COURBES ALGEBRIQUES

(Bernard Le Stum)

CHAPITRE 0

Rappels de géométrie, de topologie et d'algèbre commutative

0.1. Géométrie classique

On fixe un corps de base k.

0.1.1. Définitions Un *espace affine de dimension n sur k* est un ensemble non-vide E muni d'une application

$$\vec{E} \times E \longrightarrow E, (\vec{u}, P) \longmapsto P + \vec{u}$$

où $\vec{E}$ est un espace vectoriel de dimension n, appelé *espace directeur,* telle que

(i) Si $P \in E$, alors $P + \vec{0} = P$,

(ii) Si $P \in E$ et $\vec{u}, \vec{v} \in \vec{E}$, alors $P + (\vec{u} + \vec{v}) = (P + \vec{u}) + \vec{v}$ et

(iii) Si $P, Q \in E$, il existe un unique $\vec{PQ} \in \vec{E}$ tel que $Q = P + \vec{PQ}$.

Un espace affine de dimension 1 est une *droite*. Un espace affine de dimension 2 est un *plan*. Si E est un espace vectoriel sur k, la *structure naturelle d'espace affine sur E* est celle pour laquelle l'espace directeur est E et l'action est donnée par l'addition $E \times E \longrightarrow E$, $(x, y) \longmapsto x + y$. On dit alors que 0 est l'*origine*.

0.1.2. Définition Un sous-ensemble F d'un espace affine E est un *sous-espace affine* s'il existe $P \in F$ tel que $\vec{F} := \{\vec{PQ}, Q \in F\}$ soit un sous-espace vectoriel de $\vec{E}$. On dit que F est un *hyperplan* affine si $\vec{F}$ est un hyperplan vectoriel.

• La propriété est alors satisfaite pour tout point P de F et F est de manière naturelle un espace affine d'espace directeur $\vec{F}$.

• Toute intersection non vide de sous-espaces affines est un sous-espace affine.

• Tout sous-espace affine propre est une intersection d'hyperplans.

• Si E est un espace vectoriel (muni de sa structure naturelle d'espace affine), les sous-espaces vectoriels de E sont les sous-espaces affines contenant 0.

0.1.3. Définition. Soit $\varphi : E \longrightarrow F$ une application entre deux espaces affines. Alors φ est *affine* s'il existe un point P de E tel que l'application $\vec{\varphi} : \vec{E} \longrightarrow \vec{F}$, $\vec{PQ} \longmapsto \varphi(P)\varphi(Q)$ soit linéaire.

• La propriété est alors satisfaite pour tout point P de E et l'application $\vec{\varphi}$ est indépendante du point P.

• Si E et F sont des espaces vectoriels (munis de leur structure naturelle d'espace affine), les applications linéaires de E dans F sont les applications affines qui fixent l'origine.

0.1.4. Définitions. Si E est un espace vectoriel sur k, *l'espace projectif* $\mathbb{P}(E)$ est l'ensemble des droites de E. Si $\pi_E : E\backslash 0 \longrightarrow \mathbb{P}(E)$ est l'application qui envoie un vecteur non nul sur la droite supportée par ce vecteur et si $A \subset \mathbb{P}(E)$, on dit que $C(A) = \pi_E^{-1}(A) \cup \{0\}$ est le *cône* sur A.

• On a $C(A) = \bigcup_{P \in A} P \subset E$.

• On a toujours $C(\bigcup_\alpha A_\alpha) = \bigcup_\alpha C(A_\alpha)$ et $C(A) \subset C(B)$ si et seulement si $A \subset B$.

0.1.5. Définition. Un sous-ensemble V de $\mathbb{P}(E)$ est un *sous-espace projectif (*resp. *un hyperplan)* si $C(V)$ est un sous-espace vectoriel (resp. un hyperplan) de E. Si $\varphi : E \longrightarrow F$ est une application linéaire injective, on dit que l'application induite $\varphi : \mathbb{P}(E) \longrightarrow \mathbb{P}(F)$ est une *homographie*.

• Toute application linéaire injective $\varphi : E \longrightarrow F$ induit effectivement une application $\varphi : \mathbb{P}(E) \longrightarrow \mathbb{P}(F)$. Celle-ci ne change pas si on multiplie l'application linéaire φ par une constante non-nulle.

• On a toujours $\varphi^{-1}(C(A)) = C(\varphi^{-1}(A))$.

0.2. Topologie générale

0.2.1. Définitions. Un *espace topologique* est un ensemble E muni d'une famille $\mathcal{T}$ de parties de E, dites *ouvertes*, qui contient E et $\emptyset$ et qui est stable par union et intersection finie. Le complémentaire d'un ouvert est un *fermé*. Si $A \subset E$, la *topologie induite* sur A est la topologie pour laquelle les ouverts sont les parties de la forme $A \cap U$ avec U ouvert dans E. On dit alors que A est un *sous-espace topologique* de E. L'*adhérence* de A dans E est le plus petit fermé de E contenant A. Si l'adhérence de A est E, on dit que A est *dense* dans E. Une application $\varphi : E \longrightarrow F$ entre deux espaces topologiques est *continue* si l'image réciproque d'un ouvert (ou d'un fermé) est un ouvert (fermé). Elle est *ouverte* (resp. *fermée*) si l'image d'un ouvert (resp. fermé) est ouvert (resp. fermé). C'est un *homéomorphisme* si elle est bijective et si la bijection réciproque est continue. Elle est *dominante* si $\varphi(E)$ est dense dans F.

• Si A est une partie d'un espace topologique E, la famille des $A \cap U$ avec U ouvert dans E définit bien une topologie sur A.

• Une partie A d'un espace topologique E est dense si et seulement si tout ouvert non vide de E rencontre A.

0.2.2. Définition. Un espace topologique *non vide* est *irréductible* s'il possède une des propriétés équivalentes suivantes : (i) On ne peut pas l'écrire comme union de deux fermés propres, (ii) Deux ouverts non vides ont une intersection non vide et (iii) Tout ouvert non vide est dense.

• Ces propriétés sont bien équivalentes.

• Une partie non vide A d'un espace topologique E est irréductible pour la topologie induite si et seulement si chaque fois que $A \subset F_1 \cup F_2$ avec F_1, F_2 fermés dans E, on a $A \subset F_1$ ou $A \subset F_2$.

• L'image d'un irréductible par une application continue est irréductible.

• L'adhérence d'un irréductible est irréductible. Tout ouvert dense d'un irréductible est irréductible.

0.2.3. Définition. Un espace topologique est *noethérien* si toute famille non vide de fermés (resp. d'ouverts) contient un élément minimal (resp. maximal), ou

de manière équivalente, si toute suite décroissante de fermés (resp. croissante d'ouverts) est stationnaire.

• Ces quatre propriétés sont bien équivalentes.

• Un sous-espace non vide d'un espace noethérien est noethérien.

0.2.4. Proposition. Un espace noethérien V s'écrit de manière unique comme union finie de fermés irréductibles V_i avec $V_i \not\subset V_j$ pour $i \neq j$.

0.2.5. Définition. Les V_i sont les *composantes irréductibles* de V.

0.3. Polynômes

Si E et F sont deux ensembles, on note F^E l'ensemble des applications de E dans F.

0.3.1. Définitions. Si R est un anneau (commutatif), on dit que $R[X_1, \ldots, X_n] := \{F \in R^{\mathbb{N}^n}, F(k_1, \ldots, k_n) = 0, k_1, \ldots, k_n >> 0\}$ est l'*anneau des polynômes en n variables* sur R. On pose pour tout $i = 1, \ldots, n$, $X_i(k_1, \ldots, k_n) := 1$ si $k_j = \delta_{ij}$ pour tout $j = 1, \ldots, n$ et 0 sinon. Un *monôme de degré d* est un élément de la forme $fX_1^{d_1} \ldots X_n^{d_n}$, avec $f \in R\backslash 0$ et $d_1 + \ldots + d_n = d$.

• L'ensemble $R[X_1, \ldots, X_n]$ est bien un anneau. En fait, c'est une sous-R-algèbre de $R^{\mathbb{N}^n}$, pour la multiplication $(FG)(k_1, \ldots, k_n) = \sum_{r_i+s_i=k_i} F(r_1, \ldots, r_n)G(s_1, \ldots, s_n)$.

• Tout polynôme non nul s'écrit de manière unique comme somme de monômes.

0.3.2. Définitions. Si F est un polynôme non nul sur R, le *degré* $\deg(F)$ (resp. la *valuation* $\mathrm{val}(F)$) de F est le maximum (resp. minimum) des degrés des monômes composant F. On dit que F est *homogène* si $\mathrm{val}(F) = \deg(F)$. En général, la *composante homogène* de degré d de F est la somme des monômes de degré d dans F. Une *forme linéaire* est un polynôme homogène de degré 1. Si F est un polynôme de degré d en une seule variable X, le *coefficient dominant de F* est le coefficient de X^d. On dit que F est *unitaire* si son coefficient dominant est 1.

• Si un polynôme $F \in R[X_1, \ldots, X_n]$ est homogène de degré d, on a toujours $F(gf_1, \ldots, gf_n) = g^d F(f_1, \ldots, f_n)$.

• Étant donné une R-algèbre A et des éléments $f_1, \ldots, f_n$ de A, il existe un homomorphisme de R-algèbres et un seul $R[X_1, \ldots, X_n] \longrightarrow A$, $F \longmapsto F(f_1, \ldots, f_n)$ qui envoie $X_1, \ldots, X_n$ sur $f_1, \ldots, f_n$.

0.3.3. Définition. Étant donnés une R-algèbre A et $F \in R[X_1, \ldots, X_n]$, on dit que l'application $A^n \longrightarrow A$, $(f_1, \ldots, f_n) \longrightarrow F(f_1, \ldots, f_n)$ est l'*application polynomiale* associée à F.

• L'application canonique $R[X_1, \ldots, X_n] \longrightarrow A^{A^n}$ est un homomorphisme de R-algèbres.

• Soient $F \in R[X_1, \ldots, X_n]$, E un ensemble, A une R-algèbre, $u_1, \ldots, u_n : E \longrightarrow A$ et $P \in E$. On a alors $F(u_1, \ldots, u_n)(P) = F(u_1(P), \ldots, u_n(P))$.

• Si $F \in R[X_1, \ldots, X_n]$ et si $u : A \longrightarrow B$ est un homomorphisme de R-algèbres, alors, $F(u(g_1), \ldots, u(g_n)) = u(F(g_1, \ldots, g_n))$.

0.3.4. Dans le cas d'un corps de base infini k, on a les résultats suivants :

• Si $F \in k[X_1, \ldots, X_n]$ et si l'application associée à F est nulle, alors $F = 0$.

• L'application canonique $k[X_1, \ldots, X_n] \longrightarrow k^{k^n}$ est injective. On identifiera $k[X_1, \ldots, X_n]$ avec son image dans k^{k^n}.

• Un polynôme non nul $F \in k[X_1, \ldots, X_n]$ est homogène de degré d si et seulement si pour tout $(a_1, \ldots, a_n) \in k^n$ et tout $\lambda \in k$, on a $F(\lambda a_1, \ldots, \lambda a_n) = \lambda^d F(a_1, \ldots, a_n)$.

0.3.5. La division euclidienne peut s'interpréter comme suit

• Si $F \in R[X]$ est unitaire de degré d et $R[X]_{<d}$ désigne l'ensemble formé des polynômes de degré strictement inférieur à d et du polynôme nul, alors l'application canonique $R[X]_{<d} \hookrightarrow R[X] \longrightarrow R[X]/(F)$ est bijective.

• Si $a_1, \ldots, a_n \in k$, où k est un corps, alors $(X_1 - a_1, \ldots, X_n - a_n)$ est un idéal maximal de $k[X_1, \ldots, X_n]$ et $k[X_1, \ldots, X_n]/(X_1 - a_1, \ldots, X_n - a_n) \tilde{=} k$.

0.3.6. Notations. Si $F \in k[X_1, \ldots, X_{n+1}]$, on note $F_* = F(X_1, \ldots, X_n, 1)$. Si $F \in k[X_1, \ldots, X_n]$, on pose $0^* = 0$ et si $F \neq 0$,

$$F^* := X_{n+1}^{\deg F} F(\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}) \in k[X_1, \ldots, X_{n+1}].$$

Si S est une partie de $k[X_1, \ldots, X_{n+1}]$, on note $S_* := \{F_*, F \in S_p\}$. Si I est un idéal de $k[X_1, \ldots, X_n]$, on note I^* l'idéal de $k[X_1, \ldots, X_{n+1}]$ *engendré* par les F^*, $F \in I$.

• L'application $F \longmapsto F_*$ est un homomorphisme d'anneaux. De plus, si F est homogène non nul, on a $\deg F_* = \deg F - m$ où m est la valuation de F en X_{n+1}.

• Le polynôme F^* est homogène de même degré que F.

• Si F et $G \in k[X_1, \ldots, X_n]$, on a $(FG)^* = F^*G^*$ et $(F^*)_* = F$.

• Si $F \in k[X_1, \ldots, X_{n+1}]$ est *homogène* de valuation m en X_{n+1}, alors $X_{n+1}^m (F_*)^* = F$.

• Un polynôme $F \in k[X_1, \ldots, X_n]$ est irréductible si et seulement si F^* est irréductible.

• Si $F \in k[X_1, \ldots, X_{n+1}]$ est homogène irréductible et $F \neq cX_{n+1}$, alors $F = (F_*)^*$ et F_* est irréductible.

• Si I est un idéal de $k[X_1, \ldots, X_n]$ on a $(I^*)_* = I$.

• Si I est un idéal de $k[X_1, \ldots, X_n]$, et F homogène, alors $F \in I^*$ si et seulement si $F_* \in I$.

0.3.7. Si R est un anneau et $F := \sum f_n X^n \in R[X]$, on pose $\frac{dF}{dX} = \sum n f_n X^{n-1} \in R[X]$.

• On a

i) $\frac{d(F+G)}{dX} = \frac{dF}{dX} + \frac{dG}{dX}$, ii) $d(FG)/dX = F\frac{dG}{dX} + G\frac{dF}{dX}$ et iii) $\frac{df}{dX} = 0$ si $f \in R$.

• Si $F \in R[X, Y]$, on a $\frac{d^2F}{dXdY} = \frac{d^2F}{dYdX}$.

• Si $F \in R[X_1, \ldots, X_n]$ est homogène de degré m, alors $mF = \sum X_i \frac{dF}{dX_i}$.

• Si $F \in R[X_1, \ldots, X_n]$, A est une R algèbre et $G_i \in A[X]$, alors

$$\frac{dF(G_1, \ldots, G_n)}{dX} = \sum \frac{dF}{dX_i}(G_1, \ldots, G_n) \frac{dG_i}{dX}.$$

• Soit $F \in k[X, Y]$ et $p = car\ k$ (ou $p = \infty$ si $car\ k = 0$). Alors

$$F = \sum_{k<p} \frac{1}{k!} \sum_{i+j=k} \binom{k}{i} \frac{d^kF}{dX^iY^j}(P)(X-a)^i(Y-b)^j \ mod\ (X, Y)^p$$

• Soit F non constant $\in k[X_1, \ldots, X_n]$ tel que $\frac{dF}{dX_1} = \ldots = \frac{dF}{dX_n} = 0$. Alors, k est de caractéristique $p > 0$ et $F = G^p$.

• Si $F \in k[X_1, \ldots, X_{n+1}]$ est homogène, alors pour tout $i = 1, \ldots, n$, on a

$$(\frac{dF}{dX_i})_* = \frac{dF_*}{dX_i}.$$

0.4. Compléments sur les anneaux et idéaux

0.4.1. Définitions. Le *radical* (ou la *racine*) d'un idéal I dans un anneau A est $\sqrt{I} = \{f \in A, \exists\ n \in \mathbb{N}, f^n \in I\}$. On dit que I est *radical* si $I = \sqrt{I}$. Un anneau est *réduit* (resp. *intègre*, resp. un *corps*) si l'idéal nul est un idéal radical (resp. premier, resp. maximal).

• Le radical d'un idéal I de A est un idéal de A contenant I.

• Soient A un anneau, I un idéal de A et $\pi : A \longrightarrow A/I$ la surjection canonique. Alors, l' application $J \longmapsto \pi(J)$ est une surjection de l'ensemble des idéaux de A dans celui des idéaux de A/I.

• On a $A/(I + J) \tilde{=} (A/I)/\pi(J)$.

• L'idéal $\pi(J)$ est radical, resp. premier, resp. maximal si et seulement si $I + J$ l'est. En particulier, I est un idéal radical (resp. premier, resp. maximal) si et

seulement si A/I est réduit (resp. intègre, resp. un corps).

0.4.2. Définition. Un anneau est *noethérien* s'il satisfait les conditions équivalentes suivantes : (i) Tout idéal est de type fini, (ii) Toute famille non vide d'idéaux contient un élément maximal et (iii) Toute suite croissante d'idéaux est stationnaire.

• Ces conditions sont bien équivalentes.

• Un quotient d'un anneau noethérien est noethérien.

0.4.3. Définition. Une R-algèbre est *de type fini* si elle est isomorphe a un quotient d'un anneau de polynômes (en un nombre fini de variables) sur R.

0.4.4. Théorème (Hilbert). Toute algèbre de type fini sur un anneau noetherien est noethérien.

0.4.5. Théorème (Nullstellensatz algébrique, Hilbert). Si k est un corps, toute extension de k qui est une k-algèbre de type fini est une extension finie de k.

0.4.6. Définitions. Un anneau A est *local* s'il satisfait les propriétés équivalentes suivantes : (i) A possède un unique idéal maximal $\mathfrak{m}_A$ et (ii) $A\backslash A^\times$ est un idéal de A. On dit alors que $k(A) = A/\mathfrak{m}_A$ est le *corps résiduel* de A. Un homomorphisme d'anneaux locaux $\varphi : A \longrightarrow B$ est *local* si $\varphi(\mathfrak{m}_A) \subset \mathfrak{m}_B$.

• Les propriétés (i) et (ii) sont bien équivalentes et on a $\mathfrak{m}_A = A\backslash A^\times$.

• Si A est un anneau intègre de corps de fractions K et $\mathfrak{p}$ un idéal premier, alors $A_\mathfrak{p} := \{f/g,\, g \notin \mathfrak{p}\} \subset K$ est un anneau.

• Si I est un idéal de A, l'idéal $IA_\mathfrak{p}$ de $A_\mathfrak{p}$ engendré par I est $\{f/g,\, f \in I,\, g \notin \mathfrak{p}\}$. De plus, on a toujours $(IA_\mathfrak{p})(JA_\mathfrak{p}) = (IJ)A_\mathfrak{p}$.

• $A_\mathfrak{p}$ est un anneau local d'idéal maximal $\mathfrak{p}A_\mathfrak{p}$ et de résiduel, le corps des fractions de A/$\mathfrak{p}$.

• Si J est un idéal de $A_\mathfrak{p}$ alors $J = IA_\mathfrak{p}$ avec $I = J \cap A$.

• Si A est noethérien, $A_{\mathfrak{p}}$ aussi.

• Si $u : A \longrightarrow B$ est un homomorphisme d'anneaux et un idéal premier de B, alors $\mathfrak{p} := u^{-1}(\ )$ est un idéal premier de A et u se prolonge de manière unique en un homomorphisme (local) $u\ : A_{\mathfrak{p}} \longrightarrow B$.

• Si u est injectif, surjectif ou un isomorphisme, il en va de même de u .

0.4.7. Définitions. Un idéal I de $R[X_1, \ldots, X_{n+1}]$ est *gradué* (ou *homogène*) s'il satisfait les propriétés équivalentes suivantes : (i) Tout élément de I à ses composantes homogènes dans I et (ii) I est engendré par des polynômes homogènes. Un élément non nul de $A := R[X_1, \ldots, X_n]/I$ est *homogène de degré* d s'il possède un représentant homogène dans $R[X_1, \ldots, X_n]$. Si A est intègre, un élément f du corps de fractions K de A est dit *homogène de degré* d si on peut l'écrire $f = g/h$ avec g et h homogènes et $\deg g - \deg h = d$.

• Les propriétés (i) et (ii) ci dessus sont bien équivalentes.

• La notion de degré est bien définie.

• Si A est intègre, l'ensemble formé par 0 et par les éléments homogènes de degré nul du corps des fractions de A forment un sous-corps.

0.4.8. Définition. Une *valuation discrète* sur un corps K est une application surjective $v : K^* \longrightarrow \mathbb{Z}$ tel que $v(f.g) = v(f) + v(g)$ et $v(f + g) \geq min(v(f), v(g))$. On dit que $l \in K$ est une *uniformisante* pour v si $v(l) = 1$. L'ensemble $A := \{f \in K, v(f) \geq 0\} \cup \{0\}$ est l'*anneau de valuation* de v.

• On a $v(1) = 0$ et pour tout $f \in K^\times$, $v(f^{-1}) = -v(f)$.

• A est bien un sous-anneau de K. C'est un anneau local d'idéal maximal $\mathfrak{m}_A := \{f \in K, v(f) > 0\} \cup \{0\}$.

• On a $v(f) \geq n$ ssi $f \in \mathfrak{m}_A^n$.

• Si A contient un corps k tel que l'application composée $k \hookrightarrow A \longrightarrow k(A)$ soit bijective, alors pour tout $f \in A$, on a $v(f) = dim_k A/(f)$.

0.4.9. Proposition Pour un anneau A, les propriétés suivantes sont équivalentes

:

(i) A est un anneau de valuation discrète.

(ii) A est intègre et il existe $l \in A$ tel que tout f non nul de A s'écrive de manière unique sous la forme $f = ul^n$ avec $u \in A^\times$ et $n \in \mathbb{N}$.

(iii) A est un anneau local principal .

(iv) A est un anneau local intègre noethérien et $dim_{k(A)}\ \mathfrak{m}_A/\mathfrak{m}_A^2 = 1$.

COURBES ALGEBRIQUES

(Bernard Le Stum)

CHAPITRE 1 - COURS

Géométrie des ensembles algébriques

On fixe un corps de base *infini* k.

1.1. Zéros de polynômes dans l'espace affine

1.1.1. Définitions. Lorsque l'espace vectoriel k^n est considéré comme espace affine, on le note $\mathbb{A}^n(k)$, ou plus simplement $\mathbb{A}^n$, et on dit que c'est *l'espace affine de dimension n sur k*. On dit que $\mathbb{A}^1$ est *la droite affine sur k* et que $\mathbb{A}^2$ est *le plan affine sur k*. Si S est une partie de $k[X_1, \ldots, X_n]$, le *lieu des zéros de S* est $V(S) := \{P \in \mathbb{A}^n, \forall\ F \in S, F(P) = 0\}$. On écrira $V(F_1, \ldots, F_r) := V(\{F_1, \ldots, F_r\})$.

1.1.2. Proposition. (i) On a $V(1) = \emptyset$ et $V(0) = \mathbb{A}^n$.

(ii) Si $\{S_\alpha\}_{\alpha \in A}$ est un ensemble de parties de $k[X_1, \ldots, X_n]$, on a $V(\bigcup_\alpha S_\alpha) = \bigcap_\alpha V(S_\alpha))$,

(iii) Si $S, T \subset k[X_1, \ldots, X_n]$, alors $V(S) \cup V(T) = V(FG, F \in S, G \in T)$ et

(iv) Si $S \subset T \subset k[X_1, \ldots, X_n]$, alors $V(T) \subset V(S)$

Démonstration : i) Puisque le polynôme constant 1 ne s'annule jamais, on a $V(1) = \emptyset$. De même, puisque le polynôme constant 0 est identiquement nul, $V(0) = \mathbb{A}^n$. ii) On a

$P \in V(\bigcup_\alpha S_\alpha)$ ssi $\forall\ F \in \bigcup_\alpha S_\alpha, F(P) = 0$

$P \in V(\bigcup_\alpha S_\alpha)$ ssi $\forall\ \alpha \in A, \forall\ F \in S_\alpha, F(P) = 0$

$P \in V(\bigcup_\alpha S_\alpha)$ ssi $\forall\ \alpha \in A, F \in V(S_\alpha))$

$P \in V(\bigcup_\alpha S_\alpha)$ ssi $F \in \bigcap_\alpha V(S_\alpha)$.

iii) On a

$P \in V(S) \cup V(T)$ ssi $P \in V(S)$ ou $P \in V(T)$

$P \in V(S) \cup V(T)$ ssi $\forall\ F \in S, F(P) = 0$ ou $\forall\ G \in T, G(P) = 0$

$P \in V(S) \cup V(T)$ ssi $\forall\, F \in S, \forall G \in T, F(P) = 0$ ou $G(P) = 0$

$P \in V(S) \cup V(T)$ ssi $\forall\, F \in S, \forall G \in T\ (FG)(P) = 0$

$P \in V(S) \cup V(T)$ ssi $P \in V(FG, F \in S, \forall G \in T)$.

iv) Enfin, si $S \subset T$ et si $P \in V(T)$, alors pour tout $F \in S$, on a $F \in T$ et donc $F(P) = 0$ si bien que $P \in V(S)$.

1.1.3. Proposition. Si F et $G \in k[X, Y]$ n'ont pas de facteurs communs, alors $V(F, G)$ est fini.

Démonstration : On note $V = V(F, G)$ et on applique le théorème de Bézout à F et G dans $k(X)[Y]$ qui est un anneau principal : Puisque F et G n'ont pas de facteur commun dans $k[X, Y]$, ils n'en ont pas non plus dans $k(X)[Y]$. Ils sont donc premiers entre eux dans cet anneau. Il existe donc A et $B \in k(X)[Y]$ tels que $AF + BG = 1$. On peut trouver R non nul $\in k[X]$ tel que $A = A_0/R$ et $B = B_0/R$ avec A_0 et $B_0 \in k[X, Y]$. On a donc $A_0F + B_0G = R$ si bien que si $P = (a, b) \in V$, alors $F(P) = G(P) = 0$ et donc $R(a) = 0$. On voit ainsi que $V \subset V(R) \times \mathbb{A}^1$ où $V(R) \subset \mathbb{A}^1$ est un ensemble *fini* puisque R n'a qu'un nombre fini de racines. De même, on a $V \subset \mathbb{A}^1 \times V(S)$ avec $V(S)$ fini et donc $V \subset V(R) \times V(S)$ qui est fini.

1.2. Ensembles algébriques affines

1.2.1. Définitions. Une partie V de $\mathbb{A}^n$ est un *ensemble algébrique affine* s'il existe $S \subset k[X_1, \ldots, X_n]$ tel que $V = V(S)$. On dit alors que les "$F = 0$" avec $F \in S$ forment un système d'*équations* pour V. La partie V est une *hypersurface* de *degré* d s'il existe $F \in k[X_1, \ldots, X_n]$ *non constant* de degré d tel que $V = V(F)$. Une hypersurface du plan affine est une *courbe affine plane*. On dit *conique, cubique, quartique,* . . . si $d = 2, 3, 4, \ldots$

• $\mathbb{A}^n$ et $\emptyset$ sont des ensembles algébriques : Nous avons vu que $\mathbb{A}^n = V(0)$ et que $\emptyset = V(1)$.

• Toute intersection et toute union finie d'algébriques est algébrique : C'est aussi une conséquence immédiate de la proposition 1.1.2.

• Tout ensemble fini est algébrique : Grâce à la remarque précédente, il suffit de montrer que tout point est algébrique. Or si $P := (a_1, \ldots, a_n) \in \mathbb{A}^n$, on a $\{P\} = V(X_1 - a_1, \ldots, X_n - a_n)$.

• Tout sous-ensemble algébrique propre est une intersection d'hypersurfaces : En effet, on a $V = V(S) = V(\bigcup_{F\in S} \{F\}) = \bigcap_{F\in S} V(F) =$ **Erreur!** $V(F)$. Puisque V est non vide aucun des $F \in S\backslash 0$ n'est constant et les $V(F)$ sont donc bien des hypersurfaces.

• Les sous-ensembles algébriques propres de la droite affine sont les ensembles finis : Il suffit de montrer que, dans $\mathbb{A}^1$, toute hypersurface est finie. Or on sait que tout polynôme non nul en une variable sur un corps a un nombre fini de zéros.

1.2.2. Proposition. Si V et W sont des sous-ensembles algébriques de $\mathbb{A}^n$ et $\mathbb{A}^m$, respectivement, alors $V \times W$ est un sous-ensemble algébrique de $\mathbb{A}^{n+m}$.

Démonstration : Tout $F \in k[X_1, \ldots, X_n]$ peut être considéré comme élément de $k[X_1, \ldots, X_{n+m}]$ et on a alors pour $P \in \mathbb{A}^n$ et $Q \in \mathbb{A}^m$, $F(P, Q) = F(P)$. Si $G \in k[X_1, \ldots, X_m]$, on note $G_{n+} = G(X_{n+1}, \ldots, X_{n+m}) \in k[X_1, \ldots, X_{n+m}]$ si bien que si $P \in \mathbb{A}^n$ et $Q \in \mathbb{A}^m$, alors $G_{n+}(P, Q) = G(Q)$. Écrivons $V = V(S)$, $W = V(T)$ et notons $T_{n+} = \{G_{n+}, G \in T\}$. On a

$(P, Q) \in V \times W$ ssi $P \in V$ et $Q \in W$

$(P, Q) \in V \times W$ ssi $\forall\, F \in S, F(P) = 0$ et $\forall\, G \in T, G(Q) = 0$

$(P, Q) \in V \times W$ ssi $\forall\, F \in S, F(P, Q) = 0$ et $\forall\, G \in T, G_{n+}(P, Q) = 0$

$(P, Q) \in V \times W$ ssi $(P, Q) \in V(S)$ et $(P, Q) \in V(T_{n+})$

$(P, Q) \in V \times W$ ssi $(P, Q) \in V(S \cup T_{n+})$.

Cela montre bien que $V \times W$ est algébrique.

1.2.3. Définition. Une *variété linéaire* est un sous-espace affine de $\mathbb{A}^n$.

• Un hyperplan de $\mathbb{A}^n$ est une hypersurface définie par un polynôme de degré 1 : Par définition, une partie V de $\mathbb{A}^n$ est un hyperplan si et seulement si il existe un point $P \in V$ et une forme linéaire non nulle $\varphi : k^n \longrightarrow k$ telle que $V = \{Q \in \mathbb{A}^n, \varphi(\vec{PQ}) = 0\}$. Si on note $P =: (a_1, \ldots, a_n)$ et $\varphi(x_1, \ldots, x_n) =: \alpha_1 x_1 + \ldots + \alpha_n x_n$, on voit donc que $Q := (b_1, \ldots, b_n) \in V$ si et seulement si $\alpha_1(b_1 - a_1) + \ldots + \alpha_n(b_n - a_n) = 0$, c'est à dire, si et seulement si Q est sur l'hypersurface d'équation $\alpha_1(X_1 - a_1) + \ldots + \alpha_n(X_n - a_n) = 0$. Puisque tout polynôme de degré 1 se met sous cette forme, on voit qu'il y a bien identité entre hyperplans et hypersurfaces définies par des polynômes de degré 1.

• Une variété linéaire est un ensemble algébrique défini par des polynômes de degré 1 : Puisqu'une variété linéaire est une intersection d'hyperplans, c'est une conséquence immédiate de la première assertion.

1.2.4. Proposition. (i) Si V est un ensemble algébrique affine et L une droite non contenue dans V, alors $L \cap V$ est fini.

(ii) Si V et W sont des ensembles algébriques affines et L une droite contenue dans $V \cup W$ alors $L \subset V$ ou $L \subset W$.

(iii) Si $C = V(F)$ est une courbe plane avec F *irréductible* et V un sous-ensemble algébrique du plan ne contenant pas C, alors $C \cap V$ est fini.

Démonstration : i) On peut bien sur supposer que V est une hypersurface d'équation $F = 0$ et on peut écrire L sous forme paramétrique $L = \{(a_1 + t\alpha_1, \ldots, a_n + t\alpha_n), t \in k\}$. Si on note $\Phi : \mathbb{A}^1 \longrightarrow \mathbb{A}^n$, $t \longmapsto (a_1 + t\alpha_1, \ldots, a_n + t\alpha_n)$ et $G = F(a_1 + T\alpha_1, \ldots, a_n + T\alpha_n) \in k[T]$, on a $L \cap V = \{\Phi(t), G(t) = 0, t \in k\} = \Phi(V(G))$. Puisque L n'est pas contenu dans V, G n'est pas identiquement nul et $V(G)$ est donc fini. Il suit que $L \cap V$ est aussi fini. ii) Puisqu'une droite sur un corps infini est infinie, les hypothèses impliquent que $L \cap V$ ou $L \cap W$ est infini et donc, grâce au résultat précédent, que $L \subset V$ ou $L \subset W$. iii) On peut bien sûr supposer que V est une courbe plane d'équation $G = 0$. Puisque C n'est pas contenue dans V, G n'est pas un multiple de F. Puisque F est irréductible, cela signifie que F et G n'ont pas de facteur commun et il suit que $C \cap V = V(F, G)$ est fini.

1.3. Zéros de polynômes dans l'espace projectif

1.3.1. Définitions. On dit que $\mathbb{P}^n(k)$ ou $\mathbb{P}^n := \mathbb{P}(k^{n+1})$ est *l'espace projectif de dimension n sur k*, que $\mathbb{P}^1$ est *la droite projective sur k* et que $\mathbb{P}^2$ est *le plan projectif sur k*. Si $(a_1, \ldots, a_{n+1})$ est un vecteur directeur de P, on écrit $P =: (a_1; \ldots; a_{n+1})$ et on dit que $(a_1; \ldots; a_{n+1})$ est un *système de coordonnées homogènes pour P*. On dit que P est un *zéro* de $F \in k[X_1, \ldots, X_{n+1}]$ si $F(P) = 0$.

• Le point $P = (a_1; \ldots; a_{n+1})$ est un zéro de F si et seulement si $F(\lambda a_1, \ldots, \lambda a_{n+1}) = 0$ pour tout $\lambda \in k$: Clair.

• On a $F(P) = 0$ si et seulement si $P \subset V(F)$: Clair.

• Si $F = F_d + F_{d-1} + \ldots + F_0$ est la décomposition de F non nul $\in k[X_1, \ldots, X_{n+1}]$ en somme de ses composantes homogènes, et si $P = (a_1; \ldots; a_{n+1})$, alors $F(P) = 0$ si et seulement si $F_0(a_1, \ldots, a_{n+1}) = F_1(a_1, \ldots, a_{n+1}) = \ldots = F_d(a_1, \ldots, a_{n+1}) = 0$: Puisque k est infini, on a

$F(P) = 0$ ssi $\forall\ \lambda \in k, F(\lambda a_1, \ldots, \lambda a_{n+1}) = 0$

$F(P) = 0$ ssi $\forall\ \lambda \in k, \lambda^d F_d(a_1, \ldots, a_{n+1}) + \lambda^{d-1} F_{d-1}(a_1, \ldots, a_{n+1})$
$+ \ldots + F_0(a_1, \ldots, a_{n+1}) = 0$

$F(P) = 0$ ssi $F_0(a_1, \ldots, a_{n+1}) = F_1(a_1, \ldots, a_{n+1})$
$= \ldots = F_d(a_1, \ldots, a_{n+1}) = 0.$

1.3.2. Définition. Si $S \subset k[X_1, \ldots, X_{n+1}]$, on dit que $V_p(S) = \{P \in \mathbb{P}^n,\ \forall\ F \in S, F(P) = 0\}$ est le *lieu des zéros* de S dans $\mathbb{P}^n$.

• Si $S \subset k[X_1, \ldots, X_{n+1}]$, on a $P \in V_p(S)$ ssi $P \subset V(S)$: En effet, on a

$P \in V_p(S)$ ssi $\forall\ F \in S, F(P) = 0$

$P \in V_p(S)$ ssi $\forall\ F \in S, P \subset V(F)$

$P \in V_p(S)$ ssi $P \subset \underset{F \in S}{\cap} V(F) = V(S)$.

• Si S_p est l'ensemble des composantes homogènes des $F \in S$, alors $V_p(S) = V_p(S_p)$: Clair.

1.3.3. Proposition. On a $V_p(1) = \emptyset$, $V_p(0) = \mathbb{P}^n$, $V_p(\underset{\alpha}{\cup} S_\alpha) = \underset{\alpha}{\cap} V_p(S_\alpha)$, $V_p(S) \cup V_p(T) = V_p(FG, F \in S, G \in T)$ et $V_p(T) \subset V_p(S)$ si $S \subset T$.

Démonstration : On a

$P \in V_p(1)$ ssi $P \subset V(1) = \emptyset$

et

$P \in V_p(0)$ ssi $P \subset V(0) = \mathbb{A}^{n+1}$.

On a

$P \in V_p(\underset{\alpha}{\cup} S_\alpha)$ ssi $P \subset V(\underset{\alpha}{\cup} S_\alpha)$

$P \in V_p(\underset{\alpha}{\cup} S_\alpha)$ ssi $P \subset \cap V(S_\alpha)$

$P \in V_p(\underset{\alpha}{\cup} S_\alpha)$ ssi $\forall \alpha \in A, P \in V(S_\alpha))$

$P \in V_p(\underset{\alpha}{\cup} S_\alpha)$ ssi $\forall \alpha \in A, P \in V_p(S_\alpha))$

$P \in V_p(\underset{\alpha}{\cup} S_\alpha)$ ssi $P \in \underset{\alpha}{\cap} V_p(S_\alpha)$.

On a

$P \in V_p(S) \cup V_p(T)$ ssi $P \in V_p(S)$ ou $P \in V_p(T)$

$P \in V_p(S) \cup V_p(T)$ ssi $P \subset V(S)$ ou $P \subset V(T)$

$P \in V_p(S) \cup V_p(T)$ ssi $P \subset V(S) \cup V(T)$ par 1.2.4

$P \in V_p(S) \cup V_p(T)$ ssi $P \subset V(FG, F \in S, G \in T)$
$P \in V_p(S) \cup V_p(T)$ ssi $P \in V_p(FG, F \in S, G \in T)$.
Enfin, si $S \subset T$ alors $V(T) \subset V(S)$ et donc $V_p(T) \subset V_p(S)$.

1.3.4. La notion de lieu des zéros se comporte bien par rapport aux cônes :

• On a toujours $C(V_p(S)) \subset V(S) \cup \{O\}$: Si $(a_1, \ldots, a_{n+1}) \neq O$, on a
$(a_1, \ldots, a_{n+1}) \in C(V_p(S))$ ssi $(a_1; \ldots; a_{n+1}) \in V_p(S)$
$(a_1, \ldots, a_{n+1}) \in C(V_p(S))$ ssi $\forall F \in S, F(a_1; \ldots; a_{n+1}) = 0$
$(a_1, \ldots, a_{n+1}) \in C(V_p(S)) \Rightarrow \forall F \in S, F(a_1, \ldots, a_{n+1}) = 0$
$(a_1, \ldots, a_{n+1}) \in C(V_p(S))$ ssi $(a_1, \ldots, a_{n+1}) \in V(S)$.

• Supposons les éléments de S homogènes. Alors $C(V_p(S)) = V(S)$ si $V_p(S) \neq \emptyset$ et on a $V_p(S) = \emptyset$ si et seulement si $V(S) \subset \{O\}$: en remarquant que si F est homogène, alors
$F(a_1, \ldots, a_n) = 0$ ssi $F(a_1; \ldots; a_n) = 0$,
le même argument que ci dessus nous fournit $C(V_p(S)) = V(S) \cup \{O\}$. Il suffit alors de remarquer que si $P \in V_p(S)$, alors $O \in P \subset V(S)$ et que $V_p(S) = \emptyset$ si et seulement si $C(V_p(S)) = \{O\}$.

• Si $C(A) = V(S)$, alors $A = V_p(S)$: On a
$P \in A$ ssi $P \subset C(A) = V(S)$ ssi $P \in V_p(S)$.

1.3.5. Proposition. L'application $\mathbb{P}^{n-1} \longrightarrow \mathbb{P}^n$, $(a_1, \ldots, a_n) \longmapsto (a_1; \ldots; a_n; 0)$ est une bijection de $\mathbb{P}^{n-1}$ sur un hyperplan de $\mathbb{P}^n$ et l'application $\mathbb{A}^n \longrightarrow \mathbb{P}^n$, $(a_1, \ldots, a_n) \longmapsto (a_1; \ldots; a_n; 1)$ est une bijection de $\mathbb{A}^n$ sur le complémentaire de cet hyperplan.

Démonstration : La première assertion résulte du fait que l'image d'une homographie de $\mathbb{P}^{n-1}$ dans $\mathbb{P}^n$ est toujours un hyperplan H. Soit U le complémentaire de H dans $\mathbb{P}^n$. On définit la bijection réciproque $U \longrightarrow \mathbb{A}^n$ en envoyant $(a_1; \ldots; a_{n+1})$ sur $(a_1/a_{n+1}, \ldots, a_n/a_{n+1})$. Cette application est bien définie car si $(a_1; \ldots; a_{n+1}) \in U$ alors $a_{n+1} \neq 0$ et si $\lambda \in k$, alors $(\lambda a_1/\lambda a_{n+1}, \ldots, \lambda a_n/\lambda a_{n+1}) = (a_1/a_{n+1}, \ldots, a_n/a_{n+1})$. De plus, on a toujours $(a_1, \ldots, a_n) = (a_1/1, \ldots, a_n/1)$ et si $a_{n+1} \neq 0$, $(a_1/a_{n+1}; \ldots; a_n/a_{n+1}, 1) = (a_1; \ldots; a_{n+1})$.

On identifiera dorénavant $\mathbb{P}^{n-1}$ et $\mathbb{A}^n$ avec leurs images dans $\mathbb{P}^n$.

1.3.6. Définition. Si $A \subset \mathbb{P}^n$, on dit que $A_* := A \cap \mathbb{A}^n$ est la *partie affine* de A et que son complémentaire dans A est le *lieu à l'infini* de A.

• Si $F \in k[X_1, \ldots, X_{n+1}]$ est *homogène* et $P \in \mathbb{A}^n \subset \mathbb{P}^n$, on a $F(P) = 0$ (dans $\mathbb{P}^n$) si et seulement si $F_*(P) = 0$ (dans $\mathbb{A}^n$) : Si $P = (a_1, \ldots, a_n)$, on a

$F(P) = 0$ ssi $F(a_1; \ldots; a_n; 1) = 0$

$F(P) = 0$ ssi $F(a_1, \ldots, a_n, 1) = 0$ (car F est homogène)

$F(P) = 0$ ssi $F_*(a_1, \ldots, a_n) = 0$

$F(P) = 0$ ssi $F_*(P) = 0$.

1.3.7. Proposition. i) Si S est une partie de $k[X_1, \ldots, X_{n+1}]$, alors $V_p(S)_* = V(S_*)$.
ii) Si $F \in k[X_1, \ldots, X_n]$, on a $V(F) = V(F^*)_*$.

Démonstration : i) Si $P \in \mathbb{A}^n$, on a

$P \in V(S_*)$ ssi $\forall F \in S_p, F_*(P) = 0$

$P \in V(S_*)$ ssi $\forall F \in S_p, F(P) = 0$

$P \in V(S_*)$ ssi $P \in V_p(S_p) = V_p(S)$

$P \in V(S_*)$ ssi $P \in V_p(S)_*$.

ii) En effet, $V(F) = V((F^*)_*) = V(F^*)_*$.

1.4. Ensembles algébriques projectifs

1.4.1. Définition. Une partie V de $\mathbb{P}^n$ est un *ensemble algébrique projectif* s'il existe $S \subset k[X_1, \ldots, X_{n+1}]$ tel que $V = V_p(S)$. C'est une *hypersurface* de *degré* d s'il existe $F \in k[X_1, \ldots, X_{n+1}]$ *homogène* non constant de degré d tel que $V = V_p(F)$. Une hypersurface du plan projectif est une *courbe projective plane*. On dit *conique, cubique, quartique,* . . . si $d = 2, 3, 4, \ldots$

• Un sous-ensemble V de $\mathbb{P}^n$ est algébrique si et seulement si $C(V)$ est un ensemble algébrique affine : Nous avons vu que $C(V_p(S)) = V(S_p)$ si $V_p(S) \neq \emptyset$ et on sait que $C(\emptyset) = \{O\}$. Réciproquement, on a $V = V_p(S)$ si $C(V) = V(S)$.

• Un ensemble algébrique projectif non vide est une intersection d'hypersurfaces : En effet, on peut écrire $V = V_p(S)$ où S est composé de polynômes homogènes, et on a donc $V = V_p(\bigcup_{F \in S} \{F\}) = \bigcap_{F \in S} V_p(F)$.

1.4.2. Définition. Une *variété linéaire projective* est un sous-espace projectif de $\mathbb{P}^n$.

• Un hyperplan de $\mathbb{P}^n$ est une hypersurface définie par une *forme linéaire* (un polynôme homogène de degré 1) : En effet, V est un hyperplan si et seulement si $C(V) = V(F)$ avec F de degré 1. Puisque l'origine appartient à $C(V)$, le polynôme F est nécessairement homogène et on sait alors que $C(V) = V(F)$ si et seulement si $V = V_p(F)$.

• Une variété linéaire projective non vide est un ensemble algébrique défini par des polynômes homogènes de degré 1 : On sait qu'un sous-espace projectif non vide est une intersection d'hyperplans.

1.4.3. Proposition. Si $V \subset \mathbb{P}^n$ est une hypersurface distincte de $\mathbb{P}^{n-1}$ (resp. un ensemble algébrique, resp. un hyperplan distinct de $\mathbb{P}^{n-1}$, resp. une variété linéaire), alors V_* est une hypersurface (resp. un ensemble algébrique, resp. un hyperplan, resp. une variété linéaire). De plus, toute hypersurface (resp. ensemble algébrique, resp. hyperplan, resp. toute sous-variété linéaire de $\mathbb{A}^n$) est la partie affine d'une hypersurface, d'un ensemble algébrique, d'un hyperplan, respectivement d'une sous-variété linéaire) de $\mathbb{P}^n$.

Démonstration : On a vu que si S est une partie de $k[X_1, \ldots, X_{n+1}]$, alors $V_p(S)_* = V(S_*)$. De plus, si F est un polynôme homogène non constant tel que $F_* = c \in k$, alors $F = X_{n+1}^m (F_*)^* = cX_{n+1}^m$ et $V(F) = \mathbb{P}^{n-1}$. Aussi, si F est une forme linéaire et $V(F) \neq \mathbb{P}^{n-1}$, alors F_* est nécessairement de degré 1. Enfin, si S est une partie de $k[X_1, \ldots, X_n]$, on peut écrire $V(S) = \cap V(F) = [\cap V(F^*)]_*$.

1.4.4. Les sous-ensembles algébriques propres de $\mathbb{P}^1$ sont les ensembles finis : Remarquons que $C(\mathbb{A}^1) = \mathbb{A}^2 \backslash (OX) \cup \{O\}$ n'est pas algébrique car son intersection avec la droite d'équation $X = 1$ n'est pas finie. Il suit que $\mathbb{A}^1$ n'est pas un sous-ensemble algébrique de $\mathbb{P}^1$. Si V est un sous-ensemble algébrique infini de $\mathbb{P}^1$, alors V_* est un sous-ensemble algébrique infini de $\mathbb{A}^1$ et on a donc $V_* = \mathbb{A}^1$ si bien que $\mathbb{A}^1 \subset V$. Puisque $\mathbb{A}^1 \neq V$, on a $V = \mathbb{P}^1$.

1.5. Fonctions polynomiales, changement de coordonnées

1.5.1. Définitions. Si V est un sous-ensemble algébrique de $\mathbb{A}^n$, une fonction $f : V \longrightarrow k$ est *polynomiale* s'il existe $F \in k[X_1, \ldots, X_n]$, telle que pour tout $P \in V$, on ait $f(P) = F(P)$. Leur ensemble se note $k[V]$. Soient $W \subset \mathbb{A}^m$ un autre ensemble algébrique et $\varphi : W \longrightarrow V, P \longmapsto (f_1(P), \ldots, f_n(P))$ une application

quelconque. On dit que les fonctions $f_1, \ldots, f_n : W \longrightarrow k$ sont les *composantes* de φ, et on considérera aussi parfois φ comme un vecteur ligne $[f_1, \ldots, f_n]$. On dit que φ est une *application polynomiale* si ses composantes sont des fonctions polynomiales. L'ensemble des applications polynomiales de W dans V se note $Hom(W, V)$.

• Si V est un sous-ensemble algébrique de $\mathbb{A}^n$, les *fonctions coordonnées* $x_i : V \longrightarrow k$, $P =: (a_1, \ldots, a_n) \longmapsto a_i$, pour $i = 1, \ldots, n$ sont des fonctions polynomiales : Ces fonctions sont induites par les polynômes X_i.

• La projection $V \times W \longrightarrow V$ est une application polynomiale : Si $V \subset \mathbb{A}^n$, les composantes de la projection sont les fonctions coordonnées $x_1, \ldots, x_n$ sur $V \times W$.

• Si $V \subset \mathbb{A}^n$ et $W \subset \mathbb{A}^m$ sont deux sous-ensembles algébriques, une application $\varphi : W \longrightarrow V$ est polynomiale si et seulement si elle se prolonge en une application polynomiale $\Phi : \mathbb{A}^m \longrightarrow \mathbb{A}^n$: En effet, une application polynomiale de W dans V est une application dont les composantes se prolongent en des fonctions polynomiales sur $\mathbb{A}^m$.

• Si $\varphi : W \longrightarrow V$ est une application polynomiale et V' (resp. W') est un sous-ensemble algébrique de V (resp. W) tel que $\varphi(W') \subset V'$, alors l'application induite $\varphi' : W' \longrightarrow V'$ est une application polynomiale : C'est une conséquence immédiate de la remarque précédente.

1.5.2. Proposition. La composée de deux applications polynomiales est une application polynomiale.

Démonstration : On se donne donc $\psi : Z \longrightarrow W$ et $\varphi : W \longrightarrow V$ polynomiales et on veut montrer que $\varphi \circ \psi$ est polynomiale. Si φ et ψ se prolongent respectivement en $\Psi : \mathbb{A}^r \longrightarrow \mathbb{A}^m$ et $\Phi : \mathbb{A}^m \longrightarrow \mathbb{A}^n$, polynomiales, alors $\psi \circ \varphi$ se prolonge en $\Phi \circ \Psi$. Il suffit donc de montrer que $\Phi \circ \Psi$ est polynomiales lorsque Φ et Ψ le sont. Puisque cette condition se vérifie sur les composantes, il suffit de montre que si $\Psi : \mathbb{A}^r \longrightarrow \mathbb{A}^m$ est polynomiale, disons $\Psi = [G_1, \ldots, G_m]$, et si $F \in k[X_1, \ldots, X_m]$, alors $F \circ \Psi$ est polynomiale. Il suffit alors de remarquer que si $P \in \mathbb{A}^r$, on a $F((\Psi(P)) = F(G_1(P), \ldots, G_m(P)) = F(G_1, \ldots, G_m)(P)$.

• L'image réciproque d'une hypersurface par une application polynomiale $\Phi : \mathbb{A}^m \longrightarrow \mathbb{A}^n$ est soit vide, soit $\mathbb{A}^m$, soit une hypersurface : Nous venons de voir que si $F \in k[X_1, \ldots, X_m]$, alors $F \circ \Phi =: G \in k[X_1, \ldots, X_n]$. Il suit que si $V = V(F)$, alors $\Phi^{-1}(V) = V(G)$.

• L'image réciproque d'un ensemble algébrique affine par une application polynomiale est algébrique : C'est une conséquence du résultat précédent car l'image réciproque commute aux intersections.

1.5.3. Définitions. Une application polynomiale est un *isomorphisme* si elle est bijective et si sa réciproque est une application polynomiale. Deux ensembles algébriques sont *isomorphes* s'il existe un isomorphisme de l'un sur l'autre. Une application polynomiale $\varphi : W \longrightarrow V$ est une *immersion fermée* si φ induit un isomorphisme de W sur un sous-ensemble algébrique de V.

• Si $\varphi : W \longrightarrow V$ est un isomorphisme, V' un sous-ensemble algébrique de V et $W' := \varphi^{-1}(V')$, alors l'application induite $W' \longrightarrow V'$ est aussi un isomorphisme : C'est une application polynomiale bijective et sa réciproque qui est induite par la réciproque de φ est aussi polynomiale.

1.5.4. Proposition. Soient V et W des ensembles algébriques affines, $\Gamma \subset V \times W$ et $\pi : \Gamma \longrightarrow W$ la composée de l'inclusion $\Gamma \hookrightarrow V \times W$ et de la projection $V \times W \longrightarrow V$. Alors les conditions suivantes sont équivalentes :

(i) Γ est le graphe d'une application polynomiale de V vers W

(ii) π est un isomorphisme d'ensembles algébriques.

Démonstration : On sait que Γ est le graphe d'une application $\varphi : V \longrightarrow W$ si et seulement si π est bijective et qu'alors φ est l'application composée de $\pi^{-1} : V \longrightarrow \Gamma$, de l'inclusion $\Gamma \hookrightarrow V \times W$ et de la projection $V \times W \longrightarrow W$. En particulier, si π est un isomorphisme d'ensembles algébriques, alors φ est polynomiale comme composée d'applications polynomiales. Réciproquement, si φ est polynomiale, ses composantes sont induites par des polynômes $F_1, \ldots, F_m$ et on a donc $\Gamma = (V \times W) \cap Z$ où $Z = V(X_{n+1} - F_1, \ldots, X_{n+m} - F_m)$, ce qui montre que Γ est algébrique. De plus, π^{-1} est induit par $(X_1, \ldots, X_n, F_1, \ldots, F_m)$ et π est donc bien un isomorphisme.

1.5.5. Définitions. Un *changement de coordonnées affines* est une application affine bijective de $\mathbb{A}^n$ sur lui même.

• Soient $V \subset \mathbb{A}^n$ et $W \subset \mathbb{A}^m$ des sous-variétés linéaires. Une application $\varphi : W \longrightarrow V$ est affine si et seulement si c'est une application polynomiale induite par des polynômes de degré au plus 1 : Puisque toute application affine $\varphi : W \longrightarrow V$ se prolonge en une application affine $\mathbb{A}^m \longrightarrow \mathbb{A}^n$, on peut supposer que $V = \mathbb{A}^n$ et $W = \mathbb{A}^m$. Une application $\Phi : \mathbb{A}^m \longrightarrow \mathbb{A}^n$ est affine si et seulement si il existe $\vec{\Phi} : k^m \longrightarrow k^n$ linéaire telle que $\Phi(P) = \Phi(O) + \vec{\Phi}(\vec{OP})$. C'est à dire si et seulement si il existe des α_{ij} et des a_i tels que $\Phi(b_1, \ldots, b_m) = (\sum \alpha_{1j} b_j + a_1, \ldots, \sum \alpha_{nj} b_j + a_n)$. Autrement dit, Φ est affine si et seulement ses composantes sont des polynômes $\sum \alpha_{1j} X_j + a_1$ de degrés au plus 1.

• Toute application affine bijective entre variétés linéaires est un isomorphisme : Nous savons qu'une application affine est polynomiale, que la réciproque d'une application affine bijective est affine et qu'une application induite par une application polynomiale est polynomiale.

• Toute sous-variété linéaire de dimension d de $\mathbb{A}^n$ est isomorphe à $\mathbb{A}^d$: Nous savons que si deux espaces affines ont même dimension (finie), il existe une application linéaire bijective de l'un sur l'autre.

1.5.6. Définition. Un *changement de coordonnées projectives* est une homographie de $\mathbb{P}^n$ sur lui même. On dit que deux sous-ensembles algébriques de $\mathbb{P}^n$ sont *projectivement équivalents* s'il existe un changement de coordonnées projectives qui les échange.

• Si Φ est une homographie et V un ensemble algébrique projectif, alors $\Phi^{-1}(V)$ est algébrique : En effet, on a $C(\Phi^{-1}(V)) = \Phi^{-1}(C(V))$.

1.6. Topologie de Zariski sur un ensemble algébrique

1.6.1. Définition. La *topologie de Zariski* sur un ensemble algébrique (affine ou projectif) V est la topologie pour laquelle les fermés sont les sous-ensembles algébriques de V. Si $F \in k[X_1, \ldots, X_n]$, on dit que $D(F) = \mathbb{A}^n \setminus V(F)$ est un *ouvert principal* de $\mathbb{A}^n$. Enfin, la *fermeture algébrique* d'une partie A de V est l'adhérence de A dans V.

• Si W est un sous-ensemble algébrique de V, la topologie de Zariski sur W est induite par la topologie de Zariski sur V : Si Z est fermé dans V, alors $Z \cap W$ est fermé dans W. Si Z est fermé dans W alors Z est fermé dans V et on a $Z = Z \cap W$.

• Si $F \neq 0 \in k[X_1, \ldots, X_n]$, alors $D(F)$ est un ouvert non vide de $\mathbb{A}^n$: En effet, puisque k est infini, $V(F) \neq \mathbb{A}^n$.

• La topologie de Zariski sur $\mathbb{A}^n$ est la topologie induite par la topologie de Zariski sur $\mathbb{P}^n$: Nous avons vu que la partie affine d'un ensemble algébrique projectif est algébrique et que tout ensemble algébrique affine est la partie affine d'un ensemble algébrique projectif.

• Une application polynomiale entre ensembles algébriques affines est continue : Nous avons vu que l'image réciproque d'un ensemble algébrique par une application polynomiale est algébrique.

• Une homographie est continue : On a vu que l'image réciproque d'un ensemble algébrique est algébrique.

• Les fermés propres d'une droite ou d'une courbe affine plane de la forme $V(F)$ avec F irréductible, sont les ensembles finis. En particulier, toute partie infinie est dense : Le cas affine a déjà été traité et une droite projective est homéomorphe à $\mathbb{P}^1$ par une homographie.

• Si V et W sont deux ensembles algébriques affines infini, la topologie de Zariski sur $V \times W$ est strictement plus fine que la topologie produit des topologies de Zariski sur V et sur W! En particulier, une application $Z \longrightarrow V \times W$ dont les composantes sont continues n'est pas nécessairement continue!

1.6.2. Définition. Si V est un sous-ensemble algébrique de $\mathbb{A}^n$, on dit que la fermeture algébrique V^* de V dans $\mathbb{P}^n$ est *la fermeture projective* de V. On dit que le lieu à l'infini de V^* est le *lieu à l'infini* de V. Si P est un point à l'infini de $V \subset \mathbb{A}^2$, on peut voir P comme un point de $\mathbb{P}^1$ et donc comme une droite de k^2. C' est ce que l'on appelle une *direction asymptotique* pour V.

• Si V est un ensemble algébrique affine, alors $V \subset (V^*)_*$: On a $V = V \cap \mathbb{A}^n \subset V^* \cap \mathbb{A}^n \subset (V^*)_*$.

• Si V est un ensemble algébrique projectif, alors $(V_*)^* \subset V$: On a $V_* = V \cap \mathbb{A}^n \subset V$ et donc $(V_*)^* \subset V$ car V est fermé dans $\mathbb{P}^n$.

1.6.3. Proposition. Si V et W sont des ensembles algébriques affines, la projection $p : V \times W \longrightarrow V$ est une application ouverte.

Démonstration : On a $V \subset \mathbb{A}^n$ et $W \subset \mathbb{A}^m$ et donc $V \times W \subset \mathbb{A}^{n+m}$. Si $Q = (b_1, \ldots, b_m) \in \mathbb{A}^m$ et $F \in k[X_1, \ldots, X_{n+m}]$, on pose

$$F_Q := F(X_1, \ldots, X_n, b_1, \ldots, b_m) \in k[X_1, \ldots, X_n].$$

Soit $U \subset V \times W$ un ouvert. Si Z est le complémentaire de U dans $V \times W$, on peut écrire $Z := V(S)$ avec $S \subset k[X_1, \ldots, X_{n+m}]$. Nous allons montrer que le complémentaire de $p(U)$ dans V est un sous-ensemble algébrique de V. Soit $P \in V$. On a

$P \notin p(U)$ ssi $\forall\, Q \in W, (P, Q) \notin U$

$P \notin p(U)$ ssi $\forall\, Q \in W, (P, Q) \in Z$

$P \notin p(U)$ ssi $\forall\, Q \in W, \forall\, F \in S,\ F(P, Q) = F_Q(P) = 0$.

On voit donc que le complémentaire de $p(U)$ dans V est l'ensemble algébrique $V \cap V(T)$ avec $T = \{F_Q, Q \in W, F \in S\} \subset k[X_1, \ldots, X_n]$.

Corollaire. Si $n > 0$, alors tout ouvert non vide de $\mathbb{A}^n$ est infini.

En utilisant la projection $p : \mathbb{A}^n \longrightarrow \mathbb{A}^1$ on se ramène au cas $n = 1$. Puisque k est infini, il suffit alors de rappeler que tout fermé propre de $\mathbb{A}^1$ est fini.

1.6.4. Théorème. *(k algébriquement clos)* Soit H une hypersurface de $\mathbb{A}^n$ ou de $\mathbb{P}^n$. Alors, $H \neq \emptyset$ si $n \geq 1$ et est infinie si $n \geq 2$.

Démonstration : On démontre d'abord le résultat suivant :

• Soit H une hypersurface de $\mathbb{A}^n$. S'il n'existe pas d'hypersurface H' de $\mathbb{A}^{n-1}$ telle que $H = H' \times (OX_n)$ et si $p : \mathbb{A}^n \longrightarrow \mathbb{A}^{n-1}$ est la projection, alors $p(H)$ contient un ouvert non vide de $\mathbb{A}^{n-1}$: On écrit $F = F_d X_n^d + F_{d-1} X_n^{d-1} + \ldots + F_0$ avec $F_0, F_1, \ldots, F_d \in k[X_1, \ldots, X_{n-1}]$ et $F_d \neq 0$. Si $d = 0$, on a $F = F_0 \in k[X_1, \ldots, X_{n-1}]$ et donc $V = V(F_0) \times (OX_n)$. Si $d > 0$, $p(H)$ contient $D(F_d)$, qui est un ouvert non vide : en effet, si $F_d(a_1, \ldots, a_{n-1}) \neq 0$, alors le polynôme $F(a_1, \ldots, a_{n-1}, T) \in k[T]$ est non constant et possède donc une racine a_n dans k qui est algébriquement clos. Il suit que $(a_1, \ldots, a_n) \in H$ et donc que $(a_1, \ldots, a_{n-1}) \in p(H)$.

On démontre ensuite le théorème dans le cas affine : On procède par récurrence sur n. Le lieu des zéros d'un polynôme non constant en une variable sur un corps algébriquement clos est non vide. Le théorème est donc vrai si $n = 1$. Supposons le théorème démontré pour à l'ordre $n - 1$. Si $H = H' \times L$ où H' est une hypersurface de $\mathbb{A}^{n-1}$ et L une droite, alors H est infini comme produit d'un ensemble non vide par un ensemble infini. Sinon, $p(H)$ contient un ouvert non vide et donc infini de $\mathbb{A}^{n-1}$ et H est nécessairement infini.

Il reste à traiter le cas projectif : Quitte à faire un changement de coordonnées, on peut supposer $H \neq \mathbb{P}^{n-1}$. On a alors $H \supset H_*$ qui est une hypersurface de $\mathbb{A}^n$.

1.7. Ensembles algébriques irréductibles

1.7.1. Un ensemble algébrique est dit irréductible s'il est *irréductible* pour la topologie de Zariski.

• Si Φ est un changement de coordonnées (affines ou projectives) et si V est un ensemble algébrique irréductible, alors $\Phi^{-1}(V)$ aussi : On sait que Φ est un homéomorphisme.

• Soit Γ le graphe d'une application polynomiale $\varphi : V \longrightarrow W$. Alors, Γ est irréductible si et seulement si V est irréductible : En effet, on sait que Γ est isomorphe, et donc homéomorphe à V.

• Les droites et les courbes affines planes infinies de la forme $C = V(F)$ avec F irréductible sont irréductibles : Les fermés propres sont les ensembles finis.

1.7.2. Proposition. Si V et W sont deux ensembles algébriques affines irréductibles, il en va de même de $V \times W$.

Démonstration : Soit, pour $i = 1, 2$, $U_i \neq \emptyset$ un ouvert de $V \times W$. Si $p : V \times W \longrightarrow V$ est la projection, alors $p(U_i) \neq \emptyset$. Puisque V est irréductible, on a $p(U_1) \cap p(U_2) \neq \emptyset$. Soit $P \in p(U_1) \cap p(U_2)$, pour $i = 1, 2$, $U_i' := U_i \cap P \times W \neq \emptyset$ et est ouvert dans $P \times W$. Si $q : P \times W \to W$ est la projection, alors $q(U_i') \neq \emptyset$. Puisque W est irréductible, on a $q(U_1') \cap q(U_2') \neq \emptyset$. Si $Q \in q(U_1') \cap q(U_2')$, on a $(P, Q) \in U_1' \cap U_2' \subset U_1 \cap U_2$ qui n'est donc pas vide.

Corollaire. Toute variété linéaire affine est irréductible.

Puisque toute variété linéaire affine est isomorphe à $\mathbb{A}^d$ et qu'un produit d'ensembles affines irréductibles est irréductible, on est ramené au cas de $\mathbb{A}^1$.

1.7.3. Proposition. Soit V un ensemble algébrique projectif non vide. Alors $C(V)$ est irréductible si et seulement si V est irréductible.

Démonstration : Si $C(V)$ est irréductible et si $V = V_1 \cup V_2$ avec V_1 et V_2 algébriques, alors $C(V) = C(V_1 \cup V_2) = C(V_1) \cup C(V_2)$ si bien que $C(V) = C(V_1)$ (ou $C(V_2)$) et donc $V = V_1$. Réciproquement, si $C(V) = V(S_1) \cup V(S_2)$, on sait que quel que soit $P \in V$, on a $P \subset V(S_1)$ ou $P \subset V(S_2)$ si bien que $P \in V_p(S_1)$ ou $P \in V_p(S_2)$. On voit donc que $V \subset V_p(S_1) \cup V_p(S_2)$ et il suit que si V est irréductible, on a $V \subset V_p(S_1)$ (ou $V_p(S_2)$). On en déduit que $C(V) \subset C(V_p(S_1)) \subset V(S_1)$.

Corollaire. Toute variété linéaire projective non vide est irréductible.

En effet, le cône d'une telle variété est une variété linéaire affine.

1.7.4. Partie affine et fermeture projective d'un ensemble algébrique irréductible :

• Si V est un ensemble algébrique affine irréductible alors V^* est aussi irréductible : En effet, V est une partie dense de V^*.

• Si V est un sous-ensemble algébrique irréductible de $\mathbb{P}^n$ non contenu dans $\mathbb{P}^{n-1}$, alors V_* est irréductible et $(V_*)^* = V$: On sait déjà que $(V_*)^* \subset V$ et on a $V \subset (V_*)^* \cup \mathbb{P}^{n-1}$ si bien que $V \subset (V_*)^*$. On a donc bien $(V_*)^* = V$. De plus, V_* est un ouvert non vide de V et donc irréductible.