ELEMENTS D'ALGEBRE COMMUTATIVE

Maîtrise de Mathématiques
Université d'Angers
2003/04

D. Schaub

Chapitre 5

Introduction à la géométrie algébrique

5.1 Algèbre de polynômes

Définition 5.1.1 *Soit A un anneau commutatif unitaire, on rappelle qu'un ensemble E est muni d'une structure de A-algèbre si E est muni de deux lois internes notées $(+, \times)$, $E \times E \to E$ telles que $(E, +, \times)$ soit un anneau (commutatif unitaire) et une loi externe $\cdot : A \times E \to E$ telle que $(E, +, \cdot)$ soit un A-module avec une propriété de compatibilité entre "multiplications" : pour tous $a \in A, x, y \in E$, $(a \cdot x) \times y = a \cdot (x \times y)$ (ce qui permet d'écrire, en "oubliant" les signes axy).*

Remarque : Alternativement, E est une A-algèbre si E est un anneau et s'il y a un homomorphisme d'anneaux unitaires $f : A \to E$ (la loi externe est alors définie par $ax = f(a)x$).

On peut aussi donner la structure d'algèbre uniquement par une collection de diagrammes de flèches (exercice).

Définition 5.1.2 *Soient E et F deux A-algèbres. Une application $f : E \to F$ est un homomorphisme de A-algèbres si f est A-linéaire et commute à la multiplication interne.*

On remarquera que l'ensemble des morphismes de A-algèbres de E dans F est seulement un sous-ensemble de l'ensemble $\mathrm{Hom}_A(E, F)$ (par exemple, $f + g$ ne commute pas à la multiplication interne).

Une sous-algèbre d'une A-algèbre E est un sous-ensemble F tel que les restricitions des opérations "à" F le munit d'une structure de A-algèbre.

Soit E une A-algèbre et $(F_i)_{i \in I}$ une collection de sous-algèbres de E, Alors l'intersection $G = \bigcap_{i \in I} F_i$ est encore une sous-algèbre de E.

Définition 5.1.3 *Soit E une A-algèbre et P un sous-ensemble de E. Alors l'intersection des sous-algèbres de E contenant P est appelée sous-algèbre de E engendrée par P, notée $A[P]$. On vérifie que G est la plus petite sous-algèbre de E contenant P ou encore que $G = \{\sum_{finie} ax_1 \cdots x_n \mid a \in A,\ x_1, \ldots, x_n \in P\}$.*

Remarque : en fait, grâce à la commutativité de $(E, \times)$, on peut regrouper les produits en affectant les x_i d'exposants.

Exemple : les anneaux de polynômes à coefficients dans un anneau A sont munis d'une structure de A-algèbre. Ainsi $A[X]$, considéré par exemple comme l'ensemble des suites infinies $(a_i)_{i \in \mathbb{N}}$ où

tous les $a_i = 0$ sauf un nombre fini, a une structure naturelle de A-module ($(a_i)+(b_i) = (a_i+b_i)$ et $\lambda(a_i) = (\lambda a_i)$). On peut aussi définir une multiplication interne par $(a_i)_i \times (b_i)_i = (c_i)_i$ où $c_k = \sum_{i=0^k} a_i b_{k-i}$ et vérifier la propriété de compatibilité.

On remarque alors que : l'élément neutre de l'addition est la suite nulle, notée 0, l'élément neutre de la multiplication est la suite dont tous les termes sont 0 sauf le premier qui est 1. On définit un monomorphisme d'anneaux $A \to A[X]$ par $a \mapsto a \times 1$. Enfin, si on note X, qu'on appelle *variable* la suite dont tous les termes sont 0 sauf le deuxième qui vaut 1, on constate que X^k est la suite dont tous les termes sont nuls sauf le $k+1$-ième qui vaut 1 et ainsi la suite $(a_0, a_1, \ldots, a_d, 0, 0, \ldots) = \sum_{i=0}^{d} a_i X^i$, c'est l'écriture que l'on adoptera. Le nombre entier d s'appelle *degré* de ce polynôme. On appelle *valuation* du polynôme le plus petit entier ν tel que $a_\nu \neq 0$ et $a_k = 0, \forall k < \nu$.

On remarque que $A[X]$ est engendrée par X puisque tous les éléments peuent s'écrire comme sommes finies du type $\sum \lambda_k X^k$.

On peut de même définir l'anneau de polynômes à deux variables $A[X, Y]$ sur A comme l'ensemble des tableaux (matrices) $(a_{ij})_{i,j\in\mathbb{N}}$ infinis à coefficients dans A où tous les éléments sont nuls sauf un nombre fini. On définit les opérations d'une manière analogue à ci-dessus. L'élément neutre pour l'addition est alors le tableau constitué uniquement de zéros. L'élément neutre pour la multiplication est le tableau où tous les éléments sont nuls sauf le premier qui vaut 1. On note X le tableau tel que tous les éléments sont 0 sauf l'élément $a_{10} = 1$ et Y celui pour lequel tout est nul sauf $a_{01} = 1$. On constate alors que tout élément $P(X, Y)$ de $A[X, Y]$ peut s'écrire $\sum_{i,j} a_{ij} X^i Y^j$.

On peut remarquer qu'on peut, comme précédemment, plonger A dans $A[X, Y]$, mais aussi $A[X]$ ou $A[Y]$ (en effet, l'application $A[X] \to A[X, Y]$ telle que $P(X) = \sum_{k=0}^{d} a_k X^k \mapsto \sum ijb_{ij} X^i Y^j$ telle que $b_{ij} = 0$ pour $j \neq 0$ et $b_{i0} = a_i$ est un monomorphisme d'algèbres) et que $A[X, Y]$ est engendrée par X, Y.

On peut enfin remarquer aussi que $A[X, Y]$ est naturellement isomorphe, en tant que A-algèbre, à l'agèbre symétrique $S_A[A^2]$ du A-module libre de rang 2, A^2.

On peut bien sûr généraliser pour obtenir l'algèbre des polynômes à plusieurs variables $X_1, \ldots, X_n$ et même les polynômes à un nombre infini de variables.

Définition 5.1.4 *On dit qu'une A-algèbre E est de type fini s'il existe une partie finie $P = \{x_1, \ldots, x_r\}$ d'éléments de E telle que $E = A[x_1, \ldots, x_n]$.*

Les exemples d'algèbres de polynômes à un nombre fini de variables sont des algèbres de type fini.

Proposition 5.1.1 *Toute A-algèbre commutative unitaire de type fini est isomorphe à un quotient d'un anneau de polynômes par un idéal.*

Preuve : Si E est une A-algèbre de type fini, soit $P = \{x_1, \ldots, x_n\}$ une partie génératrice. Soit alors $\phi : A[X_1, \ldots, X_n] \to E$ définie par ϕ est l'homomorphisme de A-algèbres qui envoie $X_i \mapsto x_i$, $i = 1, \ldots, n$. Par construction, ϕ est surjective, donc si I désigne son noyau, $A[X_1, \ldots, X_n]/I \cong E$.

5.2 Notion d'intégralité

Définition 5.2.1 *Soit B un anneau et A un sous-anneau. On dit qu'un élément $x \in B$ est entier sur A si l'une des 3 conditions équivalentes suivantes est vérifiée :*

(i) il existe $a_{n-1}, \ldots, a_0 \in A$ tels que $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ (qu'on appelle équation de dépendance intégrale de x sur A) ;

(ii) $A[x]$, la sous-algèbre de B engendrée par x, est un A-module de type fini ;
(iii) il existe un $A[x]$-module fidèle qui est un A-module de type fini.

Ajoutons encore que, pour un anneau A, un A-module M est dit *fidèle* si $\alpha M = 0 \Rightarrow \alpha = 0$. Notons que A est un A-module fidèle. De plus, si $A \neq 0$, un A-module fidèle est nécessairement non réduit à 0.

Montrons que ces 3 conditions sont bien équivalentes. Les implications $(i) \Rightarrow (ii) \Rightarrow (iii)$ sont immédiates. En effet, une relation de dépendance intégrale de x sur A montre que $A[x]$ est engendré par $1, x, \ldots, x^{n-1}$ et pour la deuxième implication, il suffit de prendre comme module fidèle $A[x]$ lui-même.

Il suffit donc de prouver $(iii) \Rightarrow (i)$. Soit donc M un $A[x]$-module fidèle qui soit un A-module de type fini et soient $u_1, \ldots, u_s$ un système de générateurs de M sur A.

Considérons la multiplication par x dans $\mathrm{End}_A(M)$. On a $xu_i = \sum_{j=1}^{s} a_{ji}u_j$, $a_{ji} \in A$, autrement dit $\sum_j \delta_{ji}(x - a_{ji})u_j = 0$. Alors , si P désigne la matrice $P = (\delta_{ji}(x - a_{ji}))$, l'ensemble des relations obtenues se traduit par

$$P \begin{pmatrix} u_1 \\ \cdots \\ u_s \end{pmatrix} = 0 \ (*).$$

Mais, si $\tilde{P}$ désigne la matrice des cofacteurs de P, $\tilde{P}P = \det(P)I$, par conséquent $(*) \Rightarrow \det(P) \begin{pmatrix} u_1 \\ \cdots \\ u_s \end{pmatrix} = 0$, autrement dit $\det(P)u_i = 0$ pour tout $i = 1, \ldots, s$, soit encore $\det(P)M = 0$. Comme $\det(P) \in A$ et que M est fidèle sur A, on en déduit $\det(P) = 0$, ce qui se traduit précisément par une relation de dépendance intégrale de x sur A.

On peut généraliser cette notion au cas d'un homomorphisme d'anneaux $f : A \to B$. Un élément $x \in B$ sera dit entier sur A si, notant $J = \ker(f)$, x est entier sur A/J identifié au sous-anneau $f(A)$ de B.

Définition 5.2.2 *Soit $f : A \to B$ un homomorphisme d'anneaux. Alors B est entier sur A si tout $x \in B$ est entier sur A.*

Exemple : soit $k \in K$ une extension de corps. Alors K est entier sur k ssi K est algébrique sur k.

Proposition 5.2.1 *Soit $f : A \to B$ un homomorphisme d'anneaux. L'ensemble des élements $x \in B$ entiers sur A forme un sous-anneau B' de B.*

Preuve : Soient $x, y \in B$ entiers sur A. Il s'agit de montrer que $x \pm y$ et xy sont alors entiers sur A. Considérons alors $M = A[x]$ et $N = A[y]$. Alors MN contient 1 donc est fidèle sur A. De plus, MN est un $A[x \pm y]$-module puisqu'on sait multiplier MN par $x \pm y$, de même, c'est un $A[xy]$-module. De plus, MN est de type fini, puisque sur $u_1, \ldots, u_s$ engendre M et $v_1, \ldots, v_t$ engendre N, alors MN peut-être engendré par l'ensemble des u_iv_j. D'où d'après la condition (iii), $x \pm y$ et xy sont entiers sur A

Proposition 5.2.2 *Si B est une A-algèbre de type fini, entière sur A, alors B est un A-module de type fini.*

Preuve : on procède par récurrence sur le nombre n de générateurs. Si $B = A[x]$ et B est entier, c'est la condition (ii) qui assure que B est un A-module de type fini. Puis, on considère que $B = A[x_1, \ldots, x_{n-1}][x_n]$. Par hypothèse de récurrence, $A[x_1, \ldots, x_{n-1}]$ est un A-module de type fini et B est entier sur A implique que, a fortiori, B est entier sur $A[x_1, \ldots, x_{n-1}]$, d'où que B est un $A[x_1, \ldots, x_{n-1}]$-module de type fini. Or, de manière générale, si $D \subset E \subset F$ est une suite d'inclusions d'algèbres, et F de type fini sur E et E de type fini sur D, alors F est de type fini sur D. Autrement dit, dans le cas considéré, B est de type fini sur A.

Proposition 5.2.3 *Soit $f : A \to B$ un homomorphisme d'anneaux, J un idéal de B, I un idéal de A tel que $f(I) \subset J$, alors si B est entier sur A, B/J est entier sur A/I.*

La preuve est laissée en exercice.

Proposition 5.2.4 *Si $A \to B \to C$ est une suite d'homomorphismes d'algèbres, alors B entier sur A et C entier sur B implique que C est entier sur A.*

Preuve : Soit $x \in C$. Alors x vérifie une relation de dépendance intégrale $x^n + b_{n-1}x^{n-1} + \cdots + b_0$ où $b_i \in B$. Soit $B_1 = A[b_0, \ldots, b_{n-1}]$; alors B_1 est un A-module de type fini d'après la proposition 5.2.2 et est fidèle. Alors $B_1[x]$ qui est un B_1-module de type fini, est un A-module de type fini, donc x est entier sur A.

Définition 5.2.3 *Soit A un sous-anneau de B. On appelle clôture intégrale de A dans B l'ensemble des éléments de B entiers sur A. On dit que A est intégralement clos dans B, si A est égal à sa clôture intégrale dans B.*

Lorsque A est un anneau intègre. On dit que A est intégralement clos si A est intégralement clos dans son corps des fractions.

Proposition 5.2.5 *Un anneau intègre et factoriel est intégralement clos.*

La preuve est laissée en exercice.

Proposition 5.2.6 *Soit $f : A \to B$ tel que B est entier sur A et S une partie multiplicative de A. Alors $S^{-1}f : S^{-1}A \to S^{-1}B$ et $S^{-1}B$ est entier sur $S^{-1}A$.*

Preuve laissée en exercice.

5.3 Le lemme de normalisation

Théorème 5.3.1 ***Lemme de Normalisation de Noether*** *Soit $A = k[x_1, \ldots, x_n]$ une algèbre de type fini sur un corps k, alors il existe un entier $m \leq n$, des éléments $y_1, \ldots, y_m \in A$ tels que*

1. A soit entier sur $k[y_1, \ldots, y_m]$;

2. les y_i sont algébriquement indépendants sur k (ie. $k[y_1, \ldots, y_m]$ est isomorphe à un anneau de polynômes à m variables).

Preuve : On procède par récurrence sur n.

Si $n = 0$, il n'y a rien à prouver car A en entier sur lui-même.

Supposons donc que $A = k[X_1, \ldots, X_n]/I$ où I est un idéal de l'anneau de polynômes $k[X_1, \ldots, X_n]$. Soit $I = \{0\}$, auquel cas il n'y a rien à prouver, on prend pour y_i les x_i. Sinon $I \neq 0$; autrement dit, il existe un polynôme $f \in I$ tel que $f(x_1, \ldots, x_n) = 0$ et, quitte à réindexer les x_i, on peut supposer que x_1 apparaît effectivement dans l'expression de f.

Choisissons des entiers $r_2, \ldots, r_n$ et posons $Z_i = X_i - X_1^{r_i}$. On note z_i l'image de Z_i dans A. Alors l'inclusion naturelle $k[x_1, z_2, \ldots, z_n] \subset k[x_1, x_2, \ldots, x_n]$ est en fait une égalité et $f(x_1, \ldots, x_n) = 0 \Leftrightarrow f(x_1, z_2 + x_1^{r_2}, \ldots, z_n + x_1^{r_n}) = 0$.
Développons en monômes le polynôme $f(X_1, Z_2 + X_1^{r_2}, \ldots, Z_n + X_1^n] = \sum_\alpha a_\alpha X_1^{\alpha_1} \cdots X_n^{\alpha_n} = \sum_\alpha a_\alpha X_1^{\alpha_1}(Z_2 + X_1^{r_2})^{\alpha_2} \cdots (Z_n + X_1^{r_n})^{\alpha_n}$ où $\alpha = (\alpha_1, \ldots, \alpha_n)$ est un n-uplet d'entiers et $a_\alpha = 0$ sauf pour un nombre finie de α. Choisissons alors $r_2, \ldots, r_n$ de telle sorte que les sommes $\alpha_1 + r_2\alpha_2 + \cdots + r_n\alpha_n$ soient 2 à 2 distinctes (...) pour $a_\alpha \neq 0$. Alors si N est un entier supérieur à tous ces entiers, on peut écrire : $f(X_1, Z_2 + X_1^{r_2}, \ldots, Z_n + X_1^n] = a_\alpha X_1^N + g(Z_i, X_1)$ où g est de degré $< N$ en X_1, ce qui précisément donne une relation de dépendance intégrale de x_1 sur $k[z_2, \ldots, z_n]$, puisque $a_\alpha \neq 0$ est inversible.

Par hypothèse de récurrence, il existe un entier $m \leq n-1$ et des éléments $y_1, \ldots, y_m \in k[z_2, \ldots, z_m]$ tels que

1. $k[z_2, \ldots, z_n]$ est entier sur $k[y_1, \ldots, y_m]$
2. les y_i sont algébriquement indépendants sur k.

D'où $k[x_1, \ldots, x_n] = k[x_1, z_2, \ldots, z_n]$ est entier sur $k[z_2, \ldots, z_n]$ qui est lui-même entier sur $k[y_1, \ldots, y_m]$, donc $k[x_1, \ldots, x_n]$ est entier sur$k[y_1, \ldots, y_m]$.

Définition 5.3.1 *0n appelle m le degré de transcendance de A sur k. On peut montrer que celui-ci est égal au nombre maximal d'éléments algébriquement indépendants de A.*

5.4 Théorème des zéros de Hilbert

Nous allons d'abord prouver un résultat intermédiaire : le *Going-up theorem* sous sa forme faible.

Théorème 5.4.1 *Soit $A \to B$ un monomorphisme d'anneaux tel que B soit entier sur A, alors si B est un corps, A est un corps.*

Preuve : clairement, si B est intègre, alors A (comme sous-anneau par exemple) est intègre. Il suffit donc de montrer que tout élément non nul de A est inversible dans A. Soit donc $a \in A$, $a \neq 0$. Comme $a \in A$, $a \in B$, donc $1/a \in B$. Donc $1/a$ est entier sur A, autrement satisfait à une relation de dépendance intégrale

$$\frac{1}{a^n} + \alpha_{n-1}\frac{1}{a^{n-1}} + \cdots + \alpha_1\frac{1}{a} + \alpha_0 = 0.$$

En multipliant cette relation par a^{n-1}, on obtient

$$\frac{1}{a} + \alpha_{n-1} + \alpha_{n-2}a + \cdots + \alpha_1 a^{n-1} + \alpha_0 a^n = 0,$$

autrement dit $\frac{1}{a} \in A$.

le théorème suivant est plus souvent référencé par son nom allemand *Hilbert Nullstellensatz* dans la littérature, c'est le théorème des zéros de Hilbert :

Théorème 5.4.2 *Soit k un corps algébriquement clos, $A = k[X_1, \ldots, X_n]$ un anneau de polynômes à n indéterminées. Les idéaux maximaux de $A = k[X_1, \ldots, X_n]$ sont tous de la forme $(X_1 - a_1, \ldots, X_n - a_n)$, $a_i \in k$.*

Remarquons tout de suite que ce théorème est faux si k n'est pas algébriquement clos. En effet, déjà dans $\mathbb{R}[X]$, il existe des idéaux maxiamux qui ne sont pas de la forme $(X - a)$; par exemple, l'idéal $(X^2 + 1)$ engendré par $X^2 + 1$ (car $\mathbb{R}[X]/(X^2 + 1)$ est en fait isomorphe à $\mathbb{C}$).

Preuve : Il est bien clair que l'idéal I engendré par $X_1 - a_1, \ldots, X_n - a_n$ est un idéal maximal, car le quotient de A par cet idéal est k comme le montre la surjection de k-algèbres $k[X_1, \ldots, X_n] \longrightarrow\!\!\!\!\!\rightarrow k$ qui envoie X_i sur a_i dont le noyau est précisément l'idéal I.

Inversement, soit $\mathfrak{m}$ un idéal maximal de A. Donc $A/\mathfrak{m} = R$ est un corps. Du lemme de normalisation, on déduit alors l'existence d'éléments $y_1, \ldots, y_m \in R$, $m \leq n$ tels que R est entier sur $k[y_1, \ldots, y_m]$ et ce dernier est isomorphe à un anneau de polynômes à m indéterminées.

Par le "Going-up", R étant un coprs, on en déduit que $k[y_1, \ldots, y_m]$ est un corps, d'où que $\mathfrak{m} = 0$ (en effet, supposons $\mathfrak{m} > 0$, comme $k[y_1, \ldots, y_m]$ est un corps, $\frac{1}{y_1}$ y appartient, donc peut s'écrire $\frac{1}{y_1} = P(y_1, \ldots, y_m)$, où P désigne un polynôme, autrement dit $y_1 P(y_1, \ldots, y_m) = 1$, ce qui fournit une relation algébrique entre les y_i et donc contredit leur indépendance algébrique). Donc $R = k[X_1, \ldots, X_n]/\mathfrak{m}$ est entier (algébrique) sur k et comme k est algébriquement clos, cela signifie que la surjection $\pi : k[X_1, \ldots, X_n]/\mathfrak{m} \to k$, définie par les images $\pi(X_i)$ et envoyant 1 sur 1, est un isomorphisme, donc, en posant $a_i = \pi(X_i)$, on obtient que $\mathfrak{m}$ est un idéal maximal contenant tous les $X_i - a_i$, donc contenant l'idéal (qui est maximal !) $(X_1 - a_1, \ldots, X_n - a_n)$, d'où l'égalité.

Le théorème des zéros dit essentiellement que, pour un corps **algébriquement clos**, il y a bijection entre les n-uples $(a_1, \ldots, a_n) \in k^n$ et les idéaux maximaux de $k[X_1, \ldots, X_n]$.

5.5 Notion d'ensemble algébrique

On considère toujours k algébriquement clos.

Définition 5.5.1 *Soit I un idéal de $k[X_1, \ldots, X_n]$. I peut être engendré par un nombre fini d'éléments (par noethérianité), $I = (f_1, \ldots, f_s)$. On appelle ensemble algébrique fermé défini par I, on note $V(I)$ l'ensemble $V(I) = \{x \in k^n \mid g(x) = 0,\ \forall g \in I\}$.*

Remarque : $x \in V(I) \Leftrightarrow f_1(x) = f_2(x) = \cdots = f_s(x) = 0$.

Soit $E \subset k^n$ un sous-ensemble, on note

$$I(E) = \{f \in k[X_1, \ldots, X_n] \mid f(x) = 0, \forall x \in E\}.$$

Proposition 5.5.1 *$I(E)$ est un idéal de $k[X_1, \ldots, X_n]$.*

Preuve : Soient $f, g \in I(E)$, alors $f(x) = g(x) = 0,\ \forall x \in E$, d'où $(fg)(x) = 0$ et $(hf)(x) = 0$ pour tout $h \in k[X_1, \ldots, X_n]$.

Théorème 5.5.1 *(forme forte du théorème des zéros) Soit $\mathcal{I}$ un idéal de $k[X_1, \ldots, X_n]$. Alors*

$$I(V(\mathcal{I})) = \sqrt{\mathcal{I}} = \bigcap_{\mathcal{I} \subset \mathfrak{p} \text{ premier}} \mathfrak{p} \ = \ \{g \in k[X_1, \ldots, X_n] \mid \exists \ell \text{ t.q. } g^\ell \in \mathcal{I}\}.$$

Preuve : On a clairement l'inclusion $\sqrt{\mathcal{I}} \subset I(V(\mathcal{I}))$ puisque $g \in \sqrt{\mathcal{I}} \Rightarrow \exists s$ tq. $g^s \in \mathcal{I}$ et $g^s(x) = 0 \Rightarrow g(x) = 0$ (l'anneau de polynômes est intègre).

Etudions l'inclusion inverse. On veut montrer que $g \in I(V(\mathcal{I})) \Rightarrow g \in \sqrt{\mathcal{I}}$. Soit $f_1, \ldots, f_\ell$ un système de générateurs de $\mathcal{I}$. Considérons l'anneau $k[X_1, \ldots, X_n, X_{n+1}]$ et J l'idéal engendré par $\mathcal{I}$ et $1 - X_{n+1}g$, ie. $J = (f_1, \ldots, f_\ell, 1 - X_{n+1}g)$.

Il y a alors 2 possibilités :

(1) $J \subset \mathfrak{m}$ idéal maximal de $k[X_1, \ldots, X_{n+1}]$

(2) $J = k[X_1, \ldots, X_{n+1}]$.

Montrons que (1) est impossible. D'après le Nullstellensatz, on sait que $\mathfrak{m}$ peut s'écrire $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n, X_{n+1} - a_{n+1})$. De l'inclusion $J \subset \mathfrak{m}$, on déduit alors que $f_i(a_1, \ldots, a_n) = 0\ \forall i = 1, \ldots, \ell$ et $1 - a_{n+1}g(a_1, \ldots, a_n) = 0$. Or, puisque $g \in I(V(\mathcal{I}))$, $g(a_1, \ldots, a_n) = 0$, on en déduit donc $1 = 0$, ce qui est absurde.

Nous nous trouvons donc dans le cas (2). On peut donc écrire

$$(*)\quad 1 = \sum_{i=1}^{\ell} h_i(X_1, \ldots, X_{n+1}) f_i(X_1, \ldots, X_n) + h(X_1, \ldots, X_{n+1})(1 - X_{n+1}g(X_1, \ldots, X_n)).$$

Soit alors l'homomorphisme d'anneaux $k[X_1, \ldots, X_n] \to k(X_1, \ldots, X_{n+1})$ défini par $X_i \mapsto X_i$ pour tout $i = 1, \ldots, n$ et $X_{n+1} \mapsto 1/g$.

Alors (*) devient, dans l'image, $1 = \sum_{i=1}^{\ell} h_i(X_1, \ldots, X_n, 1/g) f_i + 0$, autrement dit, en multipliant par une puissance suffisante de g, $g^s = \sum_{i=1}^{\ell} h'_i(X_1, \ldots, X_n) f_i \in \mathcal{I}$.

Définition 5.5.2 *Soit E un ensemble algébrique fermé de k^n, l'anneau $k[X_1, \ldots, X_n]/I(E)$ est appelé l'anneau de l'ensemble algébrique fermé E, on le note généralement $A(E)$.*

Exemples : k, k^n, un nombre fini de points dans k^n, la parbole $y = x^2$, la cubique "à cusp" $y^2 = x^3$, etc ... sont des ensembles algébriques. Lorsque k est infini, alors k et k^n sont irréductibles, le sous-ensemble de k^2, $V(XY)$ n'est pas irréductible.
Remarque : Le théorème des zéros signifie qu'il y a une bijection, renversant les inclusions, entre les ensembles algébriques fermés et les idéaux de $k[X_1, \ldots, X_n]$ égaux à leur racine. En effet, si J est un idéal de $k[X_1, \ldots, X_n]$ de la forme $J = I(E)$, alors $\sqrt{I(E)} = \{f \in k[X_1, \ldots, X_n];\ \exists s\ tq. f^s(x_1, \ldots, x_n) = 0, \forall (x_1, \ldots, x_n) \in E\}$, ce qui coïncide avec $\{f \in k[X_1, \ldots, X_n]; f(x_1, \ldots, x_n) = 0, \forall (x_1, \ldots, x_n) \in E\} = I(E) = J$. Inversement, si $J = \sqrt{J}$, comme $\sqrt{J} = I(V(J)$, J est bien l'idéal de l'ensemble algébrique fermé $V(J)$.

5.6 Topologie sur k^n

Proposition 5.6.1 *Etant donnés des idéaux de $k[X_1, \ldots, X_n]$, les faits suivants sont vérifiés :*
1. $J \subset J' \Rightarrow V(J') \subset V(J) \Rightarrow \sqrt{J} \subset \sqrt{J'}$
2. $\bigcap_{i \in I} V(J_i) = V(\sum_{i \in I} J_i)$
3. $V(\bigcap_{i=1}^{n} J_i) = \bigcup_{i=1}^{n} V(J_i)$.

Preuve : Les preuves sont immédiates. En ce qui concerne le premier point, $V(J')$ est l'ensemble des $x \in k^n$ tels que $g(x) = 0$, pour tout $g \in J'$; or J étant inclus dans J', a fortiori, $g(x) = 0$, pour tout $x \in J$, donc $x \in V(J)$. D'autre part, $f \in I(V(J))$ si $f(x) = 0$ pour tout $x \in V(J)$, donc, a fortiori, $f(x) = 0$ pour tout $x \in V(J') \subset V(J)$, donc $f \in I(V(J'))$.

Pour le deuxième point, soit $x \in \cap_{i \in I} V(J_i)$, alors $x \in V(J_i)$, pour tout i, donc $f(x) = 0\ \forall f \in J_i$, d'où pour tout $f \in \sum_i J_i$. L'inclusion inverse est immédiate puisque $J_i \subset \sum_i J_i$.

Enfin, il suffit de montrer cette égalité pour deux idéaux, le résultat général s'en déduit par récurrence. Montrons donc que $V(J_1 \cap J_2) = V(J_1) \cup V(J_2)$. L'inclusion $V(J_1) \cup V(J_2) \subset V(J_1 \cap J_2)$ résulte immédiatement de $J_1, J_2 \subset J_1 \cup J_2$ et de 1. Pour la réciproque, supposons qu'il existe $x \in V(J_1 \cap J_2)$ qui n'appartienne pas à la réunion $V(J_1) \cup V(J_2)$. Alors, il existe $f_1 \in J_1, f_2 \in J_2$ tels que $f_1(x) \neq 0,\ f_2(x) \neq 0$, d'où $f_1 f_2(x) \neq 0$. Mais le produit $f_1 f_2 \in J_1 \cap J_2$; ce qui est contradictoire. Notons au passage que nous avons aussi montré que $V(J_1 \cap J_2) = V(J_1 J_2) = V(J_1) \cup V(J_2)$.

Conséquence : les ensembles algébriques fermés de k^n forment les fermés d'une topologie appelée *topologie de Zariski*.

Un ouvert de k^n pour la tolpologie de Zariski est donc le complémentaire d'un ensemble algébrique fermé. L'ensemble k^n muni de cette topologie est appelé *espace affine.*

Exemple : si $n = 1$, les ensembles algébriques sont constitués d'un nombre fini de points (l'espace des zéros d'un nombre fini de polynômes ; en réalité, puisque $k[X]$ est principal, il suffit d'un polynôme) ; les ouverts sont donc constitués de toute la "droite" affine privée d'un nombre fini de points ; ce sont des ensembles denses dans k.

Définition 5.6.1 *Un sous-ensemble non vide Y d'un espace topologique X est dit irréductible s'il n'existe pas Y_1, Y_2, deux sous-ensembles stricts, fermés dans Y, tels que $Y = Y_1 \cup Y_2$.*

Exemple : k est irréductible car ses seuls fermés sont des nombres finis de points, donc toute réunion de deux tels sous-ensemble est finie, or k étant algébriquement clos est infini.

Cette définition se traduit en ce qui concerne les ensembles algébriques par :

Définition 5.6.2 *Un sous-ensemble algébrique fermé E de k^n est irréductible s'il n'est pas la réunion de deux sous-ensembles algébriques stricts de E. On appelle "variété algébrique affine" un ensemble algébrique fermé irréductible d'un k^n, muni de la topologie induite.*

Théorème 5.6.1 *Un sous-ensemble algébrique E de k^n est irréductible ssi l'idéal $I(E)$ est premier. De plus, tout sous-ensemble algébrique est la réunion finie d'ensembles irréductibles.*

Il nous faut tout d'abord un

Lemme 5.6.1 *Soit A un anneau noethérien, alors tout idéal de A qui est intersection d'idéaux premiers est intersection finie d'idéaux premiers.*

Preuve : Supposons que le résultat soit faux et considérons J maximal parmi les idéaux intersection d'idéaux premiers qui ne sont pas intersection finie. Alors, bien sûr, J n'est pas premier, donc, il existe $\alpha \notin J, \beta \notin J$ tels $\alpha\beta \in J$. Alors, si $J = \cap_{t\in T}\mathfrak{p}_t$, $\alpha\beta \in \mathfrak{p}_t$ pour tout $t \in T$.

Soit alors $T' = \{t \in T; \alpha \in \mathfrak{p}_t\}$ et $T'' = \{t \in T; \beta \in \mathfrak{p}_t\}$. On a $T = T' \cup T''$. Soient $J' = \cap_{t\in T'}\mathfrak{p}_t$ et $J'' = \cap_{t\in T''}\mathfrak{p}_t$. Alors $J = J' \cap J''$. Or $J \subset J', J \neq J'$ et $J \subset J'', J \neq J''$, puisque $\alpha \in J'$ et $\alpha \notin \in J$ et $\beta \in J', \beta \notin J$. Ce qui implique, par la propriété de maximalité de J, que J' et J'' sont tous deux intersection finie d'idéaux premiers, et par voie de conséquence, J aussi, ce qui est impossible.

Preuve du théorème : d'après le lemme précédent, il suffit de prouver que l'équivalence de E irréductible et $I(E)$ premier. Supposons $I(E)$ premier et E non irréductible, alors $E = E' \cup E''$, $E', E'' \subset E$ strictement, d'où $I(E) \subset I(E')$, $I(E) \subset I(E'')$ strictement aussi.

Mais, de $E = E' \cup E''$, on déduit immédiatement, par la proposition ci-dessus, que $I(E) = I(E') \cap I(E'')$, donc $I(E)$ n'est pas premier. En effet, si $\alpha \in I(E'), \notin I(E)$, $\beta \in I(E''), \notin I(E)$, alors $\alpha\beta \in I(E') \cap I(E'') = I(E)$.

Réciproquement, supposons que $I(E)$ n'est pas premier, alors $I(E) = \sqrt{I(E)}$ est l'intersection des idéaux premiers qui contiennent $I(E)$, d'où est intersection finie de tels idéaux. Ecrivons, $I(E) = \cap_{i=1}^{\ell}\mathfrak{p}_i$, $\ell \geq 2$, où l'on suppose ℓ minimal. Alors, d'après la porposition ci-dessus, $E = \cup V(\mathfrak{p}_i)$. Mais, si $E' = V(\cap_{i\neq j}\mathfrak{p}_i)$ et $E'' = V(p_i)$, on a $E = E' \cup E''$, alors que $E \neq E', E''$, par minimalité de ℓ. Donc, E n'est pas irréductible.

Définition 5.6.3 *Un espace topologique X est dit noethérien s'il satisfait à la condition de chaîne descendante pour les fermés, c'est-à-dire : toute suite décroissante $Y_1 \supseteq Y_2 \supseteq \ldots$ de fermés est stationnaire ie. il existe un entier r tel que $Y_r = Y_{r+1} = \ldots$.*

Exemple : k^n est un espace topologique noethérien, car si $Y_1 \supseteq Y_2 \supseteq \ldots$ est une suite décroissante defermés, il lui correspond une suite croissante d'idéaux $I(Y_1) \subseteq I(Y_2) \subseteq \ldots$ de $k[X_1, \ldots, X_n]$ qui stationne puisque $k[X_1, \ldots, X_n]$ est un anneau noethérien.

On peut démontrer (en TD), d'une manière assez voisine du théorème ci-dessus, un résultat analogue sur les espaces topologiques :

Proposition 5.6.2 *Dans un espace topologique noethérien X, tout sous-ensemble fermé non vide Y peut s'exprimer comme réunion finie $Y = Y_1 \cup Y_2 \cup \cdots \cup Y_r$ de fermés irréductibles. Si on suppose de plus que $Y_j \not\subset Y_i$ si $i \neq j$, alors les Y_i sont uniques. On les appelle "composantes irréductibles de Y".*

On retrouve ainsi le résultat précédent comme corollaire, avec en plus l'unicité.

Définition 5.6.4 *La dimension d'un espace topologique X est le plus grand entier n tel qu'il existe une chaîne $Z_0 \subset Z_1 \subset \cdots \subset Z_n$ d'ensembles fermés irréductibles distincts de X. La dimension d'une variété affine sera sa dimension en tant qu'espace topologique.*

Définition 5.6.5 *Dans un anneau A, la hauteur d'un idéal premier $\mathfrak{p}$ est le plus grand entier n tel qu'il existe une chaîne d'idéaux premiers distincts $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$. La dimension (de Krull) d'un anneau A est la borne supérieure des hauteurs de tous ses idéaux premiers.*

Exemple : On peut montrer que la dimension de $k[X_1, \ldots, X_n]$ est n (voir Serre, Matsumura, Atiyah-McDonald, etc...).

5.7 Variétés projectives

Soit toujours k un corps algébriquement clos. On définit $\mathbb{P}^n_k$ comme l'ensemble des classes d'équivalences de $n+1$-uplets $(a_0, \ldots, a_n)$ pour la relation $(a_0, \ldots, a_n) \cong (\lambda a_0, \ldots, \lambda a_n)$, pour tout $\lambda \in k,\ \lambda \neq 0$. Un point P de $\mathbb{P}^n_k$ est donc représenté par un $n+1$-uplet $(a_0, \ldots, a_n)$, qui est *un système de coordonnées homogènes de P.*

Soit $S = k[X_0, \ldots, X_n]$; c'est un anneau gradué par le degré total. Si f est un polynôme homogène de degré d, alors $f(\lambda a_0, \ldots, \lambda a_n) = \lambda^d f(a_0, \ldots, a_n)$, pour tout $\lambda \in k,\ \lambda \neq 0$. On peut donc considérer les sous-ensembles de $\mathbb{P}^n_k$ de la forme $Z(f) = \{P \in \mathbb{P}^n_k; f(P) = 0\}$, et, plus généralement, $Z(T) = \{P \in \mathbb{P}^n_k; f(P) = 0\ \forall f \in T\}$ où T est un ensemble de polynômes homogènes. En particulier, si $\mathcal{I}$ est un idéal homogène, il peut être engendré par des polynômes homogènes (en nombre fini) $f_1, \ldots, f_s$ et on peut définir $Z(\mathcal{I}) = \{P \in \mathbb{P}^n_k; f_i(P) = 0, i = 1, \ldots, s\}$.

Définition 5.7.1 *Un sous-ensemble $Y \subset \mathbb{P}^n_k$ est un ensemble algébrique s'il existe un ensemble de polynômes homogènes T tel que $Y = Z(T)$.*

On a des résultats analogues à ceux de la section précédente qui permettent de faire des ensembles algébriques des fermés d'une topologie appellée topologie de Zariski de $\mathbb{P}^n_k$.

Définition 5.7.2 *Une variété algébrique projective est un ensemble algébrique irréductible d'un $\mathbb{P}^n_k$ muni de la topologie induite par la topologie de Zariski.*

Si $Y \subset \mathbb{P}^n_k$ est un sous-ensemble, l'idéal *homogène* associé à Y est $\{f \in S; f$ est homogène et $f(P) = 0\ \forall P \in Y\}$ et si Y est un ensemble algébrique, on définit l'anneau des coordonnées homogènes de Y comme $S(Y) = S/I(Y)$.
Remarque : On peut recouvrir $\mathbb{P}^n_k$ par n ouverts affines et, par suite, toute variété algébrique de $\mathbb{P}^n_k$ peut être recouverte par des variétés affines.

5.8 Morphismes

Définition 5.8.1 *Soient $V \subset k^n$ et $W \subset k^m$ deux variétés algébriques affines et $\phi : V \to W$ une application pouvant être écrite $\phi = (\phi_1, \ldots, \phi_n)$ où $\phi_i : V \to k$. On dit que ϕ est régulière (ou un morphisme) si les ϕ_i sont polynomiales.*

Proposition 5.8.1 *Soit $\phi : V \to W$ un morphisme. Alors $\tilde{\phi} : A(W) \to A(V)$ définie par $\tilde{\phi}(f) = f \circ \phi$ est un homomorphisme de k-algèbres.*

La preuve en est immédiate.

Pour effectuer le calcul de $\tilde{\phi}$, on peut procéder de la manière suivante. On a $A(W) = k[Y_1, \ldots, Y_m]/I(W)$ et $A(V) = k[X_1, \ldots, X_n]/I(V)$. Notons $\eta_i : W \subset k^m$ la i-ème fonction coordonnée $W \to k$. Alors $\tilde{\phi}(\eta_i) = \phi_i$. Or les ϕ_i sont des restrictions à V de polynômes $P_i(X_1, \ldots, X_n)$, alors $\tilde{\phi}$ est défini par

$$\begin{array}{rccc} \tilde{\phi} : & k[Y_1, \ldots, Y_m]/I(W) & \to & k[X_1, \ldots, X_n]/I(V) \\ & Y_i & \mapsto & \overline{P}_i \end{array} .$$

De plus, si $\phi(x) = y$, on vérifie aussitôt que $\tilde{\phi}^{-1}(\mathfrak{m}_x) = \mathfrak{m}_y$ où $\mathfrak{m}_x = \{f \in A(V) | f(x) = 0\}$ $(= I(\{x\}))$ est un idéal maximal de $k[X_1, \ldots, X_n]$ (et de même en y).

Proposition 5.8.2 *L'application $Hom(V, W) \to Hom_k(A(W), A(V))$ donnée par $\phi \mapsto \tilde{\phi}$ est bijective.*

Preuve : Cette application est injective. Si $\phi, \psi : V \to W$ sont deux applications régulières telles que $\tilde{\phi} = \tilde{\psi}$, alors, comme on le voit sur leurs composantes, $\phi = \psi$ (en effet : $\phi_i = \tilde{\phi}(\eta_i) = \tilde{\psi}(\eta_i) = \psi_i$).

Pour la surjectivité, soit $\theta : A(W) \to A(V)$ un homomorphisme de k-algèbres. Posons $\phi_i = \theta(y_i) \in A(V)$. Soit $F(Y_1, \ldots, Y_m) \in I(W)$ et $x \in V$, alors $F(\phi(x)) = F(\theta(y_1), \ldots, \theta(y_m))(x) = \theta(F(y_1, \ldots, y_m))$. Or $F(y_1, \ldots, y_m)$ est l'image dans le quotient $A(W)$ du polynôme $F(Y_1, \ldots, Y_m)$. Or cet élément est nul, donc ϕ est à valeurs dans W et $\theta = \tilde{\phi}$.

Théorème 5.8.1 *Supposons k algébriquement clos. Il y a une équivalence de catégories entre la catégorie des k-algèbres de type fini réduites munis des homomorphismes de k-algèbres et la catégorie des ensembles algébriques affines munis des applications régulières.*

Preuve : Une k-algèbre A de type fini est isomorphe à $k[X_1, \ldots, X_n]/I$ et comme A est réduite, $I = \sqrt{I}$. Si $V = V(I)$, on a alors $I(V) = \sqrt{I} = I$ par le nullstellensatz, et donc $A(V) \cong A$.

Définition 5.8.2 *Soit $\phi : V \to W$ un morphisme. Alors ϕ est un isomorphisme ssi ϕ est bijectif et ϕ^{-1} est un morphisme.*

Corollaire 5.8.1 *Soit $\phi : V \to W$ un morphisme. Alors ϕ est un isomorphisme ssi $\tilde{\phi}$ est un isomorphisme de k-algèbres ; ce qu'on peut écrire $V \cong W$ ssi $A(V) \cong A(W)$.*

Exemples : 1. La parabole $P = V(Y - X^2)$ est isomorphe à une droite. L'application $V \to D$ définie par $(x, x^2) \mapsto x$ est un morphisme dont l'inverse est $x \mapsto (x, x^2)$. Mais, on a aussi $A(V) = k[X, Y]/(Y - X^2) \cong k[T] = A(D)$ où $X \mapsto T$, $Y \mapsto T^2$.

2. Au contraire, la cubique $C = V(Y^2 - X^3)$ n'est pas isomorphe à une droite ; en effet $A(C) = k[X, Y]/(Y^2 - X^3) \cong k[T, T^2] \subset k[T]$ et n'est donc pas isomorphe à un $k[Z]$.

Bibliographie

[1] S. LANG, Algèbre, Addison-Wesley.

[2] M.F. ATIYAH, I.G. MACDONALD, Introduction to Commutative Algebra, Addison Wesley Publishing.

[3] R. GODEMENT, Cours d'Algèbre, Herrmann

[4] H. MATSUMURA, Commutative Algebra, Benjamin.

[5] N. BOURBAKI, Algèbre

[6] S. MAC LANE, G. BIRKHOFF, Algèbre 2, les Grands Théorèmes, Gauthier-Villars.

[7] J.P. SERRE, Représentation linéaire des groupes finis.

[8] FULTON, HARRIS, Representations, Springer.

[9] O. ZARISKI, P. SAMUEL, Commutative Algebra, Van Nostrand.

Table des matières