2. Variétés algébriques affines

2.1. **Parties algébriques et idéaux.** Dans cette partie, on fixe un corps algébriquement clos k.

Définition 2.1. *Soit $n \geqslant 1$ et soit $I \subset k[X_1, \dots, X_n]$ un idéal. On note*

$$V(I) := \{x = (x_1, \dots, x_n) \in k^n, \forall P \in I, P(x) = 0\}$$

Une partie de k^n de la forme $V(I)$ est appelée variété algébrique affine *ou encore* partie algébrique de k^n.

Remarque 2.2. Comme tout idéal de $k[X_1, \dots, X_n]$ est de type fini, si I est un idéal de $k[X_1, \dots, X_n]$, il existe des éléments $P_1, \dots, P_m$ dans $k[X_1, \dots, X_n]$ tels que $I = (P_1, \dots, P_m)$. On a alors

$$V(I) = \{(x_1, \dots, x_n) \in k^n, P_1(x_1, \dots, x_n) = \dots = P_m(x_1, \dots, x_n)\}$$

Exemple 2.3. Soient I et J des idéaux de $k[X_1, \dots, X_n]$.

a) On $V(0) = k^n$ et $V(k[X_1, \dots, X_n]) = \emptyset$.

b) On a $V(I + J) = V(I) \cap V(J)$.

c) On a $V(IJ) = V(I \cap J) = V(I) \cup V(J)$.

d) Si $I \subset J$, on a $V(J) \subset V(I)$.

e) Tout idéal de $k[X]$ est principal. Si $P \in k[X] \setminus \{0\}$, l'ensemble $V(P)$ est l'ensemble des racines de k. Ainsi les parties algébriques de k sont k et les parties finies de k.

f) Si $(a_1, \dots, a_n) \in k^n$, on a $V(X_1 - a_1, \dots, X_n - a_n) = \{(a_1, \dots, a_n)\}$.

Théorème 2.4 (Nullstellensatz faible)**.** *Si $I \neq k[X_1, \dots, X_n]$ est un idéal, on a $V(I) \neq \emptyset$.*

Démonstration. D'après le théorème de Krull, il existe un idéal maximal $\mathfrak{m}$ contenant I. On a donc $V(\mathfrak{m}) \subset V(I)$. Par ailleurs le théorème des zéros de Hilbert implique que $\mathfrak{m}$ est de la forme $(X_1 - a_1, \dots, X_n - a_n)$ et donc

$$\{(a_1, \dots, a_n)\} \subset V(I)$$

$\square$

Remarque 2.5. Lorsque le corps k n'est pas supposé algébriquement clos, ce résultat est loin d'être toujours valide. On peut considérer l'idéal $(X^2 + 1) \subset \mathbb{R}[X]$. On a alors $V(I) = \emptyset$ et $I \subsetneq \mathbb{R}[X, Y]$.

Définition 2.6. *Soit X une partie de k^n. On note*

$$I(X) := \{P \in k[X_1, \dots, X_n], \forall x \in X, P(x) = 0\}$$

Il s'agit d'un idéal de $k[X_1, \dots, X_n]$ nommé idéal annulateur *de la partie X.*

Exemple 2.7. a) Si $X \subset Y$, on a $I(Y) \subset I(X)$.
b) On a $I(\emptyset) = k[X_1, \ldots, X_n]$ et $I(k^n) = 0$.

Remarque 2.8. Ici encore certaines des propriétés précédentes peuvent être mises en défaut lorsque k n'est pas supposé algébriquement clos. Par exemple $I(\mathbb{F}_p) = (X^p - X)$.

Proposition 2.9. *Soit X une partie de k^n. On a toujours $X \subset V(I(X))$ avec égalité si et seulement si X est une partie algébrique de k^n.*

Démonstration. Il s'agit essentiellement de vérifier que, lorsque X est une partie algébrique de k^n, on a $X \supset V(I(X))$. On peut écrire $X = V(J)$ pour un idéal J de $k[X_1, \ldots, X_n]$. Par définition $J \subset I(X)$ et donc $V(I(X)) \subset V(J) = X$. □

Remarque 2.10. Pour une partie X de k^n, la partie algébrique $V(I(X))$ est appelée *adhérence de Zariski* de X. De façon plus générale, lorsque I parcourt les idéaux de $k[X_1, \ldots, X_n]$, l'ensemble des parties de la forme $k^n \smallsetminus V(I)$ est une topologie sur k^n. Cette topologie est appelée *topologie de Zariski.* Les parties algébriques de k^n sont les fermés pour la topologie de Zariski et l'adhérence de Zariski d'une partie de k^n n'est autre que l'adhérence pour la topologie de Zariski. Si X est une partie quelconque de k^n, la topologie induite sur X par la topologie de Zariski de k^n est appelée *topologie de Zariski* de X.

Si I est un idéal de $k[X_1, \ldots, X_n]$, on a $I \subset I(V(I))$. En général cette inclusion est stricte. Nous allons à présent étudier le cas d'égalité.

Définition 2.11. *Soit A un anneau et soit I un idéal de A. L'idéal I est dit* radical *si*

$$\forall x \in A \text{ telque } \exists n \geqslant 0,\ x^n \in I \text{ alors } x \in I$$

On vérifie immédiatement qu'une intersection d'idéaux radicaux est un idéal radical. Étant donné un idéal I il existe donc un plus petit idéal radical contenant I : il s'agit de l'intersection de tous les idéaux radicaux contenant I, on la note $\sqrt{I}$ et on l'appelle *racine* de l'idéal I.

Proposition 2.12. *Soit I un idéal d'un anneau A. On a alors*

$$\sqrt{I} = \{x \in A,\ \exists n \geqslant 0,\ x^n \in I\}$$

Démonstration. Par définition, $\sqrt{I}$ est contenu dans tous les idéaux radicaux contenant I. Il suffit donc de prouver que $\sqrt{I}$ est un idéal radical. Il est clair que $\sqrt{I}$ est stable par multiplication par les éléments de A. Soient x et y dans $\sqrt{I}$. Il existe alors $n \geqslant 0$ et $m \geqslant 0$ tels que $x^n \in I$ et $y^m \in I$. On a

$$(x+y)^{n+m} = \sum_{i+j=n+m} \binom{n+m}{i} x^i y^{n+m-i}$$

Si $i+j=n+m$, on a soit $i \geqslant n$ soit $j \geqslant m$ et donc $x^iy^j \in I$. Ainsi $(x+y)^{n+m} \in I$ et $x+y \in \sqrt{I}$. Ainsi $\sqrt{I}$ est un idéal, il est immédiat de vérifier qu'il est radical. $\square$

Si I est un idéal de $k[X_1, \ldots, X_n]$, l'idéal $I(V(I))$ est radical, on a donc une inclusion $\sqrt{I} \subset I(V(I))$. Le théorème qui suit affirme que cette inclusion est une égalité lorsque k est un corps algébriquement clos.

Théorème 2.13 (Nullstellensatz fort)**.** *Soit I un idéal de $k[X_1, \ldots, X_n]$. On a une égalité*

$$\sqrt{I} = I(V(I))$$

Démonstration. Nous allons déduire ce théorème de la version faible du Nullstellensatz en utilisant une astuce due à Artin-Tate. Soit $P \in I(V(I))$. Considérons l'idéal J de $k[X_1, \ldots, X_{n+1}]$ défini par

$$J = (X_{n+1}P - 1) + Ik[X_1, \ldots, X_{n+1}]$$

On vérifie que $V(J) = \emptyset$. Supposons par l'absurde que $V(J) \neq \emptyset$. On peut alors choisir un élément $x \in V(J)$. Soit $(x_1, \ldots, x_{n+1})$ ses coordonnées. Comme $x \in Ik[X_1, \ldots, X_{n+1}]$, on a $(x_1, \ldots, x_n) \in V(I)$. Par définition $P(x_1, \ldots, x_n) = 0$ et x est donc annulé par $X_{n+1}P$. Comme par ailleurs $x \in V(X_{n+1}P - 1)$, on en déduit $1 = 0$ ce qui est absurde. Ainsi $V(J) = \emptyset$.

Le Nullstellensatz faible implique alors $J = k[X_1, \ldots, X_{n+1}]$ et on peut écrire

$$1 = \sum_{i=0}^{k} b_i X_{n+1}^i + a(X_{n+1}P - 1)$$

où les $a \in k[X_1, \ldots, X_{n+1}]$ et les b_i sont dans I. Soit A l'anneau quotient $A := k[X_1, \ldots, X_{n+1}]/(X_{n+1}P - 1)$. Soit c_i l'image de b_i dans A. On a alors

$$1 = \sum_i c_i X_{n+1}^i \mod (X_{n+1}P - 1)$$

En multipliant cette égalité par P^k, on en déduit

$$P^k = \sum_{i=0}^{k} c_{k-i} P^i \mod (X_{n+1}P - 1)$$

Soit $R = P^k - \sum_{i=0}^{k} c_{k-i}P^i$. D'une part $R \in k[X_1, \ldots, X_n]$ et d'autre part $R = (X_{n+1}P - 1)Q$ pour un certain $Q \in k[X_1, \ldots, X_{n+1}]$. En utilisant l'additivité des degrés en X_{n+1} on en conclut que $Q = R = 0$ et donc que $P^k \in I$, c'est-à-dire $P \in \sqrt{I}$. $\square$

2.2. **Applications polynomiales.** On fixe un corps algébriquement clos k.

Définition 2.14. *Soit $V \subset k^n$ une variété algébrique affine. Une fonction sur V à valeurs dans k est dite* polynomiale *s'il s'agit de la restriction à V d'un élément de $k[X_1, \dots, X_n]$.*

Si $W \subset k^m$ est une autre variété algébrique affine, une application de V dans W est dite polynomiale *si toutes ses coordonnées sont des fonctions polynomiales.*

La somme de deux fonctions polynomiales, le produit de deux fonctions polynomiales ainsi que la multiplication d'une fonction polynomiale par un élément de k sont des fonctions polynomiales. On vérifie ainsi que l'ensemble des fonctions polynomiales sur une variété algébrique affine V est une k-algèbre que l'on note $k[V]$.

Proposition 2.15. *La k-algèbre des fonctions polynomiales sur une variété algébrique affine $V \subset k^n$ est isomorphe à la k-algèbre $k[X_1, \dots, X_n]/I(V)$.*

Démonstration. Par définition l'application de restriction donnée par $P \mapsto P|_V$ de $k[X_1, \dots, X_n]$ dans $k[V]$ est surjective. C'est de plus un morphisme de k-algèbre. Son noyau est l'ensemble des polynômes P tels que $P|_V = 0$, c'est-à-dire $I(V)$. $\square$

Considérons $V \subset k^n$ et $W \subset k^m$ deux variétés algébriques affines et $f : X \to Y$ une application polynomiale. Si $g \in k[W]$, la fonction $g \circ f$ est une fonction polynomiale sur V. Notons la $f^*(g)$. On a ainsi défini une application f^* de $k[W]$ vers $k[V]$. On vérifie aisément que f^* est un morphisme de k-algèbres. Ce procédé permet en fait de caractériser algébriquement les applications polynomiales de V vers W.

Théorème 2.16. *Soient $V \subset k^n$ et $W \subset k^m$ deux variétés algébriques affines. Soit φ un morphisme de k-algèbres de $k[W]$ vers $k[V]$. Il existe alors une* unique *application polynomiale f de V vers W telle que $\varphi = f^*$.*

Démonstration. Rappelons que les applications de restrictions $k[X_1, \dots, X_n] \to k[V]$ et $k[X_1, \dots, X_m] \to k[W]$ induisent des isomorphismes qui nous permettent d'identifier $k[V]$ et $k[X_1, \dots, X_n]/I(V)$ ainsi que $k[W]$ et $k[X_1, \dots, X_m]/I(W)$. Choisissons alors, pour tout $1 \leqslant i \leqslant m$, un polynôme $P_i \in k[X_1, \dots, X_n]$ tel que $\varphi(X_i) \equiv P_i \mod I(V)$ et posons $f := (P_1, \dots, P_m)|_V$. Par définition f est une application polynomiale de V dans k^m. Par ailleurs elle ne dépend pas du choix des polynômes P_i. Vérifions que l'image de f est bien incluse dans W. Si $x \in V$ et si $g \in I(W)$, on a

$$\begin{aligned} g(f(x)) &= g(P_1(x), \dots, P_m(x)) \\ &= g((\varphi(X_1), \dots, \varphi(X_n)))(x) \\ &= \varphi(g(X_1, \dots, X_n))(x) && \text{puisque } \varphi \text{ est un morphisme de } k\text{-algèbres} \\ &= 0 && \text{puisque } \varphi(g) \in I(W) \end{aligned}$$

Ainsi $f(x) \in V(I(W)) = W$. On vérifie alors que $\varphi = f^*$. Si $g \in k[W]$, on a

$$\varphi(g) = \varphi(g(X_1, \dots, X_n)) = g(\varphi(X_1), \dots, \varphi(X_n)) = g(P_1, \dots, P_n) = f^*(g)$$

Il nous reste à vérifier l'unicité de f. On vérifie en fait que si f et h sont deux applications polynomiales de V dans W, l'égalité $f^* = h^*$ implique $f = h$. Cela résulte du fait que si $x \in V$, on a $f(x) = (y_1, \dots, y_m)$ où chaque y_i est l'évaluation du polynôme $f^*(X_i) = h^*(X_i)$ en $(x_1, \dots, x_n)$. □

Définition 2.17. *Soient V et W deux variétés algébrique affines. Un* isomorphisme *de V sur W est une application polynomiale f de V dans W telle qu'il existe une application polynomiale g de W dans V telle que $g \circ f = \mathrm{Id}_V$ et $f \circ f = \mathrm{Id}_W$.*

Remarque 2.18. 1) Une application polynomiale bijective n'est pas nécessairement un isomorphisme.

2) Lorsqu'une application polynomiale f est un isomorphisme, l'application polynomiale g dans la définition ci-dessus est unique et est appelée *inverse* de f.

Corollaire 2.19. *Deux variétés algébriques affines sont isomorphes si et seulement si leurs algèbres de fonctions polynomiales sont isomorphes.*

Exemple 2.20. a) Posons $V = k$ et $W = V(Y - X^2) \subset k^2$. Les variétés V et W sont isomorphes. Un isomorphisme de V sur W est donné par $t \mapsto (t, t^2)$. Son inverse est donné par $(x, y) \mapsto x$.

b) Si $V = k$ et $W = V(Y^2 - X^3) \subset k^2$. L'application $t \mapsto (t^2, t^3)$ est une application polynomiale et bijective. Cependant ce n'est pas un isomorphisme.

2.3. **Variétés algébriques affines irréductibles.**

Définition 2.21. *Une variété algébrique affine $V \subset k^n$ est dite irréductible si, pour toute égalité $V = V_1 \subset V_2$ où V_1 et V_2 sont des parties algébriques de k^n, on a nécessairement $V_1 = V$ ou $V_2 = V$.*

Proposition 2.22. *Une variété algébrique affine est irréductible si et seulement si son algèbre de fonctions polynomiales est intègre.*

On en déduit que pour V et W deux variétés algébriques affines, V est irréductible si et seulement si W est irréductible.

Démonstration. Soit $V \subset k^n$ une partie algébrique. Supposons que V n'est pas irréductible. Il existe alors V_1 et V_2 des parties algébriques de k^n telles que $V_1 \subsetneq V$, $V_2 \subsetneq V$ et $V = V_1 \cup V_2$. On a donc $I(V) \subsetneq I(V_1)$ et $I(V) \subsetneq I(V_2)$. En particulier on peut trouver $F \in I(V_1) \setminus I(V)$ et $G \in I(V_2) \setminus I(V)$. Soient f et g les images de F et G dans $k[V]$. On a $f \neq 0$ et $g \neq 0$ mais $fg = 0$ donc $k[V]$ n'est pas intègre.

Réciproquement supposons que $k[V]$ n'est pas intègre. On peut donc trouver des éléments non nuls, f et g, de $k[V]$ tels que $fg = 0$. Soient F et G des relèvements de f et g dans $k[X_1, \ldots, X_n]$. Posons $V_1 = V(I(V) + (F))$ et $V_2 = V(I(V) + (F_2))$. On a bien $V = V_1 \cup V_2$ avec $V_1 \subsetneq V$ et $V_2 \subsetneq V$. □

Définition 2.23. *Soit V une variété algébrique affine. Une composante irréductible de V est une partie algébrique irréductible maximale de V.*