi(a) = [a]$; alors $R/\ker \pi \cong \operatorname{im} \pi$.

Exemple : Dans $\mathbf{R}[x]$ l'idéal $I = (x^2 + 1)$ est maximal. On a $\mathbf{R}[x]/I \cong \mathbf{C}$.

Un point $(a_1, \ldots, a_n) \in \mathbb{K}^n$ est algébrique car il est l'ensemble des zéros de l'idéal $I = (x_1 - a_1, \ldots, x_n - a_n)$. Alors I est maximal car $\mathbb{K}[x_1, \ldots, x_n]/I \cong \mathbb{K}$. On applique la division euclidienne pour démontrer ce fait : lorsqu'on divise par $x_j - a_j$ le reste est un élément de $\mathbb{K}$; on écrit $p \in \mathbb{K}[x_1, \ldots, x_n]$ comme $p = q_1(x_1 - a_1) + \cdots + q_n(x_n - a_n) + r$ avec $r \in \mathbb{K}$ la 1ère terme à droite étant dans I. L'exemple ci-dessus montre que ce n'est pas tout idéal maximal qui est de ce type, pourtant sur un corps algébriquement fermé c'est le cas. On omet la preuve du théorème suivant.

Theorem 0.6. (Théorème des zéros de Hilbert : Nullstellensatz) *Supposons que $\mathbb{K}$ est algébriquement fermé (par exemple $\mathbb{K} = \mathbf{C}$), alors les idéaux maximaux dans $\mathbb{K}[x_1, \ldots, x_n]$ sont exactement des idéaux du type $(x_1 - a_1, \ldots, x_n - a_n)$ pour $a_j \in \mathbb{K}$.*

Corollary 0.7. *Si $\mathbb{K}$ est algébriquement fermé, alors :*

(i) Il existe une corrésondance $1 - 1$:

$$\{\text{points dans } \mathbb{K}^n\} \leftrightarrow \{\text{ideax maximaux dans } \mathbb{K}[x_1, \ldots, x_n]\}$$

donnée par $(a_1, \ldots, a_n) \leftrightarrow (x_1 - a_1, \ldots, x_n - a_n)$.

(ii) Chaque idéal $I \overset{\neq}{\subset} K[x_1, \ldots, x_n]$ présente au moins un zéro dans $\mathbb{K}^n$.

Proof. (i) suit directement du Nullstellensatz ; (ii) suit du fait que chaque idéal est contenu dans un qui est maximal (théorème de la base de Hilbert). $\square$

On a trouvé une correspondance entre les points de $\mathbb{K}^n$ et des idéaux maximaux. On essaye de prolonger cette correspondance aux ensembles plus compliqués. Commençons avec une collection de points :

Soit $X = \{a_1, \ldots, a_r\} \subset \mathbb{K}$. Il est évident que $I(X)$ est engendré par le polynôme $(x - a_1)(x - a_2) \cdots (x - a_r)$ et que $V(I(X)) = X$. Donc V est la reciproque de I.

D'autre part, soit $I \subset \mathbb{K}[x]$ un idéal différent de (0) et $\mathbb{K}[x]$. Puisque $\mathbb{K}[x]$ est un anneau principal (tout idéal est engendré par un seul élément), on a $I = (f)$ pour un polynôme monique $f \in \mathbb{K}[x]$. Pour que la correspondance marche, on a besoin que $\mathbb{K}$ soit algébriquement fermé : sinon, si f n'avait pas de zéros on aurait $V(I) = \emptyset$ d'où $I(V(I)) = (1)$ qui ne donne aucune information sur I. Mais si $\mathbb{K}$ est algébriquement fermé, on peut écrire $f = (x-a_1)^{m_1} \cdots (x-a_r)^{m_r}$ avec tous les a_i distincts et avec $m_i > 0$. Alors $V(I) = \{a_1, \ldots, a_r\}$ et il s'ensuit que $I(V(I))$ est engendré par $(x - a_1) \cdots (x - a_r)$. Autrement dit, un polynôme appartient à $I(V(I))$ si et seulement si une puissance de ce polynôme appartient à I. On écrit $I(V(I)) = \sqrt{I}$:

Définition : Pour un idéal $I \lhd \mathbb{K}[x_1, \ldots, x_n]$, on définit son *radical* comme :

$$\sqrt{I} := \{f \in \mathbb{K}[x_1, \ldots, x_n : f^m \in I \text{ pour un } m > 0\}\,.$$

On voit facilement que $\sqrt{I}$ est un idéal. Un idéal est appelé *radical* si $I = \sqrt{I}$. Remarquons que l'idéal d'un ensemble algébrique est toujours radical.

Proposition 0.8. *(i) Soit $X_1, X_2 \subset \mathbb{K}^n$ tels que $X_1 \subset X_2$, alors $I(X_2) \subset I(X_1)$;*

(ii) pour un ensemble algébrique $X \subset \mathbb{K}^n$ on a $V(I(X)) = X$;

(iii) Si $\mathbb{K}$ est algébriquement fermé, alors pour tout idéal $J \subset \mathbb{K}[x_1, \ldots, x_n]$ on a $I(V(J)) = \sqrt{J}$.

Proof. (i) est évident.

(ii) Soit $x \in X$. Alors quelque soit $f \in I(X)$, on a $f(x) = 0$.
Mais $V(J) := \{x \in \mathbb{K}^n : f(x) = 0 \ \forall f \in J\}$, d'où $x \in V(I(X))$ et $X \subseteq V(I(X))$.

Reciproquement, $X = V(J)$ pour un idéal J. Si $f \in J$, alors

$$f(x) = 0 \ \forall x \in V(J) \implies f \in I(V(J)) \implies J \subseteq I(V(J))$$

d'où $J = I(V(J))$.

(iii) Si $f \in \sqrt{J}$ alors

$$\begin{aligned} \exists m \in \mathbf{N}^* \text{ tq } f^m \in J \quad &\implies f(x)^m = 0 \ \forall x \in V(J) \quad \implies f(x) = 0 \ \forall x \in V(J) \\ &\implies f \in I(V(J)) \qquad\quad \implies \sqrt{J} \subseteq I(V(J)) \end{aligned}$$

Pour la reciproque, on applique le théorème de la base de Hilbert. Soit $f \in I(V(J))$. On considère l'idéal

$$K = J + (ft - 1) \subset \mathbb{K}[x_1, \ldots, x_n, t]\,.$$

Supposons qu'il existe $x \in V(K)$. Alors

$$J \subset K \implies V(J) \supseteq V(K) \implies I(V(J)) \subseteq I(V(K)) \implies f(x) = 0$$

Mais il faut aussi que $f(x)t - 1 = 0$, ce qui est impossible, donc $V(K) = \emptyset$ et $K = (1)$. En particulier il existe une relation :

$$1 = (ft - 1)g_0 + \sum f_i g_i \in \mathbb{K}[x_1, \ldots, x_n, t]\,,$$

pour des polynômes $g_i \in \mathbb{K}[x_1, \ldots, x_n, t]$ et $f_i \in I$. Soit t^N la plus grande puissance de t dans les g_i. Alors on peut multiplier l'égalité précédente par f^N :

$$f^N = (ft - 1)G_0(x_1, \ldots, x_n, ft) + \sum f_i G_i(x_1, \ldots, x_n, ft)\,.$$

où $G_i = f^N g_i$ est considérer comme un polynôme en $x_1, \ldots, x_n, ft$. On prend le quotient par $(ft - 1)$ (en effet on pose $ft = 1$) pour en déduire que $f^N = \sum f_i G_i(x_1, \ldots, x_n, 1) \in J$. $\square$

On remarque que même si le radical d'un idéal est facile à définir, en général il est difficile à le calculer explicitement. Il est aussi bien difficile à vérifier qu'un idéal est radical ; on a besoin d'un ordinateur en général pour faire ces calculs.