COURBES ALGEBRIQUES

Bernard Le Stum
(Université de Rennes I)

Contenu

INTRODUCTION

Soit $F \in \mathbb{R}[X]$ de degré d et N le nombre de solutions, éventuellement infini, de l'équation

$$a \in \mathbb{R}, \quad F(a) = 0.$$

On sait que N est fini si $F \neq 0$ et qu'alors $N \leq d$. En fait, on a $N = d$ si on tient compte

1) des solutions imaginaires

2) de leurs multiplicités

Soit maintenant, F et $G \in \mathbb{R}[X, Y]$ de degrés respectifs d et e et N le nombre de solutions, éventuellement infini du système d'équations

$$(a, b) \in \mathbb{R}^2, \quad \begin{cases} F(a,b) = 0 \\ G(a,b) = 0. \end{cases}$$

Nous allons montrer que N est fini si F et G n'ont pas de facteurs communs et qu'alors $N \leq de$. En fait, nous montrerons que $N = de$ si on tient compte

1) des solutions imaginaires

2) de leur multiplicité

3) des points à l'infini.

Afin de démontrer ce théorème, il est nécessaire de développer la théorie des système d'équations polynomiales, c'est à dire la géométrie algébrique affine, sur un corps (infini). De plus, puisqu'il faut donner un sens à la notion de point à l'infini, il faut aussi développer la géométrie algébrique projective. Enfin, il faut définir et étudier la notion de multiplicité (invariant numérique), ce qui se fait par l'intermédiaire de la notion d'anneau local en un point (invariant algébrique).

Dans le chapitre 0, nous rappelons quelques notions de base de géométrie classique, de topologie et d'algèbre commutative. Dans le chapitre I, nous développons la théorie sans utiliser d'algèbre commutative. Dans le chapitre II, nous établissons le lien entre les notions développées dans le chapitre précédent et l'algèbre commutative. Enfin, dans le chapitre III, nous étudions les courbes algébriques planes sur un corps algébriquement clos.

L'essentiel du cours est directement inspiré du livre de Fulton: "Algebraic curves". Une partie des exercices proviennent de ce livre, de celui de Hartshorne,

"Algebraic geometry" et plus généralement des différent livres d'introduction à la géométrie algébrique que j'ai eu l'occasion de consulter. Certains exercices sont dus à L. Moret-Bailly et P. Berthelot qui m'ont directement précédé dans l'enseignement de ce cours.

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.

COURBES ALGEBRIQUES

(Bernard Le Stum)

CHAPITRE 1 - EXERCICES

1.1. Courbes algébriques réelles planes ($k = \mathbb{R}$)

1.1.1. Tracer la courbe affine plane d'équation $Y^2 = X^3$ en considérant son intersection avec les droites vectorielles.

1.1.2. Idem avec $Y^2 = X^3 + X^2$.

1.1.3. Idem avec $Y^2 + X^3 + X^2 = 0$.

1.1.4. Idem avec $Y^2 = X^2 - X^4$.

1.1.5. Idem avec $Y^2 = X^4 - X^6$.

1.1.6. Idem avec $(X^2 + Y^2)^3 = 4X^2Y^2$.

1.2. Courbes paramétrées

1.2.1. La courbe paramétrée $C = \{(t, t^2, t^3),\ t \in k\} \subset \mathbb{A}^3$ est elle algébrique?

1.2.2. Idem avec $C = \{(t, t^2, 1/t),\ t \in k^*\} \subset \mathbb{A}^3$.

1.2.3. Idem avec $C = \{(t^2, t^3),\ t \in k\} \subset \mathbb{A}^2$.

1.2.4. Idem avec $C = \{(t^3, t^4, t^5),\ t \in k\} \subset \mathbb{A}^3$.

1.2.5. ($k = \mathbb{R}$) Idem avec $C = \{(t^2, t^4),\ t \in k\} \subset \mathbb{A}^2$.

1.2.6. ($k = \mathbb{R}$) Idem avec $C = \{(t, sin\ t),\ t \in k\} \subset \mathbb{A}^2$.

1.2.7. Idem avec $C := \{(t^{d_1}, \ldots, t^{d_n}),\ t \in k\} \subset \mathbb{A}^n$, $d_1, \ldots, d_n$ strictement positifs premiers entre eux.

1.2.8. La courbe réelle plane C d'équation polaire $r = 1$ est elle algébrique?

1.2.9. Idem avec $r = \theta$.

1.2.10. Idem avec $r = sin\ 2\theta$.

1.2.11. Idem avec $r = sin\ n\theta$, n impair.

1.3. Ensembles algébriques affines et variétés linéaires

1.3.1. ($Car\ k \neq 2$) Déterminer les intersections de la courbe affine plane C d'équation $X^2Y^2 + X^2 + Y^2 = 2XY(X + Y + 1)$ avec les droites d'équation $X = a$ ainsi qu'avec les diagonales Δ et Δ' d'équations respectives $Y = X$ et $Y = -X$.

1.3.2. Montrer que $C = \{(t, t^2, t^3),\ t \in k\} \subset \mathbb{A}^3$ n'est contenu dans aucun plan de $\mathbb{A}^3$.

1.3.3. Déterminer toutes les droites contenues dans la surface S d'équation $X^3 = YZ$ dans $\mathbb{A}^3$.

1.3.4. Montrer que le sous-ensemble algébrique V de $\mathbb{A}^3$ défini par $X^3 = YZ$ et $Y^2 = XZ$ contient une unique droite.

1.3.5. Soient S_1 et $S_2 \subset \mathbb{A}^3$ les cylindres d'équations respectives $X^2 + Y^2 = 1$ et $X^2 + Z^2 = 1$. Montrer que $C := S_1 \cap S_2$ est contenu dans la réunion de deux plans.

1.3.6. Soit C une courbe plane d'équation $F = 0$ et Δ la droite de pente (finie) c du plan affine passant par le point (a, b) de C. Montrer que la première projection induit une bijection de $C \cap \Delta$ sur les racines du polynôme $G := F(X, c(X - a) + b) \in k[X]$.

1.3.7. Montrer que si la droite Δ de pente finie c coupe la courbe C d'équation $Y^2 = X^3 - X$ en trois points distincts P, P' et P'' d'abscisses respectifs a, a' et a'', alors $a + a' + a'' = c^2$.

1.4. Ensembles algébriques projectifs

1.4.1. Montrer que $C := \{(a^2;\ ab;\ b^2),\ a,\ b \in k,\ (a,\ b) \neq 0\}$ est une courbe projective plane.

1.4.2. Montrer que $C := \{(a^3;\ a^2b;\ ab^2;\ b^3)),\ a,\ b \in k,\ (a,\ b) \neq 0\}$ est un sous-ensemble algébrique de $\mathbb{P}^3$.

1.4.3. Montrer que $S := \{(a^2;\ ab;\ ac;\ b^2;\ bc;\ c^2),\ a,\ b,\ c \in k,\ (a,\ b,\ c) \neq 0\}$ est un sous-ensemble algébrique de $\mathbb{P}^5$. C'est la *surface de Veronese*.

1.4.4. Montrer que $S := \{(ac;\ ad;\ bc;\ bd),\ a,\ b,\ c,\ d \in k,\ (a,\ b) \neq 0,\ (c,\ d) \neq 0\}$ est une surface projective.

1.5. Applications polynomiales

1.5.1. Soit C la courbe affine plane d'équation $XY = 1$. Montrer que toute application polynomiale de $\mathbb{A}^n$ dans C est constante.

1.5.2. Montrer que la courbe affine plane d'équation $Y = X^2$ est isomorphe à $\mathbb{A}^1$.

1.5.3. Montrer que la courbe paramétrée $C := \{(t,\ t^2,\ t^3),\ t \in k\} \subset \mathbb{A}^3$ est isomorphe à $\mathbb{A}^1$.

1.5.4. (*k algébriquement clos et car $k \neq 2$*) Montrer que toute courbe d'équation $aX^2 + bXY + cY^2 + dX + eY + f = 0$, avec a, b, c, d et e non tous nuls, est isomorphe à une courbe d'équation $Y = 0, XY = 1, X^2 = X$ ou $XY = 0$.

1.5.5. ($Car\ k \neq 2$) Soient C et C' les courbes affines planes d'équations respectives $X^2Y^2 + X^2 + Y^2 = 2XY(X + Y + 1)$ et $4X^2 = (Y^2 + 4Y)X - Y^2$. Montrer que $\Phi : \mathbb{A}^2 \longrightarrow \mathbb{A}^2,\ (a, b) \longmapsto (a, a + b - ab)$ induit un isomorphisme sur de C sur C'.

1.5.6. Montrer que si D_1 et D_2 sont deux droites distinctes sécantes du plan affine, alors $D_1 \cup D_2$ est isomorphe à la courbe plane C d'équation $XY = 0$.

1.5.7. Montrer que si D_1, D_2 et D_3 sont trois droites distinctes concourantes du plan affine, alors $D_1 \cup D_2 \cup D_3$ est isomorphe à la courbe plane C d'équation $XY(X-Y) = 0$.

1.6. Fermeture algébrique

1.6.1. Déterminer la fermeture algébrique V de $A = \{(1, 1/t),\ t \in k^*\ \} \subset \mathbb{A}^2$.

1.6.2. ($k = \mathbb{R}$) Idem pour $A = \{(m, 0),\ m \in \mathbb{Z}\} \subset \mathbb{A}^2$.

1.6.3. ($k = \mathbb{C}$) Idem pour $A = \{z,\ |z| = 1\} \subset \mathbb{A}^1$.

1.6.4. Idem pour $A = \{(t^2, t^4),\ t \in k\ \} \subset \mathbb{A}^2$.

1.6.5. Idem pour $A = \{(t^2, t + 1/t),\ t \in k^*\} \subset \mathbb{A}^2$.

1.6.6. ($k = \mathbb{R}$) Idem pour $A = \{(t, \sin t),\ t \in \mathbb{R}\}$.

1.6.7. ($k = \mathbb{C}$) Idem pour $A = \{(z, \bar{z}),\ z \in \mathbb{C}\}$.

1.7. Topologie et applications polynomiales

1.7.1. Montrer que l'application $\Phi : \mathbb{A}^1 \longrightarrow \mathbb{A}^3,\ t \longmapsto (t^2,\ t^2(t^2-1),\ t^3)$ est un homéomorphisme de $\mathbb{A}^1$ sur un ensemble algébrique $C \subset \mathbb{A}^3$.

1.7.2. Idem avec $\Phi : \mathbb{A}^1 \longrightarrow \mathbb{A}^3,\ t \longmapsto (t^2,\ t^3 - t^2,\ t^5)$.

1.7.3. ($k = \mathbb{R}$) Idem avec $\Phi : \mathbb{A}^1 \longrightarrow \mathbb{A}^2,\ t \longmapsto (t - t^4,\ 1 - t^3)$.

1.7.4. Soit C une courbe affine plane sur $\mathbb{C}$ telle que la première projection $x : C \longrightarrow \mathbb{A}^1$ soit injective. Montrer que $x(C)$ est ouvert dans $\mathbb{A}^1$.

1.8. Irréductibilité des courbes planes

1.8.1. ($k = \mathbb{R}$) Montrer que le polynôme $Y^2 + X^2(X-1)^2$ est irréductible mais que la courbe affine d'équation $Y^2 + X^2(X-1)^2 = 0$ est réductible.

1.8.2. ($k = \mathbb{R}$) Montrer que le polynôme $X^3 + X - X^2Y - Y$ est réductible mais que la courbe affine d'équation $X^3 + X - X^2Y - Y = 0$ est irréductible.

1.8.3. Montrer que la droite affine et les courbes affines planes d'équations $XY = 1$, $X^2 = X$ et $XY = 0$ sont deux à deux non isomorphes.

1.8.4. ($k = \mathbb{C}$) Montrer que deux coniques projectives irréductibles sont projectivement équivalentes.

1.8.5. ($k = \mathbb{C}$) Déterminer les valeurs de a, b, c, d, e et $f \in k$ pour lesquelles la conique C d'équation $aX^2 + bXY + cY^2 + dX + eY + f = 0$ (a, b, et c non tous nuls) est irréductible.

1.8.6. *(k algébriquement clos)* Si $\lambda \in k$, montrer que la cubique d'équation $Y^2 = X(X-1)(X-\lambda)$ est irréductible.

1.8.7. Montrer que la courbe C d'équation $(X^2 + XY + Y^2)(X^2 + Y^2) + X^3 + Y^3 = 0$ est irréductible sur $\mathbb{C}$. En va-t-il de même sur un corps algébriquement clos de caractéristique 2?, de caractéristique 3?

1.8.8. *(k algébriquement clos)* Montrer que la courbe affine plane C d'équation $X^2Y^2 + X^2 + Y^2 = 2XY(X + Y + 1)$ est irréductible.

1.8.9. Montrer que la courbe réelle plane C d'équation polaire $r = sin\ n\theta$, n impair est irréductible.

1.8.10. Montrer que la courbe réelle plane C d'équation polaire $r = sin\ 2\theta$ est irréductible.

1.9. Irréductibilité des courbes paramétrées

1.9.1. Soient $d_1, \ldots, d_n$ des entiers strictement positifs premiers entre eux et $C := \{(t^{d_1}, \ldots, t^{d_n}),\ t \in k\} \subset \mathbb{A}^n$. Montrer que C est un ensemble algébrique irréductible.

1.9.2. Montrer que la courbe paramétrée $C = \{(t^2,\ t^2(t^2-1),\ t^3),\ t \in k\}$ est irréductible.

1.9.3. Idem avec $C = \{(t^2,\ t^3 - t^2,\ t^5),\ t \in k\}$.

1.9.4. Idem avec $C = \{(t - t^4,\ 1 - t^3),\ t \in k\}$.

COURBES ALGEBRIQUES

(Bernard Le Stum)

CHAPITRE 1 - CORRIGES

1.1.4. On a

$$V(Y^2-X^2+X^4)\cap V(Y-tX)=V(Y^2-X^2+X^4,Y-tX)$$
$$V(Y^2-X^2+X^4)\cap V(Y-tX)=V((tX)^2-X^2+X^4,Y-tX)$$
$$V(Y^2-X^2+X^4)\cap V(Y-tX)=V(X^2(X^2+t^2-1),Y-tX)$$
$$V(Y^2-X^2+X^4)\cap V(Y-tX)=V(X^2,Y-tX)\cup V(X^2+t^2-1,Y-tX)$$

$$=\begin{cases}\{O,(\sqrt{1-t^2},t\sqrt{1-t^2}),(-\sqrt{1-t^2},-t\sqrt{1-t^2})\}\text{si } |t|\leq 1\\ \{O\}\text{ sinon.}\end{cases}$$

On vérifie aussi que $V(Y^2 - X^2 + X^4) \cap V(X) = \{O\}$. On voit donc que la courbe affine plane d'équation $Y^2 = X^2 - X^4$ s'obtient par symétrie centrale de centre O à partir de la courbe paramétrée

$$\begin{cases}x=\sqrt{1-t^2}\\ y=t\sqrt{1-t^2}.\end{cases}$$

Celle ci est définie pour $|t| \leq 1$. Comme x est paire et y impaire, on peut limiter l'intervalle d'étude à [0, 1] et faire une symétrie d'axe (OX). Les fonctions x et y sont dérivables pour $t \neq 1$avec $x' = -t/\sqrt{1-t^2}$ et $y' = (1 - 2t^2)/\sqrt{1-t^2}$ si bien que la pente de la courbe est donnée par $m := y'/x' = (2t^2 - 1)/t$. En particulier, celle ci s'annule pour $t = \sqrt{2}/2$, c'est à dire au point de coordonnées $(\sqrt{2}/2 , 1/2)$. On trace donc l'arc qui part du point $(1, 0)$ avec une pente verticale, passe par le point $(\sqrt{2}/2 , 1/2)$ avec une pente horizontale et arrive en O avec la pente -1. Il ne reste plus alors qu'a effectuer les symétries d'axe (OX) et de centre O.

1.2.1. Il est clair que $(a, b, c) \in C$ si et seulement si $b = a^2$ et $c = a^3$. On a donc $C = V(Y - X^2, Z - X^3)$.

1.2.2. On vérifie que $C = V(Y - X^2, XZ - 1)$.

1.2.4. Montrons que $C = V(X^3 - YZ, Y^2 - XZ, Z^2 - X^2Y)$: L'inclusion directe est immédiate. Réciproquement, soit $(a, b, c) \in \mathbb{A}^3$ tel que $a^3 = bc$, $b^2 = ac$ et $c^2 = a^2b$. Si $a = 0$, alors $b = c = 0$ et $P \in C$. Sinon on pose $t = b/a$ et on remplace b par at. On obtient $a^3 = atc$, $a^2t^2 = ac$ et $c^2 = a^3t$. On voit donc que $a^2 = ct$, $at^2 = c$ et $c^2 = a^3t$. Il en résulte que $at^3 = at^2t = ct = a^2$ si bien que $a = t^3$ et finalement $b = at = t^4$, $c = at^2 = t^5$.

1.2.7. On a $C = V(\{X_i^{d_j} - X_j^{d_i}\}_{i,j=1,\ldots,n})$: L'inclusion directe est claire. D'autre part, puisque les d_i sont premiers entre eux, il existe des entiers $c_1, \ldots, c_n$ tels que $\Sigma_{i=1}^n c_i d_i = \mathbf{1}$. Soit $P := (a_1, \ldots, a_n) \in V(\{X_i^{d_j} - X_j^{d_i}\}_{i,j=1,\ldots,n})$. Si l'un des a_i est nul, on pose $t = 0$ et sinon, on pose $t = \prod_{i=1}^n a_i^{c_i}$. On vérifie facilement que $P = (t^{d_1}, \ldots, t^{d_n})$.

1.2.10. Soit P un point du plan affine réel de coordonnées polaires r et θ. Si $P \in C$, alors $r = sin\ 2\theta = 2sin\theta cos\theta$. En multipliant par r^2 et en élevant au carré, on trouve que P est sur la courbe d'équation $(X^2 + Y^2)^3 = 4X^2Y^2$. Réciproquement, si P est sur cette courbe, alors $\pm r = sin\ 2\theta$. On a donc, soit $r = sin\ 2\theta$, soit $-r = sin2\theta = sin2(\theta + \pi)$. Puisque le point P et le point de coordonnées polaires $-r$ et $\theta + \pi$ sont identiques, on voit que $P \in C$.

1.2.11. On a

$$sin\ n\theta = \prod_{k=0}^{n-1} (sin\ \theta + tan\frac{k\pi}{n}.cos\ \theta)\ .$$

On en déduit facilement que C est la courbe algébrique d'équation

$$(X^2 + Y^2)^{(n+1)/2} = \prod_{k=0}^{n-1} (Y + tan\frac{k\pi}{n}X)$$

1.3.1. L'intersection de la droite d'équation $X = a$ avec C est donnée par $X = a$ et $X^2Y^2 + X^2 + Y^2 = 2XY(X + Y + 1)$, soit encore $X = a$ et $(a - 1)^2Y^2 - 2a(a+1)Y + a^2 = 0$. Si $a = 1$, on voit que C et la droite se rencontrent au point $(1, 1/4)$. Sinon, on calcule le discriminant et on trouve $\Delta = 4a^3$. On voit donc que si $a = 0$, la droite coupe C a l'origine, si a est un carré non nul, la droite coupe C au point $(a, a/(1 \pm \sqrt{a}\ )^2)$ et que si a n'est pas un carré, la droite ne coupe pas C. L'intersection de C avec Δ est donnée par $X^2Y^2 + X^2 + Y^2 = 2XY(X + Y + 1)$ et $Y = X$, ou encore $X^4 = 4X^3$ et $Y = X$. On voit donc que $C \cap \Delta$ est composé de O et de $(4, 4)$. L'intersection de C avec Δ' est donné par $X^2Y^2 + X^2 + Y^2 = 2XY(X + Y + 1)$ et

$Y = -X$, ou encore $X^4 = -4X^2$ et $Y = -X$. On voit donc que $C \cap \Delta'$ est réduite à O si -1 n'est pas un carré et composé des trois points O, $(2i, -2i)$ et $(-2i, 2i)$ sinon.

1.3.2. Supposons qu'il existe un plan $P = V(\alpha X + \beta Y + \gamma Z + \delta)$ tel que $C \subset P$. Alors pour tout $t \in k$, on aurait $\alpha t + \beta t^2 + \gamma t^3 + \delta = 0$. Puisque k est infini, on aurait donc $\alpha = \beta = \gamma = \delta = 0$. Contradiction.

1.3.3. Si $D := \{(a + \alpha t, b + \beta t, c + \gamma t), t \in k\}$ est une droite contenue dans S, on a pour tout $t \in k$, $(a + \alpha t)^3 = (b + \beta t)(c + \gamma t)$. Puisque k est infini, on a nécessairement $\alpha = 0$ et donc pour tout $t \in k$, $a^3 = (b + \beta t)(c + \gamma t)$. On en déduit que $\beta\gamma = 0$. Si $\beta = 0$, alors $\gamma \neq 0$ et pour tout $t \in k$, $a^3 = b(c + \gamma t)$. On voit donc que $b = 0$ et il en résulte que $a = 0$. On obtient donc $D = \{(0, 0, c + \gamma t), t \in k\} = (OZ)$. De même, si $\gamma = 0$ on trouve $D = (OY)$. Puisque ces deux axes sont bien contenus dans S, ce sont les seules droites contenues dans S.

1.3.4. C'est l'axe des Z : si D est une droite contenue dans V, alors D est contenue dans la surface S d'équation $X^3 = YZ$. On sait alors que $D = (OY)$ ou $D = (OZ)$ et on vérifie que $(OZ) \subset V$ mais que $(OY) \not\subset V$.

1.3.6. L'intersection $C \cap \Delta$ est donné par $Y = c(X - a) + b$ et $F(X, Y) = 0$, soit encore $Y = c(X - a) + b$ et $G(X) = 0$. On voit donc que la première projection induit bien une bijection de $C \cap \Delta$ sur les racines de G.

1.3.7. L'application qui a un point du plan associe son abscisse induit une bijection de $C \cap \Delta$ sur l'ensemble des racines de $(c(X - a) + b)^2 - (X^3 - X) = -X^3 + c^2X^2 + \ldots$ L'égalité annoncée provient donc de la formule donnant la somme des racines d'un polynôme.

1.4.4. Si $a, b, c, d \in k$, on a $(ac)(bd) = (ad)(bc)$, ce qui montre que S est contenu dans la surface d'équation $XT = YZ$. Réciproquement, soit $P := (\alpha; \beta; \gamma; \delta) \in \mathbb{P}^4$ tel que $\alpha\delta = \beta\gamma$. Si $\gamma \neq 0$, on pose $a = \alpha$, $b = \gamma$, $c = 1$et $d = \delta/\gamma$, si bien que $(ac; ad; bc; bd) = (\alpha; \alpha\delta/\gamma; \gamma; \delta) = P$ avec $b, c \neq 0$. Si $\gamma = 0$ et $\alpha \neq 0$, on pose $a = 1$, $b = 0$, $c = \alpha$ et $d = \beta$ si bien que $(ac; ad; bc; bd) = (\alpha; \beta; 0; 0) = P$ avec $a, c \neq 0$. Enfin, si $\gamma = \alpha = 0$, on pose $a = \beta$, $b = \delta$, $c = 0$ et $d = 1$ si bien que $(ac; ad; bc; bd) = (0; \beta; 0; \delta) = P$ avec $d \neq 0$ et a ou $b \neq 0$ car $(0, \beta, 0, \delta) \neq 0$.

1.5.5. Dire que $(a, b) \in C$ et que $\Phi(a, b) = (a, c)$ signifie que $a^2b^2 + a^2 + b^2 = 2ab(a + b + 1)$ et que $c = a + b - ab$, ou encore que $4ab = (a + b - ab)^2$ et que $c =$

$a + b - ab$, ce qui s'écrit encore $4ab = c^2$ et $b = c - a - c^2/4$. On obtient finalement $4a^2 - (c^2 + 4c)a + c^2 = 4a^2 - 4(a + b)a + ab = 0$ et $b = c - a - c^2/4$. On voit donc que Φ est une bijection de C sur C' et que la réciproque est induite par l'application polynomiale $(a, c) \longmapsto (a, c - a - c^2/4)$. Cela signifie bien que Φ induit un isomorphisme de C sur C'.

1.5.6. On peut toujours trouver une application affine bijective Φ du plan dans lui même qui transforme D_1 et D_2 en les axes des coordonnées. C'est un isomorphisme de $D_1 \cup D_2$ sur C.

1.6.1. Puisque k est infini, A est infini et contenu dans la droite d'équation $X = 1$. Puisque les fermés propres d'une droite sont finis, on voit que V est la droite d'équation $X = 1$.

1.6.3. Comme A est infini, V est un sous-ensemble algébrique infini de $\mathbb{A}^1$, donc $V = \mathbb{A}^1$.

1.6.4. Puisque k est infini, A est infini et $A \subset V(Y - X^2)$ avec $Y - X^2$ irréductible. Il suit que V est la parabole d'équation $Y = X^2$.

6.6. Pour tout $b \in [-1, +1]$, l'intersection de A avec la droite d'équation $Y = b$ est infinie. Donc si $A \subset V(S)$ et $F \in S$, $Y - b$ divise F. Comme ceci vaut pour une infinité de valeurs de b, on en déduit $F = 0$. On a donc $F = 0$ et $V(S) = \mathbb{A}^2$.

1.7.1. Si $\Phi(t) =: P =: (a, b, c)$, on a $b = a(a - 1)$ et $c^2 = a^3$ d'où

$$\Phi(\mathbb{A}^1) \subset C := V(\, Y - X(X - 1)\,,\, Z^2 - X^3\,).$$

Inversement, si $P =: (a, b, c) \in C$, on pose $t = 0$ si $a = 0$ et $t = c/a$ sinon. On vérifie facilement que $P \longmapsto t$ est un inverse pour Φ. Il en résulte que Φ est une bijection de $\mathbb{A}^1$ sur $C = V(\, Y - X(X - 1)\,,\, Z^2 - X^3\,)$. Puisque Φ est polynomiale, elle est continue. Enfin, l'image d'un fermé de $\mathbb{A}^1$ par Φ est soit fini soit égale à C, et donc fermée. Cela montre que Φ est une application continue bijective fermée, et donc un homéomorphisme.

1.7.3. Si $t \in \mathbb{R}$ et $P := (a, b) := \Phi(t)$, on a $a = bt$. On en déduit que $a^3 = b^3 t^3$ et il suit que $b^4 = b^3(1 - t^3) = b^3 - b^3 t^3 = b^3 - a^3$. On voit donc que P est sur la courbe C d'équation $Y^4 = Y^3 - X^3$. Réciproquement, soit $P =: (a, b) \in C$. Si $P = O$, on

pose $t = 1$. Sinon, on a $b \neq 0$ et on pose $t := a/b$. Dans les deux cas, on vérifie aisément que $P = \Phi(t)$. Puisque Φ est clairement injective, cette application induit une bijection de $\mathbb{A}^1$ sur C. Puisque Φ est une application polynomiale, elle est continue. C'est un homéomorphisme car elle est fermée.

1.7.4. Puisque la première projection $x : C \longrightarrow \mathbb{A}^1$ est injective, la courbe C ne peut pas être le produit d'une partie de $\mathbb{A}^1$ et de l'axe des Y. On sait qu'alors, $x(C)$ contient un ouvert non vide. En passant aux complémentaires, on voit que le complémentaire Z de $x(C)$ dans $\mathbb{A}^1$ est contenu dans un fermé propre. Puisque les fermés propres de $\mathbb{A}^1$ sont les ensembles finis, on voit que Z est fini (ou vide) et donc fermé. Il suit que $x(C)$ est ouvert.

1.8.6. Le polynôme $X(X-1)(X-\lambda)$ étant de degré impair ne peux pas être un carré dans $k[X]$. Il suit que le polynôme $Y^2 - X(X-1)(X-\lambda)$ est unitaire de degré 2 en Y et sans racine dans $k[X]$. Il est donc est irréductible. Puisque k est algébriquement clos, C est une courbe irréductible.

1.8.7. Les facteurs irréductibles du polynôme $(X^2+XY+Y^2)(X^2+Y^2)$ sont $X-jY, X-j^2Y, X+iY$ et $X-iY$. Ceux de X^3+Y^3 sont $X+Y, X+jY$ et $X+j^2Y$. On voit donc que le polynôme qui définit C est somme de deux polynômes homogènes sans facteurs communs de degrés 4 et 3. Un tel polynôme est toujours irréductible. Puisque $\mathbb{C}$ est algébriquement clos, C est irréductible.

En caractéristique 2, on a

$$(X^2+XY+Y^2)(X^2+Y^2)+X^3+Y^3 = (X+jY)(X+j^2Y)(X+Y)(X+Y+1)$$

et C est donc composée des droites d'équation $X = jY, X = j^2Y, X = Y$ et $X = Y+1$.

En caractéristique 3, les facteurs irréductibles du polynôme $(X^2+XY+Y^2)(X^2+Y^2)$ sont $X-Y, X+iY$ et $X-iY$ et celui de X^3+Y^3 est $X+Y$. On voit donc comme sur $\mathbb{C}$ que C est irréductible.

1.8.8. Si C n'était pas irréductible, on pourrait écrire $X^2Y^2 - 2XY(X+Y) + (X-Y)^2 = (F+X-Y)(G+X-Y)$ avec F et G homogènes de degré 2. On aurait alors $(Y-X)(F+G) = 2XY(X+Y)$, ce qui est clairement impossible.

1.8.9. On sait que C est la courbe algébrique d'équation

$$(X^2+Y^2)^{(n+1)/2} = \prod_{k=0}^{n-1} (Y + tan\frac{k\pi}{n}X) \ .$$

Puisque $(X^2 + Y^2)^{(n+1)/2}$ et $\prod_{k=0}^{n-1} (Y + tan\frac{k\pi}{n}X)$ sont homogènes de degrés respectifs $n+1$ et n, et n'ont pas de facteurs communs (les racines du premier polynôme sont imaginaires et celles du second sont réelles), l'équation de C est irréductible. D'autre part, il est clair que C est infinie et il en résulte que C est irréductible.

1.8.10. On sait que C est la courbe d'équation $(X^2 + Y^2)^3 = 4X^2Y^2$. Il suffit alors puisque C est infinie, de montrer que le polynôme $(X^2 + Y^2)^3 - 4X^2Y^2$ est irréductible. En considérant les composantes homogènes des facteurs éventuels, on voit que si ce polynôme était réductible, on pourrait écrire $(X^2 + Y^2)^3 - 4X^2Y^2 = ((X^2 + Y^2)^2 + F)(X^2 + Y^2 + G)$ avec F et G homogènes de degrés respectifs 3 et 1. On aurait alors $0 = (X^2 + Y^2)^2 G + F(X^2 + Y^2)$ et $-4X^2Y^2 = FG$ si bien que $F = -(X^2 + Y^2)G$ et $4X^2Y^2 = (X^2 + Y^2)G^2$. Contradiction.

1.9.1. La courbe C est irréductible comme image de $\mathbb{A}^1$ qui est irréductible par l'application $\Phi : \mathbb{A}^1 \longrightarrow \mathbb{A}^n$, $t \longmapsto (t^{d_1}, \ldots, t^{d_n})$ qui est continue car polynomiale.

1.9.2. On sait que l'application $\Phi : \mathbb{A}^1 \longrightarrow \mathbb{A}^3$, $t \longmapsto (t^2, t^2(t^2 - 1), t^3)$ qui paramètre C est un homéomorphisme de $\mathbb{A}^1$ sur C et que $\mathbb{A}^1$ est irréductible.

1.9.4. Puisque $\mathbb{A}^1$ est irréductible, il en va de même de son image C par Φ.

COURBES ALGEBRIQUES

(Bernard Le Stum)

CHAPITRE 2 - COURS

Idéal de définition, anneau de coordonnées, anneau local en un point

2.1. Idéal d'une partie de l'espace affine

2.1.1. Définition. Si $A \subset \mathbb{A}^n$, on dit que $I(A) := \{F \in k[X_1, \ldots, X_n], \forall P \in A, F(P) = 0\}$ est l'*idéal* de A dans $\mathbb{A}^n$. On écrira aussi $I(A \subset \mathbb{A}^n)$.

• Si $A \subset \mathbb{A}^n$, alors $I(A)$ est un bien un idéal de $k[X_1, \ldots, X_n]$. C'est même un idéal radical : Si $F, G \in I(A)$ et $P \in A$, alors $(F + G)(P) = F(P) + G(P) = 0$. De même, si $F \in k[X_1, \ldots, X_n]$, $G \in I(A)$ et $P \in A$, alors $(FG)(P) = F(P)G(P) = 0$. Enfin, si $F^r \in I(A)$ et $P \in A$, alors $F(P)^r = F^r(P) = 0$ si bien que $F(P) = 0$ et donc $F \in I(A)$.

2.1.2. Proposition. (i) On a $I(\emptyset) = k[X_1, \ldots, X_n]$ et $I(\mathbb{A}^n) = 0$.

(ii) Si $\{A_\alpha\}_{\alpha \in I}$ est un ensemble de parties de $\mathbb{A}^n$, alors $I(\bigcup_\alpha A_\alpha) = \bigcap_\alpha I(A_\alpha)$.

(iii) Si $A \subset B \subset \mathbb{A}^n$, alors $I(B) \subset I(A)$.

(iv) Si $S \subset k[X_1, \ldots, X_n]$, alors $S \subset I(V(S))$ et si $A \subset \mathbb{A}^n$, alors $A \subset V(I(A))$.

Démonstration : Si $A = \emptyset$, la condition pour appartenir à $I(A)$ est vide et on a donc $I(A) = k[X_1, \ldots, X_n]$. Aussi, si $F \in I(\mathbb{A}^n)$, on a pour tout $P \in \mathbb{A}^n$, $F(P) = 0$ et donc $F = 0$ car k est *infini*. Cela démontre l'assertion i). Pour l'assertion ii), on remarque que

$F \in I(\bigcup_\alpha A_\alpha)$ ssi $\forall P \in \bigcup_\alpha A_\alpha, F(P) = 0$
$F \in I(\bigcup_\alpha A_\alpha)$ ssi $\forall \alpha \in A, \forall P \in A_\alpha, F(P) = 0$
$F \in I(\bigcup_\alpha A_\alpha)$ ssi $\forall \alpha \in A, F \in I(A_\alpha)$
$F \in I(\bigcup_\alpha A_\alpha)$ ssi $F \in \bigcap_\alpha I(A_\alpha)$

L'assertion iii) se vérifie aisément : si $A \subset B \subset \mathbb{A}^n$ et $F \in I(B)$, alors pour tout $P \in A$, on a $P \in B$ et donc $F(P) = 0$ si bien que $P \in I(A)$. Enfin, on démontre iv) : Si $S \subset k[X_1, \ldots, X_n]$, $F \in S$ et $P \in V(S)$ alors $F(P) = 0$ et donc $F \in I(V(S))$. De même,

si $A \subset \mathbb{A}^n$, $P \in A$ et $F \in I(A)$, alors $F(P) = 0$ et donc $P \in V(I(A))$.

2.1.3. De cette proposition, on dérive aisément les propriétés suivantes de la notion d'idéal d'une partie de l'espace affine :

• Si P est un point, alors $I(P)$ est un idéal maximal. En fait, si $P = (a_1, \ldots, a_n)$ alors $I(P) = (X_1 - a_1, \ldots, X_n - a_n)$: Il est clair que, pour tout $i = 1, \ldots, n$, $X_i - a_i \in I(P)$. Puisque $I(P)$ est un idéal, l'idéal *maximal* $\mathfrak{m} := (X_1 - a_1, \ldots, X_n - a_n)$ est contenu dans $I(P)$. Il suffit alors de remarquer que $I(P)$ est un idéal propre car $1 \notin I(P)$.

• Une partie V de $\mathbb{A}^n$ est algébrique si et seulement si $V(I(V)) = V$: Si $V = V(I(V))$, alors V est algébrique par définition. Réciproquement, si V est algébrique, on peut écrire $V = V(S)$ et on a $S \subset I(V(S)) = I(V)$ si bien que $V(I(V) \subset V(S) = V$. Puisque $V \subset V(I(V))$, on a bien $V(I(V)) = V$.

• Si V et W sont deux ensembles *algébriques*, alors $V = W$ si et seulement si $I(V) = I(W)$: La condition est évidemment nécessaire et elle est aussi suffisante car si $I(V) = I(W)$, alors $V = V(I(V)) = V(I(W)) = W$.

• La fermeture algébrique de $A \subset \mathbb{A}^n$ est $V := V(I(A))$ et on a $I(A) = I(V)$: Il y a identité entre fermés et sous-ensembles algébriques et on a $A \subset V = V(I(A))$ qui est algébrique. De plus, si $A \subset W$ algébrique, alors $I(W) \subset I(A)$ et donc $V = V(I(A)) \subset V(I(W)) = W$. Enfin, on sait que $I(A) \subset I(V(I(A)) = I(V)$ et puisque $A \subset V$, on a $I(V) \subset I(A)$.

2.2. Idéal d'une partie de l'espace projectif

2.2.1. Définition. Si $A \subset \mathbb{P}^n$, on dit que $I(A) := \{F \in k[X_1, \ldots, X_{n+1}], \forall\ P \in A, F(P) = 0\}$ est l'*idéal de A*. On écrira aussi $I(A \subset \mathbb{P}^n)$.

• On a $I(\emptyset) = k[X_1, \ldots, X_{n+1}]$ et si $A \neq \emptyset$, alors $I(A) = I(C(A))$: Il est clair que $I(\emptyset) = k[X_1, \ldots, X_{n+1}]$ et si $A \neq \emptyset$, on a

$F \in I(C(A))$ ssi $C(A) \subset V(F)$

$F \in I(C(A))$ ssi $A \subset V_p(F)$

$F \in I(C(A))$ ssi $F \in I(A)$.

• Si $A \subset \mathbb{P}^n$, alors $I(A)$ est un idéal gradué radical de $k[X_1, \ldots, X_{n+1}]$: On peut supposer que A est non vide et on a donc $I(A) = I(C(A))$ qui est bien un idéal radical. De plus, si $F = F_d + F_{d-1} + \ldots + F_0$ est la décomposition de F non nul $\in I(A)$ et $P \in A$, on a $F(P) = 0$ et on sait qu'alors $F_d(P) = F_{d-1}(P) = \ldots = F_0(P)$ et donc $F_d, F_{d-1}, \ldots, F_0 \in I(A)$.

2.2.2. Proposition. (i) On a $I(\emptyset) = k[X_1, \ldots, X_{n+1}]$ et $I(\mathbb{P}^n) = 0$, (ii) On a toujours $I(\bigcup_\alpha A_\alpha) = \bigcap_\alpha I(A_\alpha)$, (iii) Si $A \subset B \subset \mathbb{A}^n$, alors $I(B) \subset I(A)$ et (iv) on a toujours $S \subset I(V(S))$ et $A \subset V(I(A))$.

Démonstration : i) On a déja vu que $I(\emptyset) = k[X_1, \ldots, X_{n+1}]$ et on a $I(\mathbb{P}^n) = I(C(\mathbb{P}^n)) = I(\mathbb{A}^{n+1}) = 0$. ii) On peut clairement supposer que les $A_\alpha$sont non vides. On a alors $I(\bigcup_\alpha A_\alpha) = I(C(\bigcup_\alpha A_\alpha)) = I(\bigcup_\alpha C(A_\alpha)) = \bigcap_\alpha I(C(A_\alpha)) = \bigcap_\alpha I(A_\alpha)$. iii) Si A est vide, c'est clair. Sinon, on a $C(A) \subset C(B)$ et donc $I(B) = I(C(B)) \subset I(C(A)) = I(A)$. iv) Si $V_p(S) = \emptyset$, c'est clair. Sinon, on a $S \subset I(V(S)) \subset I(C(V_p(S))) = I(V_p(S))$. De même, on $C(A) \subset V(I(C(A))) = V(I(A)) = C(V_p(I(A))$ car $I(A)$ est un idéal gradué si bien que $A \subset V_p(I(A))$.

2.2.3. De cette proposition, on dérive comme dans le cas affine les propriétés suivantes :

• Si I est un idéal gradué et $V_p(I) \neq \emptyset$, on a $C(V_p(I)) = V(I)$: En effet, on a $C(V_p(I)) = C(V_p(I_p)) = V(I_p) = V(I)$.

• Une partie V de $\mathbb{P}^n$ est algébrique (projective) si et seulement si $V_p(I(V)) = V$: V est algébrique si et seulement si $C(V)$ est algébrique, ce qui revient à dire, si $V \neq \emptyset$, que $C(V_p(I(V))) = V(I(V)) = V(I(C(V))) = C(V)$, ou encore que $V_p(I(V)) = V$. Si V est vide, l'assertion est claire.

• Si V et W sont deux ensembles *algébriques* projectifs, alors $V = W$ si et seulement si $I(V) = I(W)$: On a

$V = W$ ssi $C(V) = C(W)$

$V = W$ ssi $I(V) = I(C(V)) = I(C(W)) = I(W)$.

• La fermeture algébrique de $A \subset \mathbb{P}^n$ est $V := V_p(I(A))$ et on a $I(A) = I(V)$: Comme dans le cas affine.

• Si V est un ensemble algébrique affine, alors la fermeture projective V^* de V est $V_p(I(V \subset \mathbb{P}^n))$: C'est un cas particulier du dernier résultat.

2.2.4. Proposition. Si V est un ensemble algébrique affine, alors $I(V^*) = I(V)^*$, $V^* = V_p(I(V)^*)$ et $(V^*)_* = V$.

Démonstration : Puisque V est dense dans V^*, on a $I(V^* \subset \mathbb{P}^n) = I(V \subset \mathbb{P}^n)$. Il suit que pour tout polynôme *homogène* F, on a

$F \in I(V^*)$ ssi $\forall\, P \in V, F(P) = 0$

$F \in I(V^*)$ ssi $\forall\, P \in V, F_*(P) = 0$

$F \in I(V^*)$ ssi $F_* \in I(V)$.

$F \in I(V^*)$ ssi $F \in I(V)^*$.

Puisque $I(V^*)$ et $I(V)^*$ sont deux idéaux gradués, ils sont nécessairement égaux. On en déduit donc que $V^* = V_p(I(V^*)) = V_p(I(V)^*)$. Finalement, on a $(V^*)_* = V_p(I(V)^*)_* = V((I(V)^*)_*) = V(I(V)) = V$.

Corollaire. Les applications $_*$ et * induisent une bijection entre les sous-ensembles algébriques irréductibles de $\mathbb{P}^n$ non contenus dans $\mathbb{P}^{n-1}$ et les sous ensembles algébriques irréductibles de $\mathbb{A}^n$.

Nous savons déjà que si V est un ensemble algébrique projectif irréductible non contenu dans $\mathbb{P}^{n-1}$, alors V_* est irréductible et que $(V_*)^* = V$. Nous savons aussi que si V est un ensemble algébrique affine irréductible, alors V^* est un ensemble algébrique projectif irréductible non contenu dans $\mathbb{P}^{n-1}$ et nous venons de voir que l'on a toujours $(V^*)_* = V$.

• Si $I(V) = (F)$ alors $I(V^*) = (F^*)$ et $V^* = V_p(F)$: On a $I(V^*) = I(V)^* = (F)^* = (F^*)$.

• Si $I(V) = (F, G)$, on a pas nécessairement $V^* = V_p(F^*, G^*)$ et donc pas non plus $I(V^*) \neq (F^*, G^*)$!

2.3. Anneau de coordonnées

2.3.1. Proposition. Si V est un sous ensemble algébrique de $\mathbb{A}^n$, alors $k[V]$ est une sous algèbre de la k–algèbre des applications de V dans k et l'application de restriction $k[X_1, \ldots, X_n] \longrightarrow k[V]$ induit un isomorphisme de k-algèbres

$$k[X_1, \ldots, X_n]/I(V) \tilde{=} k[V].$$

Démonstration : L'application canonique $k[X_1, \ldots, X_n] \longrightarrow k^V$ est un homo-

morphisme de k-algèbres, son image est $k[V]$ et son noyau est $I(V)$.

2.3.2. Définition. On dit que $k[V]$ est *l'anneau de coordonnées* de V. Si $S \subset k[V]$, on note $V(S) = \{P \in V, \forall\ f \in S, f(P) = 0\}$. On appelle *hypersurface* de V toute partie de la forme $V(f)$ avec $f \in k[V]$ non constant et *ouvert principal* toute partie de la forme $D(f) = V \setminus V(f)$ avec $f \in k[V]$. Enfin, si $A \subset V$, on note $I(A \subset V)$ (ou $I_V(A)$) : $= \{f \in k[V], \forall\ P \in A, f(P) = 0\}$.

2.3.3. Proposition. Si $S \subset k[V]$, alors $V(S)$ est un sous ensemble algébrique de V. Plus précisément, si $S' \subset k[X_1, \ldots, X_n]$ est tel que l'application canonique $\pi : k[X_1, \ldots, X_n] \longrightarrow k[V]$ induise une surjection de S' sur S, alors $V(S) = V(S') \cap V$.

Démonstration : On a pour $P \in \mathbb{A}^n$,

$P \in V(S)$ ssi $P \in V$ et $\forall\ f \in S, f(P) = 0$

$P \in V(S)$ ssi $P \in V$ et $\forall\ F \in S', F(P) = f(P) = 0$

$P \in V(S)$ ssi $P \in V$ et $P \in V(S')$

$P \in V(S)$ ssi $P \in V(S') \cap V$.

2.3.4. Corollaire. (i) On a $V(1_V) = \emptyset$ et $V(0_V) = V$, (ii) Si $S_\alpha \subset k[V]$, on a $V(\bigcup_\alpha S_\alpha) = \cap V(S_\alpha)$, (iii) Si $S, T \subset k[V]$, alors $V(S) \cup V(T) = V(fg, f \in S, g \in T)$ et (iv) Si $S \subset T \subset k[V]$, alors $V(T) \subset V(S)$.

Démonstration : i) $V(1_V) = V(1) \cap V = \emptyset \cap V = \emptyset$ et $V(0_V) = V(0) \cap V = \mathbb{A}^n \cap V = V$. ii) Si pour tout α, $\pi(S'_\alpha) = S$, alors $\pi(\bigcup_\alpha S'_\alpha) = \bigcup_\alpha S_\alpha$ et on a donc $V(\bigcup_\alpha S_\alpha) = V(\bigcup_\alpha S'_\alpha) \cap V = \bigcap_\alpha V(S'_\alpha) \cap V = \bigcap_\alpha (V(S'_\alpha) \cap V) = \bigcap_\alpha V(S_\alpha)$. iii) et iv) Si $\pi(S') = S$ et $\pi(T') = T$, alors $\pi(\{FG, F \in S', G \in T'\}) = \{fg, f \in S, g \in T\}$ et on a donc $V(S) \cup V(T) = (V(S') \cap V) \cup (V(T')) \cap V) = (V(S') \cup V(T')) \cap V = V(FG, F \in S', G \in T') \cap V = V(fg, f \in S, g \in T)$. De plus, si $S \subset T$, alors $S' \subset S' \cup T'$ et $\pi(S' \cup T') = T$ si bien que $V(T) = V(S' \cup T') \cap V \subset V(S') \cap V = V(S)$.

2.3.5. Proposition. Si $A \subset V$, alors $I_V(A)$ est un idéal radical de $k[V]$. Plus précisément, si $\pi : k[X_1, \ldots, X_n] \longrightarrow k[V]$ est l'application canonique, alors $\pi^{-1}(I_V(A)) = I(A)$ et $\pi(I(A)) = I_V(A)$.

Démonstration : On a

$F \in \pi^{-1}(I_V(A))$ ssi $F_{|V} = \pi(F) \in I_V(A)$

$F \in \pi^{-1}(I_V(A))$ ssi $\forall\ P \in A, F(P) = 0$

$F \in \pi^{-1}(I_V(A))$ ssi $F \in I(A)$

et donc $\pi^{-1}(I_V(A)) = I(A)$. Puisque π est surjectif, on en déduit que $\pi(I(A)) =$

$\pi(\pi^{-1}(I_V(A))) = I_V(A)$.

2.3.6. Corollaire. (i) On a $I_V(\emptyset) = k[V]$ et $I_V(V) = 0$, (ii) Si $A_\alpha \subset V$, on a $I_V(\cup_\alpha A_\alpha) = \cap I_V(A_\alpha)$,(ii) Si $A \subset B \subset V$, alors $I_V(B) \subset I_V(A)$ et (iv) On a toujours $S \subset I_V(V(S))$ et si $A \subset V$, $A \subset V(I_V(A))$

Démonstration : i) $I_V(\emptyset) = \pi(I(\emptyset)) = \pi(k[X_1, \ldots, X_n]) = k[V]$ et $I_V(V) = \pi(I(V)) = \pi(0) = 0$. ii) On a $I_V(\cup_\alpha A) = \pi(I(\cup A_\alpha)) = \pi(\cap_\alpha I(A_\alpha)) = \cap_\alpha \pi(I(A_\alpha)) = \cap_\alpha I_V(A_\alpha)$. iii) si $A \subset B \subset V$, alors $I_V(B) = \pi(I(B)) \subset \pi(I(A)) = I_V(A)$. iv) Si $\pi(S') = S$, on a $S' \subset I(V(S')) \subset I(V(S') \cap V) = I(V(S))$ et donc $S = \pi(S') \subset \pi(I(V(S))) = I_V(V(S))$. De même, on a $A \subset V(I(A)) \cap V = V(I_V(A))$ car $\pi(I(A)) = I_V(A)$.

2.3.7. Ici encore, on peut dériver des propositions que nous venons de démontrer les propriétés suivantes :

• Si P est un point, alors $k[P] \cong k$: Si $P = (a_1, \ldots, a_n)$, alors $I(P) = (X_1 - a_1, \ldots, X_n - a_n)$ si bien que $k[P] \cong k[X_1, \ldots, X_n]/(X_1 - a_1, \ldots, X_n - a_n) \cong k$.

• Si $A \subset V$, alors $V(I_V(A)) = V(I(A))$: Puisque π induit une surjection de $I(A)$ sur $I_V(A)$ et que $V(I(A)) \subset V(I(V)) = V$, on a $V(I_V(A)) = V(I(A)) \cap V = V(I(A))$.

• La fermeture algébrique de A dans V est $W := V(I_V(A))$ et on a $I_V(A) = I_V(W)$: On vient de voir que $W = V(I_V(A)) = V(I(A))$ et on a donc $I_V(A) = \pi(I(A)) = \pi(I(W)) = I_V(W)$.

• Une partie W de V est algébrique si et seulement si $V(I_V(W)) = W$: On sait que W est algébrique si et seulement si $V(I_V(W)) = V(I(W)) = W$.

• Si $W \subset V$ est un sous ensemble algébrique, alors l'application de restriction induit un isomorphisme $k[V]/I_V(W) \cong k[W]$: Puisque $\pi^{-1}(I_V(W)) = I(W)$, on a $k[V]/I_V(W) \cong (k[X_1, \ldots, X_n]/I(V))/I_V(W) \cong k[X_1, \ldots, X_n]/I(W) \cong k[W]$.

2.3.8. Définition. Si V est un ensemble algébrique *projectif* non-vide, on dit que $k[V] := k[C(V)]$ est *l'anneau de coordonnées homogènes* de V. On pose $k[\emptyset] = 0$.

2.4. Applications polynomiales et homomorphismes d'anneaux

2.4.1. Notations. Si $\varphi : W \longrightarrow V$ est une application polynomiale et $f \in k[V]$ on note $\varphi^*(f) := f \circ \varphi \in k[W]$.

• Si $i : W \hookrightarrow V$ est l'inclusion d'un sous ensemble algébrique et $f \in k[V]$, alors i^* est l'application canonique de restriction. En particulier, on a $Id^* = Id$: Si $P \in W$ et $f \in k[V]$, on $i^*(f)(P) = (f \circ i)(P) = f(P)$.

• Si $\varphi : W \longrightarrow V$ et $\psi : Z \longrightarrow W$ sont deux applications polynomiales, alors $(\varphi \circ \psi)^* = \psi^* \circ \varphi^*$: On a $(\varphi \circ \psi)^*(f) = f \circ (\varphi \circ \psi) = (f \circ \varphi) \circ \psi = \varphi^*(f) \circ \psi = \psi^*(\varphi^*(f)) = (\psi^* \circ \varphi^*)(f)$.

• Si une application polynomiale $\varphi : W \longrightarrow V$ se prolonge en $\Phi : \mathbb{A}^m \longrightarrow \mathbb{A}^n$, et si $f \in k[V]$ est la restriction de $F \in k[X_1, \ldots, X_n]$, alors $\varphi^*(f)$ est la restriction de $\Phi^*(F)$: Si $P \in W$, on a $\varphi^*(f)(P) = f(\varphi(P) = F(\Phi(P)) = \Phi^*(F)(P)$.

• Si $\varphi : W \longrightarrow V$ est une application polynomiale et $f \in k[V]$, alors $\varphi^{-1}(V(f)) = V(\varphi^*(f))$. En effet, on a

$P \in \varphi^{-1}(V(f))$ ssi $\varphi(P) \in V(f)$

$P \in \varphi^{-1}(V(f))$ ssi $\varphi^*(f)(P) = f(\varphi(P)) = 0$

$P \in \varphi^{-1}(V(f))$ ssi $P \in V(\varphi^*(f))$.

• Si $\varphi : W \longrightarrow V$ est une application polynomiale, alors $\varphi^* : k[V] \longrightarrow k[W]$ est un homomorphisme de k-algèbres : On a toujours $\varphi^*(f + g) = (f + g) \circ \varphi = f \circ \varphi + g \circ \varphi = \varphi^*(f) + \varphi^*(g)$ et $\varphi^*(fg) = (fg) \circ \varphi = (f \circ \varphi)(g \circ \varphi) = \varphi^*(f)\varphi^*(g)$. De plus, si c est une fonction constante, on a $\varphi^*(c) = c \circ \varphi = c$.

2.4.2. Théorème. L'application $Hom(W, V) \longrightarrow Hom_{k-alg}(k[V], k[W])$, $\varphi \longmapsto \varphi^*$ est bijective.

Démonstration : Si $x_1, \ldots, x_n$ sont les fonctions coordonnées sur V, tout point P de Vest caractérisé par ses coordonnées $x_1(P), \ldots, x_n(P)$. Si $\varphi : W \longrightarrow V$ est une application polynomiale, alors pour tout $i = 1, \ldots, n$ et tout $Q \in W$, on a $\varphi^*(x_i)(Q) = x_i(\varphi(Q))$. On voit donc que φ est caractérisée par les fonctions $\varphi^*(x_n), \ldots, \varphi^*(x_n)$ et donc par φ^*. Cela montre que l'application $\varphi \longmapsto \varphi^*$ est injective et il reste à vérifier que celle ci est surjective. Si $u : k[V] \longrightarrow k[W]$ est un homomorphisme de k-algèbres et $F \in k[X_1, \ldots, X_n]$, on a $F(u(x_1), \ldots, u(x_n)) = u(F(x_1, \ldots, x_n))$. Si $F \in I(V)$, alors $F(x_1, \ldots, x_n) = F_{|V} = 0$ et on a donc

$F(u(x_1), \ldots, u(x_n)) = u(0) = 0$. On voit donc que si $Q \in W$ et $P := (u(x_1)(Q), \ldots, u(x_n)(Q))$, on a $F(P) = F(u(x_1)(Q), \ldots, u(x_n)(Q))) = F(u(x_1), \ldots, u(x_n))(Q) = 0$, ce qui signifie que $P \in V$. On définit ainsi une application $\varphi : W \longrightarrow V$, $Q \longmapsto P$. Celle ci est polyunomiale par construction. Pour tout $i = 1, \ldots, n$, on a $u(x_i) = x_i \circ \varphi = \varphi^*(x_i)$. Puisque $k[V]$ est isomorphe à un quotient de $k[X_1, \ldots, X_n]$, l'homomorphisme de k-algèbres u est caractérisé par les $u(x_i)$ pour $i = 1, \ldots, n$ et on a donc $u = \varphi^*$.

Corollaire Une application polynomiale φ est un isomorphisme si et seulement si φ^* est bijective.

Si φ est un isomorphisme, il existe une application polynomiale ψ telle que $\varphi \circ \psi = Id$ et $\psi \circ \varphi = Id$. On a donc $\varphi^* \circ \psi^* = (\psi \circ \varphi)^* = Id^* = Id$ et $\psi^* \circ \varphi^* = (\varphi \circ \psi)^* = Id^* = Id$. Réciproquement, si φ^* est bijective, c'est un isomorphisme et il existe donc un homomorphisme de k-algèbres v tel que $v \circ \varphi^* = Id$ et $\varphi^* \circ v = Id$. Il existe alors une application polynomiale ψ telle que $u = \psi^*$ et on a donc $(\varphi \circ \psi)^* = \psi^* \circ \varphi^* = Id$ et $(\psi \circ \varphi)^* = \varphi^* \circ \psi^* = Id$ si bien que $\varphi \circ \psi = Id$ et $\psi \circ \varphi = Id$.

Corollaire Deux ensembles algébriques affines sont isomorphes si et seulement si leurs anneaux de coordonnées sont isomorphes.

Soient V et W deux ensembles algébriques. Si $\varphi : W \longrightarrow V$ est un isomorphisme, il en va de même de φ^*. Réciproquement, si u est un isomorphisme entre $k[V]$ et $k[W]$ il existe une application polynomiale $\varphi : W \longrightarrow V$ telle que $\varphi^* = u$ et c'est un isomorphisme.

2.4.3. Proposition Soit $\varphi : W \longrightarrow V$ une application polynomiale. Alors,

(i) $Ker\, \varphi^* = I_V(\varphi(W))$.

(ii) φ^* est injectif si et seulement si φ est dominante.

(iii) φ^* est surjectif si et seulement si φ est une immersion fermée

Démonstration : i) Par définition, on a $f \in Ker\, \varphi^*$ si et seulement si $\varphi^*(f) = 0$, c'est à dire $f \circ \varphi = 0$, ce qui signifie que f est nul sur $\varphi(W)$. On voit donc que $Ker\, \varphi^* = I_V(\varphi(W))$.

ii) Dire que φ est dominante signifie que la fermeture algébrique de $\varphi(W)$ dans V est V, c'est a dire que $V(I_V(\varphi(W)) = V$, ce qui est équivalent à dire que $Ker\, \varphi^* = I_V(\varphi(W) = I_V(V(I_V(\varphi(W))) = I_V(V) = 0$.

iii) Si V' est la fermeture algébrique de $\varphi(W)$ dans V, l'application φ se factorise en $\psi : W \longrightarrow V'$ (qui est dominante) suivi de l'inclusion $i : V' \hookrightarrow V$. Il suit que φ est une immersion fermée si et seulement si ψ est un isomorphisme, c'est à dire, si et seulement si ψ^* est bijective. Puisque ψ est dominante, ψ^* est injective et on voit donc que φ est une immersion fermée si et seulement si ψ^* est surjective. Puisque φ^* se factorise en i^* qui est surjective, suivie de ψ^* , cette condition est équivalente à dire que φ^* est surjective.

Corollaire Si V est un ensemble algébrique affine, les idéaux $\mathfrak{m}$ de $k[V]$ de la forme $I_V(P)$ où P est un point de V sont les idéaux satisfaisant $k[V]/\mathfrak{m} \cong k$.

Si $P \in V$, alors $k[V]/I_V(P) \cong k[P] \cong k$. Réciproquement, si $\mathfrak{m}$ est un idéal tel que $k[V]/\mathfrak{m} \cong k$, il existe une unique immersion fermée $i : \mathbb{A}^0 = \{O\} \hookrightarrow V$ telle que l'homomorphisme composé de $i^* : k[V] \longrightarrow k$ et de l'isomorphisme $k \cong k[V]/\mathfrak{m}$ soit l'homomorphisme quotient associé à $\mathfrak{m}$. On a alors, en posant $P := i(O)$,

$f \in \mathfrak{m}$ ssi $i^*(f) = 0$
$f \in \mathfrak{m}$ ssi $f(P) = f(i(O)) = i^*(f)(O) = 0$.
$f \in \mathfrak{m}$ ssi $f \in I_V(P)$.

2.4.4. Changement de coordonnées

• Si $\Phi : \mathbb{A}^m \longrightarrow \mathbb{A}^n$ est une application affine et $F \in k[X_1, \ldots, X_n]$, on a $deg\ \Phi^*(F) \leq deg\ F$: Comme Φ^* est un homomorphisme d'algèbre, les propriétés du degré nous permettent de supposer que $F = X_i$. Or les composantes $L_1, \ldots, L_n$ de Φ sont des polynômes de degré au plus 1 et on a $\Phi^*(X_i) = L_i$.

• Si $\Phi : \mathbb{A}^n \longrightarrow \mathbb{A}^n$ est une application affine bijective et $F \in k[X_1, \ldots, X_n]$, on a $deg\ \Phi^*(F) = deg\ F$: En effet, Φ^{-1} est aussi affine.

• Si $\Phi : k^{m+1} \longrightarrow k^{n+1}$ est une application linéaire et $F \in k[X_1, \ldots, X_n]$ homogène de degré d, alors $\Phi^*(F)$ est homogène de degré d ou nul : Comme Φ^* est un homomorphisme d'algèbre, les propriétés du degré nous permettent de supposer que $F = X_i$. Or les composantes $L_1, \ldots, L_n$ de Φ sont des formes linéaires et on a $\Phi^*(X_i) = L_i$..

• Si Φ est un changement de coordonnées (affines ou projectives) et V une hypersurface, alors $\Phi^{-1}(V)$ est une hypersurface de même degré. En fait, $\Phi^{-1}(V(F)) = V(\Phi^*(F))$ dans le cas affine et $\Phi^{-1}(V_p(F)) = V_p(\Phi^*(F))$ dans le cas

projectif : Le cas affine est immédiat. Dans le cas projectif non vide, on a $C(V) = C(V_p(F)) = V(F)$ et donc $C(\Phi^{-1}(V)) = \Phi^{-1}(C(V)) = \Phi^{-1}(V(F)) = V(\Phi^*(F)) = C(V_p(\Phi^*(F))$. Enfin, si $V_p(F))$ ou $V_p(\Phi^*(F)$ est vide, le résultat est immédiat.

2.5. Composantes irréductibles d'un ensemble algébrique

2.5.1. Proposition Pour un ensemble algébrique (affine ou projectif) V, les conditions suivantes sont équivalentes :

(a) V est irréductible

(b) $I(V)$ est un idéal premier

(c) $k[V]$ est un anneau intègre

Démonstration : Cas affine : Si V est irréductible et si $F, G \in k[X_1, \ldots, X_n]$ sont tels que $FG \in I(V)$, alors $V = V(I(V)) \subset V(FG) = V(F) \cap V(G)$ si bien que $V \subset V(F)$ (ou $V(G)$) et donc $F \in I(V(F)) \subset I(V)$. On voit donc que $I(V)$ est premier. Si $I(V)$ est premier, alors $k[V] \cong k[X_1, \ldots, X_n]/I(V)$ est intègre. Enfin, si $k[V]$ est intègre et si $V = W \cup Z$, alors $0 = I_V(V) = I_V(W \cup Z) = I_V(W) \cap I_V(Z) \supset I_V(W)I_V(Z)$ si bien que $I_V(W)$ (ou $I_V(Z)) = 0$ et donc $W = V(I_V(W)) = V(0) = V$. On voit donc que V est irréductible.

Cas projectif : On sait que V est irréductible si et seulement si $C(V)$ est irréductible, que $I(V) = I(C(V))$ et que $k[V] = k[C(V)]$.

2.5.2. Théorème Outre les points, les sous ensembles algébriques irréductibles propres du plan (*affine* ou *projectif*) sont les courbes planes infinies de la forme $C = V(F)$ (ou $V_p(F)$ dans le cas projectif) avec F irréductible. On a alors $I(C) = (F)$.

Démonstration : Cas affine : Nous avons déjà vu que la condition est suffisante. Montrons qu'elle est nécessaire. Si C est un sous ensemble algébrique irréductible infini propre du plan affine, alors $I(C)$ est un idéal premier propre et contient donc un polynôme irréductible F si bien que $C \subset V(F)$. Puisque C est infini, on a nécessairement $C = V(F)$. Si $G \in I(C)$, alors $C \subset V(F, G)$ qui est donc infini, ce qui implique que F et G ont un facteur commun. Comme F est irréductible, ceci signifie que F divise G. On a donc bien $I(C) = (F)$.

Cas projectif : On peut, quitte à faire un changement de coordonnées, supposer que $\mathbb{P}^1 \not\subset C$. Montrons que la condition est suffisante et qu'alors $I(C) = (F)$: Le lieu à l'infini de C est alors un fermé propre de $\mathbb{P}^1$, c'est à dire un ensemble fini. Puisque C est infinie, C_* est nécessairement infinie. D'autre part,

puisque $\mathbb{P}^1 \not\subset C$, on a $F \neq cZ$ et on a vu que dans ce cas, F_* est irréductible et que $F = (F_*)^*$. On voit donc que $C_* = V(F_*)$ est infinie et que F_* est irréductible. On sait qu'alors C_* est irréductible et que $I(C_*) = (F_*)$. On a donc $I((C_*)^*) = I(C_*)^* = (F_*)^* = (F_*{}^*) = (F)$. Il suit que $(C_*)^* = V_p(F) = C$ si bien que C est irréductible et $I(C) = (F)$. Il reste à vérifier que la condition est nécessaire. Soit C un sous ensemble algébrique irréductible propre infini du plan projectif. Puisque $\mathbb{P}^1 \not\subset C$, on a $C = (C_*)^*$ et C_* est un sous ensemble algébrique irréductible, nécessairement propre (puisque C l'est) et infini (puisque C l'est) du plan affine. On a donc $I(C_*) = (F)$ avec F irréductible et donc $C = V_p(I(C)) = V_p(I((C_*)^*)) = V_p(I(C_*)^*) = V_p((F)^*) = V_p(F^*)$ avec F^* (homogène) irréductible.

2.5.3. La notion d'anneau noetherien nous permet de ramener l'étude d'un ensemble algébrique à celle d'un nombre fini d'hypersurfaces irréductibles :

• Si V est un ensemble algébrique (affine ou projectif), alors $k[V]$ est un anneau noetherien : Nous avons vu que $k[V]$ est une algèbre de type fini sur un corps.

• Tout ensemble algébrique (affine ou projectif) non vide est intersection finie d'hypersurfaces : Tout idéal possède un nombre fini de générateurs.

2.5.4. Théorème Un ensemble algébrique (affine ou projectif) est noetherien. Il s'écrit donc de manière unique comme réunion finie d'ensembles algébriques irréductibles V_i avec $V_i \not\subset V_j$ pour $i \neq j$.

Démonstration : Si $\{V_i\}_{i\in\mathbb{N}}$ est une suite décroissante de fermés de V, alors $\{I(V_i)\}_{i\in\mathbb{N}}$ est une suite croissante d'idéaux de $k[V]$ qui est un anneau noetherien. Il existe donc un entier N tel que $I(V_i) = I(V_N)$ pour $i \geq N$ si bien que $V_i = V_N$ pour $i \geq N$.

• Si V est un ensemble algébrique projectif dont aucune composante irréductible n'est contenue dans $\mathbb{P}^{n-1}$, alors $(V_*)^* = V$: Les applications $_*$ et * préservent les unions finies.

• Si V est un ensemble algébrique affine, les composantes irréductibles de V^* sont les V_i^* où les V_i sont les composantes irréductibles de V : Même argument.

2.6. Fonctions rationnelles sur un ensemble algébrique affine

2.6.1. Définitions Si V est un ensemble algébrique affine irréductible, une *fonction rationnelle* sur V est un élément f du corps des fractions $k(V)$ de $k[V]$. Si $f = g/h$ avec $g, h \in k[V]$ et $P \in V$ avec $h(P) \neq 0$, on dit que f est *régulière* en P et on pose $f(P) = g(P)/h(P)$. Sinon, on dit que P est un *pôle* de f. On note $\mathcal{O}_{V,P}$ l'ensemble des fonctions régulières en P. Si f est régulière et s'annule en P, on dit que P est un *zéro* de f. On note $\mathfrak{m}_{V,P}$ l'ensemble des fonctions régulières en P qui s'annulent en P.

• Cette définition à bien un sens : Si $f = g'/h'$ avec $h'(P) \neq 0$, alors $gh' = g'h$ et $g(P)h'(P) = (gh')(P) = (g'h)(P) = g'(P)h(P)$ si bien que $f(P) = g(P)/h(P) = g'(P)/h'(P)$.

• Si $f \in k(V)$, alors $I_f := \{h \in k[V],\ hf \in k[V]\}$ est un idéal de $k[V]$ et l'ensemble des pôles de f est le *fermé* $V(I_f)$: Si h_1 et $h_2 \in I_f$, on a $(h_1 + h_2)f = h_1f + h_2f \in k[V]$ et si $h_1 \in k[V]$ et $h_2 \in I_f$, on a $(h_1h_2)f = h_1(h_2f) \in k[V]$. On voit donc que I_f est un idéal. Si $h \in k[V]$ est non nul, dire que $h \in I_f$ signifie que l'on peut écrire $f = g/h$ avec $g \in k[V]$. On a donc

$P \notin V(I_f)$ ssi $\exists\ h \in I_f,\ h(P) \neq 0$

$P \notin V(I_f)$ ssi $\exists\ g, h \in k[V],\ f = g/h$ et $h(P) \neq 0$.

• Si $k[V]$ est factoriel et $f = g/h$ avec g et $h \in k[V]$ sans facteur commun, alors $I_f = (h)$: Puisque $hf = g \in k[V]$, on a $h \in I_f$. Réciproquement, si $h' \in I_f$, alors $g' := h'f \in k[V]$, et on a $gh' = hg'$. Comme g et h sont premiers entre eux, h divise h' et donc $h' \in I_f$.

• Soit $f \neq 0$ régulière en P. Alors, f a un zéro en P si et seulement si $1/f$ à un pôle en P : Supposons que $f = g/h$ avec $h(P) \neq 0$. Si $1/f$ est régulière en P, on peut écrire $1/f = h'/g'$ avec $g'(P) \neq 0$. On a donc $gh' = g'h$, si bien que $g(P)h'(P) = g'(P)h(P) \neq 0$ et donc $g(P) \neq 0$. On voit donc que P n'est pas un zéro de f. Réciproquement, si $1/f = h/g$ n'est pas régulière en P, alors $g(P) = 0$, ce qui montre que P est un zéro de f.

• L'ensemble des points où $f \in k(V)$ est régulière et ne s'annule pas est un ouvert de V : En effet, c'est le complémentaire de $V(I_f) \cup V(I_{1/f})$.

2.6.2. Proposition Si V est un ensemble algébrique irréductible affine et P un

point de V, alors $\mathcal{O}_{V,P}$ est un anneau local intègre noetherien d'idéal maximal $\mathfrak{m}_{V,P}$. En fait, si $\mathfrak{m} := I_V(P)$, alors $\mathcal{O}_{V,P} = k[V]_{\mathfrak{m}}$.

Démonstration : Par définition, on a

$f \in \mathcal{O}_{V,P}$ ssi $\exists\, g, h \in k[V], f = g/h$ *et* $h(P) \neq 0$

$f \in \mathcal{O}_{V,P}$ ssi $\exists\, g,h \in k[V], h \notin \mathfrak{m}, f = g/h$

$f \in \mathcal{O}_{V,P}$ ssi $f \in k[V]_{\mathfrak{m}}$,

si bien que $\mathcal{O}_{V,P} = k[V]_{\mathfrak{m}}$. C'est donc un anneau local intègre noetherien d'idéal maximal est $\mathfrak{m}k[V]_{\mathfrak{m}}$. De plus, on a

$f \in \mathfrak{m}k[V]_{\mathfrak{m}}$ ssi $\exists\, g, h \in k[V], g \in \mathfrak{m}, h \notin \mathfrak{m}, f = g/h$

$f \in \mathfrak{m}k[V]_{\mathfrak{m}}$ ssi $\exists\, g, h \in k[V], g(P) = 0, h(P) \neq 0, f = g/h$

$f \in \mathfrak{m}k[V]_{\mathfrak{m}}$ ssi $f(P) = 0$

$f \in \mathfrak{m}k[V]_{\mathfrak{m}}$ ssi $f \in \mathfrak{m}_{V,P}$

si bien que $\mathfrak{m}k[V]_{\mathfrak{m}} = f \in \mathfrak{m}_{V,P}$.

2.6.3. Dans certains cas, on peut "composer" des fonctions rationnelles avec des applications polynomiales :

• Si $\varphi : W \longrightarrow V$ est une application polynomiale *dominante* entre deux ensembles algébriques affines irréductibles, alors φ^* se prolonge de manière unique en un homomorphisme de corps $\varphi^* : k(V) \hookrightarrow k(W)$: En effet, on sait que $\varphi^* : k[V] \longrightarrow k[W]$ est injective.

• Si f est régulière en $P := \varphi(Q)$ avec φ comme ci dessus, alors $\varphi^*(f)$ est régulière en Q et on a $\varphi^*(f)(Q) = f(P)$: On peut écrire $f = g/h$ avec $h(P)) \neq 0$. On a donc $\varphi^*(f) = \varphi^*(g)/\varphi^*(h)$ et $\varphi^*(h)(Q) = h(P) \neq 0$, ce qui montre que $\varphi^*(f)$ est régulière en Q. De plus, $\varphi^*(f)(Q) = \varphi^*(g)(Q)/\varphi^*(h)(Q) = g(P)/h(P) = f(P)$.

• Soit $\varphi : W \longrightarrow V$ une application polynomiale entre deux ensembles algébriques affines, Q un point de W et $P := \varphi(Q)$. Alors $\varphi^{*-1}(I_W(Q)) = I_V(P)$: On a

$f \in \varphi^{*-1}(I_W(Q))$ ssi $\varphi^*(f) \in I_W(Q)$

$f \in \varphi^{*-1}(I_W(Q))$ ssi $f(P) = f(\varphi(Q)) = \varphi^*(f)(Q) = 0$

$f \in \varphi^{*-1}(I_W(Q))$ ssi $f \in I_V(P)$.

• Soit $\varphi : W \longrightarrow V$ une application polynomiale entre deux ensembles algébriques affines irréductibles, $Q \in W$ et $P = \varphi(Q)$. Alors, φ^* se prolonge de manière unique en un homomorphisme $\varphi^*_Q : \mathcal{O}_{V,P} \longrightarrow \mathcal{O}_{W,Q}$: Si on pose $I_V(P) = \mathfrak{m}$ et $I_W(P) = \mathfrak{n}$, on sait que $\varphi^{*-1}(\mathfrak{n}) = \mathfrak{m}$, que $\mathcal{O}_{V,P} = k[V]_{\mathfrak{m}}$ et que $\mathcal{O}_{W,Q} = k[V]_{\mathfrak{n}}$.

• Si φ est dominante, une immersion fermée ou un isomorphisme, alors φ_Q^* est injective, bijective ou surjective : Cela résulte du fait que φ^* injective, bijective ou surjective.

• Soit V un sous ensemble algébrique irréductible $\mathbb{A}^n$ de et $i : V \hookrightarrow \mathbb{A}^n$ le morphisme d'inclusion. Si $P \in V$ et J est un idéal de $k[X_1, \ldots, X_n]$, alors l'application canonique $\mathcal{O}_{\mathbb{A}^n,P} \longrightarrow \mathcal{O}_{V,P}$ induit un isomorphisme $\mathcal{O}_{\mathbb{A}^n,P}/(J + I(V))\mathcal{O}_{\mathbb{A}^n,P} \tilde{=} \mathcal{O}_{V,P}/i^*(J)\mathcal{O}_{V,P}$. En particulier, on a toujours $\mathcal{O}_{\mathbb{A}^n,P}/I(V)\mathcal{O}_{\mathbb{A}^n,P} \tilde{=} \mathcal{O}_{V,P}$: L'application est surjective car composée d'applications surjectives. Montrons qu'elle est injective : Soient $F, G \in k[X_1, \ldots, X_n]$ avec $F(P) \neq 0$. Si $i^*(F)/\, i^*(G) \in i^*(J)\mathcal{O}_{V,P}$, on peut écrire $i^*(F)/\, i^*(G) = i^*(F_1)/\, i^*(G_1)$ avec $F_1 \in J$ et $G_1(P) \neq 0$. Posons $H := FG_1 - F_1G$. On a $i^*(H) = i^*(F)\, i^*(G_1) - i^*(F_1)/\, i^*(G)) = 0$ et donc $H \in Ker\, i^* = I(V)$. On a donc $F/G = FG_1/GG_1 = (H + GF_1)/GG_1 \in (I(V) + J)\mathcal{O}_{\mathbb{A}^n,P}$.

2.6.4. Définition Soit V un ensemble algébrique affine irréductible. Une application polynomiale $j : W \longrightarrow V$ est une *immersion ouverte* si

i) C'est un homéomorphisme de W sur un ouvert U de V et

ii) Pour tout $Q \in W$, l'application j_Q^* est un isomorphisme $\mathcal{O}_{V,j(Q)} \tilde{\to} \mathcal{O}_{W,Q}$.

On dit alors que U est un *ouvert affine* de V.

• Si V est un ensemble algébrique affine irréductible et U un ouvert de V, l'ensemble $\Gamma(U)$ des fonctions régulières sur U est une k-algèbre intègre et on a $\Gamma(U) = \bigcap_{P \in U} \mathcal{O}_{V,P}$: La seconde assertion résulte immédiatement des définitions et la première est une conséquence de la seconde.

• On a pas toujours $\Gamma(U) = \{f/g, \forall\, P \in U, g(P) \neq 0\}$. Par exemple, si $V = V(XT - YZ)$ et $U = \{(a, b, c, d) \in V, a \neq 0 \text{ ou } c \neq 0\}$, alors $y/x \in \Gamma(U)$.

• Dans la définition d'une immersion ouverte, on peut remplacer la condition ii) par la condition

ii)' L'homomorphisme j^* induit un isomorphisme entre $\Gamma(U)$ et $\Gamma(W)$:

La remarque précédente nous dit que cette condition est plus faible que la condition ii). Réciproquement, supposons cette condition remplie et choisissons $Q \in W$. Si $f \in k[W]$, on peut écrire, puisque j^* induit un isomorphisme entre $\Gamma(U)$ et $\Gamma(W)$, $f = j^*(\varphi)$ avec $\varphi \in \Gamma(U)$. De même, si $g \in k[W]$ et $g(Q) \neq 0$, on peut écrire $g = j^*(\psi)$ avec $\psi \in \Gamma(U)$ et $\psi(j(Q)) = j^*(\psi)(Q) = g(Q) \neq 0$ si bien que ψ est inversible dans $\mathcal{O}_{V,j(Q)}$. On voit donc que si $h = f/g \in \mathcal{O}_{W,Q}$, on peut écrire $h = j^*(\psi^{-1}\varphi)$ avec $\psi^{-1}\varphi \in \mathcal{O}_{V,j(Q)}$. Cela montre que j_Q^* est surjective. Enfin,

j^*_Q est injective car j est dominante.26 avril 1995

• Dans la définition d'une immersion ouverte, on peut remplacer la condition i) par la condition

i)' L'application j est une bijection de W sur U :

Bien sûr, cette condition est plus faible que la condition i). Réciproquement, soit $f \in k[W]$ et $P \in U$. On écrit $P = j(Q)$ avec $Q \in W$ et $f = j^*(\varphi)$ avec $\varphi \in \Gamma(U)$. On a donc $P \in j(D(f))$ si et seulement si $Q \in D(f)$, ce qui signifie que $\varphi(P) = \varphi(j(Q)) = j^*(\varphi)(Q) = f(Q) \neq 0$. On voit donc que $j(D(f))$ est l'ensemble des points de U où φ ne s'annule pas qui est ouvert. On en déduit que j est une application ouverte. Comme j est bijective et continue, c'est un homéomorphisme sur U.

• Si $G \in k[X_1, \ldots, X_n]$, la projection $p : \mathbb{A}^{n+1} \longrightarrow \mathbb{A}^n$ induit une immersion ouverte $j : W = V(GX_{n+1} - 1) \hookrightarrow \mathbb{A}^n$: On a $(a_1, \ldots, a_{n+1}) \in W$ si et seulement si $G(a_1, \ldots, a_n) \neq 0$ et alors $a_{n+1} = G(a_1, \ldots, a_n)$. On voit donc que j est une bijection de W sur $D(G)$. De plus, si $f \in k[W]$ se prolonge en $F \in k[X_1, \ldots, X_{n+1}]$, alors $\varphi := F(X_1, \ldots, X_n, 1/G) \in \Gamma(U)$ et $f = j^*(\varphi)$. On en déduit aisément que j^* induit une bijection entre $\Gamma(U)$ et $\Gamma(W)$.

2.7. Fonctions rationnelles sur un ensemble algébrique projectif

2.7.1. Définitions Soit V un ensemble algébrique projectif irréductible. Le corps $k(V)$ des *fonctions rationnelles* sur V est l'ensembles formé de 0 et des éléments homogènes f de degré nul du corps des fractions de $k[V]$. Si $f = g/h$ avec g et h homogènes de même degré et $P := (a_1; \ldots; a_{n+1})$ tel que $h(P) \neq 0$, on dit que f est *régulière en* P et on pose $f(P) = g(a_1, \ldots, a_{n+1})/h(a_1, \ldots, a_{n+1})$. Sinon, on dit que P est un *pôle* de f. On note $\mathcal{O}_{V,P}$ l'ensemble des fonctions régulières en P. Si f est régulière et s'annule en P, on dit que P est un *zéro* de f. On note $\mathfrak{m}_{V,P}$ l'ensemble des fonctions régulières en P qui s'annulent en P.

• Cette définition à bien un sens : Tout d'abord, si g et h sont de degré d et si $\lambda \in k$, on a $h(\lambda a_1, \ldots, \lambda a_{n+1}) = \lambda^d h(a_1, \ldots, a_{n+1}) \neq 0$ si bien que f est régulière en $(\lambda a_1, \ldots, \lambda a_{n+1})$ et $f(\lambda a_1, \ldots, \lambda a_{n+1}) = g(\lambda a_1, \ldots, \lambda a_{n+1})/h(\lambda a_1, \ldots, \lambda a_{n+1}) = \lambda^d h(a_1, \ldots, a_{n+1})/\lambda^d h(a_1, \ldots, a_{n+1}) = g(a_1, \ldots, a_{n+1})/h(a_1, \ldots, a_{n+1}) = f(a_1, \ldots, a_{n+1})$. Il faut aussi remarquer que si $f = g'/h'$ avec g' et h' homogènes de même degré et $h'(P) \neq 0$, alors $g(P)/h(P) = g'(P)/h'(P)$.

• Soit $f \in k(V)$. Alors, f est régulière en $(a_1, \ldots, a_{n+1}) \in C(V)$ si et seulement si f est régulière en $(a_1; \ldots; a_{n+1})$ et on a $f(a_1; \ldots; a_{n+1}) = f(a_1, \ldots, a_{n+1})$: La condition est clairemetn suffisante. Réciproquement, on peut écrire $f = g/h$ avec $h(a_1, \ldots, a_{n+1}) \neq 0$. D'autre part, comme $f \in k(V)$, on peut aussi écrire $f = g'/h'$ avec g' et h' homogènes de même degré. Si on note avec un indice i la composante homogène de degré i d'un élément de $k[V]$, il existe d tel que $h_d(a_1, \ldots, a_{n+1}) \neq 0$ et puisque A est une algèbre homogène, on a nécessairement $h_d g' = h' g_d$ si bien que $f = g_d/h_d$.

• Si $P = (a_1; \ldots; a_{n+1})$ et $P' = (a_1, \ldots, a_{n+1})$, on a $\mathcal{O}_{V,P} = k(V) \cap \mathcal{O}_{C(V),P'}$ et $\mathfrak{m}_{V,P} = k(V) \cap \mathfrak{m}_{C(V),P}$. En particulier, $\mathcal{O}_{V,P}$ est un anneau local intègre d'idéal maximal $\mathfrak{m}_{V,P}$: Cela résulte de la remarque précédente.

2.7.2. Les fonctions rationnelles se comportent bien par rapport aux changement de coordonnées :

• Soit Φ un changement de coordonnées projectives, V un ensemble algébrique projectif, $W := \Phi^{-1}(V)$ et $\varphi : W \longrightarrow V$ la bijection induite. Alors, l'isomorphisme canonique $k(C(V)) \xrightarrow{\sim} k(C(W))$ induit un isomorphisme $\varphi^* : k(V) \xrightarrow{\sim} k(W)$: On note encore $\varphi : C(W) \longrightarrow C(V)$, l'application induite par Φ. On sait alors que si $f \in k[V]$ est l'image de $F \in k[X_1, \ldots, X_{n+1}]$, alors $\varphi^*(f)$ est l'image de $\Phi^*(F)$ dans $k[W]$. On sait aussi que F est homogène de degré d si et seulement si $\Phi^*(F)$ l'est. On voit donc que l'isomorphisme $\varphi^* : k[V] \xrightarrow{\sim} k[W]$ préserve les éléments homogènes et leur degré. On obtient donc bien un isomorphisme $\varphi^* : k(V) \xrightarrow{\sim} k(W)$.

• L'isomorphisme $\varphi^* : k(V) \xrightarrow{\sim} k(W)$ est bien défini : Si on multiplie Φ par $\lambda \in k^\times$, l'isomorphisme obtenu $k[V] \xrightarrow{\sim} k[W]$ envoie f homogène de degré d sur $\lambda^d \varphi^*(f)$. On voit donc que si g est aussi homogène de degré d, alors f/g est envoyé sur $\lambda^d \varphi^*(f)/\lambda^d \varphi^*(g) = \varphi^*(f)/\varphi^*(g)$.

• Si $Q \in W$ et $P := \varphi(Q)$, alors φ^* induit un isomorphisme $\varphi_Q^* : \mathcal{O}_{V,P} \xrightarrow{\sim} \mathcal{O}_{W,Q}$: Si $Q = (a_1; \ldots; a_{n+1})$, $Q' = (a_1, \ldots, a_{n+1})$ et $P' := \varphi(Q')$, on sait que φ induit un isomorphisme entre $\mathcal{O}_{C(V),P'}$ et $\mathcal{O}_{C(W),Q'}$ et donc aussi entre $\mathcal{O}_{V,P} = k(V) \cap \mathcal{O}_{C(V),P'}$ et $\mathcal{O}_{W,Q} = k(W) \cap \mathcal{O}_{C(W),Q'}$.

2.7.3. Les fonctions rationnelles se comportent aussi bien par passage à la fermeture projective ou à la partie affine :

• Si V est un ensemble algébrique affine, l'homomorphisme $F \longmapsto F_*$ induit un homomorphisme d'anneaux $f \longmapsto f_*$, $k[V^*] \longrightarrow k[V]$: En effet, on sait que si $F \in I_p(V^*) = I(V)^*$, alors $F_* \in I(V)$.

• Tout élément non nul de $k[V]$ se met sous la forme f_* avec f homogène : On sait que tout élément de $k[X_1, \ldots, X_n]$ se met sous la forme F_* avec F homogène.

• Si V est irréductible, l'homomorphisme $f \longmapsto f_*$, induit un isomorphisme de corps $f = g/h \longmapsto f_* = g_*/h_*$, $k(V^*) \xrightarrow{\sim} k(V)$: Il faut d'abord s'assurer que si h est homogène et $h_* = 0$, alors $h = 0$. Cela résulte du fait que pour H homogène, on a $H \in I(V^*) = I(V)^*$ si et seulement si $H_* \in I(V)$. De plus,comme l'application $f \longmapsto f_*$, $k[V^*] \longrightarrow k[V]$ est un homomomorphisme d'anneaux, il est clair que si $g/h = g'/h'$ alors $g_*/h_* = g'_*/h$ et notre application est donc bien définie. Le même argument nous montre que l'on a bien un homomorphisme de corps. Il reste à vérifier que celui ci est surjectif. Or tout élément de $k(V)$ se met sous la forme f_*/g_* avec f et g homogènes. Quitte à multiplier en haut ou en bas par une puissance de x_{n+1}, on peut supposer que f et g ont même degré.

• L'isomorphisme de corps $f \longmapsto f_*$, $k(V^*) \xrightarrow{\sim} k(V)$ induit pour tout $P \in V$, un isomorphisme $\mathcal{O}_{V^*,P} \xrightarrow{\sim} \mathcal{O}_{V,P}$: Si $f = g/h \in k(V^*)$, avec g et h homogènes, alors $f_* := g_*/h_*$ et on a $h(P) \neq 0$ si et seulement si $h_*(P) \neq 0$.

• Si V un ensemble algébrique irréductible et P un point de V, alors $\mathcal{O}_{V,P}$ est un anneau local intègre noetherien d'idéal maximal $\mathfrak{m}_{V,P}$: Dans le cas projectif, on peut, quitte à faire un changement de coordonnées, supposer que $P \in \mathbb{A}^n$. Le résultat précédent nous permet alors de nous ramener au cas affine qui a déjà été traité.

COURBES ALGEBRIQUES

(Bernard Le Stum)

CHAPITRE 2 - EXERCICES

2.1. Idéal d'un ensemble algébrique affine

2.1.1. ($k = \mathbb{R}$) Quel est l'idéal de $V(X^2 + 1) \subset \mathbb{A}^1$.

2.1.2. ($k = \mathbb{R}$) Idem pour $V(X^2 + Y^2) \subset \mathbb{A}^2$.

2.1.3. ($k = \mathbb{R}$) Idem pour $V(X^2 + Y^2 + 1) \subset \mathbb{A}^2$.

2.1.4. Idem pour $C := \{(t^2, t^3), t \in k\}$.

2.1.5. Idem pour $C := \{(t, t^2, t^3), t \in k\}$.

2.1.6. Idem pour $C = \{(t^2, t^2(t^2 - 1), t^3), t \in k\}$.

2.1.7. Idem avec $C = \{(t^9, t^6, t^4), t \in k\}$.

2.1.8. Idem avec $C = \{(t^2, t^3 - t^2, t^5), t \in k\}$.

2.1.9. Idem avec la courbe plane C d'équation $XY = 0$.

2.1.10. Idem avec la courbe plane C d'équation $XY(X - Y) = 0$.

2.1.11. Idem avec $V := V(XY, XZ, YZ) \subset \mathbb{A}^3$.

2.2. Idéal d'un ensemble algébrique projectif

2.2.1. Montrer que l'idéal de la courbe projective plane $C := \{(a^2; ab; b^2), a, b \in k, (a, b) \neq (0,0)\}$ est le noyau de l'homomorphisme

$$u : k[X, Y, Z] \longrightarrow k[X, Y], F \longmapsto F(X^2, XY, Y^2).$$

2.2.2. Montrer que l'idéal de la courbe projective $C := \{(a^3, a^2b, ab^2, b^3)), a, b \in k, (a, b) \neq (0,0)\}$ est le noyau de l'homomorphisme

$$u : k[X,Y,Z,T] \longrightarrow k[X,Y], F \longmapsto F(X^3, X^2Y, XY^2, Y^3).$$

2.2.3. Montrer que l'idéal de la surface de Veronese est le noyau de l'homomorphisme

$$u : k[X,Y,Z,T,W] \longrightarrow k[X,Y,Z], F \longmapsto F(X^2, XY, XZ, Y^2, YZ, Z^2).$$

2.2.4. Montrer que l'idéal de la surface $S := \{(ac, ad, bc, bd), a, b, c, d \in k, (a, b) \neq (0,0), (c, d) \neq (0,0)\}$ est le noyau de l'homomorphisme

$$u : k[X,Y,Z,T] \longrightarrow k[X,Y,Z,T], F \longmapsto F(XZ, XT, YZ, YT)).$$

2.2.5. Soit $C = \{(t, t^2, t^3), t \in k\} \subset \mathbb{A}^3$. Trouver des générateurs F et G de $I(C)$ et montrer que $C^* \neq V(F^*, G^*)$.

2.3. Anneau de coordonnées

2.3.1. Soient $V \subset \mathbb{A}^4$ l'hypersurface affine d'équation $XT = YZ$ et $f, g \in k[V]$ tels que $fx = gz$. Montrer que le plan(XOY) est contenu dans $V(f)$.

2.3.2. (*k algébriquement clos)* Soient $V \subset \mathbb{A}^4$ l'hypersurface affine d'équation $XT = YZ$. Montrer que le plan (XOY) n'est pas une hypersurface de V.

2.3.3. Soit C une courbe affine plane infinie d'équation $Y^2 = F$ avec $F \in k[X]$ (*F n'étant pas un carré*) et x et y les fonctions coordonnées sur C. Montrer que si $g \in k[C]$, il existe $A, B \in k[T]$ uniques tels que $g = A(x) + B(x)y$.

2.3.4. (*k algébriquement clos et car $k \neq 2$*) Soit C la courbe affine plane d'équation $4X^2 - (Y^2 + 4Y)X + Y^2$. Montrer que si $f \in k[C]$, il existe $G, H \in k[T]$ uniques tels que si $Q =: (a, c) \in C$, on ait $f(Q) = G(c) + aH(c)$.

2.4. Applications polynomiales

2.4.1. Soit $\Phi : \mathbb{A}^1 \longrightarrow \mathbb{A}^2$, $t \longmapsto (t^2, t^3)$ et $C = \Phi(\mathbb{A}^1)$. Montrer que Φ^* induit un isomorphisme entre $k[C]$ et l'algèbre des polynômes sans composante homogène de degré 1. En déduire que $k[C]$ n'est pas factoriel.

2.4.2. Montrer que la courbe C d'équation $Y^2 = X^3$ n'est pas isomorphe à la droite affine.

2.4.3. Montrer que l'application $\Phi : \mathbb{A}^1 \longrightarrow \mathbb{A}^3$, $t \longmapsto (\ t^2, t^2(t^2 - 1),\ t^3)$, n'est pas une immersion fermée.

2.4.4. ($k = \mathbb{R}$) Idem avec $\Phi : \mathbb{A}^1 \longrightarrow \mathbb{A}^2$, $t \longmapsto (t - t^4, 1 - t^3)$.

2.4.5. Idem avec $\Phi : \mathbb{A}^1 \longrightarrow \mathbb{A}^3$, $t \longmapsto (t^2,\ t^3 - t^2,\ t^5\ )$.

2.4.6. Soit $s : \mathbb{A}^2 \longrightarrow \mathbb{A}^2$, $(a, b) \longmapsto (-a, -b)$ la symétrie centrale de centre O et C la courbe affine plane d'équation $X^2Y^2 + X^2 + Y^2 = 2XY(X + Y + 1)$. Déterminer une équation de $s^{-1}(C)$.

2.4.7. ($Car\ k \neq 2$) Soit C la courbe affine plane d'équation $X^2Y^2 + X^2 + Y^2 = 2XY(X + Y + 1)$. Montrer que si $f \in k[C]$, il existe $G, H \in k[T]$ uniques tels que si $P =: (a, b) \in C$, on ait $f(P) = G(a + b - ab) + aH(a + b - ab)$.

2.5. Ensembles algébriques projectifs irréductibles

2.5.1. Montrer que la courbe projective plane $C := \{(a^2; ab; b^2),\ a, b \in k,\ (a, b) \neq (0,0)\}$ est irréductible.

2.5.2. Montrer que la courbe projective $C := \{(a^3; a^2b; ab^2; b^3)),\ a, b \in k,\ (a, b) \neq (0, 0)\}$ est irréductible.

2.5.3. Montrer que *la surface de Veronese* est irréductible.

2.5.4. Montrer que la surface $S := \{(ac; ad; bc; bd),\ a, b, c, d \in k,\ (a, b) \neq (0,0),\ (c, d) \neq (0,0)\}$ est irréductible.

2.5.5. Montrer que les surfaces projectives d'équations $XY = ZT$ et $X^2 = YT$ sont

irréductibles mais que leur intersection ne l'est pas.

2.6. Composantes irréductibles

2.6.1. Déterminer les composantes irréductibles de la courbe plane C d'équation $XY = 0$.

2.6.2. Déterminer les composantes irréductibles de la courbe plane C d'équation $XY(X - Y) = 0$.

2.6.3. Déterminer les composantes irréductibles de $V := V(XY, XZ, YZ) \subset \mathbb{A}^3$.

2.6.4. Quelles sont les composantes irréductibles de la courbe affine plane d'équation $Y^2 - XY - X^2Y + X^3 = 0$.

2.6.5. Déterminer les composantes irréductibles de l'intersection des courbes planes d'équations $Y^4 = X^2$ et $Y^4 = X^2Y^2 - XY^2 + X^3$.

2.6.6. Montrer que les composantes irréductibles de $V(X^3 - YZ,\ Y^2 - XZ) \subset \mathbb{A}^3$ sont la courbe $C := \{(t^3,\ t^4,\ t^5),\ t \in k\} \subset \mathbb{A}^3$ et une droite que l'on déterminera.

2.6.7. (*k algébriquement clos)* Soient S_1 et $S_2 \subset \mathbb{A}^3$ les cylindres d'équations respectives $X^2 + Y^2 = 1$ et $X^2 + Z^2 = 1$. Déterminer les composantes irréductibles de $C = S_1 \cap S_2$.

2.6.8. Idem avec les surfaces d'équations $X^2 + Y^2 = 1$ et $X^2 - Z^2 = 1$.

2.6.9. Soient $\lambda \in k$ et C la courbe affine plane d'équation $(X^2 + 1)Y^2 + (X^2 - \lambda)^2 = 0$. Déterminer suivant les valeurs de λ, les composantes irréductibles de C lorsque i) $k = \mathbb{C}$, ii) $k = \mathbb{R}$ et iii) $Car\ k = 2$.

2.6.10. (*k algébriquement clos)* Déterminer selon la valeur de $\lambda \in k$ les composantes irréductibles de la courbe d'équation $X^4 - Y^4 = \lambda X^3 - XY^2$.

2.6.11. Soit C une courbe plane telle que la projection $x : C \longrightarrow \mathbb{A}^1$ soit injective. Montrer que C est irréductible et que $I(C) = (F)$ avec F de degré 1 en Y.

2.7. Fonctions rationnelles (*k algébriquement clos)*

2.7.1. Soit C la courbe plane d'équation $Y^2 = X^2(X + 1)$, x et y les fonctions coordonnées sur C et $\varphi := y/x$. Déterminer les zéros et les pôles de φ et de φ^2.

2.7.2. Montrer que $\Gamma(\mathbb{A}^2\backslash 0) = \Gamma(\mathbb{A}^2) = k[X, Y]$. Existe-t-il des fonctions rationnelles sur $\mathbb{A}^2$ ayant un unique pôle à l'origine? $\mathbb{A}^2\backslash 0$ est il un ouvert affine de $\mathbb{A}^2$?

2.7.3. Soient $V \subset \mathbb{A}^4$ l'hypersurface d'équation $XT = YZ$, x, y, z et t les fonctions coordonnées sur V et $\varphi := x/z$. Déterminer les pôles de φ et montrer qu'il n'existe pas de $f, g \in k[V]$ tels que, si φ est régulière en P, on ait $\varphi(P) = g(P)/f(P)$.

2.7.4. ($Car\ k \neq 2$) Soient $\lambda \neq \pm 1$, C la courbe plane d'équation $X^4 - Y^4 = \lambda X^3 - XY^2$ et x et y les fonctions coordonnées sur C. Montrer que la fonction rationnelle $f = y^2/x$ n'est pas régulière en O mais que la fonction $f(1 - f)$ est régulière en tout point de C.

2.7.5. ($Car\ k \neq 0$) Soient C la courbe plane d'équation $Y^2 = X^3 - X$, x et y les fonctions coordonnées sur C, f'_x et f'_y les restrictions à C de $\frac{dF}{dX}$ et $\frac{dF}{dY}$, $t := -\frac{f'_x}{f'_y}$, $u := t^2 - 2x$ et $v := t(u - x) + y$ et C_0 l'ouvert de C défini par $y \neq 0$. Montrer que les fonctions rationnelles t, u et v sont régulières sur C_0.

2.7.6. Soient C la courbe d'équation $Y^2 = X^3 - X$, $V := C \times C$ et x, y, x', y' les fonctions coordonnées sur V. Montrer que

$$\frac{y'-y}{x'-x} = \frac{x^2+xx'+x'^2-1}{y+y'}.$$

2.7.7. ($Car\ k \neq 2$) Soient C la courbe d'équation $Y^2 = X^3 - X$, $V := C \times C$, $r := \frac{y'-y}{x'-x}$, $m := r^2 - (x + x')$, $n := r(m - x) + y$ et V_0 l'ouvert de V défini par $y + y' \neq 0$. Montrer que les fonctions m et n sont régulières sur V_0.

2.7.8. ($Car\ k \neq 2$) Soient C la courbe d'équation $Y^2 = X^3 - X$, x et y les fonctions coordonnées sur C, f'_x et f'_y les restrictions à C de $\frac{dF}{dX}$ et $\frac{dF}{dY}$, $t := -\frac{f'_x}{f'_y}$, $u := t^2 - 2x$, $v := t(u - x) + y$, $V := C \times C$, $r := \frac{y'-y}{x'-x}$, $m := r^2 - (x + x')$, $n := r(m - x) + y$ et

C_0 l'ouvert de C défini par $y \neq 0$. Montrer que si $P \in C_0$, alors $m(P, P) = u(P)$ et que $n(P, P) = v(P)$.

2.8. Anneaux de fonctions régulières (k algébriquement clos)

2.8.1. Soit $\varphi := (XY, Y) : \mathbb{A}^2 \longrightarrow \mathbb{A}^2$. Montrer que φ_P^* est un isomorphisme de $\mathcal{O}_{\mathbb{A}^2,\varphi(P)}$ sur $\mathcal{O}_{\mathbb{A}^2,P}$ lorsque P n'est pas sur l'axe des X.

2.8.2. Soient C la courbe plane d'équation $XY = 1$ et x la première coordonnée sur C. Montrer que pour tout $P \in C$, φ_P^* est un isomorphisme de $\mathcal{O}_{\mathbb{A}^1,x(P)}$ sur $\mathcal{O}_{C,P}$.

2.8.3. ($car\ k \neq 2$) Calculer $\Gamma(U)$ lorsque

$$U = \mathbb{A}^1 \backslash \{ 1, -1, i, -i \}.$$

2.8.4. Soit $U \subset \mathbb{A}^1$ un ouvert non vide, $R \in \Gamma(U)$ et $E := \{(a, R(a)),\ a \in U\}$ le graphe de R. Montrer que la fermeture algébrique de E dans $\mathbb{A}^2$ est de la forme $V(GY - F)$ avec F et $G \in k[X]$ premiers entre eux.

COURBES ALGEBRIQUES

(Bernard Le Stum)

CHAPITRE 2 - CORRIGES

2.1.6. On vérifie trivialement que $I := (Y - X(X-1),\ Z^2 - X^3) \subset I(C)$ et il ne reste donc plus qu'à montrer que $I(C) \subset I$. Comme Y (resp. Z^2) est congru modulo I à $X(X-1)$ (resp. X^3), tout polynôme en X, Y, Z est congru modulo I à un polynôme de la forme $F = A + ZB$ avec A et $B \in k[X]$. Si $F \in I(C)$, alors $A(T^2) + T^3 B(T^2)$ est identiquement nul. Pour des questions de degré, ceci implique immédiatement que $A = B = 0$, et donc que $F \in I$.

2.1.7. On vérifie trivialement que $I := (X^2 - Y^3,\ Y^2 - Z^3) \subset I(C)$ et il ne reste donc plus qu'à montrer que $I(C) \subset I$. Soit $F \in I(C)$. Comme $X^2 = YZ^3 \ mod\ I$ et $Y^2 = Z^3 \ mod\ I$, on peut écrire

$$F = P + XQ + YR + XYS \ mod\ I$$

avec $P, Q, R, S \in k[Z]$. On en déduit que

$$0 = P(T^4) + T^9 Q(T^4) + T^6 R(T^4) + T^{15} S(T^4)\ .$$

Les quatre termes sont des polynômes en T dont chaque terme non nul est de degré congru respectivement à 0, 1, 2 et 3 modulo 4. Cette relation implique donc qu'ils sont tous nuls. Il en résulte que $P = Q = R = S = 0$ et donc $F \in I$. On a donc bien $I(C) \subset I$.

2.1.9. On a $C = V(XY) = V(Y) \cup V(X) = (OX) \cup (OY)$ et donc $I(C) = I((OX) \cup (OY)) = I(OX) \cap I(OY) = (Y) \cap (X) = (XY)$ car X et Y n'ont pas de facteurs communs dans $k[X, Y]$ qui est factoriel.

2.1.10. On vérifie que $I(C) = (XY(X-Y))$.

2.1.11. Puisque V est la réunion des trois axes de l'espace, dont les idéaux sont respectivement (X, Y), (X, Z) et (Y, Z), on a $I(W) = (X, Y) \cap (X, Z) \cap (Y, Z)$. On montre alors successivement que $(X, Y) \cap (X, Z) = (X, YZ)$ et que $(X, YZ) \cap (Y,$

$Z) = (XY, XZ, YZ)$, ce qui donne $I(W) = (XY, XZ, YZ)$. Montrons par exemple la seconde de ces égalités : Si $F = AX + BYZ = CY + DZ \in (X, YZ) \cap (Y, Z)$, on a $AX - CY = (BY - D)Z$ et donc, soit $AX = CY$, auquel cas $A \in (Y)$ et donc $F \in (XY, YZ) \subset (XY, XZ, YZ)$. Ou alors, Z divise A (et C) et alors $F \in (XZ, YZ) \subset (XY, XZ, YZ)$. L'inclusion réciproque est immédiate.

2.3.4. Il est clair que $4X^2 - (Y^2 + 4Y)X + Y^2$ est irréductible si bien que $I(C) = (4X^2 - (Y^2 + 4Y)X + Y^2)$. Si l'on effectue la division euclidienne en X de $F \in k[X, Y]$ par $4X^2 - (Y^2 + 4Y)X + Y^2$, on voit que F est congru à un unique $R \in k[X, Y]$ de degré au plus 1 en X modulo $4X^2 - (Y^2 + 4Y)X + Y^2$. On en déduit que l'application de restriction $k[X, Y] \longrightarrow k[C]$ induit une bijection de l'espace des polynômes de degré au plus 1 en X sur $k[C]$. Cela signifie que si $f \in k[C]$, il existe $G, H \in k[T]$ uniques tels que si $Q := (a, c) \in C'$, on ait $f(Q) = G(c) + aH(c)$.

2.4.3. L'homomorphisme $\Phi^* : k[X, Y, Z] \longrightarrow k[T]$ envoie X, Y, Z respectivement sur T^2, $T^2(T^2 - 1), T^3$. L'image de Φ^* est donc la sous algèbre A de $k[T]$ engendrée par ces polynômes. Or il est immédiat que tout élément non constant de A est de valuation au moins 2. En particulier $T \notin A$ et Φ^* n'est pas surjective. Il en résulte que Φ n'est pas une immersion fermée.

2.4.4. On sait que Φ induit une bijection φ de $\mathbb{A}^1$ sur la courbe C d'équation $Y^4 = Y^3 - X^3$, la réciproque étant donnée par

$$\varphi^{-1} : C \longrightarrow \mathbb{A}^1, (a, b) \longmapsto \begin{cases} a/b \text{ si b} \neq 0 \\ 0 \text{ sinon.} \end{cases}$$

Si Φétait une immersion fermée, alors φ^{-1} serait polynomiale et on pourrait trouver $F \in k[X, Y]$ tel que $\varphi^{-1}(a, b) = F(a, b)$, et donc $bF(a, b) = a$, pour tout $a, b \in C$. On aurait donc $YF = X \; mod \; Y^4 - Y^3 + X^3$ si bien que $F(O)Y = X$, ce qui est clairement impossible.

2.4.6. On obtient une équation de $s^{-1}(C)$ en appliquant s^* à une équation de C. On a bien sur $s^*(X) = -X$ et $s^*(Y) = -Y$. On voit donc que $s^{-1}(C)$ est la courbe d'équation $X^2Y^2 + X^2 + Y^2 + 2XY(X + Y - 1) = 0$.

2.4.7. On a vu que l'application $\Phi : \mathbb{A}^2 \longrightarrow \mathbb{A}^2, (a, b) \longmapsto (a, a + b - ab)$ induit un isomorphisme de C sur la courbe C' d'équation $4X^2 - (Y^2 + 4Y)X + Y^2$. On

voit donc que Φ^* induit un isomorphisme de $k[C']$ sur $k[C]$. Cela signifie que si $f \in k[C]$, il existe un unique $f' \in k[C']$ tel que pour tout $P := (a, b) \in C$, on ait $f(a, b) = f'(a, a + b - ab)$. Il existe donc F et $G \in k[T]$ uniques tels que $f(P) = F(a + b - ab)a + G(a + b - ab)$.

2.6.1. On sait que $C = (OX) \cup (OY)$ et que les droites (OX) et (OY) sont irréductibles. Il est clair qu'aucune de ces droites n'est contenue dans l'autre. Ce sont donc les composantes irréductibles de C.

2.6.2. Ce sont les axes des coordonnées (OX) et (OY) ainsi que la diagonale principale Δ d'équation $X = Y$,

2.6.3. Ce sont les trois axes des coordonnées dans l'espace.

2.6.6. On sait que C et (OZ) sont des ensembles algébriques irréductibles et ceux ci sont bien contenus dans V. De plus, C et (OZ) ne sont pas contenus l'un dans l'autre car ces ensembles sont infinis et leur intersection est réduite à l'origine. Il nous reste à montrer que $V \subset C \cup (OZ)$. Soit $P := (a, b, c) \in V$, on a $a^3 = bc$ et $b^2 = ac$ si bien que $(ab)c^2 = (bc)(ac) = a^3b^2 = (ab)(a^2b)$. Si $ab \neq 0$, on a $c^2 = a^2b$ si bien que $P \in C$. Sinon, on a nécessairement $a = b = 0$ et $P \in (OZ)$.

2.6.9. i) Puisque les racines dans $\mathbb{C}$ du polynôme $X^2 + 1$ sont distinctes, ce polynôme n'est pas un carré dans $\mathbb{C}[X]$. Il en résulte que F n' à pas de racines dans $\mathbb{C}(X)$. Puisque F est de degré 2 en Y, ce polynôme est nécessairement irréductible dans $\mathbb{C}(X)[Y]$.

On voit donc que si $F = F_1F_2$ dans $\mathbb{C}[X, Y]$, alors F_1 (ou F_2) $\in \mathbb{C}[X]$. En faisant $Y = 0$, on voit que F_1 divise $(X^2 - \lambda)^2$ et il en résulte que F_1 divise $(X^2 + 1)Y^2$. Puisque F_1 et Y sont premiers entre eux, on en déduit que F_1 divise $X^2 + 1$.

Si $\lambda \neq -1$, alors les polynômes $X^2 - \lambda$ et $X^2 + 1$ n'ont pas de racine commune et sont donc premiers entre eux. Le polynôme F_1 est donc nécessairement constant. On voit donc que F est irréductible. Puisque $\mathbb{C}$ est algébriquement clos, la courbe C est irréductible.

Si $\lambda = -1$, alors $F = (X - i)(X + i)(X^2 + Y^2 + 1)$ et le polynôme $X^2 + Y^2 + 1$ est irréductible car $Y^2 + 1$ n'est pas un carré dans $\mathbb{C}[Y]$. Puisque $\mathbb{C}$ est algébriquement clos, les composantes irréductibles de C sont donc les droites

d'équations $X = \pm i$ et la conique d'équation $X^2 + Y^2 + 1 = 0$.

ii) Puisque dans $\mathbb{R}$, une somme de carrés est nulle si et seulement si tous les termes sont nuls, on a $C = V(Y, X^2 - \lambda)$. On voit donc que si $\lambda > 0$, alors C est réduite aux deux points de coordonnées $(0, \pm\sqrt{\lambda})$, si $\lambda = 0$, alors C est réduite à l'origine O et si $\lambda < 0$, alors $C = \emptyset$.

iii) On a $F = G^2$ avec $G := (X - 1)Y + X^2 - \lambda$ et donc $C = V(G)$. Si $G = G_1 G_2$, alors G_1 (ou G_2) divise $X^2 - \lambda$ et $X - 1$.

Si $\lambda \neq 1$, alors les polynômes $X^2 - \lambda$ et $X + 1$ sont premiers entre eux et il en résulte que G_1 est constant. On voit donc dans ce cas, que F est irréductible. De plus, si $t \neq 1$, alors le point de coordonnés $(\frac{\lambda - 1}{(t+1)^2}, t)$ appartient à C. Il en résulte que C est infinie et donc irréductible.

Enfin, si $\lambda = 1$, on a $G = (X - 1)(X + Y - 1)$. Les composantes irréductibles de C sont donc les droites d'équations $X = 1$ et $X + Y = 1$.

2.6.10. Puisque $F := X^4 - Y^4 - \lambda X^3 + XY^2$ est somme de deux polynômes homogènes de degrés 3 et 4, ce polynôme est irréductible si et seulement si les polynômes $X^4 - Y^4$ et $-\lambda X^3 + XY^2$ sont premiers entre eux. La décomposition de $X^4 - Y^4$ en facteurs irréductibles est

$$X^4 - Y^4 = -(Y + X)(Y - X)(Y + iX)(Y - iX)$$

et celle de $-\lambda X^3 + XY^2$ est

$$-\lambda X^3 + XY^2 = X(Y - \sqrt{\lambda}\, X)(Y + \sqrt{\lambda}\, X).$$

Par suite, $X^4 - Y^4 - \lambda X^3 + XY^2$ est irréductible si et seulement si $\sqrt{\lambda} \neq \pm 1, \pm i$, c'est à dire si et seulement si $\lambda \neq \pm 1$.

Si $\lambda \neq \pm 1$, la courbe est irréductible.

Si $\lambda = 1$, on a

$$F = (X + Y)(X - Y)(X^2 + Y^2 - X),$$

et chacun des polynômes $X + Y, X - Y, X^2 + Y^2 - X$ est irréductible : c'est clair

pour les deux premiers. Pour le dernier cela résulte de l'application du même critère que précédemment. Puisque k est algébriquement clos, cette décomposition en facteurs irréductibles correspond à la décomposition de C en composantes irréductibles. On a donc, si $car\ k \neq 2$,

$$C = V(X+Y) \cup V(X-Y) \cup V(X^2+Y^2-X).$$

Si $\lambda = -1$, on montre de même que la décomposition de C en composantes irréductibles est, lorsque $car\ k \neq 2$,

$$C = V(X+iY) \cup V(X-iY) \cup V(X^2-Y^2+X).$$

Enfin, si $car\ k = 2$ et $\lambda = 1$, on trouve que $C = V(X-Y) \cup V(X^2-Y^2+X)$.

2.6.11. Soit, pour $i = 1$ ou 2, C_i une composante irréductible de C. Alors, la projection $x_i : C_i \longrightarrow \mathbb{A}^1$ est injective et cela implique, comme nous l'avons déjà vu que $x(C_i)$ est un ouvert non vide de $\mathbb{A}^1$. Puisque $\mathbb{A}^1$ est irréductible, $x(C_1) \cap x(C_2)$ est nécessairement un ouvert non vide donc un ensemble infini. Puisque x est injective, $C_1 \cap C_2$ est aussi infini. Puisque, pour $i = 1$ ou 2, C_i est irréductible, on doit donc avoir $C_1 = C_2$. Cela montre que C est irréductible. On a donc $I(C) = (F)$ avec F irréductible et on peut écrire $F := F_d Y^d + F_{d-1} Y^{d-1} + \ldots + F_0$ avec $F_0, \ldots, F_d \in \mathbb{C}[X]$ et $F_d \neq 0$. Puisque x est injective sur C, on a $d > 0$. Si $a \notin V(F_d)$, le polynôme $F_d(a)Y^d + \ldots + F_0(a)$ a au moins une racine b dans $\mathbb{C}$ et donc $P := (a, b) \in C$. Puisque x est injective, b est unique et on a donc $F_d(a)Y^d + \ldots + F_0(a) = F_d(a)(Y-b)^d$. On en déduit que $F_{d-1}(a) = -F_d(a)db$, c'est à dire que P est sur la courbe d'équation $dF_dY - F_{d-1} = 0$. Puisque $F_d \neq 0$, le complémentaire de $V(F_d)$ est infini. On voit donc que C et la courbe d'équation $dF_dY - F_{d-1} = 0$, ont une infinité de points communs. Puisque C est irréductible, elle est contenue dans la courbe d'équation $dF_dY - F_{d-1}$. Cela implique que $dF_dY - F_{d-1} \in I(C)$ et donc que F divise $dF_dY - F_{d-1}$ si bien que $d \leq 1$. On voit donc que F est de degré 1 en Y.

Si $g, h \in k[C]$ sont telles que $f = g/h$, on a $hy^2 - gx = 0$. Il suit que si g et h se prolongent en G et $H \in k[X, Y]$, il existe $K \in k[X, Y]$ tel que $HY^2 - GX = (X^4 - Y^4 - \lambda X^3 + XY^2)K$. On voit donc que $H(O)Y^2 = 0$. On a donc $h(O) = 0$ et f n'est pas régulière en O. Par contre, on a

$$f(1-f) = \frac{y^2}{x}\frac{x-y^2}{x} = \frac{xy^2-y^4}{x} = \frac{\lambda x^3 - x^4}{x} = \lambda x^2 - x^3,$$

ce qui montre que $f(1-f)$ est régulière en O.

2.7.5. On a $f'_x = -3x^2 + 1, f'_y = 2y$ et donc $t = \frac{3x^2-1}{2y}$ si bien que t est régulière sur C_0. Il suit que u et v sont aussi régulières.

2.7.6. Puisque $y^2 = x^3 - x$ et $y'^2 = x'^3 - x'$, on a $y'^2 - y^2 = (x'^3 - x') - (x^3 - x) = (x'^3 - x^3) - (x' - x) = (x^2 + xx' + x'^2 - 1)(x' - x)$. On a donc bien

$$\frac{x^2+xx'+x'^2-1}{y+y'} = \frac{y'-y}{x'-x}$$

2.7.8. Il suffit de remarquer que si $b \neq 0$, alors $r(a, b, a, b) = t(a, b)$.

2.8.3. On a $U = D(T^4 - 1)$ et donc

$$\Gamma(U) = k[T]_{(T^4-1)} = \{ \frac{F}{(T^4-1)^n}, F \in k[T], n \in \mathbb{N}\}.$$

2.8.4. Puisque $k[X]$ est factoriel, on peut écrire $R := F/G$ avec F et $G \in k[X]$ premiers entre eux. Si $a \in U$, on a donc $G(a)R(a) - F(a) = 0$, c'est à dire $P := (a, R(a)) \in V(GY - F)$. On voit donc que $E \subset V(GY - F)$. Pour conclure, il suffit de montrer que la courbe d'équation $GY = F$ est irréductible et que E est infini. Puisque U est un ouvert non vide, U est infini et il en va donc de même de E. Il nous reste donc à vérifier que $V(GY - F)$ est irréductible : Si $GY - F = H_1H_2$, alors H_1 (ou H_2) $\in k[X]$ et donc H_1 divise F, ce qui implique que H_1 divise G. Puisque F et G sont premiers entre eux, H_1 est nécessairement constant.

COURBES ALGEBRIQUES

(Bernard Le Stum)

CHAPITRE 3 - COURS

Courbes algébriques planes

On fixe un corps de base *algébriquement clos* k.

3.1. Théorème des zéros de Hilbert

3.1.1. Proposition Si V est un ensemble algébrique affine sur k, les idéaux maximaux de $k[V]$ sont les idéaux de la forme $I_V(P)$ où P est un point de V.

Si $\mathfrak{m}$ est un idéal maximal de $k[V]$, alors $k[V]/\mathfrak{m}$ est à la fois un corps et une k-algèbre de type fini. Il résulte alors du Nullstellensatz algébrique que $k[V]/\mathfrak{m}$ est une extension finie de k et donc isomorphe à k car k est algébriquement clos. Or nous avons vu que cette condition est nécessaire et suffisante pour que $\mathfrak{m}$ soit de la forme $I_V(P)$.

Corollaire Si I est un idéal propre de $k[V]$, alors $V(I) \neq \emptyset$.

L'idéal I est contenu dans un idéal maximal, qui est nécessairement de la forme $I_V(P)$ et on a donc $\{P\} = V(I_V(P)) \subset V(I)$.

3.1.2. Théorème (Nullstellensatz) Si V est un ensemble algébrique affine sur k et I un idéal de $k[V]$, alors $I_V(V(I)) = \sqrt{I}$.

Corollaire Si V est irréductible et $g \in k[V]$, alors $\Gamma(D(g)) = k[V]_g := \{h/g^n,\ h \in k[V]\}$.

Démonstration du théorème et de son corollaire : Dans le cas où $g = 1$, le corollaire nous dit que toute fonction régulière sur V est polynomiale. Ceci se vérifie aisément : l'ensemble des pôles de $f \in k(V)$ est $V(I_f)$ où $I_f = \{h \in k[V],\ fh \in k[V]\}$. Si f est régulière sur V, alors $V(I_f) = \emptyset$ et donc $1 \in I_f$ si bien que $f \in k[V]$.

Nous allons maintenant démontrer le théorème et son corollaire lorsque $V = \mathbb{A}^n$. Nous savons que si $G \in k[X_1, \ldots, X_n]$, la projection $p : \mathbb{A}^{n+1} \longrightarrow \mathbb{A}^n$ induit

une immersion ouverte $j : W := V(GX_{n+1} - 1) \hookrightarrow \mathbb{A}^n$. En particulier, j^* induit un isomorphisme entre $\Gamma(D(G))$ et $\Gamma(W) = k[W]$. On voit donc que $\Gamma(D(G)) = \{F(X_1, \ldots, X_n, 1/G), F \in k[X_1, \ldots, X_{n+1}]\} = \{F/G^d, F \in k[X_1, \ldots, X_n]\}$. Plus généralement, si I est un idéal de $k[X_1, \ldots, X_n]$, alors j^* induit un isomorphisme entre $\{F/G^d, F \in I\}$ et $j^*(I)k[W]$. Si $V(j^*(I)) \neq \emptyset$, il existe $P \in W$ tel que $j(P) \in V(I)$. Puisque $j(P) \in U$, on a $G(j(P)) \neq 0$ et donc $G \notin I(V(I))$. On voit donc que, réciproquement, si $G \in I(V(I))$, alors $V(j^*(I)) = \emptyset$ et donc $1 \in j^*(I)k[W]$ si bien que $1 = F/G^n$ avec $F \in I$, c'est à dire $G^n \in I$. On a donc $I(V(I)) \subset \sqrt{I}$ et l'inclusion inverse est triviale.

Démontrons maintenant le théorème et son corollaire dans le cas général : si $i : V \hookrightarrow \mathbb{A}^n$ est l'inclusion canonique, alors tout idéal de $k[V]$ est de la forme $i^*(I)$ où I est un idéal de $k[X_1, \ldots, X_n]$. On sait alors que $I_V(V(i^*(I)))$ est l'image de $I(V(I))$ et que $\sqrt{i^*(I)}$ est l'image de $\sqrt{I}$. On a donc bien $I_V(V(I)) = \sqrt{I}$. Enfin, comme l'ensemble des pôles de $f \in k(V)$ est $V(I_f)$, on voit que $f \in \Gamma(D(g))$ ssi $V(I_f) \subset V(g)$ ssi $g \in I(V(I_f))$ ssi $g^n \in I_f$ ssi $f = h/g^n$ avec $h \in k[V]$. On a donc bien $\Gamma(D(g)) = k[V]_g$.

3.1.3. Nous démontrons ci dessous quelques conséquences du théorème des zéros de Hilbert.

Corollaire Si V est un ensemble algébrique affine, les applications $S \longmapsto V(S)$ et $E \longmapsto I_V(E)$ induisent des bijections réciproques entre les sous-ensembles algébriques (resp. les sous-ensembles algébriques irréductibles, resp. les points) de V et les idéaux radicaux (resp. les idéaux premiers, resp. les idéaux maximaux) de $k[V]$.

Si W est un sous-ensemble algébrique de V, alors $I = I_V(W)$ est un idéal radical et $W = V(I_V(W))$. Réciproquement, si I est un idéal radical de $k[V]$, alors $W := V(I)$ est un sous-ensemble algébrique de V et $I = I_V(V(I))$. De plus, I est premier (resp. maximal) si et seulement si W est irréductible (resp. réduit à un point).

Corollaire (Nullstellensatz projectif) Si I est un idéal gradué de $k[X_1, \ldots, X_{n+1}]$, alors $V_p(I) = \emptyset$ si et seulement si il existe N tel que $X_1^N, \ldots, X_{n+1}^N \in I$. Sinon, on a $I(V_p(I)) = \sqrt{I}$.

On a
$V_p(I) = \emptyset$ ssi $V(I) \subset \{O\} = V(X_1, \ldots, X_{n+1})$
$V_p(I) = \emptyset$ ssi $X_1, \ldots, X_{n+1} \in I(V(I)) = \sqrt{I}$.

Sinon, on a $I(V_p(I)) = I(C(V_p(I))) = I(V(I)) = \sqrt{I}$.

Corollaire Les applications $S \longmapsto V_p(S)$ et $A \longmapsto I(A)$ induisent des bijections réciproques entre les sous-ensembles algébriques (resp. les sous-ensembles algébriques irréductibles) de $\mathbb{P}^n$ et les idéaux radicaux (resp. les idéaux premiers) homogènes, autres que $(X_1, \ldots, X_{n+1})$, de $k[X_1, \ldots, X_{n+1}]$.

Si V est un sous-ensemble algébrique de $\mathbb{P}^n$, alors $I := I(V)$ est un idéal radical homogène, $V = V_p(I(V)$ et $I \neq (X_1, \ldots, X_{n+1})$. Réciproquement, si I est un idéal radical homogène distincts de $(X_1, \ldots, X_{n+1})$ de $k[X_1, \ldots, X_{n+1}]$, alors $V := V_p(I)$ est un sous-ensemble algébrique de $\mathbb{P}^n$ et $I = I(V_p(I))$. De plus, I est premier si et seulement si V est irréductible.

Corollaire Si V est une hypersurface (affine ou projective) d'équation $F = 0$, les composantes irréductibles de V sont les hypersurfaces définies par les facteurs irréductibles de F.

Si $F = F_1^{r_1} \ldots F_m^{r_m}$ est la décomposition de F en produit de facteurs irréductibles, on a $V(F) = V(F_1) \cup \ldots \cup V(F_m)$. Les $V(F_i)$ sont irréductibles et ne sont pas contenus les uns dans les autres car les idéaux (F_i) sont premiers et ne sont pas contenus les uns dans les autres. Le même raisonement marche dans le cas projectif.

3.2. Multiplicité en un point d'une courbe plane irréductible.

3.2.1. Lemme Soit V un ensemble algébrique affine et $P_1, \ldots, P_r \notin V$. Il existe alors $F \in I(V)$ tel que $F(P_j) = 1$ pour tout $j = 1, \ldots, r$.

Traitons d'abord le cas $r = 1$: Comme V est algébrique, il est clair que si $P \notin V$, il existe $F \in I(V)$ avec $F(P) \neq 0$. Quitte à multiplier F par une constante, on peut supposer que $F(P) = 1$. En général, on peut appliquer ça à chaque P_i et donc trouver $F_i \in I(V)$ avec $F_i(P_i) = 1$. D'autre part, comme $\{P_1, \ldots, P_{i-1}, P_{i+1}, \ldots, P_r\}$ est un ensemble fini et donc algébrique et que l'on peut supposer $P_1, \ldots, P_r$ tous distincts, on voit qu'il existe $G_i \in I(P_1, \ldots, P_{i-1}, P_{i+1}, \ldots, P_r)$ tel que $G_i(P_i) = 1$, c'est à dire, tel que pour tout $j = 1, \ldots, r$, on ait $G_i(P_j) = \delta_{ij}$. Il suffit alors de prendre $F = F_1G_1 + \ldots + F_rG_r$.

3.2.2. Proposition (local au global) Soit I un idéal de $k[X_1, \ldots, X_n]$. Alors, $V(I)$ est fini si et seulement si $k[X_1, \ldots, X_n]/I$ est une k-algèbre finie. Si c'est le cas, l'application canonique

$$k[X_1, \ldots, X_n]/I \longrightarrow \prod_{P \in V} \mathcal{O}_{\mathbb{A}^n,P}/I\mathcal{O}_{\mathbb{A}^n,P}$$

est un isomorphisme.

Démonstration : On note par une lettre minuscule f l'image d'un polynôme $F \in k[X_1, \ldots, X_n]$ dans $R := k[X_1, \ldots, X_n]/I$. Soient $P_1, \ldots, P_r \in V(I)$ et $F_1, \ldots, F_r \in k[X_1, \ldots, X_n]$ tels que pour tous $i, j = 1, \ldots, r$, on ait $F_i(P_j) = \delta_{ij}$. Si $\Sigma a_i f_i = 0$, alors $\Sigma a_i F_i \in I$ et on a donc, pour tout $j = 1, \ldots, r$, $a_j = \Sigma a_i \delta_{ij} = \Sigma a_i F_i(P_j) = 0$. Cela montre que les f_i sont linéairement indépendants sur k. On en déduit que si R est de dimension finie sur k, alors $V(I)$ est fini. Réciproquement, si $V(I) = \{P_1, \ldots, P_r\}$ avec pour tout $i = 1, \ldots, r$, $P_i = (a_{i1}, \ldots, a_{in})$, on pose pour tout $j = 1, \ldots, n$, $H_j = \Pi(X_j - a_{ij})$. On voit que pour tous i, j, $H_j(P_i) = 0$ si bien que pour tout j, $H_j \in I(V(I)) = \sqrt{I}$. Il existe donc N tel que pour tout $j = 1, \ldots, n$, $H_j^N \in I$. On voit donc que pour tout j, $h_j^N = 0$, ce qui implique que x_j^{Nr} appartient au sous espace de R engendré par les x_j^k pour $k = 1, \ldots, Nr - 1$. On en déduit que les $x_1^{k_1} \ldots x_n^{k_n}$ avec $k_i < Nr$ forment un système générateur de R et donc que R est de dimension finie.

Montrons que si $V(I) = \{P_1, \ldots, P_r\}$ et si pour tout $i = 1, \ldots, r$, on note $\mathfrak{m}_i := I(P_i)$, il existe pour tout $d > 0$, $E_1, \ldots, E_r \in k[X_1, \ldots, X_n]$ tels que $E_i = \delta_{ij} \ mod\ \mathfrak{m}_j^d$ pour tous $i, j = 1, \ldots, r$: Il résulte du lemme qu'il existe $F_1, \ldots, F_r$ satisfaisant cette condition pour $d = 1$. En général, on prend $E_i = 1 - (1 - F_i^d)^d$.

Montrons que $\Sigma e_i = 1$, que pour tout $i = 1, \ldots, r$, on a $e_i^2 = e_i$ et que si $j \neq i = 1, \ldots, r$, alors $e_i e_j = 0$: Il résulte du Nullstellensatz que $\sqrt{I} = I(P_1, \ldots, P_r) = \cap \mathfrak{m}_i$. Puisque $k[X_1, \ldots, X_n]$ est noetherien, il existe d tel que $(\cap \mathfrak{m}_i)^d \subset I$. Enfin, puisque les $\mathfrak{m}_i$ sont des idéaux maximaux, on a $\cap \mathfrak{m}_i^d = (\cap \mathfrak{m}_i)^d$. D'autre part, on a $E_i = \delta_{ij} \ mod\ \mathfrak{m}_j^d$ pour tous $i, j = 1, \ldots, r$. Il suffit alors de remarquer que pour $k = 1, \ldots, r$, on a $1 - \Sigma E_i = (1 - E_k) - \sum_{i \neq k} E_i \in \mathfrak{m}_k^d$, pour tout $i = 1, \ldots, r$, $(1 - E_i)E_i \in \mathfrak{m}_k^d$, et pour tout $j \neq i$, $E_i E_j \in \mathfrak{m}_k^d$.

Montrons que a) pour tous $j = 1, \ldots, r$, $E_i = \delta_{ij} \ mod\ I\mathcal{O}_{\mathbb{A}^n,P_j}$ et b) si $H \in k[X_1, \ldots, X_n]$ est tel que $H(P_i) \neq 0$, il existe $S \in k[X_1, \ldots, X_n]$ tel que $hs = e_i$: a) On a pour $j \neq i$, $e_i e_j = 0$ et donc $E_i E_j = 0 \ mod\ I\mathcal{O}_{\mathbb{A}^n,P_i}$ dans $\mathcal{O}_{\mathbb{A}^n,P_i}$. Puisque $E_i(P_i) = 1 \neq 0$, E_i est inversible dans $\mathcal{O}_{\mathbb{A}^n,P_i}$ et on voit donc que $E_j = 0 \ mod\ I\mathcal{O}_{\mathbb{A}^n,P_i}$ pour $j \neq i$. Enfin, puisque $\Sigma e_i = 1$, on a $E_i = \Sigma E_j = 1 \ mod\ I\mathcal{O}_{\mathbb{A}^n,P_i}$. b) Si $a := H(P_i)$, on a $(a - H)^d \in \mathfrak{m}_i^d$ et donc $(a - H)^d E_i \in I$, c'est à dire $(a - h)^d e_i = 0$. Puisque h divise $a^d - (a - h)^d$, on voit que h divise $a^d e_i - (a - h)^d e_i = a^d e_i$ et donc aussi e_i.

Montrons enfin que l'application canonique

$$R \longrightarrow \mathcal{O}_{\mathbb{A}^n,P_1}/I\mathcal{O}_{\mathbb{A}^n,P_1} \times \ldots \times \mathcal{O}_{\mathbb{A}^n,P_r}/I\mathcal{O}_{\mathbb{A}^n,P_r}.$$

est bijective : Si $F \in k[X_1, \ldots, X_n]$ est tel que $F \in I\mathcal{O}_{\mathbb{A}^n,P_i}$, alors il existe $H_i \in k[X_1, \ldots, X_n]$ tel que $H_i(P_i) \neq 0$ et $FH_i \in I$, c'est à dire $fh_i = 0$. D'autre part, comme $H_i(P_i) \neq 0$, on peut écrire $e_i = h_i s_i$. On voit donc que si $F \in I\mathcal{O}_{\mathbb{A}^n,P_i}$ pour tout $i = 1, \ldots, r$, alors $f = f(\Sigma e_i) = \Sigma f e_i = \Sigma f h_i s_i = 0$. Cela montre que l'application est injective et il reste à vérifier qu'elle est surjective : Donnons nous, pour $i = 1, \ldots, r$, $G_i/H_i \in \mathcal{O}_{\mathbb{A}^n,P_i}$. On a alors $H_i(P_i) \neq 0$ si bien qu'il existe $S_i \in k[X_1, \ldots, X_n]$ tel que $e_i = h_i s_i$ et donc $E_i = H_i S_i \ mod\ I\mathcal{O}_{\mathbb{A}^n,P_i}$ dans $\mathcal{O}_{\mathbb{A}^n,P_i}$. Si on pose $F := \Sigma G_i S_i E_i$, on a bien $F = \Sigma G_j S_j E_j = G_i S_i = G_i/H_i \ mod\ I\mathcal{O}_{\mathbb{A}^n,P_i}$.

3.2.3. Théorème Si C est une courbe irréductible plane et P un point de C, il existe un (unique) entier m tel que $dim_k\, \mathfrak{m}_{C,P}^n/\mathfrak{m}_{C,P}^{n+1} = m$ pour $n \geq m$. Si C est affine, $I(C) = (F)$ et $P = O$, alors $m = val(F)$.

Démonstration : On sait que si Φ est un changement de coordonnées, alors $\mathcal{O}_{C,P} \tilde{=} \mathcal{O}_{\Phi(C),\Phi(P)}$ et que si C est affine, alors $\mathcal{O}_{C,P} \tilde{=} \mathcal{O}_{C^*,P}$. On peut donc supposer que C est affine et que $P = O$. Il s'agit de montrer que si $I(C) = (F)$, $m = val(F)$ et $n \geq m$, alors $dim_k\, \mathfrak{m}_{C,O}^n/\mathfrak{m}_{C,O}^{n+1} = m$.

Si $G \in k[X, Y]$, on a par définition $FG \in (X, Y)^n$ si et seulement si $val(FG) \geq n$. Puisque $val(FG) = val(F) + val(G)$, cette dernière condition est équivalente à $val(G) \geq n - m$, c'est à dire $G \in (X, Y)^{n-m}$. On voit donc que le noyau de l'application linéaire composée de la multiplication par F sur $k[X, Y]$ et de la projection $k[X, Y] \longrightarrow k[X, Y]/(X, Y)^n$ est $(X, Y)^{n-m}$. On a donc une suite exacte courte

$$0 \longrightarrow k[X, Y]/(X, Y)^{n-m} \longrightarrow k[X, Y]/(X, Y)^n \longrightarrow k[X, Y]/((X, Y)^n + (F)) \longrightarrow 0$$

D'autre part, puisque $V((X, Y)^n + (F)) = \{O\}$, on a

$k[X, Y]/((X, Y)^n + (F)) \tilde{=} \mathcal{O}_{\mathbb{A}^2,O}/((X, Y)^n + (F))\mathcal{O}_{\mathbb{A}^2,O}$

$k[X, Y]/((X, Y)^n + (F)) \tilde{=} \mathcal{O}_{C,O}/(x, y)^n \mathcal{O}_{C,O}$

$k[X, Y]/((X, Y)^n + (F)) \tilde{=} \mathcal{O}_{C,O}/\mathfrak{m}_{C,O}^n$.

On vérifie aisément que $dim_k\, k[X, Y]/(X, Y)^n = n(n+1)/2$ et on en déduit que

$$dim_k\, \mathcal{O}_{C,O}/\mathfrak{m}_{C,O}^n = nm - m(m-1)/2$$

On conclut grâce à la suite exacte

$$0 \longrightarrow \mathfrak{m}_{C,O}^n/\mathfrak{m}_{C,O}^{n+1} \longrightarrow \mathcal{O}_{C,O}/\mathfrak{m}_{C,O}^{n+1} \longrightarrow \mathcal{O}_{C,O}/\mathfrak{m}_{C,O}^n \longrightarrow 0.$$

3.2.4. Définition On dit que $m_P(C) := m$ est *la multiplicité de C en P*. Si $P \notin C$, on pose $m_P(C) := 0$.

3.3. Diviseurs dans le plan

3.3.1. Définitions Le *groupe des diviseurs du plan* (affine ou projectif) est le groupe abelien libre sur les courbes irréductibles. Si $C = \sum e_i C_i$, on dit que C_i est une *composante de multiplicité* e_i dans C. Si $e_i = 1$, on dit que C_i est une composante *simple*. On dit que C est *effectif* si les e_i sont positifs (ou nuls) et non tous nuls. Si C est un diviseur de $\mathbb{P}^2$, la *partie affine* de C est $C_* := \sum e_i C_{i*}$. Si C est un diviseur de $\mathbb{A}^2$, la *fermeture projective* de C est $C^* = \sum e_i C_i^*$.

• Si C et D sont deux diviseurs de $\mathbb{P}^2$, alors $(C + D)_* = C_* + D_*$ et si C et D sont deux diviseurs de $\mathbb{A}^2$, alors $(C + D)^* = C^* + D^*$: Clair.

• Si C est un diviseur de $\mathbb{A}^2$, on a $C = (C^*)_*$. De même, si C est un diviseur de $\mathbb{P}^2$ et si la droite à l'infini n'est pas une composante de C, alors $C = (C_*)^*$: Résulte par additivité du cas irréductible.

3.3.2. Définition Si Φ est un changement de coordonnées et $C := \sum e_i C_i$ est un diviseur, on pose $\Phi^{-1}(C) := \sum e_i \Phi^{-1}(C_i)$.

• On a toujours $\Phi^{-1}(C + D) = \Phi^{-1}(C) + \Phi^{-1}(D)$: Clair.

3.3.3. Définition Si $C := \sum e_i C_i$ est un diviseur effectif et P un point du plan, la *multiplicité* de C en P est $m_P(C) := \sum e_i m_P(C_i)$.

• On a toujours $m_P(C + D) = m_P(C) + m_P(D)$: Clair.

• Si P est un point d'un diviseur effectif C du plan affine, alors $m_P(C) = m_P(C^*)$: Par additivité, on peut supposer C est irréductible et on sait alors que $\mathcal{O}_{C,P} \tilde{=} \mathcal{O}_{C^*,P}$.

• Si Φ est un changement de coordonnées et C un diviseur effectif, alors $m_P(\Phi^{-1}(C)) = m_{\Phi(P)}(C)$: Par additivité, on peut supposer que C est irréductible et on sait alors que $\mathcal{O}_{C,\Phi(P)} \tilde{=} \mathcal{O}_{\Phi^{-1}(C),P}$.

3.3.4. Définition Si $F = \prod F_i^{e_i}$ est la décomposition d'un polynôme (homogène, dans le cas projectif) non constant en produit de facteurs irréductibles, on dit que $[F] := \sum e_i V(F_i)$ est le *diviseur de* F.

• Les diviseurs effectifs sont les diviseurs des polynômes (homogènes, dans le cas

projectif) non constants : Cela résulte du cas irréductible.

• On a toujours $[FG] = [F] + [G]$: Si $F = \prod F_i^{e_i}$ et $G = \prod F_i^{f_i}$, alors $FG = \prod F_i^{e_i+f_i}$ et on a donc $[FG] = \sum (e_i + f_i)V(F_i) = \sum e_i V(F_i) + \sum f_i V(F_i) = [F] + [G]$.

• On a toujours $[F]_* = [F_*]$ et $[F]^* = [F^*]$: Résulte de l'additivité des applications qui interviennent car le résultat est déjà connu dans le cas irréductible.

• Si Φ est un changement de coordonnées, alors $\Phi^{-1}([F]) = [\Phi^*(F)]$: Par additivité, il suffit de rappeler que $\Phi^{-1}(V(F)) = V(\Phi^*(F))$.

• Si C est le diviseur de $F \in k[X, Y]$, alors $m_O(C) = val(F)$: On procède par récurrence sur le degré de F. Si F est irréductible, on connaît déjà le résultat. Sinon, on écrit $F = GH$ avec G et H de plus bas degrés si bien que $C = [GH] = [G] + [H]$, et on a $m_O(C) = m_O([G] + [H]) = m_O(G) + m_O(H) = val(G) + val(H) = val(F)$.

3.3.5. Définition Si $C = [F]$ avec F de degré n, on dit que C est un diviseur effectif *de degré* n.

• Si C et D sont deux diviseurs du plan, on a $deg\ (C + D) = deg\ C + deg\ D$: On a $[FG] = [F] + [G]$ et $deg\ FG = degF + deg\ G$.

• On a toujours $deg\ C^* = deg\ C$ et $deg\ C_* = deg\ C - m$ où m est la multiplicité de la droite à l'infini dans C : Résulte par additivité du cas irréductible. Si $I(C) = (F)$, alors $I(C^*) = I(C)^* = (F)^* = (F^*)$ et $deg\ F^* = deg\ F$. De plus, si C est une courbe projective plane infinie irréductible autre que la droite à l'infini, alors $deg\ C_* = deg\ C$ car $(C_*)^* = C$.

• Si Φ est un changement de coordonnées, alors $deg\ \Phi^{-1}(C) = deg\ C$: Résulte par additivité du cas irréductible : on a $\Phi^{-1}(C) = V(\Phi^*(F))$ (ou $\Phi^{-1}(C) = V_p(\Phi^*(F))$) et $deg\ \Phi^*(F) = deg\ F$.

3.4. Points singuliers et non singuliers

3.4.1. Définition Soit C un diviseur effectif. On dit que P appartient à C si $m_P(C) > 0$, que P est *singulier* si $m_P(C) > 1$ et que P est *non singulier* si $m_P(C) =$

1. Enfin, on dit que C est *non singulier* si tous les points de C sont non singuliers.

• Si C est le diviseur de F, on a $P \in C$ si et seulement si $F(P) = 0$: Par définition, si $F = \prod F_i^{e_i}$ est la décomposition de F, dire que $P \in C$ signifie qu'il existe i tel que $F_i(P) = 0$ ce qui équivaut encore à dire que $F(P) = \prod F_i(P)^{e_i} = 0$.

• Un point P du plan affine est un point singulier de C si et seulement si P est un point singulier de C^* : Clair.

• Si Φ est un changement de coordonnées, alors P est un point singulier de $\Phi^{-1}(C)$ si et seulement si $\Phi(P)$ est un point singulier de C.

• Si C est le diviseur de $F \in k[X, Y]$, alors O est un point non singulier de C si et seulement si $val(F) = 1$: Clair.

3.4.2. Si $\Phi := [F_1, \ldots, F_n] : \mathbb{A}^m \longrightarrow \mathbb{A}^n$ est une application polynomiale, on note $\Phi' := [dF_i/X_j] \in M_{n,m}(k[X_1, \ldots, X_m])$.

• Si Φ est une application affine, alors Φ' est la matrice $[\vec{\Phi}\,] \in M_{n,m}(k)$ de $\vec{\Phi}$. En particulier, $\Phi' = 1$ si Φ est une translation : Si $\Phi = (\Sigma\, c_{1j}X_j + d_1 \ldots, \Sigma\, c_{mj}X_j + d_m)$, alors $[\vec{\Phi}\,] = [c_{ij}]$ et on a bien aussi $\Phi' = [c_{ij}] = [\vec{\Phi}\,]$.

• Si $\Psi : \mathbb{A}^n \longrightarrow \mathbb{A}^r$ est une autre application polynomiale, on a $(\Psi \circ \Phi)' = \Phi^*(\Psi').\Phi'$ avec $\Phi^*(\Psi') := [\Phi^*(dG_i/dX_j)]$ si $\Psi := [G_1, \ldots, G_n]$: On sait que pour tout $i = 1, \ldots, r$ et $j = 1, \ldots, m$, on a $d\,G_i(F_1, \ldots, F_n)/dX_j = \sum_k (dG_i/dX_k)(F_1, \ldots, F_n)\,.dF_k/dX_j$.

• Si $F \in k[X_1, \ldots, X_n]$, alors $\Phi^*(F)' = \Phi^*(F').\Phi'$ avec $\Phi^*(F') := [\Phi^*(dF/X_j)]$: On a $\Phi^*(F)' = (F \circ \Phi)' = F'(\Phi).\Phi'$ et $F'(\Phi) = [dF/X_j(\Phi)] = [\Phi^*(dF/X_j)] = \Phi^*(F')$.

3.4.3. Proposition Un point P du diviseur de F est singulier si et seulement si $F'(P) = 0$.

Démonstration : On a vu que si Φ est une application polynomiale, alors $\Phi^*(F)' = \Phi^*(F').\Phi'$ et il suit que $\Phi^*(F)'(P) = \Phi^*(F')(P).\Phi'(P) = F'(\Phi(P)).\Phi'(P)$. En particulier, on voit que si $\Phi'(P)$ est inversible et $F'(\Phi(P)) = 0$, alors $\Phi^*(F)'(P) = 0$. Il suit que la condition est invariante par changement de coordonnées et on peut donc supposer que $P = O$. D'autre part, si $F \in k[X, Y, Z]$ est homogène de degré r, on dispose de la formule d'Euler : $XdF/dX + YdF/dY + ZdF/dZ = rF$ et on

sait que $(dF/dX)_* = (dF_*/dX)$ et $(dF/dY)_* = (dF_*/dY)$. On en déduit que $F'(P) = 0$ si et seulement si $(F_*)'(P) = 0$. On peut donc supposer que C est affine et on a alors $F = dF/dX(O)X + dF/dY(O)Y \ mod\ (X, Y)^2$. On sait que C est singulière en O si et seulement si $val(F) > 1$, et on voit que cette condition est équivalente à dire que $dF/dX(O) = dF/dY(O) = 0$.

Corollaire Si C n'a pas de composante multiple, l'ensemble des points singuliers de C est fini.

Puisque deux courbes irréductibles distinctes se rencontrent en un nombre fini de points, on peut supposer que C est irréductible. Supposons que C ait un nombre infini de points singuliers et posons $I(C) =: (F)$. L'ensemble $V(F, dF/dX)$ étant infini et F irréductible, F divise dF/dX. Pour des raisons de degrés, on doit donc avoir $dF/dX = 0$. De même, on doit avoir dF/dY $(= dF/dZ$, dans le cas projectif$) = 0$. On en déduit que k est de caractéristique $p \neq 0$ et que $F = G^p$, ce qui contredit l'hypothèse que C est irréductible.

3.4.4. La notion de valuation discrète est bien pratique pour étudier les points non singuliers :

• Une courbe irréductible C est non singulière en un point P si et seulement si $\mathcal{O}_{C,P}$ est un anneau de valuation discrète : On sait que $\mathcal{O}_{C,P}$ est un anneau local intègre noetherien d'idéal maximal $\mathfrak{m}_{C,P}$ et de corps résiduel k. Un tel anneau est un anneau de valuation discrète si et seulement si $dim_k\ \mathfrak{m}_{C,P}/\mathfrak{m}_{C,P}^2 = 1$.

• Soit P un point non singulier d'une courbe irréductible C et $v_{C,P}$ la valuation associée. Alors, pour tout $f \in k(C)$, on a

$v_{C,P}(f) < 0$ ssi P est un pôle de f ssi $f \notin \mathcal{O}_{C,P}$
$v_{C,P}(f) \geq 0$ ssi f est régulière en P ssi $f \in \mathcal{O}_{C,P}$
$v_{C,P}(f) = 0$ ssi f est régulière en P et $f(P) \neq 0$ ssi $f \in \mathcal{O}_{C,P}^{\times}$
$v_{C,P}(f) > 1$ ssi P est un zéro de f ssi $f \in \mathfrak{m}_{C,P}$

• Soit P un point non singulier d'une courbe irréductible C et $f \in \mathcal{O}_{C,P}$. Alors $v_{C,P}(f) \geq n$ ssi $f \in \mathfrak{m}_{C,P}^n$. On a aussi $v_{C,P}(f) = dim_k\ \mathcal{O}_{C,P}/(f)$.

• Si D est l'axe des X et si $F \in k[X] \subset \mathcal{O}_{D,O}$, alors $v_{D,O}(F) = val(F)$: En effet, on sait que $v_{D,O}(F) \geq n$ si et seulement si $F \in \mathfrak{m}_{D,O}^n = X^n\mathcal{O}_{D,O}$. Mais dire que $F \in X^n\mathcal{O}_{D,O}$ signifie qu'il existe $G \in k[X]$ avec $G(P) \neq 0$ tel que $FG \in (X^n) \subset k[X]$, c'est a dire avec $val(G) = 0$ et $val(F) = val(F) + val(G) = val(FG) \geq n$.

3.5. Tangentes, points d'inflexions

3.5.1. Définition Soient C et D les diviseurs de F et G et P un point du plan. Alors, la *multiplicité d'intersection* de C et D en P est

$$I(C, D; P) := dim_k \mathcal{O}_{\mathbb{A}^2,P}/(F, G)$$

dans le cas affine et

$$I(C, D; P) := dim_k \mathcal{O}_{\mathbb{P}^2,P}/(F/L^{degF}, G/L^{degG}),$$

L étant une forme linéaire telle que $L(P) \neq 0$, dans le cas projectif.

• Cette définition a bien un sens : Si M est une autre forme linéaire telle que $M(P) \neq 0$, alors $F/M^{degF} = (L/M)^{degF} F/L^{degF}$ et $G/M^{degG} = (L/M)^{degG} G/L^{degG}$. On voit donc que dans la définition de I, l'idéal $(F/L^{degF}, G/L^{degG})$ ne dépend pas du choix de L.

• Si Φ est un changement de coordonnées, alors $I(\Phi^{-1}(C), \Phi^{-1}(D); P) = I(C, D; \Phi(P))$: Dans le cas projectif, par exemple, on sait qu'un changement de coordonnées induit un automorphisme de $\mathcal{O}_{\mathbb{P}^2,P}$ et il suffit donc de remarquer que $\Phi_P^*(F/L^d) = \Phi^*(F)/\Phi^*(L)^d$ et que $\Phi^*(L)$ est une forme linéaire tel que $\Phi^*(L)(P) \neq 0$ car $L(\Phi(P)) \neq 0$.

• Si P est un point du plan affine, on a $I(C, D; P) = I(C_*, D_*; P)$: On sait que l'application $F \longmapsto F_*$, fournit un isomorphisme $F = G/H \longmapsto F_* = G_*/H_*$, $\mathcal{O}_{\mathbb{P}^2,P} \xrightarrow{\sim} \mathcal{O}_{\mathbb{A}^2,P}$. On a donc un isomorphisme

$$\mathcal{O}_{\mathbb{P}^2,P}/(F/Z^{degF}, G/Z^{degG}) \xrightarrow{\sim} \mathcal{O}_{\mathbb{A}^2,P}/(F_*, G_*).$$

• Si D est une courbe affine irréductible non singulière en P, si C est le diviseur de F et si f est la restriction de F à D, alors $I(C, D; P) = v_{D,P}(f)$: En effet, on a vu que

$$\mathcal{O}_{\mathbb{A}^2,P}/(F, G) \tilde{=} (\mathcal{O}_{\mathbb{A}^2,P}/G)/F(\mathcal{O}_{\mathbb{A}^2,P}/G) \tilde{=} \mathcal{O}_{D,P}/f.$$

et on sait que $v_{D,P}(f) = dim_k \mathcal{O}_{D,P}/f$.

3.5.2. Définition Si $I(C, D; P) > m_P(C) m_P(D)$, on dit que les diviseurs C et D sont *tangents en P*. Les *tangentes* à C en un point P sont les droites tangentes à C en P. On dit que P est un *point ordinaire* de C si le nombre de tangentes à C en P

est $m_P(C)$.

• Si Φ est un changement de coordonnées et D et C tangents en $\Phi(P)$, alors $\Phi^{-1}(D)$ est tangent à $\Phi^{-1}(C)$ en P : On sait que les invariants $I(C, D; P)$ et $m_P(C)$ sont préservés par changement de coordonnées.

• Les diviseurs C et D sont tangents C en un point P du plan affine si et seulement si C_* et D_* sont tangentes en P : On sait que $I(C, D; P) = I(C_*, D_*; P)$ et que $m_P(C) = m_P(C_*)$.

3.5.3. Proposition Si F_m est la composante homogène de plus bas degré de $F \in k[X, Y]$, alors les tangentes au diviseur de F en O sont les composantes du diviseur de F_m.

Démonstration : Soit D une droite passant par O. Nous voulons montrer que le diviseur C de F et la droite D sont tangents en O si et seulement si D est une composante du diviseur de F_m. On a $m_O(D) = 1$, $m_O(C) = degF_m = val(F)$. De plus, quitte à faire un changement de coordonnées, on peut supposer que D est l'axe des X si bien que $I(C, D; P) = v_{D,O}(F(X, 0)) = val(F(X, 0))$. On voit donc que C et D sont tangentes en O si et seulement si $val(F(X, 0)) > val(F)$, ce qui signifie bien que Y divise F_m.

3.5.4. Proposition Si P est un point non singulier du diviseur C de F, alors, la tangente à C en P est la droite d'équation

$$\frac{dF}{dX}(P)(X - a) + \frac{dF}{dY}(P)(Y - b) = 0,$$

si $P := (a, b)$ dans le cas affine, et

$$\frac{dF}{dX}(P)\ X + \frac{dF}{dY}(P)\ Y + \frac{dF}{dZ}(P)\ Z = 0$$

dans le cas projectif.

Démonstration : Cas affine : Si $P = O$, on sait que la tangente à C en P est le diviseur de la composante homogène de degré 1 de F, c'est à dire de $\frac{dF}{dX}(O)\,X + \frac{dF}{dY}(O)\ Y$. En général, on considère la translation Φ de vecteur $\overrightarrow{OP}$. Si D est la droite d'équation $L = 0$ avec $L = \frac{dF}{dX}(P)(X - a) + \frac{dF}{dY}(P)(Y - b)$, alors $\Phi^{-1}(D)$ est la droite d'équation $\Phi^*(L) = 0$. Puisque Φ est une translation, on a $\Phi^*(F)'(O) = \Phi^*(F')(O) = F'(\Phi(O)) = F'(P)$ et on voit donc que $\Phi^*(L) = \frac{d}{dX}(\Phi^*(F))(O)\ X + \frac{d}{dY}(\Phi^*(F))(O)\ Y$. Cela montre que $\Phi^{-1}(D)$ est la tangente à $\Phi^{-1}(C)$ en O. Puisque les tangentes sont conservées par changement de coordonnées, D est

bien la tangente à C en 0.

Cas projectif : Quitte à échanger X ou Y avec Z, on peut supposer que $P \in C_*$. On sait que si F est de degré r, alors $XdF/dX + YdF/dY + ZdF/dZ = rF$. Il suit que si $P = (a, b)$, alors $adF/dX(a, b, 1) + bdF/dY(a, b, 1) + dF/dZ(a, b, 1) = 0$ et on a donc

$$\frac{dF_*}{dX}(P)(X-a) + \frac{dF_*}{dY}(P)(Y-b) = \frac{dF}{dX}(a, b, 1)(X-a) + \frac{dF}{dY}(a, b, 1)(Y-b)$$
$$= \frac{dF}{dX}(a, b, 1)\, X + \frac{dF}{dY}(a, b, 1)\, Y + \frac{dF}{dZ}(a, b, 1)\ .$$

On voit donc que si D est la droite d'équation

$$\frac{dF}{dX}(a, b, 1)\, X + \frac{dF}{dY}(a, b, 1)\, Y + \frac{dF}{dZ}(a, b, 1)\, Z = 0,$$

alors D_* est la tangente à C en P. Il suit que D est bien la tangente à C en P.

3.5.5. Définition Soient C un diviseur effectif, P un point non singulier de C et Δ la tangente à C en P. On dit que P est un *point d'inflexion* de C si $I(C, \Delta; P) > 2$.

• Soit Φ un changement de coordonnées, C un diviseur du plan et P un point du plan. Alors, P est un point d'inflexion de $\Phi^{-1}(C)$ si et seulement si $\Phi(P)$ est un point d'inflexion de C : Clair.

• Un point P du plan affine est un point d'inflexion de C_* si et seulement si P est un point d'inflexion de C : Clair.

• Si C est le diviseur de $F = F_1 + \ldots + F_d = 0$ avec F_i homogène de degré i et $F_1 \neq 0$. Alors, O est un point d'inflexion de C si et seulement si F_1 divise F_2 : On peut supposer que la tangente à C est l'axe des X et donc que $F_1 = Y$. Dans ce cas, O est un point d'inflexion si et seulement si $val\ F(X, 0) > 2$, ce qui signifie que $F_2(X, 0) = 0$ et donc que Y divise F_2.

3.5.6. Définition Si $F \in k[X_1, \ldots, X_n]$, le *hessien* de F est $Hess(F) = det(F'')$.

• Si Φ est un changement de coordonnées affines, alors $Hess(\Phi^*(F)) = (det\vec{\Phi})^2\Phi^*(Hess(F))$: On sait que $\Phi^*(F)' = \Phi^*(F')\Phi'$ et on en déduit que $\Phi^*(F)'' = \Phi^*(F')'\Phi' = (\Phi^*(F'')\Phi')\Phi'$. On a donc $Hess(\Phi^*(F)) = det\Phi^*(F)'' = det\Phi^*(F'')det\vec{\Phi}^2 = \Phi^*(detF'')(det\vec{\Phi})^2 = (det\vec{\Phi})^2\Phi^*(Hess(F))$.

3.5.7. Proposition (*Car $k \neq 2$*) Soit C un diviseur effectif du plan projectif ne contenant pas de droite. Supposons que C soit le diviseur de F et soit H le

hessien de F. Alors, un point non singulier P de C est un point d'inflexion si et seulement si $H(P) = 0$.

Démonstration : On peut supposer que $P = O$ et que la tangente à C en O est l'axe des X. On peut donc écrire $F_* = Y + aX^2 + bXY + cY^2 \ mod\ (X, Y)^3$ si bien que

$$F''(O) = \textbf{Erreur!}\ ) \ .$$

On a donc $H(O) = -2a$ et on sait que O est un point d'inflexion si et seulement si $a = 0$.

3.6. Multiplicité d'intersection

3.6.1. Proposition (i) On a $I(C, D; P) \neq 0$ si et seulement si $P \in C$ et $P \in D$.

(ii) On a $I(C, D; P) = \infty$ si et seulement si C et D ont une composante commune passant par P.

(iii) On a $I(C, D + E; P) = I(C, D; P) + I(C, E; P)$.

Démonstration : Il suffit de traiter le cas affine et on écrit $C = [F]$, $D = [G]$ et $E = [H]$.

On a $I(C, D; P) = 0$ si et seulement si $(F, G) = \mathcal{O}_{\mathbb{A}^2,P}$, c'est à dire s'il existe A, $B \in k[X, Y]$ tels que $(AF + BG)(P) \neq 0$ et cela implique que $F(P) \neq 0$ ou $G(P) \neq 0$, c'est à dire que $P \notin C$ ou $P \notin D$. Réciproquement, si pour tout A, $B \in k[X, Y]$, on a $(AF + BG)(P) = 0$, il est clair que $F(P) = G(P) = 0$. L'assertion i) est donc démontrée.

On démontre ensuite iii) dans le cas où $P \notin E$: Si $H(P) \neq 0$, alors $(F, GH) = (F, G) \subset \mathcal{O}_{\mathbb{A}^2,P}$ et on a donc bien $I(C, D + E; P) = I(C, D; P)$.

On démontre maintenant l'assertion ii) : Grâce à i) et au cas particulier de iii) que nous venons de traiter, on peut supposer que toutes les composantes de C et de D passent par P. Si C et D n'ont pas de composante commune, alors $V(F, G)$ est fini, si bien que $dim_k k[X, Y]/(F, G) < \infty$. On voit donc que $\mathcal{O}_{\mathbb{A}^2,P}/(F, G)$ qui est un facteur de $k[X, Y]/(F, G)$ est de dimension finie. Réciproquement, si C et D ont une composante irréductible commune E passant par P, on écrit $I(E) = (H)$ si bien que $E = V(H)$ et $k[E] = k[X, Y]/(H)$. Puisqu'une courbe plane est infinie, on a $dim_k\ k[E] = \infty$. Puisque $\mathcal{O}_{E,P} \supset k[E]$, on en déduit que $dim_k \mathcal{O}_{E,P} = \infty$. Enfin, on a $\mathcal{O}_{\mathbb{A}^2,P}/(H) = \mathcal{O}_{E,P}$ et $(F, G) \subset (H)$ si bien que $I(C, D; P) \geq dim_k\ \mathcal{O}_{E,P}$.

Enfin, on démontre l'assertion iii) : Grâce au cas particulier déjà traité et à (ii), on peut supposer que C et D n'ont pas de composante en commun. Montrons

que le noyau de l'application composée de la multiplication par G sur $\mathcal{O}_{\mathbb{A}^2,P}$ et de la surjection canonique $\mathcal{O}_{\mathbb{A}^2,P} \longrightarrow \mathcal{O}_{\mathbb{A}^2,P}/(F, GH)$ n'est autre que $(F, H)\mathcal{O}_{\mathbb{A}^2,P}$. On a bien $G(F, H) \subset (F, GH)$. Réciproquement, si C/S, A/S et $B/S \in \mathcal{O}_{\mathbb{A}^2,P}$ sont tels que $G(C/S) = (A/S)F + (B/S)GH$ alors $AF = G(C - BH)$. Puisque F et G n'ont pas de facteur commun, F divise $C - BH$ et on peut donc écrire $C - BH = DF$ si bien que $C/S = (D/S)F + (B/S)H \in (F, H)$. On dispose donc d'une suite exacte courte

$$0 \longrightarrow \mathcal{O}_{\mathbb{A}^2,P}/(F, H) \longrightarrow \mathcal{O}_{\mathbb{A}^2,P}/(F, GH) \longrightarrow \mathcal{O}_{\mathbb{A}^2,P}/(F, G) \longrightarrow 0,$$

d'où la formule.

3.6.2. Théorème On a toujours $I(C, D; P) \geq m_P(C)m_P(D)$. De plus, C et D sont tangentes en P si et seulement si C et D ont une tangente commune en P.

Démonstration : On peut supposer que $P = O$ et que C et D sont des courbes affines sans composante commune dont toutes les composantes passent par O. On pose $m = val(F)$ et $n = val(G)$ et on note F_m et G_n les composantes homogènes de plus bas degré de F et G.

Si $val(A) \geq n$ alors $val(AF) \geq m + n$ et si $val(B) \geq m$ alors $val(BG) \geq m + n$. On voit donc que l'application linéaire $(A, B) \longmapsto AF + BG$, $k[X, Y] \oplus k[X, Y] \longrightarrow k[X, Y]$ induit une application linéaire

$$k[X, Y]/(X, Y)^n \oplus k[X, Y]/(X, Y)^m \longrightarrow k[X, Y]/(X, Y)^{m+n}.$$

Si cette application n'est pas injective, il existe A tel que $val(A) < n$ (ou B tel que $val(B) < m$) et $val(AF + BG) \geq m + n$. On a donc $val(AF + BG) > val(AF)$. En notant A_d et B_e les parties homogènes de plus bas degré de A et B, on voit que $A_dF_m + B_eG_n = 0$, ou encore que $A_dF_m = -B_eG_n$. Puisque $d < n$, G_n ne divise pas A_d si bien que F_m et G_n ont un facteur commun. Il suit que C et D ont une tangente en commun. Réciproquement, si la droite d'équation L est une tangente commune à C et D en O, la partie homogène de plus bas degré de F s'écrit $-LB$ avec $val(B) = m - 1$ et celle de G s'écrit LA avec $val(A) = n - 1$, et on a nécessairement $val(AF + BG) > m + n - 1$, ce qui montre que l'application n'est pas injective.

Nous disposons donc d'une suite exacte à droite

$$\begin{aligned} k[X, Y]/(X, Y)^n \oplus k[X, Y]/(X, Y)^m &\longrightarrow k[X, Y]/(X, Y)^{m+n} \\ &\longrightarrow k[X, Y]/((X, Y)^{m+n} + (F, G)) \longrightarrow 0 \end{aligned}$$

et nous venons de voir que celle ci est exacte à gauche si et seulement si C et D ont des tangentes distinctes en O. On en déduit que $dim_k\ k[X, Y]/((X, Y)^{m+n} +$

$(F, G)) \geq mn$ avec égalité si et seulement si C et D n'ont pas de tangente en commun.

Si $V(F, G) = \{O, P_1, \ldots, P_s\}$, on sait qu'il existe $H \in k[X, Y]$ tel que $H(P_k) = 0$ pour $k = 1, \ldots, s$ et $H(O) \neq 0$. On a donc $HX \in I(V(F, G)) = \sqrt{(F, G)}$ et il existe donc N tel que $(HX)^N \in (F, G)$ si bien que $X^N \in (F, G)\mathcal{O}_{\mathbb{A}^2,O}$. De même, on a $Y^N \in (F, G)\mathcal{O}_{\mathbb{A}^2,O}$ et on voit donc que pour $d \geq 2N$, on a $(X, Y)^d \subset (F, G)\mathcal{O}_{\mathbb{A}^2,O}$. Montrons par récurrence descendante que, si C et D n'ont pas de tangente en commun, cette inclusion est vraie pour $d \geq m + n$: On écrit les parties homogènes de plus bas degré de F et G comme produit de formes linéaires $L_1 \ldots L_m$ et $M_1 \ldots M_n$. On pose $L_i = L_m$ pour $i \geq m$ et $M_j = L_n$ pour $j \geq n$. Si $d \geq m + n$, alors $i \geq m$ (ou $d - i \geq n$) et on a donc $L_1 \ldots L_i M_1 \ldots M_{d-i} = (L_1 \ldots L_m)(L_{m+1} \ldots L_i M_1 \ldots M_{d-i}) = H \ mod \ F$ avec $val(H) > d$. Par récurrence, on a $H \in (F, G)\mathcal{O}_{\mathbb{A}^2,O}$ et donc $L_1 \ldots L_i M_1 \ldots M_{d-i} \in (F, G)\mathcal{O}_{\mathbb{A}^2,O}$. Pour conclure, il suffit donc de montrer que si $L_1, L_2, \ldots$ et $M_1, M_2, \ldots$ sont des suites de formes linéaires telles que aucune des M_j n'est proportionnelle à l'une des L_i, alors, pour tout d, les $L_1 \ldots L_i M_1 \ldots M_{d-i}$ forment une base de l'espace $k[X, Y]_d$ des polynômes homogènes de degré d : Pour des questions de dimension, il suffit de montrer que ceux ci sont linéairement indépendants. On procède par récurrence sur d : Si $\Sigma \alpha_i L_1 \ldots L_i M_1 \ldots M_{d-i} = 0$, alors $\alpha_0 M_1 \ldots M_d + L_1 \Sigma \alpha_i L_2 \ldots L_i M_1 \ldots M_{d-i} = 0$. Puisque L_1 ne divise pas $M_1 \ldots M_d$, on a nécessairement $\alpha_0 = 0$ et $\Sigma \alpha_i L_2 \ldots L_i M_1 \ldots M_{d-i} = 0$, ce qui par récurrence, implique que $\alpha_1 = \ldots = \alpha_d = 0$.

Finalement, puisque $V((X, Y)^{m+n} + (F, G)) = \{O\}$, on a un isomorphisme $k[X, Y]/((X, Y)^{m+n} + (F, G)) \tilde{\to} \mathcal{O}_{\mathbb{A}^2,O}/((X, Y)^{m+n} + (F, G))$ qui devient lorsque C et D n'ont pas de tangente commune, $k[X, Y]/((X, Y)^{m+n} + (F, G)) \tilde{\to} \mathcal{O}_{\mathbb{A}^2,O}/(F, G)$. On en déduit comme annoncé que $I(C, D; O) \geq mn$ avec égalité si et seulement si C et D n'ont pas de tangente en commun en O.

3.7. Théorème de Bézout

3.7.1. Théorème (de Bézout) Si C et D sont deux diviseurs effectifs du plan projectif sans composante commune, alors

$$\sum_P I(C, D; P) = degC.degD$$

Démonstration : On note avec un indice d l'espace des éléments homogènes de degré d (ou nuls) dans une algèbre graduée. On écrit $C = [F]$, $D = [G]$, $m = deg\ F$, $n = deg\ G$ et $R := k[X, Y, Z]/(F, G)$. Il est clair que si $d \geq m$ et $A \in k[X, Y, Z]_{d-m}$, alors $AF \in k[X, Y, Z]_d$ et que si $d \geq n$ et $B \in k[X, Y, Z]_{d-n}$, alors $BG \in k[X, Y, Z]_d$. On en déduit, pour tout $d \geq m, n$ une application linéaire $(A, B) \longmapsto AF$

$+ BG$, $k[X, Y, Z]_{d-m} \times k[X, Y, Z]_{d-n} \longrightarrow k[X, Y, Z]_d$. De même, si $d \geq m + n$ et $C \in k[X, Y, Z]_{d-m-n}$ alors $CG \in k[X, Y, Z]_{d-m}$ et $-CF \in k[X, Y, Z]_{d-n}$. On définit ainsi une application linéaire $k[X, Y, Z]_{d-m-n} \longrightarrow k[X, Y, Z]_{d-m} \times k[X, Y, Z]_{d-n}$, $C \longmapsto (CG, -CF)$ et on vérifie aisément que la suite

$$0 \to k[X, Y, Z]_{d-m-n} \to k[X, Y, Z]_{d-m} \times k[X, Y, Z]_{d-n} \to k[X, Y, Z]_d \to R_d \to 0$$

est exacte. Puisque $dim_k\, k[X, Y, Z]_d = d(d+1)/2$, on en déduit que $dim_k R_d = mn$ pour $d \geq m + n$.

Quitte à faire un changement de coordonnées, on peut supposer que C et D ne se coupent pas à l'infini. Si pour un polynôme $H \in k[X, Y, Z]$, on note $H_\infty := H(X, Y, 0) \in k[X, Y]$, cette condition s'écrit $V_p(F_\infty, G_\infty) = \emptyset \subset \mathbb{P}^1$, ou encore $V(F_\infty, G_\infty) = \{O\} \subset \mathbb{A}^2$, ce qui signifie que F_∞ et G_∞ n'ont pas de facteur commun. Montrons que, si on note avec une minuscule h l'image de $H \in k[X, Y, Z]$ dans R, alors la multiplication par z sur R est injective : Si $H \in k[X, Y, Z]$ est tel que $zh = 0$, on peut écrire $ZH = AF + BG$ et on a donc $0 = A_\infty F_\infty + B_\infty G_\infty$. Puisque F_∞ et G_∞ n'ont pas de facteur commun, on peut écrire $B_\infty = F_\infty C$ avec $C \in k[X, Y]$. On a donc $(A + CG)_\infty = 0$ et on peut écrire $A + CG = ZA_1$. De même, on peut écrire $B - CF = ZB_1$, si bien que $H = A_1F + B_1G$ et donc $h = 0$. Par composition, on voit que pour tout r, la multiplication par z^r est injective sur R. Celle ci induit donc une application (linéaire) injective de R_{m+n} sur R_{m+n+r} qui est nécessairement un isomorphisme car ces deux espaces ont même dimension mn. On choisit alors $H_1, \ldots, H_{m\,n} \in k[X, Y, Z]$ tels que $\{h_i\}$ soit une base de R_{m+n} et on sait qu'alors $\{z^r h_i\}$ est une base de R_{m+n+r}. Montrons que les images des H_{i*} dans $R_* := k[X, Y]/(F_*, G_*)$ forment une base de R_*. Si $H \in k[X, Y]$ est de degré r, alors $z^{n+m}h^* \in R_{n+m+r}$ et on peut donc écrire $z^{n+m}h^* = \Sigma\, \alpha_i z^r h_i$, c'est à dire $Z^{n+m}H^* = \Sigma\, \alpha_i Z^r H_i + AF + BG$, et on a donc $H = \Sigma\, \alpha_i H_{i*} + A_*F_* + B_*G_*$. Le système est donc générateur et il reste à montrer qu'il est libre : Si $\Sigma\, \alpha_i H_{i*} = AF_* + BG_*$, alors $(\Sigma\, a_i H_{i*}\,)^* = (AF_* + BG_*,)^*$ et on peut donc écrire $Z^r \Sigma a_i H_i = Z^{n+r-j}A^*F + Z^{m+r-k}B^*G$ avec $j = degA$ et $k = degB$. On a donc $\Sigma\, \alpha_i z^r h_i = 0$, ce qui implique que tous les α_i sont nuls. On voit donc que $dim\, R_* = mn$ et on en déduit, puisque C et D ne se coupent pas à l'infini, que

$$\sum_P\, I(C, D; P) = \sum_P\, I(C_*, D_*; P) = dim_k\, R_* = mn.$$

Corollaire Si C et D sont des diviseurs effectifs sans composantes en commun, alors $\sum_P\, m_P(C)m_P(D) \leq degC.degD$.

Il suffit bien sur de traiter le cas projectif et on a alors

$$\sum_P\, m_P(C)m_P(D) \leq \sum_P\, I(C, D; P) = degC.degD.$$

Corollaire Un diviseur non singulier du plan projectif est irréductible.

On applique Bézout à deux composantes de C.

Corollaire Si C est une courbe irréductible de degré au moins deux et P et Q deux points de C, alors $m_P(C) + m_Q(C) \leq degC$.

On applique Bézout à C et à (PQ).

Corollaire Si C est une courbe irréductible, alors

$$\sum_P m_P(C)(m_P(C) - 1)) \leq degC(degC - 1).$$

Il suffit de traiter le cas affine. De plus, quitte à échanger X avec Y, on peut supposer que C est le diviseur de $F \in k[X, Y]$ avec $dF/dX \neq 0$. Il suffit alors de montrer d'une part que, si C' est le diviseur de dF/dX, alors $deg\ C' \leq degC - 1$ et d'autre part, que pour tout P, $m_P(C') \geq m_P(C) - 1$. Pour la première assertion, il suffit de remarquer que $degdF/dX < degF$. Pour la seconde, on peut, quitte à faire une translation, supposer que $P = O$ et il suffit alors de remarquer que $val(dF/dX) \geq val(F) - 1$.

Corollaire Une courbe irréductible de degré n a au plus $n(n-1)/2$ points singuliers.

3.7.2. Définition Le groupe des 0-*cycles* du plan (affine ou projectif) est le groupe abélien libre sur les points du plan. Le degré du 0-cycle $\Sigma i_k P_k$ est $d := \Sigma i_k$. Un 0-cycle $\Sigma i_k P_k$ est *positif* si les i_k sont des entiers positifs. Si C et D sont deux diviseurs effectifs du plan sans composantes communes, le *cycle d'intersection* de C et D est $C.D := \Sigma I(C, D; P).P$.

• On a toujours $C.D = D.C$ et $C.(D + E) = C.D + C.E$: Clair.

• Si C et D sont deux diviseurs effectifs du plan projectif sans composantes communes de degrés respectifs m et n, alors $C.D$ est un 0-cycle positif de degré mn : C'est Bézout.

Exercices du chapitre III

1. Points singuliers des courbes affines planes

1.1. Déterminer les points singuliers du diviseur de $Y - X^2$.

1.2. Idem avec $Y^2 - X^3$.

1.3. Idem avec $Y^2 - X^3 - X^2$.

1.4. Idem avec $Y^3 - (X^2 + Y^2)^2 - 3X^2Y$.

1.5. Idem avec $4X^2Y^2 - (X^2 + Y^2)^3$.

1.6. Idem avec $Y^3 - Y^2 + X^3 - X^2 + 3XY^2 + 3X^2Y + 2XY$.

1.7. Idem avec $X^4 + Y^4 - X^2Y^2$.

1.8. Idem avec $X^2 - X^4 - Y^4$.

1.9. Idem avec $XY - X^6 - Y^6$.

1.10. Idem avec $X^3 - Y^2 - X^4 - Y^4$.

1.11. Idem avec $X^2Y + XY^2 - X^4 - Y^4$.

1.12. Idem avec $Y^2 + (X^2 - 5)(4X^4 - 20X^2 + 25)$.

2. Singularités des courbes affines planes

2.1. $(Car\ k \neq 2)$ Soit $F := Y^2 - X^3 + X$. Calculer $\frac{dF}{dX}$ et $\frac{dF}{dY}$ puis montrer que le diviseur de F est non singulier.

2.2. $(Car\ k \neq 2)$ Déterminer les points singuliers du diviseur de $X^4 - Y^4 - \lambda X^3 + XY^2 = 0$, $\lambda \in k$.

2.3. $(k = \mathbb{C})$ Idem avec $X^3 + Y^3 + 1 - 3\lambda XY$, $\lambda \in k$.

2.4. ($Car\ k \neq 2$) Idem avec $Y^2 - F$, $F \in k[X]$.

2.5. ($Car\ k \neq 2$) Montrer que l'origine est un point double de la courbe d'équation $X^2Y^2 + X^2 + Y^2 = 2XY(X + Y + 1)$ et que c'est l'unique point singulier de C.

2.6. ($k = \mathbb{C}$) Montrer que les composantes du diviseur de $X^3 + Y^3 - 3XY + 1$ sont trois droites que l'on déterminera.

2.7. Montrer qu'une conique irréductible est non singulière.

2.8. Montrer que si P est un point non singulier d'une courbe irréductible C, il n'existe pas de fonction rationnelle f sur C qui ait un pôle en P et telle que $f(1 - f)$ soit régulière en P. Montrer que cela est faux si P est singulier.

3. Singularités des courbes projectives planes

3.1. Déterminer les points singuliers du diviseur de $XY^4 - YZ^4 - XZ^4$.

3.2. Idem avec $X^2Y^3 - X^2Z^3 - Y^2Z^3$.

3.3. Idem avec $Y^2Z - X(X - Z)(X - \lambda Z)$, $\lambda \in k$.

3.4. Idem avec $X^n + Y^n + Z^n = 0$, $n > 0$.

4. Tangentes aux points singuliers des courbes affines

4.1. Déterminer en chaque point singulier du diviseur de $Y^2 - X^3 + X$, la multiplicité et les équation des tangentes.

4.2. Idem avec $Y^2 - X^3$.

4.3. Idem avec $Y^2 - X^3 - X^2$.

4.4. Idem avec $Y^3 - (X^2 + Y^2)^2 - 3X^2Y$.

4.5. Idem avec $4X^2Y^2 - (X^2 + Y^2)^3$.

4.6. Idem avec $Y^3 - Y^2 + X^3 - X^2 + 3XY^2 + 3X^2Y + 2XY$.

4.7. Idem avec $X^4 + Y^4 - X^2Y^2$.

4.8. Idem avec $X^2 - X^4 - Y^4$.

4.9. Idem avec $XY - X^6 - Y^6$.

4.10. Idem avec $X^3 - Y^2 - X^4 - Y^4$.

4.11. Idem avec $X^2Y + XY^2 - X^4 - Y^4$.

4.12. Idem avec $Y^2 + (X^2 - 5)(4X^4 - 20X^2 + 25)$.

5. Tangentes aux courbes affines

5.1. ($Car\ k \neq 2$) Déterminer en chaque point singulier du diviseur de $X^4 - Y^4 - \lambda X^3 + XY^2$, $\lambda \in k$, la multiplicité et les équation des tangentes.

5.2. ($Car\ k \neq 2$) Idem avec $Y^2 - F$, $F \in k[X]$.

5.3. Déterminer les points du diviseur de $Y^2 + (X^2 - 5)(4X^4 - 20X^2 + 25)$ en lesquels la tangente est horizontale ou verticale.

5.4. ($Car\ k \neq 2$) On considère la courbe affine plane C d'équation $X^2Y^2 + X^2 + Y^2 = 2XY(X + Y + 1)$. Montrer que la diagonale principale Δ est l'unique tangente à l'origine et que C n'a pas de tangente horizontale. Déterminer les points de C en lesquels la tangente est parallèle à Δ ainsi qu'a l'autre diagonale Δ' .

5.5. ($Car\ k \neq 2$) Montrer que si la droite Δ de pente finie c est tangente à la courbe C d'équation $Y^2 = X^3 - X$ en P, d'abscisse a et coupe C en un autre point P', d'abscisse a', alors $2a + a' = c^2$.

5.6. ($Car\ k \neq 2$) Soit C la courbe d'équation $Y^2 = X^3 - X$, f'_x et f'_y les restrictions à C de $\frac{dF}{dX}$ et $\frac{dF}{dY}$, $t := -\frac{f_x}{f_y}$, $u := t^2 - 2x$, $v := t(u - x) + y$ et C_0 l'ouvert de C défini par $y \neq 0$. Montrer que l'application $\psi : C_0 \longrightarrow \mathbb{A}^2$, $P \longmapsto P' := (u(P), v(P))$ est à valeurs dans C.

5.7. Soit C la courbe d'équation $Y^2 = X^3 - X$, $V := C \times C$, x, y, x', y' les fonctions coordonnées sur V, $r := \frac{y'-y}{x'-x}$, $m := r^2 - (x + x')$, $n := r(m - x) + y$ et V_0 l'ouvert de V défini par $y + y' \neq 0$. Montrer que l'application φ définie sur V_0 dont les composantes sont m et n est à valeurs dans C.

5.8. Soit C une courbe affine plane irréductible. On suppose que C passe par $J = (0, 1)$ et que la tangente D à C en J n'est pas horizontale. Si $P \in C$ est distinct de J, on note D_P la droite joignant les points J et P et si D_P n'est pas horizontale, on note $\varphi(P)$ le point d'intersection de D_P avec l'axe des X (identifié à $\mathbb{A}^1$). Montrer que φ est régulière en J et que $\varphi(J)$ est l'intersection de D et de l'axe des X.

6. Tangentes aux courbes projectives

6.1. ($Car\ k \neq 2$) Déterminer en chaque point singulier du diviseur de $XY^4 - YZ^4 - XZ^4$ la multiplicité et les équation des tangentes.

6.2. Idem avec $X^2Y^3 - X^2Z^3 - Y^2Z^3$.

6.3. Idem avec $Y^2Z - X(X - Z)(X - \lambda Z)$, $\lambda \in k$.

6.4. ($Car\ k \neq 2$) Montrer que deux cubiques irréductibles avec point de rebroussement sont projectivement équivalentes.

6.5. Idem avec deux cubiques irréductibles avec point double ordinaire.

7. Points d'inflexion ($Car\ k \neq 2$)

7.1. Déterminer les points d'inflexion du diviseur de $Y - X^3$.

7.2. Idem avec $Y^2 - X^3$.

7.3. Idem avec $Y^2 - X^3 + X$.

7.4. Montrer que le point à l'infini de la courbe C d'équation $Y = X^3 - X$ est un point d'inflexion et déterminer la tangente en ce point.

7.5. Montrer qu'une conique irréductible ne possède pas de point d'inflexion.

8. Multiplicité d'intersection à l'origine

8.1. Déterminer les multiplicités d'intersection à l'origine des diviseurs de $Y - X^2$ et $Y^2 - X^3 + X$.

8.2. Idem avec $Y - X^2$ et $Y^2 - X^3$.

8.3. Idem avec $Y^2 - X^3 + X$ et $Y^2 - X^3$.

8.4. Idem avec $Y - X^2$ et $Y^2 - X^3 - X^2$.

8.5. Idem avec $Y^2 - X^3 + X$ et $Y^2 - X^3 - X^2$.

8.6. Idem avec $Y^2 - X^3$ et $Y^2 - X^3 - X^2$.

8.7. Idem avec $Y - X^2$ et $Y^3 - (X^2 + Y^2)^2 - 3X^2Y$.

8.8. Idem avec $Y^2 - X^3 + X$ et $Y^3 - (X^2 + Y^2)^2 - 3X^2Y$.

8.9. Idem avec $Y^2 - X^3$ et $Y^3 - (X^2 + Y^2)^2 - 3X^2Y$.

8.10. Idem avec $Y^2 - X^3 - X^2$ et $Y^3 - (X^2 + Y^2)^2 - 3X^2Y$.

8.11. Idem avec $Y - X^2$ et $4X^2Y^2 - (X^2 + Y^2)^3$.

8.12. Idem avec $Y^2 - X^3 + X$ et $4X^2Y^2 - (X^2 + Y^2)^3$.

8.13. Idem avec $Y^2 - X^3$ et $4X^2Y^2 - (X^2 + Y^2)^3$.

8.14. Idem avec $Y^2 - X^3 + X^2$ et $4X^2Y^2 - (X^2 + Y^2)^3$.

8.15. Idem avec $Y^3 - (X^2 + Y^2)^2 - 3X^2Y$ et $4X^2Y^2 - (X^2 + Y^2)^3$.

9. Points d'intersection de deux courbes

9.1. Chercher les points d'intersection des diviseurs de $Y^2 - X(X - 2)(X + 1)$ et $Y^2 - 2X + X^2$ et déterminer les multiplicités d'intersection en ces points.

9.2. Idem avec $X^2+Y^2+X^3+Y^3$ et X^3+Y^3-2XY.

9.3. Idem avec $Y^5-X(Y^2-X)^2$ et $X^2-Y^4-Y^3$.

9.4. Idem avec $Y^3-(X^2+Y^2)^2-3X^2Y$ et $(X^2+Y^2)^3-4X^2Y^2$.

9.5. Idem avec $Y^2Z-X(X-2Z)(X+Z)$ et Y^2+X^2-2XZ.

9.6. Idem avec $(X^2+Y^2)Z+X^3+Y^3$ et X^3+Y^3-2XYZ.

9.7. Idem avec $Y^5-X(Y^2-XZ)^2$ et $Y^4+Y^3Z-X^2Z^2$.

9.8. Idem avec $(X^2+Y^2)^2=Y^3Z-3X^2YZ$ et $(X^2+Y^2)^3=4X^2Y^2Z^2=0$

9.9. ($Car\ k\neq 2$) Soit C la courbe affine plane d'équation $X^2Y^2+X^2+Y^2=2XY(X+Y+1)$ et $s:\mathbb{A}^2\longrightarrow\mathbb{A}^2$, $(a,b)\longmapsto(-a,-b)$ la symétrie centrale de centre O. Déterminer les points d'intersection de C et $s^{-1}(C)$ et leur multiplicité d'intersection en ces points.

10. Intersection de fermetures projectives

10.1. Soient C et C' les diviseurs respectifs de $X^4-X^3+2XY^2$ et $X^3-X^2Y-X^2+2Y^2$. Déterminer les points d'intersection de C^* et C'^* ainsi que leurs multiplicités d'intersection en ces points.

10.2. Idem avec les diviseurs de $X^4-Y^4+X^3+Y^3$ et $X^4+Y^4+X^3-Y^3$.

10.3. Idem avec les diviseurs de$(X-1)\ Y^2+X^2Y+X$ et $Y=X^2-2X$.

10.4. Idem avec les diviseurs de $2X^2-Y^2-XY-4\ (X+Y)$ et $X^3-X^2+Y^2$.

10.5. ($Car\ k\neq 2$) Idem avec les diviseurs de $Y^2-2X^3-X^2$ et $Y-\lambda X^2$, $\lambda\in k$.

11. Applications du théorème de Bézout

11.1. Soit C la courbe d'équation $Y^2=X^3-X$, P un point de C et Δ la droite verticale passant par P. Montrer que si Δ n'est pas tangente à C en P, alors Δ coupe C en un unique autre point P' et Δ n'est pas tangente à C en P' .

11.2. Soit P un point de la courbe C d'équation $Y^2 = X^3 - X$ et Δ la droite verticale passant par P. Montrer que si Δ est tangente à C en P, alors $\Delta \cap C = \{P\}$.

11.3. Soit P un point de la courbe C d'équation $Y^2 = X^3 - X$ tel que la tangente Δ à C en P ne soit pas verticale. Montrer que Δ rencontre C en un unique autre point P' éventuellement égal à P.

11.4. Soient P et P' deux points distincts de la courbe C d'équation $Y^2 = X^3 - X$ et Δ la droite joignant P à P'. Montrer que si Δ est tangente à C en P, alors $\Delta \cap C = \{P, P'\}$ et Δ n'est pas tangente à C en P'.

11.5. Soient P et P' deux points distincts de la courbe C d'équation $Y^2 = X^3 - X$ et Δ la droite joignant P à P'. Montrer que si Δ n'est tangente à C ni en P, ni en P' et n'est pas verticale, alors Δ et C se coupent en un troisième point P''.

11.6. Montrer qu'une cubique irréductible a au plus un point double comme singularité.

11.7. Montrer qu'une cubique non singulière a exactement 9 points d'inflexion ou une infinité.

11.8. Montrer que toute cubique non singulière est projectivement équivalente à une courbe de Legendre C^* où C est la courbe d'équation $Y^2 = X(X-1)(X-\lambda)$, $\lambda \in k\backslash\{0,1\}$.

Corrigé des exercices du chapitre III

1.12. Remarquons tout d'abord que $4X^4 - 20X^2 + 25 = (2X^2 - 5)^2$. Nous devons donc résoudre le système suivant

$$\begin{cases} Y^2 + (X^2-5)(2X^2-5)^2 = 0 \\ 2X(2X^2-5)(6X^2-25) = 0 \\ 2Y = 0 \end{cases}$$

En caractéristique 2, on a $Y^2 + (X^2 - 5)(4X^4 - 20X^2 + 25) = (X + Y + 1)^2$ et tous les points sont donc singuliers. Sinon, le système est équivalent au système

$$\begin{cases} (X^2-5)(2X^2-5)^2 = 0 \\ X(2X^2-5)(6X^2-25) = 0 \\ Y = 0 \end{cases} .$$

En caractéristique 5, on a $Y^2 + (X^2 - 5)(4X^4 - 20X^2 + 25) = Y^2 - X^6$ et O est le seul point singulier.

En caractéristique différente de 2 et de 5, il y a exactement deux points singuliers de coordonnées $(\pm\frac{\sqrt{10}}{2}, 0)$.

2.1. On a $\frac{dF}{dX} = -3X^2 + 1$ et $\frac{dF}{dY} = 2Y$. Puisque k est de caractéristique $\neq 2$, on montre sans problème que le système $Y^2 = X^3 - X$, $0 = 3X^2 - 1$ et $2Y = 0$ n'a pas de solution.

2.2. On trouve les points singuliers en résolvant le système

$$\begin{cases} X^4 - Y^4 - \lambda X^3 + XY^2 = 0 \\ 4X^3 - 3\lambda X^2 + Y^2 = 0 \\ -4Y^3 + 2XY = 0. \end{cases}$$

En formant la combinaison $4L_1 - XL_2 - YL_3$, on voit qu'un tel point vérifie les deux équations

$$X^4 - Y^4 = 0 \text{ et } \lambda X^3 - XY^2 = 0.$$

On en déduit la discussion suivante.

a) Si $\lambda \neq \pm 1$, on voit que ces deux équations n'ont pas d'autre solution commune que $X = 0$, $Y = 0$. L'origine est alors l'unique point singulier.

b) Si $\lambda = 1$, les composantes du diviseur sont les droites d'équation $X = \pm Y$ et la conique d'équation $X^2 + Y^2 - X$ qui est non singulière. Il en résulte que les

points singuliers de C sont les points d'intersection de ces trois courbes, c'est à dire l'origine et les points de coordonnés $(1/2, \pm 1/2)$.

c) Le cas $\lambda = -1$ se traite de la même façon.

2.3. On trouve les points singuliers de en résolvant le système

$$\begin{cases} X^3+Y^3+1-3\lambda XY=0 \\ 3(X^2-\lambda Y)=0 \\ 3(Y^2-\lambda X)=0 \end{cases}.$$

On voit qu'un tel point vérifie $X^2=\lambda Y$ et $Y^2=\lambda X$. En remplaçant X^2 et Y^2 par λY et λX dans la première égalité, on voit que $\lambda XY=1$. Puis en remplaçant λY par X^2 que $X^3=1$. Par symétrie, on doit aussi avoir $Y^3=1$ et donc $\lambda^3=1$. On voit donc que le diviseur est non singulier si $\lambda \neq 1, j, j^2$.

On vérifie ensuite que si $\lambda = 1$, les points singuliers sont les points de coordonnées $(1, 1)$, (j, j^2) et (j^2, j), que si $\lambda = j$, ce sont les points de coordonnées $(1, j^2)$, (j, j) et $(j^2, 1)$ et enfin, que si $\lambda = j^2$, ce sont les points de coordonnées $(1, j)$, $(j, 1)$ et (j^2, j^2).

2.5. L'origine est un clairement un point double. De plus, les points de la courbe qui sont singuliers satisfont $X^2Y^2 + X^2 + Y^2 = 2XY(X + Y + 1)$ et $2XY^2 + 2X = 4XY + 2Y(Y + 1)$, soit, puisque k est de caractéristique $\neq 2$, $X^2Y^2 + X^2 + Y^2 = 2XY(X + Y + 1)$ et $XY^2 + X = 2XY + Y(Y + 1)$. En multipliant par X les termes de la seconde équation et en retranchant terme à terme à la première, on voit que les points que nous cherchons satisfont $Y^2 = XY^2 + XY$ et $XY^2 + X = 2XY + Y(Y + 1)$. Mis à part l'origine on voit donc que ces points satisfont $XY = Y - X$ et $XY^2 + X = 2XY + Y(Y + 1)$. En substituant $Y - X$ à XY dans la seconde équation, on trouve $XY = Y - X$ et $XY = 3(X - Y)$, soit, puisque k est de caractéristique $\neq 2$, $X = Y = 0$. On voit donc que O est l'unique point singulier de C.

2.6. Nous savons que les points singuliers sont $P=(1,1)$, $Q=(j,j^2)$ et $R=(j^2,j)$. Si C est réunion de 3 droites, leurs intersections sont les points singuliers de C. Ceci suggère de considérer les droites (PQ), (QR), (RP) qui ont respectivement pour équations

$$jX + j^2Y + 1=0, X + Y + 1=0 \text{ et } j^2X + jY + 1=0.$$

On vérifie alors bestialement que

$$X^3+ Y^3 - 3XY + 1 = (jX + j^2Y + 1)\ (X + Y + 1)\ (j^2X + jY + 1).$$

2.7. Il s'agit de montrer que si P est un point d'une conique irréductible C, alors P est non singulier. Quitte à faire un changement de coordonnées, et à remplacer C par sa partie affine dans le cas projectif, on peut supposer que C est affine et que $P = O$. Si O était un point singulier de C, alors F n'aurait pas de composante homogène de degré ≤ 1 et serait donc un polynôme quadratique homogène. Ce serait donc un produit de facteurs linéaires, ce qui est impossible car C est irréductible.

2.8. Si f n'est pas régulière en P, on a $v_{C,P}(f) < v_{C,P}(1) = 0$ et il suit que $v_{C,P}(1 - f) < 0$. On en déduit que

$$v_{C,P}(f(1-f)) = v_{C,P}(f) + v_{C,P}(1-f) < 0,$$

et $f(1-f)$ n'est pas régulière non plus. Enfin, si C est la courbe d'équation $X^4 - Y^4 = X^3 - XY^2$, alors la fonction $f = y^2/x$, où x et y les restrictions de X et Y, a un pôle en O mais $f(1-f)$ est polynomiale.

4.12. En caractéristique 2, on a $Y^2 + (X^2 - 5)(4X^4 - 20X^2 + 25) = (X + Y + 1)^2$ si bien que tous les points sont singuliers de multiplicité 2 avec tangente d'équation $Y = X + 1$. En caractéristique 5, on a $Y^2 + (X^2 - 5)(4X^4 - 20X^2 + 25) = Y^2 - X^6$ et O est le seul point singulier. C'est un point double avec l'axe des X pour tangente.

Nous avons vu que, en caractéristique différente de 2 et de 5, il y a exactement deux points singuliers de coordonnées $(\pm\frac{\sqrt{10}}{2}, 0)$. Pour déterminer les tangentes en ces points, nous allons tout d'abord nous ramener à l'origine. L'équation de la courbe devient alors

$$Y^2 + 4X^2(X^2 \pm X\sqrt{10} - \frac{5}{2}\ )(X \pm \sqrt{10})^2 = 0$$

La partie de plus bas degré est $Y^2 - 100X^2 = 0$. On voit donc que les points singuliers sont des points doubles ordinaires et que les tangentes en ces points ont pour équations $Y = \pm 10(X - (\pm\frac{\sqrt{10}}{2}))$.

5.1. a) Si $\lambda \neq \pm 1$, nous avons vu que O est l'unique point singulier. Sa multiplicité est 3 et les tangentes sont les composantes du diviseur de la composante homogène de degré 3, c'est à dire l'axe des Y et les droites d'équations $Y = \pm\sqrt{\lambda}\, X$.

b) Si $\lambda = 1$, nous avons vu que C est l'union des droites d'équation $X = \pm Y$ et de la conique d'équation $X^2 + Y^2 - X$ qui est non singulière et que les points singuliers sont les points d'intersection de ces trois courbes, c'est à dire l'origine de

multiplicité 3 et les points de coordonnés $(1/2, \pm 1/2)$ de multiplicité 2. Les tangentes sont donc données par les droites d'équation $X = \pm Y$ et les tangentes à la conique en ces trois points, c'est à dire l'axe des X et les droites d'équation $Y \pm X = \pm 1$.

c) Le cas $\lambda = -1$ se traite de la même façon.

5.3. En caractéristique 2, la seule tangente à la courbe est la droite d'équation $Y = X + 1$ qui n'est ni horizontale, ni verticale. En caractéristique 5, on a $Y^2 + (X^2 - 5)(4X^4 - 20X^2 + 25) = Y^2 - X^6$ et on voit clairement qu'il n'y à pas de tangentes verticales et que O est l'unique point en lequel la tangente est horizontale.

En caractéristique différente de 2 et de 5, O est l'unique point singulier et la tangente en ce point est oblique. Les points en lesquels la tangente est horizontale sont donc les points autre que l'origine satisfaisant $(2X^2 - 5)(6X^2 - 25) = 0$, c'est à dire les 6 points $(0, \pm 5\sqrt{5}\ )$ et $(\pm 5\sqrt{6}\ /6, \pm 5/3)$. De même, les points en lesquels la tangente est verticale sont les points autre que l'origine satisfaisant $Y = 0$, c'est à dire $(\pm\sqrt{5}\ , 0)$.

5.4. Les tangentes à l'origine sont données par $X^2 + Y^2 = 2XY$, soit $(Y - X)^2 = 0$. On voit donc que Δ est bien l'unique tangente à l'origine. Les points de la courbe en lesquels la tangente est horizontale satisfont $X^2Y^2 + X^2 + Y^2 = 2XY(X + Y + 1)$ et $2XY^2 + 2X = 4XY + 2Y(Y + 1)$, soit, puisque k est de caractéristique $\neq 2$, $X^2Y^2 + X^2 + Y^2 = 2XY(X + Y + 1)$ et $XY^2 + X = 2XY + Y(Y + 1)$. En multipliant par X les termes de la seconde équation et en retranchant terme à terme à la première, on voit que les points que nous cherchons satisfont $Y^2 = XY^2 + XY$ et $XY^2 + X = 2XY + Y(Y + 1)$. On voit donc que ces points sont donnés par $XY = Y - X$ et $XY^2 + X = 2XY + Y(Y + 1)$. En substituant $Y - X$ à XY dans la seconde équation, on trouve $XY = Y - X$ et $XY = 3(X - Y)$, soit, puisque k est de caractéristique $\neq 2$, $X = Y = 0$, ce qui est impossible.

Les points de la courbe en lesquels la tangente est parallèle à Δ sont donnés par $X^2Y^2 + X^2 + Y^2 = 2XY(X + Y + 1)$ et $(2XY^2 + 2X - 4XY - 2Y(Y + 1)) + (2X^2Y + 2Y - 4XY - 2X(X + 1)) = 0$, soit, puisque k est de caractéristique $\neq 2$, $X^2Y^2 + X^2 + Y^2 = 2XY(X + Y + 1)$ et $XY^2 + X^2Y = 2XY + (X + Y)^2$. En ajoutant terme à terme, on obtient $X^2Y^2 = XY(X + Y + 6)$ et $XY^2 + X^2Y = 2XY + (X + Y)^2$. Puisque, à part O, les points situés sur les axes des coordonnées ne conviennent pas, on voit que les points que nous cherchons sont O et ceux donnés par $XY = X + Y + 6$ et $XY^2 + X^2Y = 2XY + (X + Y)^2$. En substituant $X + Y + 6$ à XY dans la seconde équation, on trouve $XY = X + Y + 6$ et $(X + Y + 6)(X + Y) = 2(X + Y + 6) + (X +$

$Y)^2$, ce qui donne $XY = X + Y + 6$ et $4(X + Y) = 12$, soit, puisque k est de caractéristique $\neq 2$, $XY = 9$ et $X + Y = 3$. Si k est de caractéristique $\neq 3$, on trouve O et les points $(-3j,-3j^2)$ et $(-3j^2,-3j)$. Sinon, on trouve seulement O.

Les points de la courbe en lesquels la tangente est parallèle à Δ' sont, l'origine exceptée, donnés par $X^2Y^2 + X^2 + Y^2 = 2XY(X + Y + 1)$ et $2XY^2 + 2X - 4XY - 2Y(Y + 1) = 2X^2Y + 2Y - 4XY - 2X(X + 1)$, soit, puisque k est de caractéristique $\neq 2$, par $X^2Y^2 + X^2 + Y^2 = 2XY(X + Y + 1)$ et $XY(Y - X) = (Y - X)(X + Y + 2)$. On trouve donc le point $(4, 4)$ et les points donnés par $X^2Y^2 + X^2 + Y^2 = 2XY(X + Y + 1)$ et $XY = X + Y + 2$. En remplaçant $X + Y$ par $XY - 2$ dans la première équation, on trouve $(X + Y)^2 = X^2Y^2$ et $XY = X + Y + 2$, ce qui est équivalent à $X + Y = -1$ et $XY = 1$. Si k est de caractéristique $\neq 3$, on trouve $(4, 4)$ et les points (j, j^2) et (j^2, j). Sinon, on trouve seulement $(1, 1)$.

5.5. Si $P = (a, b)$, l'application qui a un point du plan associe son abscisse est une bijection de $C \cap \Delta$ sur l'ensemble des racines de $(c(X - a) + b)^2 - (X^3 - X) = -X^3 + c^2X^2 + \ldots$ De plus, puisque Δ est tangente à C en P, a est racine double. L'égalité annoncée provient donc de la formule donnant la somme des racines d'un polynôme.

5.6. Si $P \in C_0$, la tangente Δ à C en P, de pente finie c, coupe C au point P' d'abscisse $a' := c^2 - 2a = u(P)$. Il suit que $\psi(P) = (u(P), v(P)) \in C$.

5.7. Soient $(P, P') =: (a, b, a', b') \in V_0$ avec $P \neq P'$ et Δ la droite joignant P et P'. Alors, Δ est une droite de pente finie c qui coupe C en un troisième point P'' (éventuellement égal à P ou à P') d'abscisse $a'' := c^2 - a - a' = m(P, P')$. Cela montre bien que $\varphi(P, P') \in C$. Enfin, on sait que si $F = Y^2 - X^3 + X$, f'_x et f'_y sont les restrictions à C de $\frac{dF}{dX}$ et $\frac{dF}{dY}$, $t := -\frac{f_x}{f_y}$, $u := t^2 - 2x$, $v := t(u - x) + y$ et C_0 est l'ouvert de C défini par $y \neq 0$, alors $\varphi(P, P) = (u(P), v(P)) \in C$.

7.4. En échangeant Y et Z, on obtient la courbe C' d'équation $Y = X^3 - XY^2$. Il est clair que l'origine est un point d'inflexion de C' et que la tangente à C' en ce point est l'axe des X. Il suit que l'origine de la droite à l'infini $(0; 1; 0)$ est un point d'inflexion de C et que la tangente à C en ce point est la droite à l'infini.

7.5. Il s'agit de montrer que si P est un point d'une conique irréductible C, alors P n'est pas un point d'inflexion. Quitte à faire un changement de coordonnées, et à remplacer C par sa partie affine dans le cas projectif, on peut supposer que C est affine et que $P = O$. Si O était un point d'inflexion de C, la composante homogène

F_1 de degré 1 de F diviserait la composante homogène F_2 de degré 2 de F. Puisque F est quadratique, on a $F = F_1 + F_2$ et F serait donc divisible par F_1, ce qui est impossible car C est irréductible.

9.3. En caractéristique 2, on vérifie aisément que les deux courbes se rencontrent uniquement à l'origine et avec la multiplicité 9. Nous supposons donc dans ce qui suit que le corps de base est de caractéristique $\neq 2$.

Posons $F := Y^5 - X(Y^2 - X)^2$ et $G := X^2 - (Y^4 + Y^3)$. Soit P un point du plan. En substituant $Y^4 + Y^3$ à X^2 dans F, ce qui ne change pas $I(F, G; P)$, on obtient Y^3F_1 avec $F_1 = -X(2Y + 1) + 3Y^2 + 2Y^3$. Il en résulte que

$$I(F, G; P) = 3I(Y, G; P) + I(F_1, G; P)$$

et on a $I(Y, G; P) = 2I(X, Y; P)$. Nous avons donc

$$I(F, G; P) = 6I(X, Y; P) + I(F_1, G; P)$$

Pour calculer $I(F_1, G; P)$, on remarque tout d'abord que la droite d'équation $2Y + 1 = 0$ ne rencontre pas la courbe d'équation $F_1 = 0$. Il en résulte que $I(F_1, G; P) = I(F_1, (2Y + 1)G; P)$. On remarque alors que

$$(X - Y^2)F_1 + (2Y + 1)G = Y^2(Y - 2X)$$

et on en déduit que

$$I(F_1, G; P) = I(F_1, Y^2(Y - 2X); P) = 2I(F_1, Y; P) + I(F_1, Y - 2X; P).$$

Puisque $I(F_1, Y; P) = I(X, Y; P)$, nous avons donc

$$I(F, G; P) = 8I(X, Y; P) + I(F_1, Y - 2X; P).$$

En substituant Y à $2X$ dans F_1, puis en multipliant par 2, ce qui ne change pas $I(F_1, Y - 2X; P)$, on obtient YF_2 avec $F_2 = 4Y(Y + 1) - 1$. Il en résulte que

$$I(F_1, Y - 2X; P) = I(Y, Y - 2X; P) + I(F_2, Y - 2X; P).$$

Puisque $I(Y, Y - 2X; P) = I(X, Y; P)$, nous voyons donc que pour tout point P du plan, nous avons

$$I(Y^5 - X(Y^2 - X)^2, X^2 - (Y^4 + Y^3); P) = 9I(X, Y; P) + I(4Y(Y + 1) - 1, Y - 2X; P).$$

et on voit facilement que les courbes d'équations $4Y(Y + 1) = 1$ et $Y = 2X$ se rencontrent avec la multiplicité 1 en les point de coordonnées $(\frac{1\pm\sqrt{2}}{4}, \frac{1\pm\sqrt{2}}{2})$.

Nous en déduisons que les deux courbes se rencontrent en O avec la multi-

plicité 9 et en les deux points de coordonnés $(\frac{1\pm\sqrt{2}}{4}, \frac{1\pm\sqrt{2}}{2})$ avec la multiplicité 1.

9.9. La courbe $s^{-1}(C)$ a pour d'équation $X^2Y^2 + X^2 + Y^2 + 2XY(X + Y - 1) = 0$. Si on pose $A = X^2Y^2 + X^2 + Y^2 - 2XY$ et $B = 2XY(X + Y)$, on voit que C est la courbe d'équation $A - B = 0$ et que $s^{-1}(C)$ est la courbe d'équation $A + B = 0$. Puisque la multiplicité d'intersection ne dépend que de l'idéal engendré par les polynômes et que k est de caractéristique $\neq 2$, on a $I(C, s^{-1}(C); P) = I(A, B; P) = I(A, X; P) + I(A, Y; P) + I(A, X + Y; P) = I(Y^2, X; P) + I(X^2, Y; P) + I(X^2(X^2 + 4), X + Y; P) = 6I(X, Y; P) + I(X - 2i, Y + 2i; P) + I(X + 2i, Y - 2i; P)$. On voit donc que C et $s^{-1}(C)$ se rencontrent à l'origine avec la multiplicité 6 ainsi qu'aux points $(2i, -2i)$ et $(-2i, 2i)$ avec la multiplicité 1.

11.1. On sait que Δ^* n'est tangente à C^* ni en P, ni au point P_∞ à l'infini. On a donc $I(\Delta^*, C^*; P) + I(\Delta^*, C^*; P_\infty) = 1 + 1 = 2$. D'autre part, on a $deg\Delta^*.degC^* = 1.3 = 3$. Le théorème de Bézout nous dit alors que les courbes Δ^* et C^* se coupent en un unique autre point P' et que Δ^* n'est pas tangente à C^* en P'. Puisque C n'a qu'un point à l'infini, on a nécessairement $P' \in C$.

11.2. Les courbes projectives Δ^* et C^* se coupent en P avec la multiplicité au moins 2 puisque Δ est tangente à C en P. D'autre part, elles se coupent au point à l'infini de C. Le théorème de Bézout nous dit qu'elles ne peuvent pas se couper en un autre point.

11.5. On utilise le théorème de Bézout qui nous dit que Δ^* et C^* se coupent nécessairement en un troisième point P''. Si Δ n'est pas verticale, alors Δ^* et C^* ne se coupent pas à l'infini et $P'' \in C$.