

## Courbes algébriques planes

### Sous-ensembles algébriques de $\mathbb{C}$

Dans tout ce cours, les anneaux considérés sont commutatifs avec unité.

Soit  $K$  un corps,  $I$  un ensemble, et pour chaque  $i \in I$ ,  $\phi_i \in K[X]$  un polynôme à une indéterminée à coefficients dans  $K$ . Que peut-on dire de l'ensemble

$$V((\phi_i)_{i \in I}) = \{x \in K \mid \forall i \in I, \phi_i(x) = 0\}?$$

Tout d'abord, on a

$$V((\phi_i)_{i \in I}) = V(\mathcal{J}) = \{x \in K \mid \forall f \in \mathcal{J}, f(x) = 0\},$$

où  $\mathcal{J}$  est l'idéal de  $K[X]$  engendré par les  $\phi_i$ , c'est-à-dire

$$\begin{aligned} \mathcal{J} = \{f \in K[X] \mid \exists p \in \mathbb{N}, \exists i_1, \dots, i_p \in I, \exists g_1, \dots, g_p \in K[X], \\ f = g_1\phi_{i_1} + \dots + g_p\phi_{i_p}\}. \end{aligned}$$

Contrairement aux apparences, nous avons beaucoup gagné à augmenter ainsi le nombre des équations. Rappelons en effet que si  $K$  est un corps,  $K[X]$  est un anneau *principal* : tout idéal  $\mathcal{J}$  de  $K[X]$  est principal, c'est-à-dire engendré par un seul élément (il suffit de prendre un élément  $f \in \mathcal{J}$  de degré minimum et d'effectuer la division euclidienne par  $f$  de tous les éléments de  $\mathcal{J}$  ; on note alors  $\mathcal{J} = (f)$ ).

Si  $f$  est un générateur de l'idéal engendré par les  $(\phi_i)_{i \in I}$ , on obtient

$$V((\phi_i)_{i \in I}) = V(f) = \{x \in K \mid f(x) = 0\}.$$

Pour étudier  $V(f)$  il faut maintenant comprendre la structure de  $f$  ; commençons par rappeler deux définitions :

**Définition 0.0.1** – Soit  $A$  un anneau intègre (i.e. sans diviseur de zéro) ; un élément  $a \in A$  est dit *irréductible* (ou *premier*) si  $a \neq 0$ ,  $a$  n'est pas une unité (i.e. un élément inversible), et si chaque fois que  $a = bc$  avec  $b, c \in A$ , ou  $b$  ou  $c$  est une unité.

**Définition 0.0.2** – Un anneau  $A$  est dit *factoriel* s'il est intègre et si tout élément  $a \neq 0 \in A$  admet une unique<sup>1</sup> factorisation en éléments irréductibles : cela signifie qu'il existe une unité  $u$  et des éléments irréductibles  $p_1, \dots, p_r$  tels que  $a = up_1 \dots p_r$ , et que si  $a = vq_1 \dots q_s$  est une autre factorisation, on a  $r = s$  et, après permutation éventuelle des indices,  $p_i = u_i q_i$  où les  $u_i$  sont des unités.

**Théorème 0.0.3** – Un anneau intègre et principal est factoriel.

Par exemple,  $\mathbb{Z}$  est factoriel.

*Démonstration* : Soit  $a_0 \neq 0 \in A$  n'admettant pas de factorisation en éléments irréductibles ; en particulier,  $a_0$  n'est pas irréductible, et s'écrit donc  $a_0 = a_1 \cdot a'_1$ , où ni  $a_1$  ni  $a'_1$  n'est une unité et où l'un au moins, par exemple  $a_1$ , n'admet pas de factorisation en éléments irréductibles ; on construit ainsi une suite infinie d'idéaux distincts

$$(a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \dots$$

( $(a_0)$  désigne l'idéal de  $A$  engendré par  $a_0$ ).

Mais il est facile de voir qu'une telle suite devient stationnaire à un cran fini si  $A$  est principal, ce qui est une contradiction.

L'unicité vient d'un argument bien connu de divisibilité. (Voir Lang p. 71, 72).

**Corollaire 0.0.4** – Si  $K$  est un corps,  $K[X]$  est factoriel

Si  $f = u \prod_{i=1}^k f_i^{m_i}$  est une factorisation en éléments irréductibles, on voit que

$$V(f) = \bigcup_{i=1}^k V(f_i^{m_i}) = \bigcup_{i=1}^k V(f_i).$$

Il est en particulier clair que la donnée de  $V(f)$  ne permet pas de retrouver  $f$ . Si  $K = \mathbb{R}$ , l'exemple  $f(X) = X^2 + 1 \in \mathbb{R}[X]$  montre que la situation est désespérée. Sur  $\mathbb{C}$ , tout se passe le mieux possible grâce au théorème de d'Alembert–Gauss. Avant d'énoncer ce dernier, énonçons une proposition (dont la démonstration est laissée en exercice).

**Proposition 0.0.5** – Soit  $K$  un corps, les trois assertions suivantes sont équivalentes.

- (a) Tout polynôme  $F$ , de degré supérieur ou égal à 1, de  $K[X]$  admet une racine dans  $K$ .
- (b) Tout polynôme irréductible de  $K[X]$  est de degré 1.
- (c) Tout polynôme non constant de  $K[X]$  se décompose en un produit de polynômes de degré 1.

**Définition 0.0.6** – On dit qu'un corps  $K$  est *algébriquement clos* s'il vérifie l'une des trois propriétés équivalentes ci-dessus.

<sup>1</sup> Il peut y avoir existence sans qu'il y ait unicité : dans  $\mathbb{Z}[\sqrt{-5}]$ , on a les deux décompositions  $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$  ; ce genre d'exemple est à la base de la théorie des idéaux de Kummer.

**Remarques 0.0.7** – 1. Un corps algébriquement clos a forcément une infinité d'éléments : si  $K = \{x_1, \dots, x_n\}$ , le polynôme  $f = \prod_{i=1}^n (X - x_i) + 1$  n'a pas de racine.

2. Tout corps peut être plongé dans un corps algébriquement clos (voir Lang : Algebra, p. 169–170).

**Théorème 0.0.8** – (D'Alembert-Gauss) - Le corps  $\mathbb{C}$  est algébriquement clos.

*Démonstration* : Il y en a beaucoup ; l'une des plus intuitives se trouve en exercice dans le livre d'Algèbre de Godement (exercice 25, p. 614) ; voir aussi « Topologie algébrique » de C. Godbillon (Hermann) et « Fonctions de variables complexes » de H. Cartan (Hermann).

Remarquer que ce théorème équivaut au théorème suivant :

**Théorème 0.0.8'** – Une fonction polynôme  $F : \mathbb{C} \rightarrow \mathbb{C}$  est constante ou surjective.

**Définition 0.0.9** – Soit  $f \in K[X]$ ,  $x \in K$ . On appelle multiplicité de  $x$  comme racine de  $f$  l'entier  $m = m_x(f)$  défini par la condition suivante :

1.  $f(X) = (X - x)^m g(X)$ , avec  $g(x) \neq 0$ .
2.  $\frac{\partial^i f}{\partial X^i}(x) = 0$  pour  $i \leq m - 1$ ,  $\frac{\partial^m f}{\partial X^m}(x) \neq 0$ .

On déduit du théorème 0.8 que tout  $f \in \mathbb{C}[X]$  s'écrit

$$f = \alpha \prod_{x \in \mathbb{C}} (X - x)^{m_x(f)} = \alpha \prod_{i=1}^k (X - x_i)^{m_i}$$

(où  $x_1, \dots, x_k$  sont les racines de  $f$ ,  $m_i = m_{x_i}(f)$ , et  $\alpha \in K$ ).

**Corollaire 0.0.10** – Soient  $f$  et  $g$  deux éléments de  $\mathbb{C}[X]$ . On suppose que  $\forall x \in V(f), g(x) = 0$ . Alors il existe un entier  $M$  tel que  $g^M \in (f)$ .

*Démonstration* :  $f = \alpha \prod_{i=1}^k (X - x_i)^{m_i}$ ,  $V(f) = \{x_1, \dots, x_k\}$  ; l'hypothèse s'écrit donc  $g(x_i) = 0$  pour  $i = 1, \dots, k$ , ce qui montre que  $g$  est divisible par  $X - x_i$  pour tout  $i$ . Il suffit alors de prendre pour  $M$  le sup. des  $m_i$ .

**Définition 0.0.11** – Soient  $A$  un anneau et un idéal de  $A$ . On appelle radical (ou racine) de , et on note  $\text{rad}$ , l'idéal (vérifier que c'en est un)

$$\text{rad} = \{a \in A \mid \exists n \in \mathbb{N}, a^n \in \mathfrak{a}\}.$$

Si  $E$  est un sous-ensemble de  $K$ , notons

$$I(E) = \{f \in K[X] \mid \forall x \in E, f(x) = 0\}.$$

C'est évidemment un idéal de  $K[X]$ .

Le corollaire 0.0.10 s'écrit encore

**Corollaire 0.0.10'** – Si  $\mathcal{J}$  est un idéal de  $\mathbb{C}[X]$ , on a

$$I(V(\mathcal{J})) = \text{rad } \mathcal{J}.$$

Revenons maintenant sur le polynôme  $f \in \mathbb{C}[X]$ ,

$$f(X) = \alpha \prod_{i=1}^k (X - x_i)^{m_i}.$$

Le degré de  $f$  est attaché *globalement* au polynôme  $f$ , alors que  $m_x(f)$  est attaché au comportement *local* de  $f$  « au voisinage de  $x$  ». La relation entre global et local est donnée par

$$m = \sum_{x \in \mathbb{C}} m_x(f) = \sum_{i=1}^k m_i.$$

Nous allons préciser cette relation local  $\leftrightarrow$  global ; pour cela, rappelons que, si est un idéal de l'anneau  $A$ , on peut définir un *anneau quotient*  $A/$ . D'autre part, un anneau tel que  $K[X]$  a une structure supplémentaire, à savoir une structure d'espace vectoriel sur  $K$  compatible avec sa structure d'anneau (on dit que  $K[X]$  est une *K-algèbre*) ; en particulier, un idéal  $\mathcal{J}$  de  $K[X]$  est aussi un sous-espace vectoriel de  $K[X]$ , et  $K[X]/\mathcal{J}$  est de façon naturelle une  $K$ -algèbre, ce qui permet de parler de sa dimension sur  $K$ .

**Lemme 0.0.12** – Soit  $K$  un corps,  $f \in K[X]$  un polynôme de degré  $m$ , on a

$$\dim_K K[X]/(f) = m.$$

*Démonstration* : Si  $g \in K[X]$ , on peut écrire de façon *unique*  $g = qf + r$  avec un reste  $r$  tel que  $\deg r < \deg f$  ; cela montre que les classes des  $m$  éléments  $1, X, X^2, \dots, X^{m-1}$  forment une base de  $K[X]/(f)$ .

Pour interpréter de façon semblable les  $m_x(f)$ , remarquons que d'après le lemme 0.0.12, on a

$$m_x(f) = \dim_K K[X]/(X - x)^{m_x(f)}.$$

Un moyen de concentrer l'attention sur  $x$  est de « rendre inversibles » les polynômes qui ne s'annulent pas en  $x$ . Ceci nous amène à considérer les anneaux suivants :

$K(X)$  = corps des fractions de l'anneau intègre  $K[X]$ , dont les éléments sont appelés « fractions rationnelles » ;

${}_x(K)$  défini par

$${}_x(K) = \left\{ \frac{p}{q} \in K(X) \mid q(x) \neq 0 \right\}.$$

On voit que  $K[X] \subset {}_x(K) \subset K(X)$ .

**Lemme 0.0.13** – Soit  $K$  un corps,  $f \in K[X]$ ,  $x \in \mathbb{C}$ ,  $f_x(K)$  l'idéal de  ${}_x(K)$  engendré par  $f$  ; on a

$$\dim_K {}_x(K)/f_x(K) = m_x(f).$$

*Démonstration* : Par définition de  $m_x(f)$ , on peut écrire  $f(X) = (X-x)^{m_x(f)}g(x)$ , avec  $g(x) \neq 0$ . En particulier,  $g$  est une unité de  ${}_x(K)$  et il reste à voir que  ${}_x(K)/(X-x)^{m_x(f)}$  est engendré les classes de  $1, X-x, \dots, (X-x)^{m_x(f)-1}$  (utiliser l'algorithme de division suivant les puissances croissantes de  $X$ , après s'être ramené par translation à  $x = 0$ ).

Nous pouvons maintenant déduire de l'égalité  $m = \sum_{x \in \mathbb{C}} m_x(f) = \sum_{i=1}^k m_i$  (valable si  $k$  est algébriquement clos) le

**Théorème 0.0.14** – Soit  $K$  un corps algébriquement clos (par exemple  $K = \mathbb{C}$ ),  $f \in K[X]$ . Soient  $x_1, \dots, x_k$  les racines de  $f$  ; il existe un isomorphisme naturel de  $K$ -algèbres

$$K[X]/(f) \xrightarrow{\sim} \prod_{i=1}^k {}_{x_i}(K)/f_{x_i}(K).$$

*Démonstration* : Considérés comme e.v. sur  $K$ , les deux membres ont la même dimension (d'après les lemmes 0.0.12, 0.0.13 et l'égalité  $m = \sum_{i=1}^k m_i$ ). Pour voir que la flèche est un isomorphisme d'espaces vectoriels sur  $K$ , il suffit de vérifier que c'est un homomorphisme injectif, ce qui est facile ; le fait que la structure d'anneau soit préservée est tout aussi évident.

Bien entendu, un tel isomorphisme ne peut exister pour  $K = \mathbb{R}$ , comme le montre l'exemple  $f(X) = X^2 + 1$ .

*Plan du Cours* :

Dans le chapitre 1, nous verrons ce qui subsiste des propriétés que nous venons de passer en revue lorsqu'on remplace  $K[X]$  par  $K[X_1, \dots, X_n]$ .

Dans les chapitres suivants, nous nous limiterons au cas  $n = 2$ . Nous démontrons en particulier le théorème de Bézout sur les intersections des courbes planes, ce qui nous amènera à parler de l'espace projectif.

Dans la deuxième partie, nous interpréterons en termes locaux les multiplicités d'intersections, et donnerons une autre démonstration du théorème de Bézout.

## Bibliographie

Pour rédiger ce cours, j'ai puisé sans vergogne dans les sources suivantes :

- Sur les rappels d'algèbre  
R. Godement, Cours d'algèbre. Hermann 1966.

S. Lang, Algebra. Addison-Wesley 1965.

N. Bourbaki, Algèbre Chapitre 7. Hermann 1964.

- Sur le point de vue global

W. Fulton, Algebraic curves. Benjamin 1969.

Berthelot, Cours à Paris VII, 1971–1972. (Géométrie algébrique élémentaire).

B. Teissier, Multiplicités. Cours à l'E.N.S. 1973–1974.

- Sur le point de vue local

R.J. Walker, Algebraic curves, 1950 (Dover 1962).

F. Pham, cours de 3ème cycle à Paris VII.

Pour ceux qui veulent poursuivre en algèbre commutative, je recommande vivement :

M.F. Atiyah et I.G. Macdonald, Introduction to commutative algebra, Addison-Wesley 1969.

Pour ceux qui veulent poursuivre en géométrie algébrique :

Shafarevitch, Foundations of algebraic geometry.

Enfin, pour ceux qui veulent remonter aux sources :

Sir I. Newton, Méthode des fluxions, Blanchard, 1966.

J. Dieudonné, Traité de Géométrie algébrique, Vol. 1, P.U.F., 1974.



<http://www.springer.com/978-3-540-33707-2>

Courbes Algébriques Planes

Chenciner, A.

2008, X, 160 p., Softcover

ISBN: 978-3-540-33707-2