François Brunault

GÉOMÉTRIE ALGÉBRIQUE ÉLÉMENTAIRE

François Brunault
E-mail : brunault@umpa.ens-lyon.fr
ÉNS Lyon, UMPA, 46 allée d'Italie, 69007 Lyon, France.

Version du 6 mai 2011

GÉOMÉTRIE ALGÉBRIQUE ÉLÉMENTAIRE

François Brunault

Résumé. — Ce cours est donné à l'ÉNS Lyon (M1 approfondi, second semestre 2010/2011).

TABLE DES MATIÈRES

Une des motivations de la géométrie algébrique est la recherche des solutions des systèmes d'équations polynomiales. Soit k un corps et n un entier ≥ 1. Étant donnés des polynômes $P_1, \ldots, P_r \in k[X_1, \ldots, X_n]$, une question naturelle est de trouver tous les $(x_1, \ldots, x_n) \in k^n$ vérifiant le système

$$(*) \begin{cases} P_1(x_1, \ldots, x_n) = 0 \\ \qquad \vdots \\ P_r(x_1, \ldots, x_n) = 0. \end{cases}$$

Une première approche, de nature algébrique, consiste à essayer de se ramener à un problème à $n-1$ inconnues en *éliminant* l'une des variables du système ci-dessus. C'est l'objet de la théorie de l'élimination, développée au 19e siècle notamment par Kronecker. Le théorème fondamental de l'élimination projective dit (en gros) que si k est algébriquement clos, et si l'on tient compte des « solutions à l'infini », alors une telle réduction est toujours possible. L'exemple le plus simple est donné par le résultant, qui permet de ramener l'étude de $(*)$ pour $r = n = 2$ à la recherche des racines d'un polynôme en une variable.

Une autre approche consiste à étudier les propriétés géométriques de l'ensemble des points de k^n vérifiant $(*)$. Lorsque $r \leq n$, cet objet géométrique est « en général » de dimension $n - r$ (un des premiers buts de la géométrie algébrique a été de développer une théorie satisfaisante de la dimension pour de tels objets). Cette interprétation géométrique amène de nombreuses questions : comment deux ou plusieurs tels objets s'intersectent-ils ? Peut-on construire de tels objets en leur imposant certaines conditions géométriques ? Peut-on en obtenir des équations plus simples en appliquant une transformation géométrique judicieuse ?

La véritable richesse de la géométrie algébrique vient de la complémentarité des deux approches, algébrique et géométrique. Nous essaierons d'en donner quelques exemples dans ce cours.

CHAPITRE 1

COURBES AFFINES

1.1. L'espace affine et ses fermés algébriques

Soit k un corps *algébriquement clos*.

Définition 1.1.1. — Soit $n \geq 1$ un entier. L'ensemble k^n est appelé *espace affine de dimension n sur k*. On le note $\mathbf{A}^n(k)$, ou simplement $\mathbf{A}^n$ lorsque k est sous-entendu.

Définition 1.1.2. — Pour toute partie S de $k[X_1, \ldots, X_n]$, le *lieu des zéros communs de S* est

$$V(S) = \{x = (x_1, \ldots, x_n) \in \mathbf{A}^n(k) : \forall P \in S, P(x_1, \ldots, x_n) = 0\}.$$

Un *fermé algébrique* de $\mathbf{A}^n(k)$ est une partie $F \subset \mathbf{A}^n(k)$ de la forme $F = V(S)$ avec $S \subset k[X_1, \ldots, X_n]$.

Remarque 1.1.3. — L'hypothèse que k est algébriquement clos est absolument nécessaire pour ce qui va suivre. L'étude des solutions de systèmes d'équations polynomiales dans un corps non algébriquement clos, tel $k = \mathbf{Q}$ ou $k = \mathbf{F}_p$, est infiniment plus compliquée et nécessite souvent de commencer par considérer les solutions dans un corps algébriquement clos contenant k.

Exemples 1.1.4. — Les parties k^n et $\emptyset$ sont des fermés algébriques de $\mathbf{A}^n(k)$ (prendre $S = \emptyset$ et $S = k[X_1, \ldots, X_n]$ respectivement). Tout sous-espace affine de k^n est un fermé algébrique de $\mathbf{A}^n(k)$. Si $n = 1$, les fermés algébriques stricts de $\mathbf{A}^1(k)$ sont exactement les parties finies de $\mathbf{A}^1(k)$.

Si S est une partie de $k[X_1, \ldots, X_n]$, et si I est l'idéal de $k[X_1, \ldots, X_n]$ engendré par S, on vérifie immédiatement que $V(S) = V(I)$, de sorte que tout fermé algébrique de $\mathbf{A}^n(k)$ est le lieu des zéros d'un idéal de $k[X_1, \ldots, X_n]$. De plus, l'anneau $k[X_1, \ldots, X_n]$ étant noethérien, tout fermé algébrique de $\mathbf{A}^n(k)$ est le lieu des zéros communs d'un nombre *fini* de polynômes de $k[X_1, \ldots, X_n]$.

Exercice. — Soit S une partie de $k[X_1, \ldots, X_n]$ et I l'idéal de $k[X_1, \ldots, X_n]$ engendré par S. Montrer qu'il existe une partie finie de S qui engendre I. En déduire qu'il existe une partie finie $T \subset S$ telle que $V(S) = V(T)$.

Exercice. — Montrer que pour tous idéaux $I_1, I_2 \subset k[X_1, \ldots, X_n]$, on a $V(I_1) \cup V(I_2) = V(I_1 I_2) = V(I_1 \cap I_2)$. En déduire que l'ensemble des fermés algébriques de $\mathbf{A}^n(k)$ est l'ensemble des fermés d'une topologie sur $\mathbf{A}^n(k)$ (appelée topologie de Zariski). Montrer qu'une réunion infinie de fermés algébriques n'est pas toujours un fermé algébrique.

Il est important de remarquer que si F est un fermé algébrique, l'idéal I tel que $F = V(I)$ n'est en général pas unique. Par exemple, si $I = (P)$ est l'idéal engendré par $P \in k[X_1, \ldots, X_n]$, alors $V(I) = V(I^m)$ pour tout $m \geq 1$.

Définition 1.1.5. — Pour toute partie A de $\mathbf{A}^n(k)$, l'*idéal associé à* A est

$$I(A) = \{P \in k[X_1, \ldots, X_n] : P|_A = 0\}.$$

$I(A)$ est bien un idéal de $k[X_1, \ldots, X_n]$: c'est le noyau du morphisme de k-algèbres $k[X_1, \ldots, X_n] \to k^A$ donné par $P \mapsto P|_A$.

Lemme 1.1.6. — *Soit F un fermé algébrique de $\mathbf{A}^n(k)$. L'idéal $I(F)$ associé à F est le plus grand des idéaux $I \subset k[X_1, \ldots, X_n]$ tels que $F = V(I)$.*

Démonstration. — On a par définition $F \subset V(I(F))$. De plus, soit J un idéal de $k[X_1, \ldots, X_n]$ tel que $F = V(J)$. Comme tous les éléments de J s'annulent sur F, on a $J \subset I(F)$ et donc $V(I(F)) \subset V(J) = F$. Ainsi $V(I(F)) = F$, et on vient de montrer que $I(F)$ est le plus grand des idéaux définissant F. □

Le lemme 1.1.6 dit en particulier que pour tout fermé algébrique F de $\mathbf{A}^n(k)$, on a $F = V(I(F))$. Signalons également la conséquence suivante : tout fermé algébrique F de $\mathbf{A}^n(k)$ peut s'écrire $F = V(P_1, \ldots, P_r)$ avec $P_1, \ldots, P_r$ engendrant $I(F)$ (ce qui, répétons-le, n'est pas toujours vrai si on sait seulement que $F = V(P_1, \ldots, P_r)$).

Exercice. — Si A est une partie quelconque de $\mathbf{A}^n(k)$, montrer que $I(A) = I(\overline{A})$, où $\overline{A}$ est l'adhérence de A dans $\mathbf{A}^n(k)$ pour la topologie de Zariski. En déduire que $V(I(A)) = \overline{A}$.

1.2. Le théorème des zéros de Hilbert

Un résultat fondamental sur les fermés algébriques est le *théorème des zéros* (en allemand *Nullstellensatz*), démontré par David Hilbert. Nous allons donner plusieurs versions de ce théorème. Rappelons que dans tous ces énoncés k est algébriquement clos.

Théorème 1.2.1 **(Nullstellensatz I)**. — *Les idéaux maximaux de $k[X_1, \ldots, X_n]$ sont exactement les $(X_1 - a_1, \ldots, X_n - a_n)$ pour $(a_1, \ldots, a_n) \in k^n$.*

Le Nullstellensatz I a été démontré dans le cours d'Algèbre approfondie. En voici une formulation équivalente :

Théorème 1.2.2 **(Nullstellensatz I bis)**. — *Soit $P_1, \dots, P_r$ des polynômes de $k[X_1, \dots, X_n]$. Alors on a l'équivalence*

$$V(P_1, \dots, P_r) = \emptyset \Leftrightarrow \exists Q_1, \dots, Q_r \in k[X_1, \dots, X_n] \text{ tels que } \sum_{i=1}^{r} P_i Q_i = 1.$$

Démonstration. — Le sens $\Leftarrow$ est immédiat. Supposons $V(P_1, \dots, P_r) = \emptyset$ et notons I l'idéal engendré par $P_1, \dots, P_r$. Supposons par l'absurde $I \neq k[X_1, \dots, X_n]$. Alors I est contenu dans un idéal maximal $\mathfrak{m}$ et par le Nullstellensatz I, on a $\mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n)$. On vérifie alors que $(a_1, \dots, a_n) \in V(P_1, \dots, P_r)$, ce qui est absurde. □

Exercice. — Déduire la version I de la version I bis.

Voici maintenant une autre version, plus forte, du théorème des zéros.

Théorème 1.2.3 **(Nullstellensatz II)**. — *Soit $P_1, \dots, P_r \in k[X_1, \dots, X_n]$. Pour tout polynôme $Q \in k[X_1, \dots, X_n]$, on a l'équivalence*

$$Q|_{V(P_1,\dots,P_r)} = 0 \Leftrightarrow \exists m \geq 1 \text{ tel que } Q^m \in (P_1, \dots, P_r).$$

Remarque 1.2.4. — En prenant $Q = 1$, on retrouve la version I.

Démonstration du Nullstellensatz II.. — Le sens $\Leftarrow$ est immédiat. Pour l'implication directe, posons $F = V(P_1, \dots, P_r)$ et supposons $Q|_F = 0$. Introduisons une nouvelle variable X_0 et notons $\widetilde{F} \subset \mathbf{A}^{n+1} = \mathbf{A}^1 \times \mathbf{A}^n$ le lieu des zéros communs de $P_1, \dots, P_r$ vus comme polynômes de $k[X_0, \dots, X_n]$. On a alors $\widetilde{F} = \mathbf{A}^1 \times F$. Par hypothèse, on a $\widetilde{F} \cap V(1 - X_0 Q) = \emptyset$. D'après le Nullstellensatz I bis, il existe des polynômes $Q_1, \dots, Q_r, R \in k[X_0, \dots, X_n]$ tels que

$$\sum_{i=1}^{r} P_i Q_i + (1 - X_0 Q) R = 1.$$

Si $Q = 0$, ce que l'on veut montrer est vrai. Si $Q \neq 0$, on substitue $\frac{1}{Q}$ à X_0 pour obtenir l'identité suivante dans $k(X_1, \dots, X_n)$

$$\sum_{i=1}^{r} P_i(X_1, \dots, X_n) Q_i\left(\frac{1}{Q(X_1, \dots, X_n)}, X_1, \dots, X_n\right) = 1.$$

Le résultat souhaité s'obtient en multipliant par Q^d avec d suffisamment grand. □

Le théorème précédent se traduit immédiatement en un énoncé sur les idéaux associés aux fermés algébriques de $\mathbf{A}^n$.

Théorème 1.2.5 **(Nullstellensatz II bis)**. — *Pour tout idéal J de $k[X_1, \dots, X_n]$, on a $I(V(J)) = \sqrt{J}$, où $\sqrt{J}$ désigne la* racine de J, *c'est-à-dire l'ensemble des polynômes ayant une puissance dans J.*

Exercice. — Pour tout anneau commutatif A et tout idéal I de A, vérifier que $\sqrt{I}$ est un idéal de A contenant I, et que $\sqrt{I} = I$ si et seulement si le seul élément nilpotent de A/I est 0 (on dit alors que I est un idéal *radiciel* et que A/I est un anneau *réduit*).

Exemple 1.2.6 **(Hypersurface)**. — . Une hypersurface de $\mathbf{A}^n$ est une fermé algébrique de la forme $V(P)$ avec $P \in k[X_1, \ldots, X_n]$ non constant. Posons $P = \lambda \cdot P_1^{m_1} \cdots P_\ell^{m_\ell}$, avec $\lambda \in k^*$ et les P_i irréductibles et deux à deux non associés (l'anneau $k[X_1, \ldots, X_n]$ est factoriel). Alors l'idéal $\sqrt{(P)}$ est l'idéal principal engendré par $Q = P_1 \cdots P_r$, de sorte que pour tout $f \in k[X_1, \ldots, X_n]$, on a

$$f|_{V(P)} = 0 \Leftrightarrow f \text{ est divisible par } Q.$$

Le Nullstellensatz permet d'établir une correspondance précise entre fermés algébriques de $\mathbf{A}^n(k)$ et idéaux de $k[X_1, \ldots, X_n]$.

Théorème 1.2.7. — *Lorsque k est algébriquement clos, on a une bijection renversant l'inclusion entre :*

(1) *les fermés algébriques de $\mathbf{A}^n(k)$;*

(2) *les idéaux J de $k[X_1, \ldots, X_n]$ tels que $\sqrt{J} = J$.*

Cette bijection est donnée par $F \mapsto I(F)$ et $J \mapsto V(J)$.

Démonstration. — L'application allant de (1) à (2) est bien définie car $\sqrt{I(F)} = I(F)$. De plus, les égalités $V(I(F)) = F$ et $I(V(J)) = \sqrt{J}$ ont déjà été établies. □

Si F_1, F_2 sont des fermés algébriques, on a $I(F_1 \cup F_2) = I(F_1) \cap I(F_2)$ et $I(F_1 \cap F_2) = \sqrt{I(F_1) + I(F_2)}$, mais cet idéal n'est en général pas égal à $I(F_1) + I(F_2)$.

Exemple 1.2.8. — Prenons $n = 2$ et $F_1 = V(Y - X^2)$ et $F_2 = V(Y)$. Les polynômes $Y - X^2$ et Y étant irréductibles et non associés dans $k[X, Y]$, on a $I(F_1) = (Y - X^2)$, $I(F_2) = (Y)$. Comme $F_1 \cap F_2 = \{(0, 0)\}$, on a $I(F_1 \cap F_2) = (X, Y)$, tandis que $I(F_1) + I(F_2) = (Y - X^2, Y) = (X^2, Y)$. On a donc $I(F_1) + I(F_2) \subsetneq I(F_1 \cap F_2)$. On remarque d'ailleurs que l'anneau $k[X, Y]/(X^2, Y) \cong k[X]/(X^2)$ n'est pas réduit. Ce résultat s'interprète géométriquement en remarquant que $(0, 0)$ est un point d'intersection « double » de F_1 et F_2.

Considérons maintenant $F_3 = V(Y - 1)$ et étudions $F_1 \cap F_3$. Si $\mathrm{car}(k) \neq 2$, alors $F_1 \cap F_3 = \{(\pm 1, 1)\}$ et l'on vérifie que $I(F_1 \cap F_3) = I(F_1) + I(F_3)$. Mais si $\mathrm{car}(k) = 2$, on a $F_1 \cap F_3 = \{(1, 1)\}$ et $I(F_1 \cap F_3) = (X - 1, Y - 1)$ tandis que $I(F_1) + I(F_3) = (Y - X^2, Y - 1) = ((X - 1)^2, Y - 1) \neq (X - 1, Y - 1)$: encore une intersection « double ». Si $\mathrm{car}(k) = 2$, toutes les droites horizontales sont tangentes à la parabole F_1 !

1.3. Définition des courbes affines planes

Nous allons dès maintenant nous restreindre à l'étude des fermés algébriques du plan affine $\mathbf{A}^2(k)$.

Définition 1.3.1. — Une *courbe affine plane* est une partie C de $\mathbf{A}^2(k)$ de la forme $C = V(P)$ avec $P \in k[X,Y]$ polynôme non constant.

Lemme 1.3.2. — *Une courbe affine plane possède une infinité de points.*

Démonstration. — Soit $C = V(P)$ une courbe affine plane. Posons $P(X,Y) = P_n(X)Y^n + P_{n-1}(X)Y^{n-1} + \cdots + P_0(X)$ avec $P_n \neq 0$. Si $n = 0$, alors pour toute racine λ de P_0, on a $\{\lambda\} \times k \subset C$, et comme k est infini, il en va de même pour C. Si $n \geq 1$, pour chaque $\lambda \in k$ tel que $P_n(\lambda) \neq 0$, il existe $y \in k$ tel que $P(\lambda, y) = 0$. Par suite C est infinie. □

Remarque 1.3.3. — Le lemme 1.3.2 devient bien sûr faux lorsque k n'est pas algébriquement clos (même infini). Par exemple, le polynôme $X^2 + Y^2 + 1$ n'a pas de zéro dans $\mathbf{R}^2$. Si l'on veut faire de la géométrie algébrique sur $\mathbf{R}$, il est préférable de « voir » $V(X^2 + Y^2 + 1)$ comme une partie de $\mathbf{C}^2$ munie d'une involution sans point fixe (ici la conjugaison complexe).

Rappelons que deux polynômes $P_1, P_2 \in k[X,Y]$ sont dits *associés* s'il existe $\lambda \in k^*$ tel que $P_2 = \lambda P_1$ (ce qui revient à dire qu'ils engendrent le même idéal de $k[X,Y]$).

Lemme 1.3.4. — *Soit $C = V(P)$ une courbe affine plane, avec $P \in k[X,Y]$ non constant. Posons $P = \lambda P_1^{m_1} \cdots P_\ell^{m_\ell}$ avec $\lambda \in k^*$ et $P_1, \ldots, P_\ell$ irréductibles deux à deux non associés dans $k[X,Y]$. Alors $C = \cup_{i=1}^{\ell} C_i$ avec $C_i = V(P_i)$, et $I(C)$ est l'idéal principal engendré par $P_1 \cdots P_\ell$.*

Démonstration. — L'assertion concernant C est immédiate, de même que $P_1 \cdots P_\ell \in I(C)$. Soit maintenant $Q \in I(C)$. Par le Nullstellensatz (théorème 1.2.3), il existe $d \geq 1$ tel que Q^d soit divisible par P. Comme $k[X,Y]$ est factoriel, on a $P_i | Q$ pour tout $1 \leq i \leq \ell$ et par suite $Q \in (P_1 \cdots P_\ell)$. □

Exercice. — Montrer que deux courbes affines planes $V(P)$ et $V(P')$ sont égales si et seulement si P et P' ont les mêmes facteurs irréductibles dans $k[X,Y]$.

Proposition 1.3.5. — *Soit C une courbe affine plane. Les conditions suivantes sont équivalentes :*

(i) *Il existe $P \in k[X,Y]$ irréductible tel que $C = V(P)$.*

(ii) *C n'est pas réunion de deux courbes affines planes distinctes.*

(iii) *L'idéal $I(C)$ est premier.*

Démonstration. — Montrons (i) ⇒ (ii). Par l'absurde, supposons $C = C_1 \cup C_2$ avec $C_1 \neq C_2$. D'après le lemme 1.3.4, on a $I(C) = (P)$ avec $P \in k[X,Y]$ irréductible, ainsi que $I(C_i) = (P_i)$ avec P_i non constant. Comme $I(C) \subset I(C_i)$, il vient $P_i | P$, donc P_1 et P_2 sont associés à P, ce qui contredit le fait que $C_1 \neq C_2$.

Montrons (ii) ⇒ (iii). Avec les notations du lemme 1.3.4, on a $I(C) = (P_1 \cdots P_\ell)$ où les P_i sont irréductibles dans $k[X,Y]$ et deux à deux non asociés. Par l'absurde, supposons $I(C)$ non premier. Comme $k[X,Y]$ est factoriel, on a nécessairement $\ell \geq 2$. Par suite $C = V(P_1) \cup V(P_2 \cdots P_\ell)$ est réunion de deux courbes distinctes.

Enfin, montrons (iii) $\Rightarrow$ (i). Toujours avec les notations du lemme 1.3.4, on a $I(C) = (P_1 \cdots P_\ell)$ et la primalité de cet idéal entraîne $\ell = 1$, d'où $C = V(P_1)$ avec P_1 irréductible. □

Définition 1.3.6. — Une courbe affine plane est dite *irréductible* lorsqu'elle satisfait les conditions équivalentes de la proposition 1.3.5.

Remarque 1.3.7. — L'irréductibilité de $V(P)$ n'entraîne pas celle de P. En effet, on a déjà remarqué que $V(P) = V(P^m)$ pour tout $m \geq 1$. De même, l'égalité $V(P) = V(Q)$ n'entraîne pas que P et Q sont associés dans $k[X, Y]$.

Le lemme 1.3.4 montre que toute courbe affine plane C est réunion finie de courbes irréductibles C_i. Cette décomposition est appelée *décomposition de C en composantes irréductibles*. Elle permet souvent de ramener la preuve de certaines propriétés des courbes au cas irréductible.

Exercice. — Montrer que la décomposition d'une courbe affine plane en courbes irréductibles est unique.

Voici un tableau résumant la correspondance entre fermés algébriques et idéaux de polynômes, dans le cas du plan affine.

Fermés algébriques de $\mathbf{A}^2$	Idéaux de $k[X, Y]$
$\mathbf{A}^2$	$\{0\}$
$C = V(P)$ (P irréductible)	$I(C) = (P)$
$\{(x_0, y_0)\}$	$\mathfrak{m} = (X - x_0, Y - y_0)$
$\emptyset$	$k[X, Y]$

Nous verrons (cf. TD) qu'il n'y a essentiellement pas d'autre fermé algébrique dans $\mathbf{A}^2$, c'est-à-dire que tout fermé algébrique de $\mathbf{A}^2$ distinct de $\mathbf{A}^2$ est réunion finie de courbes et de points.

1.4. Fonctions et applications régulières

Définition 1.4.1. — Soit V un fermé algébrique de $\mathbf{A}^n$ ($n \geq 1$). Une *fonction régulière* sur V est une application $f : V \to k$ qui est restriction d'une fonction polynomiale de k^n dans k, c'est-à-dire telle qu'il existe un polynôme $P \in k[X_1, \ldots, X_n]$ tel que $f = P|_V$.

On note $k[V]$ l'ensemble des fonctions régulières sur V. C'est une sous-k-algèbre de k^V et par définition, on a un morphisme surjectif de k-algèbres $k[X_1, \ldots, X_n] \to k[V]$. Le noyau de ce morphisme étant $I(V)$, on a un isomorphisme de k-algèbres $k[V] \cong k[X_1, \ldots, X_n]/I(V)$.

Exemple 1.4.2. — Pour $n = 1$ et $V = \mathbf{A}^1$, on a $k[\mathbf{A}^1] = k[X_1]$. Plus généralement, on a $k[\mathbf{A}^n] = k[X_1, \ldots, X_n]$. Si V est réduit à un point, on a $k[V] = k$.

Soit $C \subset \mathbf{A}^2$ une courbe affine plane. D'après la discussion précédente, la k-algèbre $k[C]$ des fonctions régulières sur C s'identifie au quotient $k[X,Y]/I(C)$. On note souvent x (resp. y) l'image de X (resp. Y) dans $k[C]$, de sorte que la k-algèbre $k[C]$ est engendrée par x et y.

Proposition 1.4.3. — *Les idéaux maximaux de $k[C]$ sont exactement les $(x - x_0, y - y_0)$ pour $(x_0, y_0) \in C$.*

Démonstration. — Soit $(x_0, y_0) \in C$ et $\varphi : k[C] \to k$ le morphisme de k-algèbres donné par l'évaluation en (x_0, y_0). Comme φ est surjectif (puisque $\varphi|_k = \mathrm{id}_k$), son noyau $\mathfrak{m} = \ker \varphi$ est un idéal maximal de $k[C]$. Montrons que $\mathfrak{m} = (x - x_0, y - y_0)$. L'inclusion réciproque étant claire, donnons-nous $f : C \to k$ telle que $f(x_0, y_0) = 0$. Soit $P \in k[X,Y]$ tel que $P|_C = f$. En développant P suivant les puissances de $X - x_0$ et $Y - y_0$ et comme $P(x_0, y_0) = 0$, il vient $P \in (X - x_0, Y - y_0)$ et donc $f \in (x - x_0, y - y_0)$. Ainsi $(x - x_0, y - y_0)$ est un idéal maximal de $k[C]$.

Réciproquement, si $\mathfrak{m}$ est un idéal maximal de $k[C] = k[X,Y]/I(C)$, alors la préimage $\widetilde{\mathfrak{m}}$ de $\mathfrak{m}$ dans $k[X,Y]$ est un idéal maximal contenant $I(C)$. D'après le Nullstellensatz (théorème 1.2.1), il existe $(x_0, y_0) \in \mathbf{A}^2$ tel que $\widetilde{\mathfrak{m}} = (X - x_0, Y - y_0)$. On en déduit $C = V(I(C)) \supset V(\widetilde{\mathfrak{m}}) = \{(x_0, y_0)\}$. On a donc $\mathfrak{m} = (x - x_0, y - y_0)$ avec $(x_0, y_0) \in C$.

Enfin, les idéaux maximaux $(x - x_0, y - y_0)$ sont deux à deux distincts car leurs images réciproques dans $k[X,Y]$ le sont. □

Remarquons qu'une courbe affine plane C est irréductible si et seulement si la k-algèbre $k[C]$ est intègre (c'est une simple traduction de la condition (iii) de la proposition 1.3.5).

Exercice. — Soit $\varphi : k[C] \to k$ un morphisme de k-algèbres. Montrer qu'il existe $P_0 \in C$ tel que φ soit le morphisme d'évaluation en P_0.

Définition 1.4.4. — Soient V et W des fermés algébriques de $\mathbf{A}^m$ et $\mathbf{A}^n$ respectivement $(m, n \geq 1)$. Une *application régulière* (ou *morphisme*) de V dans W est une application $f : V \to W$ telle qu'il existe des fonctions régulières $f_1, \ldots, f_n \in k[V]$ avec $f = (f_1, \ldots, f_n)$.

Étant données $f_1, \ldots, f_n \in k[V]$, ces fonctions ne définissent une application régulière $V \to W$ que si $(f_1, \ldots, f_n)$ est à valeurs dans W, ce qui équivaut à dire, en posant $W = V(P_1, \ldots, P_r) \subset \mathbf{A}^n$, que pour tout $1 \leq i \leq r$, on a $P_i(f_1, \ldots, f_n) = 0$.

Exemple 1.4.5. — Si $W = \mathbf{A}^1$, une application régulière $V \to \mathbf{A}^1$ n'est autre qu'une fonction régulière sur V.

Exercice. — Montrer que si $f : V \to W$ et $g : W \to X$ sont des applications régulières entre fermés algébriques, alors l'application $g \circ f : V \to X$ est régulière.

Définition 1.4.6. — Soit $f : V \to W$ une application régulière entre fermés algébriques. On dit que f est un *isomorphisme* s'il existe une application régulière

$g : W \to V$ telle que $g \circ f = \mathrm{id}_V$ et $f \circ g = \mathrm{id}_W$. On dit alors que V et W sont *isomorphes*.

Si $f : V \to W$ une application régulière entre fermés algébriques, on définit l'application $f^* : k[W] \to k[V]$ par $f^*(h) = h \circ f$ pour tout $h \in k[W]$. On vérifie que f^* est un morphisme de k-algèbres. De plus, si $f : V \to W$ et $g : W \to V$ sont des applications régulières, alors on a $(g \circ f)^* = f^* \circ g^*$.

Exercice. — Montrer que l'application $f \mapsto f^*$ définit une bijection entre l'ensemble des applications régulières $V \to W$ et l'ensemble des morphismes de k-algèbres $k[W] \to k[V]$. En déduire que V et W sont isomorphes si et seulement si les k-algèbres $k[V]$ et $k[W]$ le sont.

Il faut prendre garde au fait qu'une application régulière bijective n'est pas nécessairement un isomorphisme. Considérons par exemple la courbe affine plane $C = V(Y^2 - X^3)$ et l'application régulière $f : \mathbf{A}^1 \to C$ définie par $f(t) = (t^2, t^3)$. On a $f(0) = (0, 0)$ et si $(x, y) \in C$ vérifie $x \neq 0$, alors $(x, y) = f(t)$ avec $t = y/x$. Par suite f est bijective. Par l'absurde, supposons qu'il existe $g : C \to \mathbf{A}^1$ telle que $g \circ f = \mathrm{id}_{\mathbf{A}^1}$. Soit $P \in k[X, Y]$ tel que $g = P|_C$. Alors $P(t^2, t^3) = t$ pour tout $t \in k$, d'où $P(T^2, T^3) = T$ ce qui est impossible car le membre de gauche n'a pas de terme en T. Ainsi f n'est pas un isomorphisme (on verra par la suite qu'il n'existe aucun isomorphisme entre $\mathbf{A}^1$ et C).

Exercice. — Montrer que le morphisme f^* est injectif, et en déduire que $k[C]$ est isomorphe à $k[T^2, T^3]$.

Un autre exemple d'application régulière bijective qui n'est pas un isomorphisme est donné, lorsque $\mathrm{car}(k) = p > 0$, par le morphisme (dit de Frobenius) $f : \mathbf{A}^1 \to \mathbf{A}^1$ défini par $f(t) = t^p$.

Remarque 1.4.7. — Bien que ce cours soit essentiellement consacré aux courbes *planes*, il est bon de savoir que beaucoup de courbes algébriques ne sont pas planes. La bonne définition, que nous ne développerons pas, est la suivante : une courbe affine (irréductible) est un fermé algébrique C de $\mathbf{A}^n$ tel que :

(1) l'idéal $I(C)$ est premier (on dit alors que C est irréductible) ;

(2) la k-algèbre $k[C]$ est de degré de transcendance 1 sur k : il existe $f \in k[C]$ non constante telle que $k[C]$ soit algébrique sur $k[f]$.

D'après le lemme de normalisation d'Emmy Noether, vu dans le cours d'algèbre approfondie au premier semestre, il est même possible, dans ce cas, de trouver f telle que $k[C]$ soit entière sur $k[f]$. Un exemple de courbe affine est donné par $C = \{(t, t^2, t^3) : t \in k\} \subset \mathbf{A}^3$ (qui est en fait isomorphe à $\mathbf{A}^1$). Plus généralement, l'image d'une application régulière non constante $f : \mathbf{A}^1 \to \mathbf{A}^n$ est une courbe affine. Un exemple où une telle courbe n'est pas isomorphe à une courbe affine plane est obtenu en prenant $f(t) = (t^3, t^4, t^5)$. Dans un autre ordre d'idées, beaucoup de courbes affines ne peuvent pas s'obtenir comme l'image d'une application régulière $\mathbf{A}^1 \to \mathbf{A}^n$.

1.5. Fonctions rationnelles

Définition 1.5.1. — Soit V un fermé algébrique de $\mathbf{A}^n$ ($n \geq 1$) tel que la k-algèbre $k[V]$ soit intègre. On appelle *corps des fonctions rationnelles sur* V, et on note $k(V)$, le corps des fractions de $k[V]$.

Noter qu'un élément de $k(V)$ n'est pas, a priori, une fonction sur V, mais seulement un élément abstrait dans le corps des fonctions de $k[V]$.

Exemple 1.5.2. — Pour $V = \mathbf{A}^1$, on a $k[\mathbf{A}^1] \cong k[T]$ et donc $k(\mathbf{A}^1) \cong k(T)$: les fonctions régulières sur $\mathbf{A}^1$ sont les polynômes et les fonctions rationnelles sur $\mathbf{A}^1$ sont les fractions rationnelles. De même $k(\mathbf{A}^n) = k(X_1, \ldots, X_n)$.

Donnons-nous maintenant une courbe affine plane C, et supposons C irréductible, de sorte que le corps $k(C)$ est bien défini.

Définition 1.5.3. — Soit $f \in k(C)$ et $P \in C$. On dit que f est *régulière* (ou *définie*) en P s'il existe $g, h \in k[C]$ avec $h(P) \neq 0$ tels que $f = g/h$. On pose alors $f(P) := g(P)/h(P)$. Le *domaine de définition* de f est l'ensemble des points de C où f est régulière.

Remarque 1.5.4. — Si f est régulière en P, alors $f(P)$ ne dépend pas du choix de (g, h) tel que $f = g/h$ et $h(P) \neq 0$. En effet si $g/h = g'/h'$ alors $gh' = g'h$ et en évaluant en P, il vient $g(P)/h(P) = g'(P)/h'(P)$.

Dans la pratique, pour déterminer si une fonction $f \in k(C)$ est régulière en $P \in C$, on procède ainsi. On commence par écrire $f = g/h$ avec $g, h \in k[C]$ et $h \neq 0$. Trois cas se présentent alors :

(1) Si $h(P) \neq 0$, alors f est régulière en P (par définition).

(2) Si $g(P) \neq 0$ et $h(P) = 0$, alors f n'est pas régulière en P. En effet, si elle l'était, on aurait $f = g'/h'$ avec $h'(P) \neq 0$, il viendrait $gh' = g'h$, d'où une contradiction en évaluant en P.

(3) Si $g(P) = h(P) = 0$, on ne peut pas conclure. On cherche alors, en utilisant la relation algébrique liant les fonctions x et y, à écrire f sous une autre forme, de manière à vérifier (1) ou (2). Il est d'ailleurs possible qu'une telle écriture n'existe pas, auquel cas la fonction ne sera pas régulière en P.

Exemple 1.5.5. — Prenons $C = V(X^2 + Y^2 - 1)$ avec $\mathrm{car}(k) \neq 2$. Par le critère d'Eisenstein utilisé dans $(k[X])[Y]$ avec l'irréductible $X - 1$, le polynôme $X^2 + Y^2 - 1$ est irréductible dans $k[X, Y]$ et donc C est irréductible. Considérons $f = \frac{x-1}{y} \in k(C)$, ce qui a un sens car la fonction régulière $y \in k[C]$ n'est pas nulle (elle vaut 1 au point $(0, 1)$). Alors f est définie en tout point $(x_0, y_0) \in C$ tel que $y_0 \neq 0$. Si $(x_0, 0) \in C$ alors $x_0 = \pm 1$; il reste donc à étudier la régularité de f en $(\pm 1, 0)$. Pour le point $(-1, 0)$, on est dans le cas (2) et donc f n'est pas régulière en $(-1, 0)$. Pour le point $(1, 0)$, on est dans le cas (3) mais on a $(x + 1)(x - 1) = y^2$ dans $k[C]$, ce qui fait que $f = -y/(x + 1)$ et donc, d'après (1), f est régulière en $(1, 0)$. Ainsi le domaine de définition de f est $C - \{(-1, 0)\}$.

Exercice. — Soit $C = V(Y^2 - X^3)$. Montrer que C est irréductible et déterminer le domaine de définition de $t = y/x \in k(C)$.

Proposition 1.5.6. — *Soit C une courbe affine plane irréductible et C' une courbe affine plane ne contenant pas C. Alors $C \cap C'$ est fini.*

Démonstration. — Soit P (resp. P') un générateur de $I(C)$ (resp. $I(C')$). Le polynôme P est irréductible et ne divise pas P'. Montrons que P et P' sont premiers entre eux dans $k(X)[Y]$. Par l'absurde, supposons qu'il existe $F \in k(X)[Y] - k(X)$ divisant P et P' dans $k(X)[Y]$. En multipliant par un polynôme convenable de $k[X]$, on obtient l'existence de $F \in k[X,Y] - k[X]$ et de $Q \in k[X]$ tels que F divise QP et QP' dans $k[X,Y]$. Donc F divise $\mathrm{pgcd}(QP, QP') = Q \cdot \mathrm{pgcd}(P, P') = Q$, ce qui contredit le fait que F n'est pas un polynôme en X. Par suite, il existe une relation de Bézout $AP + A'P' = 1$ avec $A, A' \in k(X)[Y]$ et en multipliant à nouveau par un polynôme en X convenable, on obtient l'existence de $B, B' \in k[X,Y]$ et $Q \in k[X]$ non nul tels que $BP + B'P' = Q$, d'où $C \cap C' = V(P,P') \subset V(Q) = S \times \mathbf{A}^1$ où S est l'ensemble fini des racines de Q dans k. En échangeant les rôles de X et Y, on obtient également $C \cap C' \subset \mathbf{A}^1 \times T$ avec T fini, et donc $C \cap C' \subset S \times T$ est fini. □

Proposition 1.5.7. — *Soit C une courbe affine plane irréductible et $f \in k(C)$. Alors le domaine de définition de f est le complémentaire d'une partie finie de C.*

Démonstration. — Posons $f = g/h$ avec $g, h \in k[C]$ et $h \neq 0$. Si h est constante, alors le résultat est clair. Sinon, soit $Q \in k[X,Y]$ tel que $h = Q|_C$. Comme $h \neq 0$, la courbe affine plane $C' = V(Q)$ ne contient pas C et la proposition 1.5.6 entraîne que $C \cap C'$ est fini, c'est-à-dire que h n'a qu'un nombre fini de zéros dans C, d'où le résultat. □

Proposition 1.5.8. — *Soit C une courbe affine plane irréductible. Si $f_1, f_2 \in k(C)$ sont définies et coïncident sur une partie infinie de C, alors $f_1 = f_2$.*

Démonstration. — Soit S une partie infinie de C telle que f_1 et f_2 sont régulières sur S et vérifient $f_1(P) = f_2(P)$ pour tout $P \in S$. Posons $f_i = g_i/h_i$ avec $g_i, h_i \in k[C]$ et $h_i \neq 0$. Quitte à restreindre S, on peut supposer que h_1 et h_2 ne s'annulent pas sur S. Soit $Q \in k[X,Y]$ tel que $Q|C = g_1h_2 - g_2h_1$. L'ensemble $C \cap V(Q)$ contient S donc est infini. Si Q est constant, alors nécessairement $Q = 0$, et si Q est non constant, la proposition 1.5.6 entraîne $C \subset V(Q)$. Dans tous les cas, on obtient $g_1h_2 - h_2g_1 = 0$ et donc $f_1 = f_2$. □

Remarque 1.5.9. — La proposition 1.5.8 montre que la terminologie de « fonction » rationnelle est légitime ; autrement dit, il est permis d'identifier un élément de $k(C)$ avec la fonction qu'il définit.

Proposition 1.5.10. — *Soit C une courbe affine plane irréductible et $f \in k(C)$. Alors f appartient à $k[C]$ si et seulement si f est régulière en tout point de C.*

Démonstration. — L'implication $\Rightarrow$ étant immédiate, supposons que $f \in k(C)$ est régulière en tout point de C. Posons $I = \{h \in k[C] : hf \in k[C]\}$. Alors I est un idéal

de $k[C]$, et I est non nul par définition du corps des fractions. Il s'agit de montrer que $1 \in I$ c'est-à-dire $I = k[C]$. Par l'absurde, si I est un idéal strict de $k[C]$, alors il existe un idéal maximal $\mathfrak{m} \subset k[C]$ tel que $I \subset \mathfrak{m}$. D'après la proposition 1.4.3, il existe $(x_0, y_0) \in C$ tel que $\mathfrak{m} = (x - x_0, y - y_0)$. Comme f est régulière en (x_0, y_0), il existe $h \in k[C] - \mathfrak{m}$ telle que $hf \in k[C]$, et donc $h \in I$, ce qui est absurde. □

1.6. Anneau local d'une courbe en un point

Soit C une courbe affine plane irréductible.

Définition 1.6.1. — Soit $P \in C$. On appelle *anneau local de C en P*, et on note $\mathcal{O}_{C,P}$, le sous-anneau suivant de $k(C)$:

$$\mathcal{O}_{C,P} = \{f \in k(C) : f \text{ est régulière en } P\}. \tag{1}$$

On vérifie immédiatement que $\mathcal{O}_{C,P}$ est une sous-k-algèbre de $k(C)$. On a des inclusions $k[C] \subset \mathcal{O}_{C,P} \subset k(C)$. En particulier, le corps des fractions de $\mathcal{O}_{C,P}$ est $k(C)$.

Lemme 1.6.2. — *L'anneau $\mathcal{O}_{C,P}$ est le localisé de $k[C]$ en l'idéal maximal $\mathfrak{m}_P$ associé à P.*

Démonstration. — Par définition, $\mathcal{O}_{C,P}$ est l'ensemble des éléments de la forme g/h avec $g, h \in k[C]$ et $h(P) \neq 0$, c'est-à-dire $h \notin \mathfrak{m}_P$. Donc $\mathcal{O}_{C,P}$ est bien le localisé de $k[C]$ par rapport à la partie multiplicative $S_P = k[C] - \mathfrak{m}_P$. □

Il résulte du lemme 1.6.2 et des résultats généraux sur la localisation vus en algèbre approfondie que l'anneau $\mathcal{O}_{C,P}$ est local. Son unique idéal maximal, noté $\mathfrak{m}_{C,P}$, est l'idéal engendré par $\mathfrak{m}_P$ dans $\mathcal{O}_{C,P}$: autrement dit, on a $\mathfrak{m}_{C,P} = \mathfrak{m}_P \cdot \mathcal{O}_{C,P}$. Par ailleurs, on a un morphisme de k-algèbres $\varphi_P : \mathcal{O}_{C,P} \to k$ défini en évaluant en P. Comme $\varphi_P|_k = \mathrm{id}_k$, le morphisme φ_P est surjectif et son noyau est un idéal maximal de $\mathcal{O}_{C,P}$, qui ne peut être que $\mathfrak{m}_{C,P}$. Ainsi

$$\mathfrak{m}_{C,P} = \{f \in \mathcal{O}_{C,P} : f(P) = 0\}.$$

On en déduit $\mathfrak{m}_P = \mathfrak{m}_{C,P} \cap k[C]$. On a un diagramme commutatif de morphismes de k-algèbres

$$\begin{array}{ccc} k[C] & \longrightarrow & \mathcal{O}_{C,P} \\ & \searrow \quad \swarrow & \\ & k & \end{array} \tag{2}$$

où la flèche horizontale est l'inclusion, et les flèches diagonales sont données par l'évaluation en P. Ce diagramme induit des isomorphismes $\mathcal{O}_{C,P}/\mathfrak{m}_{C,P} \cong k[C]/\mathfrak{m}_P \cong k$.

Enfin, le lemme 1.6.2 incite à définir l'anneau local en un point sans faire l'hypothèse que la courbe est irréductible.

Définition 1.6.3. — Soit C une courbe affine plane (non supposée irréductible) et $P \in C$. On appelle *anneau local de C en P* le localisé de $k[C]$ en l'idéal maximal $\mathfrak{m}_P$ associé à P.

Exercice. — Montrer qu'on a encore un isomorphisme $\mathcal{O}_{C,P}/\mathfrak{m}_{C,P} \cong k$.

L'anneau $\mathcal{O}_{C,P}$ est local, noethérien (c'est le localisé d'un anneau noethérien en un idéal maximal), mais pas nécessairement intègre (on pourra considérer $C = V(XY)$ et $P = (0,0)$).

Exercice. — Montrer que $\mathcal{O}_{C,P}$ est intègre si et seulement si P appartient à une unique commposante irréductible de C.

1.7. Courbes rationnelles

Intuitivement, les courbes rationnelles sont les courbes pouvant être paramétrées par des fractions rationnelles. Nous allons préciser cette définition et donner en fait plusieurs définitions équivalentes de cette notion importante.

Commençons par quelques rappels sur le résultant. Soit A un anneau commutatif et $p, q \geq 1$ des entiers. Soient $P = a_p X^p + \cdots + a_1 X + a_0$ et $Q = b_q X^q + \cdots b_1 X + b_0$ des polynômes de $A[X]$. On appelle *matrice de Sylvester* de P et Q la matrice carrée de taille $p+q$ suivante :

$$\begin{pmatrix}
a_p & \cdots & \cdots & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\
0 & a_p & \cdots & \cdots & \cdots & a_1 & a_0 & \ddots & \vdots \\
\vdots & \ddots & a_p & \cdots & \cdots & \cdots & a_1 & a_0 & 0 \\
0 & \cdots & 0 & a_p & \cdots & \cdots & \cdots & a_1 & a_0 \\
b_q & \cdots & \cdots & b_1 & b_0 & 0 & \cdots & \cdots & 0 \\
0 & b_q & \cdots & \cdots & b_1 & b_0 & \ddots & 0 & \vdots \\
\vdots & \ddots & b_q & \cdots & \cdots & b_1 & b_0 & \ddots & \vdots \\
\vdots & 0 & \ddots & b_q & \cdots & \cdots & b_1 & b_0 & 0 \\
0 & \cdots & \cdots & 0 & b_q & \cdots & \cdots & b_1 & b_0
\end{pmatrix}$$

dans laquelle les q premières lignes contiennent les coefficients de P, et les p lignes suivantes ceux de Q. On pourra remarquer que la diagonale principale de la matrice de Sylvester est formée du coefficient a_p écrit q fois, suivi du coefficient b_0 écrit p fois.

Définition 1.7.1. — Le *résultant* de P et Q en degré (p,q), est le déterminant de la matrice de Sylvester associée à P et Q (et à p et q). On le note $\text{Rés}_{p,q}(P,Q) \in A$.

Notons que $\text{Rés}_{p,q}(P,Q)$ dépend a priori de p et q : par exemple, si l'on a simultanément $\deg(P) \leq p-1$ et $\deg(Q) \leq q-1$, alors $\text{Rés}_{p,q}(P,Q) = 0$. En degré fixé, le résultant se comporte bien vis-à-vis des morphismes d'anneaux : si $\varphi : A \to B$ est un morphisme d'anneaux, alors $\varphi(\text{Rés}_{p,q}(P,Q)) = \text{Rés}_{p,q}(\varphi(P), \varphi(Q))$ où $\varphi(P)$ et

$\varphi(Q)$ sont les polynômes obtenus en appliquant φ à chaque coefficient. La propriété fondamentale du résultant est donnée par la proposition suivante.

Proposition 1.7.2. — *Soit k un corps algébriquement clos. Soit P (resp. Q) un polynôme de $k[X]$ de degré $\leq p$ (resp. $\leq q$). On suppose* $\deg P = p$ ou $\deg Q = q$. *Alors $Rés_{p,q}(P,Q) = 0$ si et seulement si P et Q ont une racine commune dans k.*

Démonstration. — Notons $k[X]_{\leq d}$ le k-espace vectoriel formé des polynômes de degré $\leq d$. Considérons l'application linéaire

$$f_{P,Q} : k[X]_{\leq q-1} \oplus k[X]_{\leq p-1} \to k[X]_{\leq p+q-1}$$
$$(U,V) \mapsto PU + QV.$$

La matrice de Sylvester de P et Q est la transposée de la matrice de $f_{P,Q}$ dans les bases $(X^{q-1}, \ldots, X, 1, X^{p-1}, \ldots, X, 1)$ et $(X^{p+q-1}, \ldots, X, 1)$. Donc $\text{Rés}_{p,q}(P,Q) = 0$ équivaut au fait que $f_{P,Q}$ n'est pas bijective. Si P et Q ont une racine commune $\alpha \in k$, alors tous les polynômes dans l'image de $f_{P,Q}$ s'annulent en α, donc $1 \notin \text{im}(f_{P,Q})$ et $\text{Rés}_{p,q}(P,Q) = 0$. Réciproquement, si $\text{Rés}_{p,q}(P,Q) = 0$ alors il existe $(U,V) \neq (0,0)$ tel que $PU + QV = 0$. Supposons $\deg P = p$ (le raisonnement est le même si $\deg Q = q$). Par l'absurde, supposons que P et Q n'ont pas de racine commune dans k. Comme k est algébriquement clos, il suit que P et Q sont premiers entre eux dans $k[X]$. Comme $P|QV$, on en déduit $P|V$. Comme $\deg V < p$, il vient $V = 0$, puis $U = 0$, contradiction. □

Revenons aux courbes algébriques, et commençons par montrer que « toute courbe dans le plan paramétrée par des fractions rationnelles est algébrique ». Considérons d'abord une version simplifiée du problème : donnons-nous des polynômes $P, Q \in k[T]$ et étudions l'ensemble

$$Z = \{(P(t), Q(t)) \in \mathbf{A}^2 : t \in \mathbf{A}^1\}, \tag{3}$$

qui n'est autre que l'image de l'application régulière $(P,Q) : \mathbf{A}^1 \to \mathbf{A}^2$.

Théorème 1.7.3. — *Si P ou Q est non constant, alors Z est une courbe affine plane irréductible.*

Démonstration. — Si un seul des polynômes P, Q est constant, alors Z est une droite (horizontale ou verticale) et le résultat est vrai. Supposons donc désormais $p = \deg P \geq 1$ et $q = \deg Q \geq 1$. Posons

$$F(X,Y) = \text{Rés}_{p,q}(P(T) - X, Q(T) - Y), \tag{4}$$

où $P(T) - X$ et $Q(T) - Y$ sont vus comme des polynômes en T à coefficients dans $k[X,Y]$, de sorte que $F \in k[X,Y]$. Un examen de la matrice de Sylvester révèle que F est de degré q en X et de degré p en Y ; en particulier F est non constant. De plus, pour $(x,y) \in \mathbf{A}^2$, on a les équivalences

$$\begin{aligned} F(x,y) = 0 &\Leftrightarrow \mathrm{Rés}_{p,q}(P(T) - x, Q(T) - y) = 0 \\ &\Leftrightarrow \exists\, t \in k \text{ tel que } P(t) - x = Q(t) - y = 0. \end{aligned}$$

La première équivalence résulte de la fonctorialité du résultant pour le morphisme $k[X,Y] \to k$ donné par l'évaluation en (x,y), tandis que la seconde équivalence découle de la proposition 1.7.2.

Ainsi $Z = V(F)$, ce qui montre que Z est une courbe affine plane. Pour montrer l'irréductibilité, supposons par l'absurde $Z = C_1 \cup C_2$ avec $C_1 \neq C_2$ des courbes affines planes. Alors $V_i = \{t \in \mathbf{A}^1 : (P(t), Q(t)) \in X_i\}$ est un fermé algébrique de $\mathbf{A}^1$, nécessairement infini car C_i est infini. Donc $V_1 = V_2 = \mathbf{A}^1$ et $C_1 = C_2 = Z$, ce qui contredit l'hypothèse. Ainsi Z est irréductible. □

Remarque 1.7.4. — (1) Le polynôme F obtenu au cours de la démonstration du théorème n'est pas toujours irréductible : en effet, on peut changer (P,Q) en $(P \circ R, Q \circ R)$ avec $\deg(R) \geq 1$ sans changer Z, tandis que les degrés de F en X et Y sont multipliés par $\deg R$.

(2) L'argument pour l'irréductibilité de Z est purement topologique : plus généralement, l'image continue d'un espace topologique irréductible est irréductible.

Plus généralement, on a le résultat suivant (cf. TD).

Théorème 1.7.5. — *Soient $F(t), G(t) \in k(t)$ des fractions rationnelles. Si F ou G est non constante, alors l'image de l'application $t \mapsto (F(t), G(t))$ (définie sur le complémentaire des pôles de F et G) est contenue dans une unique courbe affine plane irréductible.*

Une courbe affine plane obtenue de cette manière est dite *paramétrable par des fractions rationnelles*. On parlait autrefois de courbe *unicursale*, ce qui fait référence au fait que la courbe peut être tracée d'un seul trait (ce n'est pas tout à fait vrai, à cause des pôles de F et G). Le théorème suivant donne des conditions nécessaires et suffisantes pour qu'une courbe soit paramétrable par des fractions rationnelles.

Théorème 1.7.6. — *Soit C une courbe affine plane irréductible. Les conditions suivantes sont équivalentes :*

(1) *C est paramétrable par des fractions rationnelles.*

(2) *Il existe $f \in k(C)$ telle que $k(C) = k(f)$.*

(3) *Le corps $k(C)$ est k-isomorphe à $k(t)$.*

De plus, si ces conditions sont vérifiées, alors il existe un paramétrage de C qui est essentiellement bijectif : il existe des parties finies $S \subset \mathbf{A}^1$ et $T \subset C$ telles que le paramétrage induise une bijection $\mathbf{A}^1 \backslash S \to C \backslash T$.

Pour la démonstration, nous allons avoir besoin du théorème de Lüroth (cf. TD) : tout sous-corps de $k(t)$ contenant strictement k est de la forme $k(F)$ avec $F \in k(t)$ non constante. En particulier, tout sous-corps de $k(t)$ contenant strictement k est abstraitement k-isomorphe à $k(t)$.

Démonstration du théorème 1.7.6. — Les conditions (2) et (3) sont visiblement équivalentes. Supposons (1). Notons $t \mapsto (F(t), G(t))$ un paramétrage de C. Montrons que $k(C)$ est isomorphe au sous-corps $k(F(t), G(t))$ de $k(t)$. Soit $S \subset k$ l'ensemble fini formé des pôles de F et G. Considérons le morphisme de k-algèbres

$$\begin{aligned} \varphi : k[X, Y] &\to k(t) \\ X &\mapsto F(t) \\ Y &\mapsto G(t). \end{aligned}$$

Si $P \in I(C)$, alors la fraction rationnelle $P(F(t), G(t))$ est définie et s'annule sur la partie infinie $k - S$, donc est nulle. Par suite, φ induit un morphisme de k-algèbres $\widetilde{\varphi} : k[C] \to k(t)$. D'après la proposition 1.5.8, le morphisme $\widetilde{\varphi}$ est injectif et induit un morphisme (injectif) de corps $k(C) \to k(t)$. Ainsi $k(C)$ est isomorphe à un sous-corps de $k(t)$ contenant strictement k. Par le théorème de Lüroth, on en déduit (3).

Réciproquement, si la condition (3) est satisfaite, on note $F(t)$ (resp. $G(t)$) l'image de x (resp. y) par l'isomorphisme $k(C) \cong k(t)$, et on vérifie que $t \mapsto (F(t), G(t))$ est un paramétrage de C. Finalement, montrons que ce paramétrage est essentiellement bijectif. Notons $f \in k(C)$ la préimage de t par l'isomorphisme $k(C) \cong k(t)$. On vérifie alors que les parties $S = \{\text{pôles de } F \text{ et } G\} \subset \mathbf{A}^1$ et $T = \{\text{pôles de } f\} \subset C$ conviennent. □

Remarque 1.7.7. — L'argument de la remarque 1.7.4 montre qu'il y a des paramétrages qui ne sont pas essentiellement bijectifs. D'ailleurs, il n'y a pas unicité du paramétrage essentiellement bijectif : on peut composer à la source par des homographies $t \mapsto (at + b)/(ct + d)$ avec $a, b, c, d \in k$ tels que $ad - bc \neq 0$.

Définition 1.7.8. — Lorsque les conditions équivalentes du théorème 1.7.6 sont vérifiées, on dit que C est une *courbe rationnelle*. Dans le cas contraire, on dit que C est *irrationnelle*.

Donnons des exemples de courbes rationnelles et irrationnelles. Toute droite affine est une courbe rationnelle. Si $Q \in k[X]$ est un polynôme, son graphe $C = V(Y - Q(X))$ est une courbe rationnelle (en fait isomorphe à $\mathbf{A}^1$). Plus généralement, le graphe d'une fraction rationnelle est une courbe rationnelle.

Exemple 1.7.9. — Le cercle $C = V(X^2 + Y^2 - 1)$ est une courbe rationnelle. En effet si $\mathrm{car}(k) = 2$ alors $C = V(X + Y + 1)$ est une droite ; si $\mathrm{car}(k) \neq 2$, un paramétrage de C est donné par $t \mapsto \left(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}\right)$. L'application réciproque est donnée par $(x, y) \mapsto y/(1 - x)$. Ce paramétrage induit une bijection $\mathbf{A}^1 \backslash \{\pm i\} \to C \backslash \{(1, 0)\}$, où l'on note $\pm i$ les racines carrées de -1 dans k.

Nous verrons plus tard que toute conique irréductible est une courbe rationnelle et que toute cubique irréductible possédant un point singulier est une courbe rationnelle.

Exemple 1.7.10. — Si $n \geq 3$ n'est pas divisible par $\mathrm{car}(k)$, alors la courbe affine plane irréductible $C = V(X^n + Y^n - 1)$, dite *courbe de Fermat de degré* n, est irrationnelle (c'est une conséquence de théorème de Mason).

La notion de courbe rationnelle permet d'opérer une première distinction entre les courbes algébriques. Plus généralement, deux courbes affines planes irréductibles C et C' sont dites *birationnelles* si on a un k-isomorphisme $k(C) \cong k(C')$ (notons que les courbes rationnelles sont exactement les courbes birationnelles à $\mathbf{A}^1$). Une question naturelle est alors de classifier les courbes à équivalence birationnelle près. Un résultat important de géométrie algébrique, dû à Max Noether (1873) et Bertini (1882), mais qui dépasse le cadre de ce cours, affirme que toute courbe algébrique irréductible est birationnelle (mais pas nécessairement isomorphe) à une courbe affine plane irréductible dont les singularités sont au plus des points doubles.

1.8. Points lisses

Soit C une courbe affine plane et $F \in k[X, Y]$ un générateur de $I(C)$.

Définition 1.8.1. — Soit $P = (x_0, y_0) \in C$. On dit que P est un *point lisse* de C si $(\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y})(x_0, y_0) \neq (0, 0)$. Un point non lisse est un *point singulier* de C. On dit que C est lisse si tous ses points sont lisses.

Exemples 1.8.2. — (1) Toute droite affine est une courbe lisse.

(2) Le graphe d'une fonction polynomiale est une courbe lisse. En effet si $F = Y - Q(X)$ alors F est irréductible et $\frac{\partial F}{\partial Y} = 1$.

(3) Soit $C = V(X^2 + Y^2 - 1)$. Si $\mathrm{car}(k) \neq 2$ alors $F = X^2 + Y^2 - 1$ est irréductible et $(\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}) = (2X, 2Y)$ ne s'annule pas sur C, donc C est lisse. Si $\mathrm{car}(k) = 2$ alors $C = V(X + Y + 1)$ est une droite affine, donc est lisse.

(4) La courbe $C = V(XY)$ n'est pas lisse : $(0, 0)$ est un point singulier.

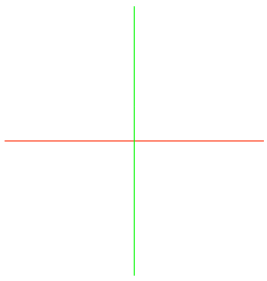

FIGURE 1. $C = V(XY)$

Remarque 1.8.3. — La définition de la lissité ne dépend pas du choix du générateur F de $I(C)$. Cependant, il faut prendre garde au fait que la définition ne marche plus si l'on sait seulement que $C = V(F)$. Par exemple si $C = V(F)$ on a aussi $C = V(F^2)$ et les dérivées partielles de F^2 sont divisibles par F, donc s'annulent identiquement sur C. Rappelons à ce sujet que si $C = V(F)$, on a

$I(C) = (F)$ si et seulement si F est sans facteur carré. Une condition nécessaire et suffisante pour qu'un polynôme soit sans facteur carré est donnée par la proposition suivante.

Proposition 1.8.4. — *Un polynôme $F \in k[X,Y]$ est sans facteur carré si et seulement si* $\mathrm{pgcd}(F, \frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}) = 1$ *dans* $k[X,Y]$.

Démonstration. — Si D^2 divise F dans $k[X,Y]$ avec D non constant, alors D divise les polynômes $F, \frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}$, et donc $\mathrm{pgcd}(F, \frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}) \neq 1$.

Réciproquement, supposons F sans facteur carré. Supposons par l'absurde qu'il existe un polynôme irréductible D divisant F, $\frac{\partial F}{\partial X}$ et $\frac{\partial F}{\partial Y}$. Posons $F = DE$ avec $E \in k[X,Y]$. Alors D divise $\frac{\partial F}{\partial X} = D\frac{\partial E}{\partial X} + E\frac{\partial D}{\partial X}$ et comme $\mathrm{pgcd}(D,E) = 1$, on en déduit $D | \frac{\partial D}{\partial X}$. Comme $\deg_X(\frac{\partial D}{\partial X}) \leq \deg_X(D) - 1$, il vient $\frac{\partial D}{\partial X} = 0$. De même $\frac{\partial D}{\partial Y} = 0$. Si $\mathrm{car}(k) = 0$, alors D est constant, ce qui est absurde. Si $\mathrm{car}(k) = p > 0$, alors D est un polynôme en X^p et Y^p, mais comme k est algébriquement clos, on en déduit que D est une puissance p-ième, contradiction. □

Définition 1.8.5. — Soit $P = (x_0, y_0)$ un point lisse de C. La *tangente* de C en P, notée $T_P C$, est la droite

$$T_P C : \frac{\partial F}{\partial X}(P) \cdot (X - x_0) + \frac{\partial F}{\partial Y}(P) \cdot (Y - y_0) = 0, \tag{5}$$

où F est un générateur de $I(C)$.

Notons que $T_P C$ est une droite affine passant par P et qu'elle ne dépend pas du choix du générateur F.

Exemple 1.8.6. — Si $Q \in k[X]$ alors la tangente de $C = V(Y - Q(X))$ en (x_0, y_0) est donnée par l'équation habituelle $Y - y_0 = Q'(x_0)(X - x_0)$.

Exercice. — (cf. TD) On suppose seulement $C = V(F)$ et on se donne $P \in C$. Montrer que si $(\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y})(P) \neq (0,0)$ alors P est lisse et que $T_P C$ est encore donnée par l'équation (5).

On peut aussi définir la notion de « tangente » en un point singulier, mais c'est plus délicat : une courbe peut avoir plusieurs tangentes en un point singulier, comme on le devine avec la courbe $C = V(XY)$ de l'exemple (4). Pour simplifier, supposons que le point de C à étudier est $P = (0,0)$ (on peut toujours se ramener à ce cas par une translation). Soit F un générateur de $I(C)$. La *multiplicité* de C en P, notée $m_P(C)$ est le plus petit degré d'un monôme de F. Notons que $m_P(C) \geq 1$, avec égalité si et seulement si P est lisse. Si $m = m_P(C)$, on peut écrire $F = G + H$ avec G homogène non nul de degré m et $H \in (X,Y)^{m+1} = (X^{m+1}, X^m Y, \ldots, XY^m, Y^{m+1})$. Alors $V(G)$ est réunion d'un nombre fini de droites de la forme $\alpha X + \beta Y = 0$ avec $\alpha, \beta \in k$ et $(\alpha, \beta) \neq (0,0)$. Par définition, ces droites sont les *tangentes* de C en P.

Définition 1.8.7. — On dit que $P \in C$ est un *point double ordinaire* si $m_P(C) = 2$ et C possède exactement 2 tangentes en P.

Les points doubles ordinaires sont les singularités les « moins méchantes » dans le monde des courbes planes. Voici quelques exemples.

Exemples 1.8.8. — (1) La courbe $C = V(XY)$ présente un point double ordinaire en $(0,0)$. Avec la définition ci-dessus, les deux tangentes de C en $(0,0)$ sont bien les axes de coordonnées.

(2) La courbe $C = V(Y^2 - X^3 - X^2)$ admet $P = (0,0)$ comme point singulier de multiplicité 2. Avec les notations ci-dessus, on a $G = Y^2 - X^2$ et $H = -X^3$. Si $\mathrm{car}(k) \neq 2$, alors $G = (Y+X)(Y-X)$ donc P est un point double ordinaire, les deux tangentes en P étant données par $Y = \pm X$, cf. figure 2. Si $\mathrm{car}(k) = 2$, alors la seule tangente en P est la droite $Y = X$, donc P n'est pas un point double ordinaire.

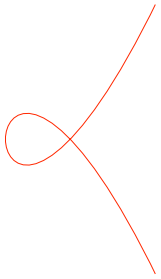

FIGURE 2. $C = V(Y^2 - X^3 - X^2)$ et $P = (0,0)$

(3) La courbe $C = V(Y^2 - X^3)$ admet $P = (0,0)$ comme point singulier, cf. figure 3. On a $m_P(C) = 2$ mais C ne possède qu'une tangente en P (la droite $Y = 0$), donc P n'est pas un point double ordinaire. On parle de *point de rebroussement* (quoique la terminologie est discutable sur un corps algébriquement clos), ou *cusp* en anglais.

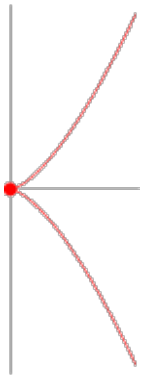

FIGURE 3. $C = V(Y^2 - X^3)$ et $P = (0,0)$

Nous allons maintenant chercher à donner une caractérisation intrinsèque de la lissité, c'est-à-dire ne faisant pas référence à une équation de C. Commençons par donner quelques propriétés de l'anneau local $\mathcal{O}_{C,P}$.

Lemme 1.8.9. — *Soit C une courbe affine plane irréductible et $P \in C$. L'anneau $\mathcal{O}_{C,P}$ est local, intègre, noethérien, et les seuls idéaux premiers de $\mathcal{O}_{C,P}$ sont $\{0\}$ et $\mathfrak{m}_{C,P}$.*

Démonstration. — On sait déjà que $\mathcal{O}_{C,P}$ est local et noethérien. Comme C est irréductible, $\mathcal{O}_{C,P}$ est intègre. Soit $S = k[C]\backslash\mathfrak{m}$ où $\mathfrak{m}$ est l'idéal maximal associé à P. D'après le cours sur la localisation, tout idéal premier de $\mathcal{O}_{C,P}$ est de la forme $S^{-1}I$ avec I un idéal premier de $k[C]$ ne rencontrant pas S, c'est-à-dire inclus dans $\mathfrak{m}$. Supposons I non nul. Soit $g \in I\backslash\{0\}$ et $G \in k[X,Y]$ un relèvement de g. D'après la proposition 1.5.6, l'ensemble $C \cap V(G)$ est fini. Par suite le k-espace vectoriel $k[C]/(g) \cong k[X,Y]/(G, I(C))$ est de dimension finie. Donc $k[C]/I$ est une k-algèbre intègre de dimension finie, c'est donc un corps et I est maximal, d'où $I = \mathfrak{m}$ et $S^{-1}I = \mathfrak{m}_{C,P}$. □

Lemme 1.8.10. — *Soit C une courbe affine plane irréductible et $P \in C$. Tout idéal non nul de $\mathcal{O}_{C,P}$ contient un idéal de la forme $\mathfrak{m}_{C,P}^n$ avec $n \geq 1$.*

Démonstration. — Soit Σ l'ensemble des idéaux non nuls de $\mathcal{O}_{C,P}$ qui ne vérifient pas cette propriété. Supposons Σ non vide et choisissons un élément maximal I de Σ. On a $I \neq \mathcal{O}_{C,P}$, $I \neq \mathfrak{m}_{C,P}$ et d'après le lemme 1.8.9, l'idéal I n'est pas premier. Soit $x, y \notin I$ tel que $xy \in I$. Alors (x, I) et (y, I) contiennent un idéal de la forme $\mathfrak{m}_{C,P}^n$, d'où $I \supset (x, I) \cdot (y, I) \supset \mathfrak{m}_{C,P}^{2n}$. □

Lemme 1.8.11. — *Soit C une courbe affine plane et $P \in C$. Notons $\mathfrak{m}$ l'idéal maximal de $k[C]$ associé à P, et $\mathfrak{m}_{C,P}$ l'idéal maximal de $\mathcal{O}_{C,P}$. Alors on a un isomorphisme de k-espaces vectoriels $\mathfrak{m}/\mathfrak{m}^2 \cong \mathfrak{m}_{C,P}/\mathfrak{m}_{C,P}^2$.*

Démonstration. — Considérons la suite exacte de $k[C]$-modules

$$0 \to \mathfrak{m}^2 \to \mathfrak{m} \to \frac{\mathfrak{m}}{\mathfrak{m}^2} \to 0.$$

D'après le cours sur la localisation, la suite obtenue en localisant en $\mathfrak{m}$ est encore exacte. Par suite $\mathfrak{m}_{C,P}/\mathfrak{m}_{C,P}^2$ s'identifie au localisé de $\mathfrak{m}/\mathfrak{m}^2$. Mais le $k[C]$-module $\mathfrak{m}/\mathfrak{m}^2$ est annulé par $\mathfrak{m}$, donc il s'identifie à son localisé, d'où le lemme. □

La proposition suivante donne une interprétation de la lissité en P en termes de l'idéal maximal associé à P.

Proposition 1.8.12. — *Soit C une courbe affine plane et $P \in C$. Notons $\mathfrak{m}$ l'idéal maximal de $k[C]$ associé à P. Les conditions suivantes sont équivalentes :*

(1) *Le point P est lisse.*

(2) *Le k-espace vectoriel $\mathfrak{m}/\mathfrak{m}^2$ est de dimension* 1.

(3) *Le k-espace vectoriel $\mathfrak{m}_{C,P}/\mathfrak{m}_{C,P}^2$ est de dimension* 1.

Démonstration. — L'équivalence (2) ⇔ (3) résulte du lemme 1.8.11.

Quitte à effectuer une translation des données, on peut supposer $P = (0,0)$, de sorte que $\mathfrak{m} = (x, y)$. Notons $\overline{x}, \overline{y}$ les images de x, y dans $\mathfrak{m}/\mathfrak{m}^2$. Remarquons que le $k[C]$-module $\mathfrak{m}/\mathfrak{m}^2$ est annulé par $\mathfrak{m}$. Par suite $\overline{x}$ et $\overline{y}$ engendrent $\mathfrak{m}/\mathfrak{m}^2$ comme $(k[C]/\mathfrak{m})$-module, c'est-à-dire comme k-espace vectoriel. On a donc $\dim_k(\mathfrak{m}/\mathfrak{m}^2) \leq 2$.

Supposons (1). Soit F un générateur de $I(C)$. Comme $F(0,0) = 0$, on a $F = \frac{\partial F}{\partial X}(P) \cdot X + \frac{\partial F}{\partial Y}(P) \cdot Y + H$ avec $H \in (X,Y)^2$. En prenant l'image dans $k[C]$, on obtient $0 = \frac{\partial F}{\partial X}(P) \cdot x + \frac{\partial F}{\partial Y}(P) \cdot y + h$ avec $h \in \mathfrak{m}^2$. En réduisant modulo $\mathfrak{m}^2$, on obtient une relation de dépendance linéaire entre $\overline{x}$ et $\overline{y}$, d'où $\dim_k(\mathfrak{m}/\mathfrak{m}^2) \leq 1$. Par ailleurs, si $\mathfrak{m} = \mathfrak{m}^2$ alors en prenant l'image réciproque dans $k[X,Y]$, on aurait $(X,Y) = (X,Y)^2 + (F)$, ce qui contredit le fait que le k-espace vectoriel $(X,Y)/(X,Y)^2$ est de dimension 2 (engendré par $\overline{X}$ et $\overline{Y}$). D'où (2).

Réciproquement, supposons (2). Par l'absurde, supposons que P n'est pas lisse. Alors $F \in (X,Y)^2$ et donc $I(C) \subset (X,Y)^2$. Si $a\overline{x} + b\overline{y} = 0$ avec $a, b \in k$ alors on en déduit $aX + bY \in (X,Y)^2$ d'où $a = b = 0$. Par suite $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 2$, contre l'hypothèse. □

La proposition suivante est un exemple typique d'application du lemme de Nakayama en géométrie algébrique.

Proposition 1.8.13. — *Soit C une courbe affine plane et $P \in C$. Alors P est lisse si et seulement si $\mathfrak{m}_{C,P}$ est un idéal principal de $\mathcal{O}_{C,P}$.*

Démonstration. — Supposons que P est lisse. Montrons que tout élément $t \in \mathfrak{m}_{C,P} - \mathfrak{m}_{C,P}^2$ engendre $\mathfrak{m}_{C,P}$. Considérons le $\mathcal{O}_{C,P}$-module $M = \mathfrak{m}_{C,P}/(t)$. On a $M/\mathfrak{m}_{C,P}M \cong \mathfrak{m}_{C,P}/(t, \mathfrak{m}_{C,P}^2) = 0$ puisque le k-espace vectoriel $\mathfrak{m}_{C,P}/\mathfrak{m}_{C,P}^2$ est de dimension 1 (proposition 1.8.12), engendré par la classe de t. Ainsi $M = \mathfrak{m}_{C,P}M$. Comme $\mathfrak{m}_{C,P}$ est de type fini (c'est le localisé d'un idéal de type fini), il en va de même de M. D'après le lemme de Nakayama, on a $M = 0$ et donc $\mathfrak{m}_{C,P} = (t)$.

Réciproquement, si $\mathfrak{m}_{C,P}$ est principal, alors le k-espace vectoriel $\mathfrak{m}_{C,P}/\mathfrak{m}_{C,P}^2$ est de dimension ≤ 1, et on a déjà vu qu'il est non nul, donc P est lisse par la proposition 1.8.12. □

Remarque 1.8.14. — En général, l'idéal maximal de $k[C]$ associé à un point P n'a aucune raison d'être principal, même si P est lisse (cf. TD).

Le théorème suivant montre que la lissité est une propriété locale : elle ne dépend que du localisé de l'anneau des fonctions régulières au point considéré.

Théorème 1.8.15. — *Soit C une courbe affine plane irréductible et $P \in C$. Les conditions suivantes sont équivalentes :*

(1) *Le point P est lisse.*

(2) *L'anneau $\mathcal{O}_{C,P}$ est principal.*

(3) *L'anneau $\mathcal{O}_{C,P}$ est intégralement clos.*

Démonstration du thérème 1.8.15. — Supposons que P est lisse et montrons (2). D'après la proposition 1.8.13, l'idéal $\mathfrak{m}_{C,P}$ est principal. Soit t un générateur de $\mathfrak{m}_{C,P}$. On a donc $\mathfrak{m}_{C,P}^n = (t^n)$ pour tout $n \geq 1$. Nous allons montrer que tout idéal de $\mathcal{O}_{C,P}$ est de cette forme. Commençons par montrer que $\cap_{n\geq 1}\mathfrak{m}_{C,P}^n = \{0\}$. Posons $M = \cap_{n\geq 1}\mathfrak{m}_{C,P}^n$. Comme $\mathcal{O}_{C,P}$ est noethérien, M est un idéal de type fini de $\mathcal{O}_{C,P}$. Si $f \in M$, alors, $f = tg$ avec $g \in \mathcal{O}_{C,P}$ et $tg \in (t^n)$ pour tout $n \geq 1$. Comme C est irréductible, $\mathcal{O}_{C,P}$ est intègre et donc $g \in M$. Ainsi $M = \mathfrak{m}_{C,P}M$ et le lemme de

Nakayama donne $M = 0$. Soit maintenant I un idéal de $\mathcal{O}_{C,P}$, avec $I \neq \{0\}, \mathcal{O}_{C,P}$. Comme $\cap_{n\geq 1}\mathfrak{m}_{C,P}^n = 0$, il existe un entier $n \geq 1$ tel que $I \subset \mathfrak{m}_{C,P}^n$ et $I \not\subset \mathfrak{m}_{C,P}^{n+1}$ Soit $f \in I$ tel que $f \notin \mathfrak{m}_{C,P}^{n+1}$. Alors $f = t^n g$ avec $g \notin (t)$ c'est-à-dire $g(P) \neq 0$. Mais alors $g \in \mathcal{O}_{C,P}^\times$ d'où $t^n \in I$ et $I = (t^n)$, ce que l'on voulait montrer.

Il est clair que (2) $\Rightarrow$ (3).

Enfin, supposons que $\mathcal{O}_{C,P}$ est intégralement clos et montrons (1). D'après la proposition 1.8.13, il suffit de montrer que $\mathfrak{m}_{C,P}$ est principal. Soit $f \in \mathfrak{m}_{C,P}\backslash\{0\}$. Si $\mathfrak{m}_{C,P} = (f)$, alors on a gagné. Sinon, d'après le lemme 1.8.10 il existe $n \geq 2$ tel que $\mathfrak{m}_{C,P}^n \subset (f)$ et $\mathfrak{m}_{C,P}^{n-1} \not\subset (f)$. Soit $g \in \mathfrak{m}_{C,P}^{n-1}$, $g \notin (f)$. La fraction g/f appartient à $k(C)$ mais pas à $\mathcal{O}_{C,P}$. Comme $\mathcal{O}_{C,P}$ est intégralement clos, g/f n'est pas entier sur $\mathcal{O}_{C,P}$. Comme $\mathfrak{m}_{C,P}$ est un $\mathcal{O}_{C,P}$-module de type fini, l'astuce du déterminant montre que $(g/f)\cdot\mathfrak{m}_{C,P} \not\subset \mathfrak{m}_{C,P}$. De plus $(g/f)\cdot\mathfrak{m}_{C,P} = f^{-1}g\cdot\mathfrak{m}_{C,P} \subset f^{-1}\mathfrak{m}_{C,P}^n \subset \mathcal{O}_{C,P}$. Ainsi $(g/f)\cdot\mathfrak{m}_{C,P}$ est un idéal de $\mathcal{O}_{C,P}$ non contenu dans $\mathfrak{m}_{C,P}$. Cela entraîne $(g/f)\cdot\mathfrak{m}_{C,P} = \mathcal{O}_{C,P}$ et donc $\mathfrak{m}_{C,P} = (f/g)$ est principal. □

On en déduit du théorème 1.8.15 le résultat fondamental suivant, qui caractérise la lissité d'une courbe affine en termes de son anneau des fonctions régulières.

Corollaire 1.8.16. — *Soit C une courbe affine plane irréductible. Alors C est lisse si et seulement si $k[C]$ est intégralement clos.*

Démonstration. — D'après le cours sur la localisation, l'anneau $k[C]$ est intégralement clos si et seulement si pour tout idéal maximal $\mathfrak{m}$ de $k[C]$, l'anneau $k[C]_\mathfrak{m}$ est intégralement clos. D'après le théorème 1.8.15, cela équivaut à dire que tous les points de C sont lisses, c'est-à-dire que C est lisse. □

Si l'anneau $k[C]$ est intègre mais pas intégralement clos, on peut considérer sa clôture intégrale dans $k(C)$. Si cette clôture intégrale est de la forme $k[C']$, alors C' est lisse et l'inclusion canonique $k[C] \to k[C']$ provient d'une application régulière $C' \to C$. On dit alors que l'on a « désingularisé » la courbe C.

Exemple 1.8.17. — Reprenons l'exemple de la courbe $C = V(Y^2 - X^3)$, qui n'est pas lisse puisque $(0,0)$ est un point singulier. On a vu en TD que $k[C] \cong k[T^2, T^3]$. Conformément au corollaire 1.8.16, cet anneau n'est pas intégralement clos. En effet, son corps des fractions est $k(T)$ et la fermeture intégrale de $k[T^2, T^3]$ dans $k(T)$ est $k[T]$. Remarquons que l'on a $k[T] = k[\mathbf{A}^1]$ et que la composition

$$k[C] \cong k[T^2, T^3] \subset k[T] \cong k[\mathbf{A}^1] \tag{6}$$

correspond géométriquement à l'application régulière

$$\begin{aligned} \varphi : \mathbf{A}^1 &\to C \\ t &\mapsto (t^2, t^3). \end{aligned}$$

On dit que le couple $(\mathbf{A}^1, \varphi)$ est une désingularisation de C.

Exercice. — Trouver une désingularisation de $C = V(Y^2 - X^3 + X^4)$ (on pourra montrer que la fermeture intégrale de $k[C]$ dans $k(C)$ est $k[x, y/x]$).

1.9. Anneaux de valuation discrète

Soit K un corps quelconque.

Définition 1.9.1. — Une valuation discrète sur K est une application $v : K \to \mathbf{Z} \cup \{+\infty\}$ vérifiant les propriétés suivantes :

(1) Pour $x \in K$, on a $v(x) = +\infty \Leftrightarrow x = 0$;

(2) L'application $v|_{K^\times} : K^\times \to \mathbf{Z}$ est un morphisme surjectif de groupes ;

(3) Pour tout $x, y \in K$, on a $v(x + y) \geq \min(v(x), v(y))$.

Exemples 1.9.2. — (1) Soit $K = \mathbf{Q}$ et p un nombre premier. Pour $x \in \mathbf{Q}^\times$, on pose $v_p(x) = n$ si $x = p^n \cdot \frac{a}{b}$ avec $a, b \in \mathbf{Z}$ non divisibles par p. On pose de plus $v_p(0) = +\infty$. Alors v_p est une valuation discrète sur $\mathbf{Q}$ (appelée *valuation p-adique*).

(2) Plus généralement si A est un anneau factoriel et $\pi \in A$ est irréductible, on peut définir de manière analogue une valuation discrète v_π sur $K = \mathrm{Frac}(A)$.

(3) Un cas particulier de (2) est donné par $A = K[T]$ (K corps quelconque) et $\pi = T$. La valulation discrète $\mathrm{val} = v_T$ associée n'est autre que l'application « valuation », définie pour $P = \sum_{n \geq 0} a_n T^n \in K[T]$ par $\mathrm{val}(P) = \min\{n \geq 0 : a_n \neq 0\}$ si $P \neq 0$, et $\mathrm{val}(0) = +\infty$.

(4) De même, en prenant $A = K[[T]]$ et $\pi = T$, on obtient une valuation discrète val sur le corps $K((T))$ des séries de Laurent à coefficients dans K.

(5) L'application $v : K[T] \to \mathbf{N} \cup \{+\infty\}$ définie par $v(P) = -\deg(P)$ se prolonge en une unique valuation discrète sur $K(T)$.

Lemme 1.9.3. — *Soit v une valuation discrète sur un corps K. Posons*

$$A_v = \{x \in K : v(x) \geq 0\}. \tag{7}$$

Alors A_v est un sous-anneau de K, est intègre, et vérifie $\mathrm{Frac}\, A_v = K$.

Démonstration. — L'axiome (1) entraîne que $0 \in A_v$. D'après (2) et (3), A_v est stable par addition et multiplication. Par (2), on a $v(1) = 0$ donc $1 \in A_v$. De même $2v(-1) = v((-1)^2) = v(1) = 0$ donc $-1 \in A_v$ et A_v est stable par $x \mapsto -x$. Ainsi A_v est un sous-anneau de K.

En particulier A_v est intègre et $\mathrm{Frac}\, A_v$ s'identifie à un sous-anneau de K. Soit $x \in K$. Si $v(x) \geq 0$ alors $x \in A_v$. Sinon on peut écrire $x = \frac{1}{y}$ avec $v(y) = -v(x) > 0$ donc $y \in A_v$. Ainsi $\mathrm{Frac}\, A_v = K$. □

Avec les notations du lemme précédent, on dit que A_v est *l'anneau de valuation* de (K, v). Cela nous amène à la définition suivante.

Définition 1.9.4. — Soit A un anneau commutatif. On dit que A est un *anneau de valuation discrète* si A est intègre et s'il existe une valuation discrète v sur $K = \mathrm{Frac}(A)$ telle que A est l'anneau de valuation de (K, v).

Proposition 1.9.5. — *Soit v une valuation discrète sur un corps K. L'anneau de valuation discrète A associé à (K, v) vérifie les propriétés suivantes :*

(1) *On a $A^\times = \{x \in A : v(x) = 0\}$.*

(2) *L'anneau A est local, d'idéal maximal $\mathfrak{m} = \{x \in A : v(x) \geq 1\}$.*

(3) *L'idéal $\mathfrak{m}$ est principal, et on a $\mathfrak{m} = (t) \Leftrightarrow v(t) = 1$.*

(4) *Pour tout $n \geq 1$, on a $\mathfrak{m}^n = \{x \in A : v(x) \geq n\}$.*

(5) *Tout idéal de A non nul et distinct de A est de la forme $\mathfrak{m}^n$ avec $n \geq 1$.*

(6) *L'anneau A est principal.*

Démonstration. — (1) Si $a, b \in A$ vérifient $ab = 1$ alors $v(a) + v(b) = 0$ donc $v(a) = v(b) = 0$. Réciproquement si $v(a) = 0$ alors $v(\frac{1}{a}) = -v(a) = 0$ donc $\frac{1}{a} \in A$ et $a \in A^\times$.

(2) résulte du fait que $A - A^\times = \{x \in A : v(x) \geq 1\}$ est un idéal de A.

(3) Soit $t \in A$ tel que $v(t) = 1$. En particulier $t \in \mathfrak{m}$ et donc $(t) \subset \mathfrak{m}$. Soit $x \in \mathfrak{m}$. Alors $v(\frac{x}{t}) = v(x) - v(t) \geq 0$ donc $\frac{x}{t} \in A$ et $x \in (t)$, d'où $\mathfrak{m} = (t)$. Réciproquement si $\mathfrak{m} = (t)$ alors $v(t) \geq 1$ et en considérant $x \in \mathfrak{m}$ tel que $v(x) = 1$, on obtient $1 \geq v(t)$ d'où $v(t) = 1$.

(4) Fixons $t \in A$ tel que $v(t) = 1$. D'après (3), on a $\mathfrak{m} = (t)$ et donc $\mathfrak{m}^n = (t^n)$. Si $x \in (t^n)$ alors $v(x) \geq v(t^n) = n$. Réciproquement si $v(x) \geq n$ alors $v(x/t^n) = v(x) - nv(t) \geq 0$ et donc $x \in (t^n)$.

(5) Soit $t \in A$ comme en (3), de sorte que $\mathfrak{m} = (t)$. Soit I un idéal de A, avec $I \neq \{0\}$ et $I \neq A$. Posons $n = \min\{v(x) : x \in I \backslash \{0\}\}$. D'après (4), on a $I \subset \mathfrak{m}^n$. Soit $x \in I$ tel que $v(x) = n$. On peut écrire $x = t^n u$ avec $v(u) = 0$ donc $u \in A^\times$ par (1). Alors $t^n = u^{-1}x \in I$ et par suite $\mathfrak{m}^n \subset I$, d'où finalement $I = \mathfrak{m}^n$.

(6) résulte de (5) et (3). □

Définition 1.9.6. — Soit A un anneau de valuation discrète, d'idéal maximal $\mathfrak{m}$. Le *corps résiduel* de A est le corps $k := A/\mathfrak{m}$. Une *uniformisante* de A est un générateur de $\mathfrak{m}$.

Remarque 1.9.7. — Avec les notations de la proposition 1.9.5, on a les équivalences : t uniformisante de $A \Leftrightarrow v(t) = 1 \Leftrightarrow (t \in \mathfrak{m}$ et $t \notin \mathfrak{m}^2)$.

Lemme 1.9.8. — *Soit A un anneau de valuation discrète, d'idéal maximal $\mathfrak{m}$ et de corps résiduel k. Soit t une uniformisante de A. Alors pour tout $n \geq 1$, le quotient $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ est un k-espace vectoriel de dimension 1, engendré par la classe de t^n.*

Démonstration. — Le A-module $M = \mathfrak{m}^n/\mathfrak{m}^{n+1}$ est annulé par $\mathfrak{m}$ donc est un k-espace vectoriel. Comme l'idéal $\mathfrak{m}^n$ est principal, engendré par t^n, le k-espace vectoriel M est engendré par la classe de t^n. En notant v la valuation discrète sur A, on a $v(t^n) = n$ donc $t^n \notin \mathfrak{m}^{n+1}$ et l'image de t^n dans M est non nulle. □

Exercices. — (1) Soit K un corps et v une valuation discrète sur K. Montrer que si $x, y \in K$ vérifient $v(x) \neq v(y)$, alors $v(x+y) = \min(v(x), v(y))$.

(2) Soit K un corps et v une valuation discrète sur K. Montrer que l'anneau de valuation de (K, v) est un sous-anneau maximal de K.

(3) Soit K un corps. Montrer que si deux valuations discrètes v et v' sur K ont le même anneau de valuation, alors $v = v'$.

(4) Soit A un anneau factoriel, $K = \mathrm{Frac}(A)$ et $\pi \in A$ irréductible. Montrer que l'anneau de valuation associé à (K, v_π) est le localisé $A_{(\pi)}$. En déduire qu'un anneau A est de valuation discrète si et seulement si A est principal, local et n'est pas un corps.

(5) Soit A le sous-anneau de $\mathbf{C}[[z]]$ formé des séries entières ayant un rayon de convergence > 0. Montrer que l'application val s'étend de manière unique en une valuation discrète sur $K = \mathrm{Frac}(A)$ et que A est l'anneau de valuation discrète associé à (K, val).

Revenons à la géométrie algébrique. Un exemple très naturel d'anneau de valuation discrète est fourni par l'anneau local d'une courbe en un point lisse. Donnons-nous donc, jusqu'à la fin du paragraphe, une courbe affine plane irréductible C définie sur un corps k algébriquement clos.

Définition 1.9.9. — Soit P un point lisse de C et $f \in \mathcal{O}_{C,P} \backslash \{0\}$. On appelle *ordre d'annulation de f en P*, et l'on note $\mathrm{ord}_P(f)$, le plus grand entier $n \geq 0$ tel que $f \in \mathfrak{m}_{C,P}^n$. On convient que $\mathrm{ord}_P(0) = +\infty$.

La définition 1.9.9 est licite car au cours de la démonstration du théorème 1.8.15, on a vu que $\cap_{n \geq 0} \mathfrak{m}_{C,P}^n = \{0\}$. De plus, pour $f \in \mathcal{O}_{C,P}$, on a les équivalences :

$$\mathrm{ord}_P(f) = 0 \Leftrightarrow f(P) \neq 0 \Leftrightarrow f \in \mathcal{O}_{C,P}^\times$$
$$\text{et } \mathrm{ord}_P(f) \geq 1 \Leftrightarrow f(P) = 0 \Leftrightarrow f \in \mathfrak{m}_{C,P}.$$

L'entier $\mathrm{ord}_P(f)$ est l'analogue de l'ordre d'annulation d'une fonction holomorphe en un point donné.

Lemme 1.9.10. — *Soit P un point lisse de C et $\mathfrak{m} \subset k[C]$ l'idéal maximal associé à P. Si $f \in k[C]$ vérifie $f \in \mathfrak{m}^n$ et $f \notin \mathfrak{m}^{n+1}$, alors* $\mathrm{ord}_P(f) = n$.

Démonstration. — On peut supposer $n \geq 1$. Si $f \in \mathfrak{m}^n$ alors $f \in \mathfrak{m}_{C,P}^n$ donc $\mathrm{ord}_P(f) \geq n$. En raisonnant comme dans le lemme 1.8.11, on montre que l'on a un isomorphisme de k-espaces vectoriels $\mathfrak{m}^n/\mathfrak{m}^{n+1} \cong \mathfrak{m}_{C,P}^n/\mathfrak{m}_{C,P}^{n+1}$. Par suite $f \notin \mathfrak{m}_{C,P}^{n+1}$ et donc $\mathrm{ord}_P(f) = n$. □

Exemple 1.9.11. — Prenons $C = \mathbf{A}^1$. Alors $k[C] \cong k[T]$ et d'après le lemme 1.9.10, l'ordre d'annulation de $F \in k[T]$ en un point $\lambda \in \mathbf{A}^1$ n'est autre que la multiplicité de λ comme racine de F (avec bien sûr $\mathrm{ord}_\lambda(F) = 0$ si λ n'est pas racine de F).

Lemme 1.9.12. — *Si P est un point lisse de C et $f, g \in \mathcal{O}_{C,P}$ alors* $\mathrm{ord}_P(fg) = \mathrm{ord}_P(f) + \mathrm{ord}_P(g)$.

Démonstration. — D'après la proposition 1.8.13, l'idéal $\mathfrak{m}_{C,P}$ est principal ; soit t un générateur. On peut supposer $f, g \neq 0$. Soit $m = \mathrm{ord}_P(f)$ et $n = \mathrm{ord}_P(g)$. Comme $f \in \mathfrak{m}_{C,P}^m$, on peut écrire $f = t^m u$ avec $u \in \mathcal{O}_{C,P}$. Comme $f \notin \mathfrak{m}_{C,P}^{m+1}$, on a $u \in \mathcal{O}_{C,P}^\times$. De même $g = t^n v$ avec $v \in \mathcal{O}_{C,P}^\times$. Alors $fg = t^{m+n}uv \in \mathfrak{m}_{C,P}^{m+n}$. Par l'absurde, si l'on avait $fg \in \mathfrak{m}_{C,P}^{m+n+1} = (t^{m+n+1})$ alors on aurait $uv \in (t) = \mathfrak{m}_{C,P}$, ce qui est impossible. D'où $\mathrm{ord}_P(fg) = \mathrm{ord}_P(f) + \mathrm{ord}_P(g)$. □

Théorème 1.9.13. — *Si P est un point lisse de C, alors l'application* ord_P *s'étend de manière unique en une valuation discrète sur $k(C)$, et $\mathcal{O}_{C,P}$ est l'anneau de valuation discrète associé à* ord_P.

Démonstration. — On a $k(C) = \mathrm{Frac}\,\mathcal{O}_{C,P}$. Pour $f \in k(C)^*$, on peut écrire $f = g/h$ avec $g, h \in \mathcal{O}_{C,P}$ et $g, h \neq 0$. On pose alors $\mathrm{ord}_P(f) = \mathrm{ord}_P(g) - \mathrm{ord}_P(h)$, ce qui ne dépend pas du choix de g et h grâce au lemme 1.9.12. L'application $\mathrm{ord}_P : k(C)^* \to \mathbf{Z}$ ainsi obtenue est un morphisme de groupes, surjectif puisque $\mathfrak{m}_{C,P} \neq \mathfrak{m}_{C,P}^2$. Vérifions que ord_P satisfait l'axiome (3) de la définition d'une valuation discrète. Lorsque les fonctions sont dans $\mathcal{O}_{C,P}$, cela résulte de la définition de ord_P. Si $f, g \in k(C)$ on peut écrire $f = f_0/h$ et $g = g_0/h$ avec $f_0, g_0, h \in \mathcal{O}_{C,P}$ de sorte que

$$\begin{aligned}\mathrm{ord}_P(f+g) &= \mathrm{ord}_P(f_0+g_0) - \mathrm{ord}_P(h)\\ &\geq \min(\mathrm{ord}_P(f_0), \mathrm{ord}_P(g_0)) - \mathrm{ord}_P(h)\\ &= \min(\mathrm{ord}_P(f), \mathrm{ord}_P(g)).\end{aligned}$$

Il reste à montrer que $\mathcal{O}_{C,P} = \{f \in k(C) : \mathrm{ord}_P(f) \geq 0\}$. L'inclusion directe étant immédiate, donnons-nous $f \in k(C)$ telle que $\mathrm{ord}_P(f) \geq 0$ et montrons que $f \in \mathcal{O}_{C,P}$. Posons $f = g/h$ avec $g, h \in \mathcal{O}_{C,P}$, $h \neq 0$ et $\mathrm{ord}_P(g) \geq \mathrm{ord}_P(h)$. Soit t un générateur de $\mathfrak{m}_{C,P}$. Comme dans la démonstration du lemme 1.9.12, on peut écrire $g = t^m u$ et $h = t^n v$ avec $u, v \in \mathcal{O}_{C,P}^\times$ et $m \geq n$, d'où $f = t^{m-n}u/v \in \mathcal{O}_{C,P}$. □

Exemple 1.9.14. — Reprenons l'exemple 1.9.11, à savoir $C = \mathbf{A}^1$. Alors $k(C) \cong k(T)$ et une fraction rationnelle $F \in k(T)$ vérifie $\mathrm{ord}_\lambda(F) < 0$ si et seulement si F a un pôle en λ ; dans ce cas $\mathrm{ord}_\lambda(F)$ est l'opposé de l'ordre du pôle de F en λ.

Définition 1.9.15. — Soit P un point lisse de C. On appelle *uniformisante de C en P* une uniformisante de l'anneau de valuation discrète $\mathcal{O}_{C,P}$.

Autrement dit, une uniformisante de C en P est une fonction $f \in k(C)$ telle que $\mathrm{ord}_P(f) = 1$.

Remarque 1.9.16. — Soit t une uniformisante de C en P. Alors toute fonction $f \in k(C)^\times$ s'écrit de manière unique $f = t^{\mathrm{ord}_P(f)}u$ avec $u \in \mathcal{O}_{C,P}^\times$. Ce fait est l'analogue exact du fait suivant bien connu pour les fonctions holomorphes. Soit U un ouvert de $\mathbf{C}$ et $z_0 \in U$. Alors toute fonction holomorphe h sur U, non identiquement nulle au voisinage de z_0, s'écrit de manière unique $h(z) = (z - z_0)^n u(z)$ avec $n \geq 0$,

u holomorphe sur U et $u(z_0) \neq 0$. Dans le cadre algébrique, on peut donc penser à t comme à l'analogue d'un « paramètre local » de la courbe en P.

Voyons, sur des exemples, comment calculer l'ordre d'annulation d'une fonction. Considérons la courbe affine plane irréductible $C = V(Y^2 - X^3 + X)$. Le point $P = (0,0)$ est lisse. Commençons par déterminer une uniformisante de C en P. Posons $\mathfrak{m} = (x,y)$. On a $y^2 = x^3 - x$ dans $k[C]$ ce qui entraîne que $x = x^3 - y^2 \in \mathfrak{m}^2$. Donc $\mathfrak{m} = (y) + \mathfrak{m}^2$. Comme l'on sait que $\mathfrak{m} \neq \mathfrak{m}^2$, cela entraîne que $y \notin \mathfrak{m}^2$ et donc, par le lemme 1.9.10, que y est une uniformisante en P. Ainsi $\mathrm{ord}_P(y) = 1$. Déterminons maintenant l'ordre d'annulation de x en P. Comme $x \in \mathfrak{m}^2$, on a $\mathrm{ord}_P(x) \geq 2$. Si l'on avait $\mathrm{ord}_P(x) \geq 3$, alors on en déduirait que $\mathrm{ord}_P(y^2) = \mathrm{ord}_P(x^3 - x) \geq 3$, ce qui est impossible car $\mathrm{ord}_P(y^2) = 2$. Donc $\mathrm{ord}_P(x) = 2$.

Considérons maintenant la courbe $C' = V(Y^2 + Y - X^3 - X)$. Le point $P' = (0,0)$ est lisse. Posons $\mathfrak{m}' = (x,y)$. Dans $k[C']$, on a $y^2 + y = x^3 - x$ donc $y \in -x + (\mathfrak{m}')^2$ et $\mathfrak{m}' = (x) + (\mathfrak{m}')^2$. Le même raisonnement que ci-dessus entraîne $\mathrm{ord}_{P'}(x) = 1$. On a de même $\mathrm{ord}_{P'}(y) = 1$, de sorte que x et y sont des uniformisantes en P'. Calculons maintenant l'ordre d'annulation de $f = x + y$ en P'. Comme $\mathrm{ord}_{P'}(x) = \mathrm{ord}_{P'}(y) = 1$, on ne peut pas déterminer directement $\mathrm{ord}_{P'}(f)$. Mais grâce à l'équation de C', on a $f = x^3 - y^2$ avec $\mathrm{ord}_{P'}(x^3) = 3 \cdot \mathrm{ord}_{P'}(x) = 3$ et $\mathrm{ord}_{P'}(-y^2) = 2 \cdot \mathrm{ord}_{P'}(y) = 2$ donc $\mathrm{ord}_{P'}(f) = 2$ (cf. exercice (1)).

1.10. Développements limités

Dans ce paragraphe, on fixe une courbe affine plane irréductible C et un point lisse $P \in C$.

Soit t une uniformisante en P et $f \in \mathcal{O}_{C,P} \backslash \{0\}$. Posons $n = \mathrm{ord}_P(f)$. Comme $f \in \mathfrak{m}_{C,P}^n$, on peut écrire $f = t^n u$ avec $u \in \mathcal{O}_{C,P}^\times$. Alors $h = f - u(P)t^n$ vérifie $h = t^n(u - u(P)) \in \mathfrak{m}_{C,P}^{n+1}$ puisque $u - u(P) \in \mathfrak{m}_{C,P}$. On a donc écrit

$$f = u(P)t^n + h \qquad \text{avec } u(P) \in k^\times \text{ et } \mathrm{ord}_P(h) \geq n+1. \tag{8}$$

En itérant ce procédé (avec la fonction h), on aboutit à la notion de développement limité de f au point P. Introduisons d'abord la notation commode suivante.

Notation 1.10.1. — Soit $f, g \in k(C)$ et $n \in \mathbf{Z}$. On note $f = g + O(t^n)$ si et seulement si $f - g \in \mathfrak{m}_{C,P}^n$.

Avec cette notation, (8) se réécrit sous la forme suggestive

$$f = u(P)t^n + O(t^{n+1}). \tag{9}$$

Théorème 1.10.2. — *Soit t une uniformisante en P et $f \in \mathcal{O}_{C,P}$. Alors il existe une unique série formelle $\sum_{n=0}^{+\infty} a_n T^n \in k[[T]]$ telle que pour tout $r \geq 0$, on ait*

$$f = a_0 + a_1 t + \cdots + a_r t^r + O(t^{r+1}). \tag{10}$$

La série formelle $\sum_{n=0}^{+\infty} a_n T^n$ *est appelée* développement limité de f en P relativement à l'uniformisante t.

Démonstration. — Montrons par récurrence sur $r \geq 0$ que pour tout $f \in \mathcal{O}_{C,P}$, il existe un unique polynôme $F \in k[T]$ de degré $\leq r$ tel que $f = F(t) + O(t^{r+1})$.

Pour $r = 0$, l'unique polynôme qui convient est $F = f(P) \in k$, d'où le résultat dans ce cas. Soit maintenant $r \geq 1$ tel que le résultat est vrai à l'ordre $r-1$. Soit $f \in \mathcal{O}_{C,P}$. On a $f - f(P) \in \mathfrak{m}_{C,P}$ d'où $f - f(P) = tg$ avec $g \in \mathcal{O}_{C,P}$. En appliquant l'hypothèse de récurrence à g, on trouve un polynôme $G \in k[T]$ de degré $\leq r-1$ tel que $g = G(t) + O(t^r)$. On en déduit $f = f(P) + tG(t) + O(t^{r+1})$ et donc $F = f(P) + TG$ convient. L'unicité de F est laissée en exercice. □

Remarque 1.10.3. — (1) Le développement limité de f en P dépend, de manière essentielle, du choix de l'uniformisante t en P.

(2) Les règles usuelles pour calculer les développements limités (addition, multiplication, division) restent valables dans le cadre algébrique.

On peut formaliser la dernière remarque par la proposition suivante.

Proposition 1.10.4. — *Soit t une uniformisante de C en P. Alors l'application « développement limité en P relativement à t » est un morphisme injectif de k-algèbres de $\mathcal{O}_{C,P}$ dans $k[[T]]$.*

Remarque 1.10.5. — Insistons sur le fait que le morphisme $\mathcal{O}_{C,P} \to k[[T]]$ n'est pas canonique : il dépend du choix de t. De plus, ce morphisme est loin d'être surjectif : en général, une série formelle en t n'a aucune raison de définir une fonction régulière en P. On peut s'en convaincre en considérant la courbe $C = \mathbf{A}^1$ et en remarquant que les développements limités des fractions rationnelles sont très particuliers : ils vérifient tous des relations de récurrence linéaire.

La notion de développement limité s'étend aux fonctions rationnelles.

Théorème 1.10.6. — *Soit t une uniformisante en P et $f \in k(C)^\times$. Posons $n_0 = \mathrm{ord}_P(f) \in \mathbf{Z}$. Alors il existe une unique série de Laurent $\sum_{n=n_0}^{+\infty} a_n T^n \in k((T))$ telle que pour tout $r \geq n_0$, on ait*

$$f = \sum_{n=n_0}^{r} a_n t^n + O(t^{r+1}). \tag{11}$$

La série de Laurent $\sum_{n=n_0}^{+\infty} a_n T^n$ *est appelée* développement limité de f en P relativement à l'uniformisante t.

Démonstration. — On peut supposer $n_0 < 0$, et dans ce cas il suffit d'appliquer le théorème 1.10.2 à $g = t^{-n_0} f \in \mathcal{O}_{C,P}$. □

Le théorème 1.10.6 fournit une application $k(C) \to k((T))$ qui est une k-extension de corps. Cette application s'obtient aussi à partir du morphisme $\mathcal{O}_{C,P} \to k[[T]]$ de la proposition 1.10.4 en passant aux corps des fractions.

Exemple 1.10.7. — Prenons $C = V(Y^2 - X^3 + 1)$. Le point $P = (1, 0)$ est lisse si $\mathrm{car}(k) \neq 3$. Sous cette hypothèse, on trouve $\mathrm{ord}_P(y) = 1$ et $\mathrm{ord}_P(x-1) = 2$, de sorte que y est une uniformisante en P. Calculons le développement limité de x en P relativement à y à l'ordre 6. Posons $u = x - 1$. On a $y^2 = x^3 - 1 = (1+u)^3 - 1 = 3u + 3u^2 + u^3$. Comme $\mathrm{ord}_P(3u^2 + u^3) = 4$, il vient $u = \frac{1}{3}y^2 + O(y^4)$. En réinjectant, il vient $3u^2 + u^3 = \frac{1}{3}y^4 + O(y^6)$ et donc $3u = y^2 - \frac{1}{3}y^4 + O(y^6)$. Finalement, on obtient

$$x = 1 + \frac{1}{3}y^2 - \frac{1}{9}y^4 + O(y^6).$$

Il n'est pas difficile de se convaincre que l'on peut ainsi déterminer le développement limité de x à un ordre donné. La présence des dénominateurs confirment que si $\mathrm{car}(k) = 3$, le calcul du développement limité n'a pas de sens (dans ce cas P n'est pas lisse). En fait, on trouve exactement le développement limité de la fonction réelle $y \mapsto \sqrt[3]{1 + y^2}$ en $y = 0$ (on pourra vérifier que dans ce développement limité, les dénominateurs sont des puissances de 3).

Exercice. — Montrer que le développement limité de x en P relativement à y ne contient que des puissances paires de y.

CHAPITRE 2

COURBES PROJECTIVES

2.1. Introduction à la géométrie projective

Soit k un corps (dans cette section seulement, on ne suppose pas que k est algébriquement clos).

De manière naïve, la *droite projective sur k* est une droite affine k à laquelle on a rajouté un point à l'infini, noté ∞. La définition rigoureuse est la suivante.

Définition 2.1.1. — La droite projective sur k, notée $\mathbf{P}^1(k)$, est l'ensemble des droites vectorielles de k^2.

Pour $\lambda \in k$, notons D_λ la droite vectorielle de k^2 engendrée par le point $(\lambda, 1)$. De plus, notons D_∞ la droite vectorielle de k^2 engendrée par le point $(1, 0)$. On vérifie alors que l'application

$$\begin{aligned} k \cup \{\infty\} &\to \mathbf{P}^1(k) \\ \lambda &\mapsto D_\lambda \end{aligned} \tag{12}$$

est bijective, ce qui permet de justifier la définition naïve précédente. Cependant, on voit que l'on a fait un choix de $\infty \in \mathbf{P}^1(k)$.

De manière un tout petit peu plus intrinsèque, notons $\mathcal{D}$ la droite affine de k^2 d'équation $y = 1$. Si $D \in \mathbf{P}^1(k)$ rencontre $\mathcal{D}$ au point $(\lambda, 1)$, alors $D = D_\lambda$. De plus $D_\infty \in \mathbf{P}^1(k)$ est parallèle à $\mathcal{D}$. Par analogie, on a donc envie de dire que les droites D_∞ et $\mathcal{D}$ se rencontrent « à l'infini ». Plus précisément, on a une bijection

$$\begin{aligned} \mathbf{P}^1(k) &\xrightarrow{\cong} \mathcal{D} \cup \{\infty\} \\ D &\mapsto \text{l'unique point de } D \cap \mathcal{D}, \end{aligned} \tag{13}$$

où l'on convient que $D_\infty \cap \mathcal{D} = \{\infty\}$. La bijection (13) n'est autre que la bijection réciproque de (12), une fois k identifié avec $\mathcal{D}$ au moyen de $\lambda \mapsto (\lambda, 1)$.

On va maintenant définir l'espace projectif de dimension quelconque sur k.

Définition 2.1.2. — Soit $n \geq 1$ un entier. L'*espace projectif de dimension n sur k*, noté $\mathbf{P}^n(k)$, est l'ensemble des droites vectorielles de k^{n+1}.

Considérons la relation d'équivalence $\sim$ sur $k^{n+1} - \{0\}$ définie par

$$x \sim y \Leftrightarrow \exists \lambda \in k^* : y = \lambda x.$$

Lemme 2.1.3. — *L'ensemble* $\mathbf{P}^n(k)$ *s'identifie au quotient de* $k^{n+1} - \{0\}$ *par la relation d'équivalence* $\sim$.

Démonstration. — On considère l'application $\pi : k^{n+1} - \{0\} \to \mathbf{P}^n(k)$ qui à un vecteur x associe la droite vectorielle engendrée par x. L'application π est surjective, et pour $x, y \in k^{n+1} - \{0\}$, on a $\pi(x) = \pi(y)$ si et seulement si y est un multiple non nul de x, c'est-à-dire si et seulement si $x \sim y$. □

Notation 2.1.4. — Pour tout $(x_0, \ldots, x_n) \in k^{n+1} - \{0\}$, on note $(x_0 : \ldots : x_n)$ son image canonique dans $\mathbf{P}^n(k)$.

Remarquons que $(0 : \ldots : 0)$ n'a aucun sens dans $\mathbf{P}^n(k)$. De plus, étant donnés deux vecteurs $(x_0, \ldots, x_n)$ et $(y_0, \ldots, y_n)$ dans $k^{n+1} - \{0\}$, on a

$$(x_0 : \ldots : x_n) = (y_0 : \ldots : y_n) \Leftrightarrow \exists \lambda \in k^* : \forall i \in \{0, \ldots, n\}, y_i = \lambda x_i.$$

Remarque 2.1.5. — Plus généralement, si V est un k-espace vectoriel, l'espace projectif associé à V, noté $\mathbf{P}(V)$, est l'ensemble des droites vectorielles de V. On a une identification $\mathbf{P}(V) \cong (V - \{0\})/k^*$. Lorsque V est de dimension finie, on *définit* la dimension de $\mathbf{P}(V)$ par $\dim \mathbf{P}(V) = (\dim V) - 1$. Ainsi l'espace projectif $\mathbf{P}^n(k) = \mathbf{P}(k^{n+1})$ est bien de dimension n.

Notons que si W est un sous-k-espace vectoriel de V, alors $\mathbf{P}(W)$ s'identifie canoniquement à une partie de $\mathbf{P}(V)$.

Définition 2.1.6. — Une partie E de $\mathbf{P}^n(k)$ est un *sous-espace projectif* si elle est de la forme $\mathbf{P}(V)$, où V est un sous-k-espace vectoriel non nul de k^{n+1}.

Exemple 2.1.7. — Pour tout point $m \in \mathbf{P}^n(k)$, la partie $E = \{m\}$ est un sous-espace projectif (de dimension 0) de $\mathbf{P}^n(k)$.

Soit $E = \mathbf{P}(V)$ un sous-espace projectif de $\mathbf{P}^n(k)$. On dit que :
- E est une droite de $\mathbf{P}^n(k)$ lorsque $\dim E = 1$ (et donc $\dim V = 2$) ;
- E est un plan de $\mathbf{P}^n(k)$ lorsque $\dim E = 2$ (et donc $\dim V = 3$) ;
- E est un hyperplan de $\mathbf{P}^n(k)$ lorsque $\dim E = n - 1$ (et donc $\dim V = n$) ;
- etc.

Soit $\pi : k^{n+1} - \{0\} \to \mathbf{P}^n(k)$ la surjection canonique et $d \in \{0, \ldots, n\}$ un entier fixé. On a une bijection

$$\{\text{sous-espaces vectoriels de } k^{n+1} \text{ de dimension } d+1\}$$
$$\cong \{\text{sous-espaces projectifs de } \mathbf{P}^n(k) \text{ de dimension } d\}$$

donnée par $V \mapsto \mathbf{P}(V)$; la bijection réciproque est $E \mapsto \pi^{-1}(E) \cup \{0\}$.

Si $(V_i)_{i \in I}$ est une famille quelconque de sous-espaces vectoriels de k^{n+1}, alors $\mathbf{P}(\cap_{i \in I} V_i) = \cap_{i \in I} \mathbf{P}(V_i)$ dans $\mathbf{P}^n(k)$, de sorte qu'une intersection quelconque de sous-espaces projectifs de $\mathbf{P}^n(k)$ est soit vide, soit un sous-espace projectif de $\mathbf{P}^n(k)$.

Si m et m' sont deux points distincts de $\mathbf{P}^n(k)$, alors il existe une unique droite de $\mathbf{P}^n(k)$ passant par m et m'. On la note (mm'). Plus généralement, si S est une partie non vide de $\mathbf{P}^n(k)$, alors il existe un plus petit sous-espace projectif de $\mathbf{P}^n(k)$ contenant S, appelé *sous-espace projectif engendré par* S. En effet, l'intersection de tous les sous-espaces projectifs contenant S est un sous-espace projectif, et c'est clairement le plus petit.

Proposition 2.1.8. — *Soit E et F des sous-espaces projectifs de $\mathbf{P}^n(k)$. Si $\dim E + \dim F \geq n$, alors $E \cap F$ est non vide.*

Exemple 2.1.9. — Deux droites de $\mathbf{P}^2(k)$ se coupent toujours (cet énoncé n'est autre que la traduction projective du fait que deux plans vectoriels de k^3 ont toujours une intersection non triviale). Plus précisément, si D et D' sont des droites de $\mathbf{P}^2(k)$, alors ou bien $D = D'$, ou bien $D \cap D'$ est un singleton.

Proposition 2.1.10. — *Soit D une droite de $\mathbf{P}^2(k)$ et $m \notin D$. Alors l'ensemble des droites de $\mathbf{P}^2(k)$ passant par m est en bijection avec D.*

Démonstration. — Notons m^* l'ensemble des droites de $\mathbf{P}^2(k)$ passant par m. Considérons l'application $h : D \to m^*$ qui à un point p associe la droite (mp). Elle est bien définie car $m \notin D$. Pour tout $p \in D$, on a $(mp) \cap D = \{p\}$ et donc h est injective. De plus, soit $D' \in m^*$. Alors $D \cap D'$ est un singleton $\{p\}$ et comme $m, p \in D'$, on a $D' = (mp) = h(p)$, donc h est surjective. □

Nous allons maintenant faire le lien entre espace affine et espace projectif. L'application

$$k^n \to \mathbf{P}^n(k)$$
$$(x_1, \ldots, x_n) \mapsto (1 : x_1 : \ldots : x_n)$$

est bien définie et injective. Cela permet d'identifier l'espace affine k^n à une partie de $\mathbf{P}^n(k)$. Cette identification n'est pas canonique (on a fait le choix que « la première coordonnée » vaut 1). Le complémentaire de k^n dans $\mathbf{P}^n(k)$ vaut

$$\mathbf{P}^n(k) - k^n = \{(0 : x_1 : \ldots : x_n) | (x_1, \ldots, x_n) \in k^n - \{0\}\} = \mathbf{P}(\{0\} \times k^n).$$

En particulier $\mathbf{P}^n(k) - k^n$ s'identifie à $\mathbf{P}^{n-1}(k)$. On a donc une décomposition (ensembliste, non canonique)

$$\mathbf{P}^n(k) = k^n \sqcup \mathbf{P}^{n-1}(k).$$

On dit que $\mathbf{P}^{n-1}(k)$ est l'*hyperplan à l'infini* de k^n.

Proposition 2.1.11. — *Soit V un sous-espace projectif de $\mathbf{P}^n(k)$. Si V rencontre k^n, alors $V \cap k^n$ est un sous-espace affine de k^n de même dimension que V. Réciproquement, si E est un sous-espace affine de k^n, alors il existe un unique sous-espace projectif V de $\mathbf{P}^n(k)$ (appelé* complétion projective de E*) tel que $V \cap k^n = E$.*

Démonstration. — Posons $V = \mathbf{P}(\widetilde{V})$, avec $\widetilde{V}$ sous-espace vectoriel de k^{n+1}. Soit $(a_1, \ldots, a_n) \in V \cap k^n$. Soit $p_0 : \widetilde{V} \to k$ l'application linéaire définie par $p_0(x_0, \ldots, x_n) = x_0$. Cette application est surjective puisque $(1, a_1, \ldots, a_n) \in \widetilde{V}$. Soit $F = \ker p_0$. On a $\dim F = (\dim \widetilde{V}) - 1 = \dim V$. De plus

$$\begin{aligned}(x_1, \ldots, x_n) \in V \cap k^n &\Leftrightarrow (1 : x_1 : \ldots : x_n) \in V \\ &\Leftrightarrow (1, x_1, \ldots, x_n) \in \widetilde{V} \\ &\Leftrightarrow (0, x_1 - a_1, \ldots, x_n - a_n) \in \widetilde{V} \\ &\Leftrightarrow (0, x_1 - a_1, \ldots, x_n - a_n) \in F.\end{aligned}$$

On a donc $V \cap k^n = (a_1, \ldots, a_n) + p_1(F)$, où $p_1 : F \to k^n$ est l'application linéaire injective définie par $p_1(0, x_1, \ldots, x_n) = (x_1, \ldots, x_n)$. Ainsi $V \cap k^n$ est un sous-espace affine de k^n de même dimension que V.

Réciproquement, soit $E = (a_1, \ldots, a_n) + F$ un sous-espace affine de k^n, avec $F \subset k^n$ sous-espace vectoriel. Soit $\widetilde{V} = \mathrm{Vect}(1, a_1, \ldots, a_n) + (\{0\} \times F)$ et $V = \mathbf{P}(\widetilde{V})$. Alors $V \cap k^n$ contient E. D'après ce qui précède, $V \cap k^n$ est un sous-espace affine de k^n de dimension $\dim V = (\dim \widetilde{V}) - 1 = \dim F$ puisque la somme définissant $\widetilde{V}$ est directe. D'où $\dim(V \cap k^n) = \dim E$ et l'on en déduit $V \cap k^n = E$. De plus, si $W = \mathbf{P}(\widetilde{W})$ convient alors $\{1\} \times E \subset \widetilde{W}$, d'où l'on déduit $\widetilde{V} \subset \widetilde{W}$. Puisque les dimensions sont égales, il vient $\widetilde{V} = \widetilde{W}$. □

On déduit de la proposition 2.1.11 une bijection

$$\begin{aligned}&\{\text{sous-espaces affines de } k^n\} \\ &\cong \{\text{sous-espaces projectifs de } \mathbf{P}^n(k) \text{ non inclus dans l'hyperplan à l'infini de } k^n\}.\end{aligned}$$

Cette bijection associe à un sous-espace affine sa complétion projective. La bijection réciproque envoie un sous-espace projectif sur son intersection avec k^n. De plus, cette bijection préserve la dimension.

Exemples 2.1.12. —
- La complétion projective de k^n est $\mathbf{P}^n(k)$.
- Si $a \in k^n$, la complétion projective du sous-espace affine $\{a\}$ de k^n est le sous-espace projectif réduit au point $(1 : a) \in \mathbf{P}^n(k)$.
- Prenons $n = 2$ et déterminons la complétion projective d'une droite affine D de k^2. Notons $\overline{D}$ la complétion projective de D. Posons $\overline{D} = \mathbf{P}(E)$ avec $E \subset k^3$ sous-espace vectoriel de dimension 2. La droite à l'infini de k^2 est $D_\infty = \mathbf{P}(E_\infty)$, avec $E_\infty = \{0\} \times k^2$. Comme $\overline{D} \neq D_\infty$, on a $E \neq E_\infty$ et donc $E \cap E_\infty$ est une droite vectorielle. Par suite $\overline{D} \cap D_\infty$ est réduit à un point, que l'on note ∞_D. On a donc $\overline{D} = D \sqcup \{\infty_D\}$. On voit sur un dessin (pour $k = \mathbf{R}$) que ∞_D est la « limite » de la droite vectorielle engendrée par un point de D tendant vers l'infini. On remarque également qu'étant données deux droites affines D_1, D_2 de k^2, on a $\infty_{D_1} = \infty_{D_2}$ si et seulement si D_1 et D_2 sont parallèles. On en déduit que l'ensemble des points à l'infini de k^2 est l'ensemble des directions possibles

pour les droites affines de k^2, c'est-à-dire l'ensemble des droites vectorielles de k^2. On retrouve ainsi l'identification entre la droite à l'infini de k^2 et $\mathbf{P}^1(k)$.

Dans ce qui précède, on a choisi d'identifier k^n à une partie de $\mathbf{P}^n(k)$ au moyen de $(x_1, \ldots, x_n) \mapsto (1 : x_1 : \ldots : x_n)$. L'hyperplan à l'infini de k^n est alors $H_\infty = \mathbf{P}(\{0\} \times k^n)$. En fait, il n'y a aucune raison de privilégier cet hyperplan : on peut prendre pour H_∞ n'importe quel hyperplan de $\mathbf{P}^n(k)$.

Fait : le complémentaire d'un hyperplan H de $\mathbf{P}^n(k)$ est naturellement muni d'une structure d'espace affine de dimension n sur k.

En effet, posons $H = \mathbf{P}(\widetilde{H})$, avec $\widetilde{H}$ hyperplan vectoriel de k^{n+1}. Soit $\mathcal{E}$ un hyperplan affine de k^{n+1} parallèle à $\widetilde{H}$ et ne passant pas par 0. Alors l'application $\pi|_{\mathcal{E}} : \mathcal{E} \to \mathbf{P}^n(k)$ est injective et identifie $\mathcal{E}$ au complémentaire de H dans $\mathbf{P}^n(k)$. On a donc ensemblistement $\mathbf{P}^n(k) = \mathcal{E} \sqcup H$, et l'on peut voir H comme l'hyperplan à l'infini de $\mathcal{E}$.

Si l'on choisit de plus une bijection affine $\mathcal{E} \cong k^n$, on obtient une application injective $\iota : k^n \hookrightarrow \mathbf{P}^n(k)$, que l'on appelle une *carte affine de* $\mathbf{P}^n(k)$.

Le fait que l'on puisse choisir librement une carte affine est d'une grande utilité pour étudier un objet projectif. Illustrons cela avec les coniques réelles. Prenons $k = \mathbf{R}$ et $n = 2$. Soit $C = \{(x : y : z) \in \mathbf{P}^2(\mathbf{R}) : x^2 + y^2 = z^2\}$. La définition fait sens car si $x^2 + y^2 = z^2$ alors $(\lambda x)^2 + (\lambda y)^2 = (\lambda z)^2$ pour tout $\lambda \in \mathbf{R}^*$. La préimage de C dans $\mathbf{R}^3 - \{0\}$ est un cône (épointé à l'origine).

(1) Choisissons comme carte affine l'application $\mathbf{R}^2 \xrightarrow{\iota_1} \mathbf{P}^2(\mathbf{R})$ donnée par $(x, y) \mapsto (x : y : 1)$. Alors $C_1 := \iota_1^{-1}(C) = \{(x, y) \in \mathbf{R}^2 : x^2 + y^2 = 1\}$ est un cercle. De plus C est tout entier contenu $\iota_1(\mathbf{R}^2)$, puisque $(x : y : 0) \in C$ entraîne $x = y = 0$, ce qui est impossible. Donc $C = \iota_1(C_1)$ et C_1 n'a pas de point à l'infini.

(2) Choisissons maintenant la carte affine $\mathbf{R}^2 \xrightarrow{\iota_2} \mathbf{P}^2(\mathbf{R})$ donnée par $(x, y) \mapsto (1 : x : y)$. Alors $C_2 := \iota_2^{-1}(C) = \{(x, y) \in \mathbf{R}^2 : 1 + x^2 = y^2\}$ est une hyperbole. On a $C = \iota_2(C_2) \cup \{(0 : 1 : 1), (0 : 1 : -1)\}$, de sorte que C_2 possède deux points à l'infini. Géométriquement, ces deux points correspondent aux deux asymptotes de C_2.

Exercice. — Trouver une carte affine $\iota : \mathbf{R}^2 \to \mathbf{P}^2(\mathbf{R})$ telle que $\iota^{-1}(C)$ soit une parabole. Combien y a-t-il de points à l'infini ?

Le groupe linéaire $\mathrm{GL}_{n+1}(k)$ agit sur l'ensemble des droites vectorielles de k^{n+1}, c'est-à-dire sur $\mathbf{P}^n(k)$. En coordonnées, si la matrice de $g \in \mathrm{GL}_{n+1}(k)$ dans la base canonique est $(g_{i,j})_{0 \leq i,j \leq n}$ alors $g(x_0 : \ldots : x_n) = (y_0 : \ldots : y_n)$ avec $y_i = \sum_{j=0}^n g_{i,j} x_j$.

Rappelons que le *groupe projectif linéaire* est défini par $\mathrm{PGL}_{n+1}(k) = \mathrm{GL}_{n+1}(k)/\{\lambda \cdot I_{n+1} : \lambda \in k^*\}$. L'action de $\mathrm{GL}_{n+1}(k)$ sur $\mathbf{P}^n(k)$ se factorise par $\mathrm{PGL}_{n+1}(k)$. Le groupe $\mathrm{PGL}_{n+1}(k)$ agit transitivement sur l'ensemble des sous-espaces projectifs de $\mathbf{P}^n(k)$ de dimension donnée.

Exercice. — Montrer que si $\iota_1, \iota_2 : k^n \hookrightarrow \mathbf{P}^n(k)$ sont deux cartes affines de $\mathbf{P}^n(k)$, il existe un unique $g \in \mathrm{PGL}_{n+1}(k)$ tel que $\iota_2 = g \circ \iota_1$.

2.2. L'espace projectif et ses fermés algébriques

On suppose désormais que le corps k est *algébriquement clos*. Soit $n \geq 1$ un entier. Pour tout $d \geq 0$, on note $k[X_0, \ldots, X_n]_d$ le sous-k-espace vectoriel de $k[X_0, \ldots, X_n]$ formé des polynômes homogènes de degré d. Une base en est donnée par les monômes $X_0^{d_0} \cdots X_n^{d_n}$ avec $d_0, \ldots, d_n \geq 0$ et $d_0 + \cdots + d_n = d$. Tout polynôme $P \in k[X_0, \ldots, X_n]$ s'écrit de manière unique $P = \sum_{d=0}^{\deg P} P_d$ avec $P_d \in k[X_0, \ldots, X_n]_d$. Le polynôme P_d est la *composante homogène de degré d de P*. On a donc une décomposition en somme directe

$$k[X_0, \ldots, X_n] = \bigoplus_{d \geq 0} k[X_0, \ldots, X_n]_d$$

et pour tout $d, d' \geq 0$, on a $k[X_0, \ldots, X_n]_d \cdot k[X_0, \ldots, X_n]_{d'} \subset k[X_0, \ldots, X_n]_{d+d'}$. On dit que $k[X_0, \ldots, X_n]$ est une *k-algèbre graduée*.

Définition 2.2.1. — Soit $(P_i)_{i \in I}$ une famille de polynômes *homogènes* de $k[X_0, \ldots, X_n]$. On pose

$$V((P_i)_{i \in I}) = \{(x_0 : \ldots : x_n) \in \mathbf{P}^n(k) : \forall i \in I, P_i(x_0, \ldots, x_n) = 0\}.$$

Cette définition fait sens car si P_i est homogène de degré d_i, on a $P_i(\lambda x_0, \ldots, \lambda x_n) = \lambda^{d_i} P_i(x_0, \ldots, x_n)$ pour tout $\lambda \in k^*$; en particulier $P_i(\lambda x_0, \ldots, \lambda x_n) = 0$ si et seulement si $P_i(x_0, \ldots, x_n) = 0$.

Définition 2.2.2. — Une partie F de $\mathbf{P}^n(k)$ est un *fermé algébrique* si et seulement si elle est de la forme $F = V((P_i)_{i \in I})$ avec $(P_i)_{i \in I}$ famille de polynômes homogènes de $k[X_0, \ldots, X_n]$.

Exemple 2.2.3. — (1) Tout sous-espace projectif de $\mathbf{P}^n(k)$ est un fermé algébrique de $\mathbf{P}^n(k)$ (prendre des polynômes P_i homogènes de degré 1).

(2) La partie vide est un fermé algébrique de $\mathbf{P}^n(k)$: on a $\emptyset = V(1)$.

(3) Le groupe $\mathrm{PGL}_{n+1}(k)$ respecte la notion de fermé algébrique.

On peut également définir la notion de fermé algébrique dans un produit d'espaces affines ou projectifs. Par exemple, si $m, n \geq 1$ sont deux entiers, un fermé algébrique de $\mathbf{P}^n(k) \times \mathbf{A}^m(k)$ est une partie de la forme

$$F = \{((x_0 : \ldots : x_n), (y_1, \ldots, y_m)) \in \mathbf{P}^n(k) \times \mathbf{A}^m(k) | \\ \forall i \in I, P_i(x_0, \ldots, x_n, y_1, \ldots, y_m) = 0\}$$

où les polynômes $P_i \in k[X_0, \ldots, X_n, Y_1, \ldots, Y_m]$ sont homogènes par rapport au groupe de variables $(X_0, \ldots, X_n)$.

De même, un fermé algébrique de $\mathbf{P}^n(k) \times \mathbf{P}^m(k)$ est une partie de la forme $F = V((P_i)_{i \in I})$ où les polynômes $P_i \in k[X_0, \ldots, X_n, Y_0, \ldots, Y_m]$ sont homogènes par rapport à chacun des groupes de variables $(X_0, \ldots, X_n)$ et $(Y_0, \ldots, Y_m)$.

Soit $\pi : \mathbf{A}^{n+1}(k) - \{0\} \to \mathbf{P}^n(k)$ la surjection canonique.

Proposition 2.2.4. — *Une partie F de $\mathbf{P}^n(k)$ est un fermé algébrique si et seulement si $\pi^{-1}(F) \cup \{0\}$ est un fermé algébrique de $\mathbf{A}^{n+1}(k)$.*

Démonstration. — Si $F = V((P_i)_{i\in I})$ où les P_i sont homogènes, alors $\pi^{-1}(F)\cup\{0\} = V((P_i)_{i\in I}) \cup \{0\}$ est un fermé algébrique de $\mathbf{A}^{n+1}(k)$.

Réciproquement, supposons $\pi^{-1}(F)\cup\{0\} = V(P_1, \ldots, P_r)$ avec $P_i \in k[X_0, \ldots, X_n]$ (non nécessairement homogène). Soit $x \in \pi^{-1}(F) \cup \{0\}$ et $\lambda \in k^*$. Comme $\lambda x \in \pi^{-1}(F)\cup\{0\}$, on a $P_i(\lambda x) = 0$ pour tout $1 \leq i \leq r$. Décomposons P_i en composantes homogènes : $P_i = \sum_{j=0}^{d_i} P_{i,j}$ avec $P_{i,j}$ homogène de degré j. On a alors

$$0 = P_i(\lambda x) = \sum_{j=0}^{d_i} \lambda^j P_{i,j}(x).$$

Ceci étant vrai pour tout $\lambda \in k^*$, et le corps k étant infini, il vient $P_{i,j}(x) = 0$ pour tout i et j. On vérifie alors que $F = V((P_{i,j})_{i,j})$, donc F est un fermé algébrique de $\mathbf{P}^n(k)$. □

Proposition 2.2.5. — *Soit I un idéal de $k[X_0, \ldots, X_n]$. Les conditions suivantes sont équivalentes :*

(1) *Pour tout $P \in I$ et $\lambda \in k^*$, on a $P(\lambda X_0, \ldots, \lambda X_n) \in I$.*

(2) *Pour tout $P \in I$, les composantes homogènes de P sont dans I.*

(3) *L'idéal I est engendré par des polynômes homogènes.*

(4) *L'idéal I est engendré par un nombre fini de polynômes homogènes.*

(5) *On a $I = \bigoplus_{d\geq 0} I \cap k[X_0, \ldots, X_n]_d$.*

Définition 2.2.6. — Soit I un idéal de $k[X_0, \ldots, X_n]$. On dit que I est *homogène* lorsqu'il vérifie les conditions équivalentes de la proposition 2.2.5.

Remarque 2.2.7. — (1) Attention, un idéal homogène n'est pas formé uniquement de polynômes homogènes (il est seulement engendré par de tels polynômes).

(2) Tout idéal homogène *strict* de $k[X_0, \ldots, X_n]$ est contenu dans l'idéal $(X_0, \ldots, X_n)$. En effet si I est un idéal homogène distinct de $k[X_0, \ldots, X_n]$ alors pour tout $P \in I$, on a $P(0, \ldots, 0) \in I$ (composante homogène de degré 0) ce qui force $P(0, \ldots, 0) = 0$ et donc $P \in (X_0, \ldots, X_n)$.

On va maintenant définir, comme dans le cas affine, des applications « V » et « I » pour l'espace projectif $\mathbf{P}^n$.

Notation 2.2.8. — Dans ce qui suit, on note $\widetilde{V}$ et $\widetilde{I}$ les applications (définies dans la section 1.1) entre l'ensemble des fermés algébriques de $\mathbf{A}^{n+1}$ et l'ensemble des idéaux de $k[X_0, \ldots, X_n]$.

Définition 2.2.9. — Pour tout idéal homogène I de $k[X_0, \ldots, X_n]$, on pose $V(I) = \pi(\widetilde{V}(I) - \{0\}) \subset \mathbf{P}^n$.

Lemme 2.2.10. — *Les fermés algébriques de $\mathbf{P}^n(k)$ sont exactement les parties de la forme $V(I)$, où I est un idéal homogène de $k[X_0, \ldots, X_n]$.*

Démonstration. — Il suffit de montrer que si $(P_i)_{i\in I}$ est une famille de polynômes homogènes, alors $V((P_i)_{i\in I}) = V(I)$, où I est l'idéal engendré par les P_i.

Si $(x_0 : \ldots : x_n) \in V((P_i)_{i\in I})$ alors $P_i(x_0, \ldots, x_n) = 0$ pour tout $i \in I$. D'où $P(x_0, \ldots, x_n) = 0$ pour tout $P \in I$ et donc $(x_0, \ldots, x_n) \in \widetilde{V}(I) - \{0\}$.

Réciproquement, si $(x_0, \ldots, x_n) \in \widetilde{V}(I) - \{0\}$ alors $P_i(x_0, \ldots, x_n) = 0$ pour tout $i \in I$, et donc $(x_0 : \ldots : x_n) \in V((P_i)_{i\in I})$. □

Exercice. — Montrer que les fermés algébriques de $\mathbf{P}^n(k)$ sont les fermés d'une topologie (on l'appelle *topologie de Zariski sur* $\mathbf{P}^n(k)$).

Définition 2.2.11. — Pour toute partie A de $\mathbf{P}^n$, on pose $I(A) = \widetilde{I}(\pi^{-1}(A) \cup \{0\})$.

Lemme 2.2.12. — *L'idéal $I(A)$ est un idéal homogène strict de $k[X_0, \ldots, X_n]$.*

Démonstration. — On a $I(A) \subset \widetilde{I}(\{0\}) = (X_0, \ldots, X_n)$ donc $I(A)$ est strict. Pour montrer que $I(A)$ est homogène, il suffit de vérifier la condition (1) de la proposition 2.2.5. Or cela résulte de la stabilité de $\pi^{-1}(A) \cup \{0\}$ par les homothéties $x \mapsto \lambda x$ avec $\lambda \in k^*$. □

Proposition 2.2.13. — *Si F est un fermé algébrique de $\mathbf{P}^n$, alors $V(I(F)) = F$.*

Démonstration. — Si $F = \emptyset$, on a $I(\emptyset) = (X_0, \ldots, X_n)$ et donc $V(I(\emptyset)) = \emptyset$. On peut donc supposer F non vide.

Si $(x_0 : \ldots : x_n) \in F$ alors $(x_0, \ldots, x_n) \in \pi^{-1}(F)$ annule tous les polynômes de $I(F)$, d'où $(x_0, \ldots, x_n) \in \widetilde{V}(I(F)) - \{0\}$ et donc $(x_0 : \ldots : x_n) \in V(I(F))$, ce qui montre $F \subset V(I(F))$.

Dans l'autre sens, posons $F = V((P_i)_{i\in I})$, où les P_i sont homogènes. Comme F est non vide, les P_i sont non constants, et l'on a $P_i \in I(F)$ pour tout $i \in I$. Notant I l'idéal (homogène) de $k[X_0, \ldots, X_n]$ engendré par les P_i, il vient $I \subset I(F)$ et donc $V(I(F)) \subset V(I) = F$. □

Voici maintenant la version projective du Nullstellensatz.

Théorème 2.2.14. — *Si J est un idéal homogène strict de $k[X_0, \ldots, X_n]$, alors $I(V(J)) = \sqrt{J}$.*

Démonstration. — Posons $F = V(J)$. Par définition, on a $F = \pi(\widetilde{V}(J) - \{0\})$. Comme J est strict, on a $0 \in \widetilde{V}(J)$. De plus $\widetilde{V}(J)$ est stable par les homothéties car J est homogène. On en déduit $\pi^{-1}(F) \cup \{0\} = \widetilde{V}(J)$ puis

$$I(F) = \widetilde{I}(\pi^{-1}(F) \cup \{0\}) = \widetilde{I}(\widetilde{V}(J)) = \sqrt{J},$$

la dernière égalité résultant du Nullstellensatz affine dans $\mathbf{A}^{n+1}$. □

Le Nullstellensatz projectif donne en particulier un critère pour que le lieu des zéros d'un idéal homogène soit vide : pour tout idéal homogène J de $k[X_0, \ldots, X_n]$, on a les équivalences :

$$\begin{aligned} V(J) = \emptyset &\Leftrightarrow \sqrt{J} = (X_0, \ldots, X_n) \\ &\Leftrightarrow \forall i \in \{0, \ldots, n\}, \exists d \geq 1 : X_i^d \in J \\ &\Leftrightarrow \exists N \geq 1 : J \text{ contient tous les monômes de degré } N \\ &\Leftrightarrow \exists N \geq 1 : J \supset \bigoplus_{d \geq N} k[X_0, \ldots, X_n]_d. \end{aligned}$$

Comme dans le cas affine, le Nullstellensatz permet d'établir une correspondance entre fermés algébriques et idéaux, à la condition cette fois de se restreindre aux idéaux homogènes stricts (et radiciels).

Corollaire 2.2.15. — *Lorsque k est algébriquement clos, on a une bijection renversant l'inclusion entre :*

(1) *les fermés algébriques de $\mathbf{P}^n(k)$;*

(2) *les idéaux homogènes stricts de de $k[X_0, \ldots, X_n]$ tels que $\sqrt{J} = J$.*

Cette bijection est donnée par $F \mapsto I(F)$ et $J \mapsto V(J)$.

Démonstration. — Soit F un fermé algébrique de $\mathbf{P}^n$. On a déjà vu que $I(F)$ est un idéal homogène strict de $k[X_0, \ldots, X_n]$. De plus, on a $\sqrt{I(F)} = I(F)$ car pour toute partie A de $\mathbf{A}^{n+1}$, l'idéal $\widetilde{I}(A)$ est radiciel. L'application de (1) vers (2) est donc bien définie. L'application de (2) vers (1) est bien définie, et on sait déjà que $V(I(F)) = F$. Enfin, si J est un idéal homogène radiciel strict de $k[X_0, \ldots, X_n]$, on a $I(V(J)) = \sqrt{J}$ d'après le Nullstellensatz, d'où $I(V(J)) = J$. □

Exemples 2.2.16. — Le fermé algébrique vide correspond, via cette bijection, à l'idéal $(X_0, \ldots, X_n)$. Le fermé algébrique $\mathbf{P}^n$ correspond à l'idéal $\{0\}$.

Soit $p = (x_0 : \ldots : x_n) \in \mathbf{P}^n$. Déterminons l'idéal associé à $\{p\}$. Choisissons $i \in \{0, \ldots, n\}$ tel que $x_i \neq 0$. Alors $I(\{p\})$ est l'idéal engendré par les polynômes homogènes $X_j - \frac{x_j}{x_i} X_i$ pour $j \neq i$. En effet, si l'on note J l'idéal (homogène) engendré par ces polynômes, alors l'anneau $k[X_0, \ldots, X_n]/J \cong k[X_i]$ est intègre, donc réduit, donc J est radiciel. Comme $V(J) = \{p\}$, on en déduit $I(\{p\}) = J$.

Soit $(\alpha_0, \ldots, \alpha_n) \in k^{n+1} - \{0\}$ et H l'hyperplan de $\mathbf{P}^n(k)$ d'équation homogène $\alpha_0 x_0 + \cdots + \alpha_n x_n = 0$. Par le même raisonnement, on a $I(H) = (\sum_{i=1}^n \alpha_i X_i)$.

Définition 2.2.17. — Une hypersurface projective est un fermé algébrique de $\mathbf{P}^n(k)$ de la forme $H = V(P)$ avec $P \in k[X_0, \ldots, X_n]$ homogène non nul de degré ≥ 1.

Exemples 2.2.18. — (1) Si $\deg(P) = 1$, alors H est un hyperplan.

(2) Si $\deg(P) = 2$, alors H est une *quadrique* (conique si $n = 2$).

(3) Si $\deg(P) = 3$, alors H est une *hypersurface cubique*, etc.

2.3. Le théorème fondamental de l'élimination projective

Considérons un système d'équations polynomiales

$$(*)\begin{cases} P_1(x_0,\dots,x_n,y_1,\dots,y_m)=0 \\ \vdots \\ P_r(x_0,\dots,x_n,y_1,\dots,y_m)=0 \end{cases}$$

où les polynômes $P_i \in k[X_0,\dots,X_n,Y_1,\dots,Y_m]$ sont homogènes en $(X_0,\dots,X_n)$.

Question : Pour quelles valeurs des paramètres $y_1,\dots,y_m \in k$ le système $(*)$ admet-il une solution $(x_0,\dots,x_n) \neq (0,\dots,0)$?

Notons $p_2 : \mathbf{P}^n \times \mathbf{A}^m \to \mathbf{A}^m$ la projection canonique. La question précédente revient alors à décrire $p_2(V(P_1,\dots,P_r))$, où $V(P_1,\dots,P_r)$ est le fermé algébrique de $\mathbf{P}^n \times \mathbf{A}^m$ défini par les P_i.

Théorème 2.3.1 **(Théorème fondamental de l'élimination projective)** *Pour tout fermé algébrique F de $\mathbf{P}^n \times \mathbf{A}^m$, l'ensemble $p_2(F)$ est un fermé algébrique de $\mathbf{A}^m$.*

En appliquant ce théorème à $F = V(P_1,\dots,P_r)$, l'ensemble des $(y_1,\dots,y_m) \in k^m$ tels que $(*)$ admette une solution non triviale est un fermé algébrique.

Historiquement, le théorème fondamental de l'élimination projective a d'abord été démontré par la théorie des *systèmes résultants*, qui généralise la notion de polynôme résultant et fut développée notamment par Kronecker au milieu du 19ème siècle.

Nous donnons ici une preuve moderne de ce résultat. Il s'agit d'un bel exemple d'utilisation de la noethérianité. Le désavantage de cette preuve est qu'elle ne fournit pas des équations explicites pour la projection $p_2(F)$.

Démonstration du théorème fondamental de l'élimination projective

Posons $F = V(P_1,\dots,P_r)$. Pour $y \in \mathbf{A}^m$, notons J_y l'idéal (homogène) de $k[X_0,\dots,X_n]$ engendré par les polynômes $P_{i,y} = P_i(X_0,\dots,X_n,y)$ pour $1 \leq i \leq r$. On a les équivalences

$$\begin{aligned} y \in p_2(F) &\Leftrightarrow V(J_y) \neq \emptyset \\ &\Leftrightarrow \forall N \geq 1, \text{ il existe un monôme de degré } N \text{ qui n'est pas dans } J_y. \end{aligned}$$

Soit d_i le degré homogène de P_i en $(X_0,\dots,X_n)$. Notons $T_{y,N}$ l'application linéaire

$$\begin{aligned} k[X_0,\dots,X_n]_{N-d_1} \oplus \cdots \oplus k[X_0,\dots,X_n]_{N-d_r} &\to k[X_0,\dots,X_n]_N \\ (Q_1,\dots,Q_r) &\mapsto \sum_{i=1}^r P_{i,y}Q_i \end{aligned}$$

où l'on convient que $k[X_0,\dots,X_n]_d = 0$ si $d < 0$. L'image de $T_{y,N}$ est exactement $J_y \cap k[X_0,\dots,X_n]_N$. En effet si $P \in J_y \cap k[X_0,\dots,X_n]_N$ alors $P = \sum_{i=1}^r P_{i,y}Q_i$

avec $Q_i \in k[X_0, \ldots, X_n]$, et l'égalité reste vraie en remplaçant Q_i par sa composante homogène de degré $N - d_i$. Par suite

$$y \in p_2(F) \Leftrightarrow \forall N \geq 1, T_{y,N} \text{ n'est pas surjective.}$$

Notons δ_N la dimension de $k[X_0, \ldots, X_n]_N$. Dire que $T_{y,N}$ n'est pas surjective équivaut à dire que tous les mineurs de taille δ_N de $T_{y,N}$ sont nuls. Cette dernière condition est algébrique en y, puisque les coefficients d'une représentation matricielle de $T_{y,N}$ sont des polynômes en $y_1, \ldots, y_m$. Par suite $p_2(F)$ est le lieu des zéros d'une famille (a priori) infinie de polynômes, d'où le résultat. □

Remarque 2.3.2. — Le théorème de l'élimination projective reste valable si l'on remplace $\mathbf{A}^m$ par $\mathbf{P}^m$ ou même par un espace de la forme $\mathbf{P}^{n_1} \times \mathbf{P}^{n_s} \times \mathbf{A}^m$ (même preuve). En revanche, l'analogue du théorème pour la projection $p_2 : \mathbf{A}^n \times \mathbf{A}^m \to \mathbf{A}^m$ est faux. On pourra s'en convaincre en considérant le cas $n = m = 1$ et le fermé algébrique $F = V(XY - 1)$. Il est essentiel que les « variables éliminées » soient projectives.

Comme application du théorème fondamentale de l'élimination projective, mentionnons le fait que pour toute application régulière $f : \mathbf{P}^m \to \mathbf{P}^n$ et tout fermé algébrique $F \subset \mathbf{P}^m$, son image $f(F)$ est un fermé algébrique de $\mathbf{P}^n$ (cf. TD).

2.4. Définition des courbes projectives planes

Définition 2.4.1. — Une *courbe projective plane* est un fermé algébrique de $\mathbf{P}^2(k)$ de la forme $V(F)$ avec $F \in k[X, Y, Z]$ polynôme homogène non constant.

Lemme 2.4.2. — *Soit $F \in k[X, Y, Z]$ un polynôme homogène non nul. Si $F = F_1 F_2$, alors F_1 et F_2 sont homogènes.*

Démonstration. — Soit d_i le degré de F_i, de sorte que $\deg F = d_1 + d_2$. Notons $F_i = \sum_{d=e_i}^{d_i} F_{i,d}$ la décomposition de F_i en composantes homogènes, avec $F_{i,e_i} \neq 0$. Alors $F_{1,e_1} F_{2,e_2}$ est une composante homogène non nulle de F, ce qui entraîne $F = F_{1,e_1} F_{2,e_2}$, d'où $d_1 = e_1$ et $d_2 = e_2$, c'est-à-dire que F_1 et F_2 sont homogènes. □

Lemme 2.4.3. — *Si C est une courbe projective plane, alors l'idéal $I(C)$ de $k[X, Y, Z]$ associé à C est principal, engendré par un polynôme homogène non constant.*

Démonstration. — Soit $C = V(F)$ avec F homogène non constant. Décomposons F en irréductibles dans $k[X, Y, Z]$: posons $F = \lambda \prod_{i=1}^{\ell} F_i^{m_i}$ avec $\lambda \in k^*$, F_i irréductible, $m_i \geq 1$ et les F_i deux à deux non associés dans $k[X, Y, Z]$. D'après le lemme 2.4.2, les polynômes F_i sont homogènes. D'après le Nullstellensatz projectif, on a $I(C) = I(V(F)) = \sqrt{(F)}$, et comme $k[X, Y, Z]$ est factoriel, il vient $\sqrt{(F)} = (F_1 \cdots F_\ell)$, et le polynôme $F_1 \cdots F_\ell$ est bien homogène. □

Définition 2.4.4. — Une courbe projective plane est dite *irréductible* si elle est de la forme $V(F)$ avec $F \in k[X, Y, Z]$ homogène irréductible.

Remarque 2.4.5. — Attention, comme pour les courbes affines, l'irréductibilité d'une courbe projective $V(F)$ n'entraîne pas l'irréductibilité de F.

Proposition 2.4.6. — *Soit C une courbe projective plane. Alors C est irréductible si et seulement si $I(C)$ est premier.*

Démonstration. — Posons $C = V(F)$ avec F homogène non constant. Comme dans la démonstration du lemme 2.4.3, écrivons $F = \lambda \prod_{i=1}^{\ell} F_i^{m_i}$ avec $\lambda \in k^*$, F_i irréductible, $m_i \geq 1$ et les F_i deux à deux non associés dans $k[X, Y, Z]$. On a vu alors que $I(C) = (F_1 \cdots F_\ell)$.

Si C est irréductible, alors on peut prendre F irréductible dans ce qui précède, d'où $I(C) = (F)$ et cet idéal est premier puisque $k[X, Y, Z]$ est factoriel.

Réciproquement, si $I(C)$ est premier alors nécessairement $\ell = 1$, d'où $C = V(I(C)) = V(F_1)$ est bien irréductible. □

Remarque 2.4.7. — La proposition 2.4.6 conduit à la définition générale de fermé algébrique irréductible : un fermé algébrique $V \subset \mathbf{P}^n$ est dit irréductible si l'idéal $I(V)$ de $k[X_0, \ldots, X_n]$ associé à V est premier.

Exercice. — Montrer qu'un fermé algébrique non vide $V \subset \mathbf{P}^n$ est irréductible si et seulement si V est irréductible pour la topologie induite par la topologie de Zariski sur $\mathbf{P}^n$.

Exercice. — Montrer que toute courbe projective plane s'écrit de manière unique comme réunion de courbes projectives planes irréductibles.

Exercice. — Soit C une courbe projective plane. Montrer les équivalences

$$\begin{aligned} C \text{ irréductible} &\Leftrightarrow \text{la seule courbe projective plane incluse dans } C \text{ est égale à } C \\ &\Leftrightarrow C \text{ n'est pas réunion de deux courbes strictement incluses dans } C \\ &\Leftrightarrow C \text{ n'est pas réunion de deux fermés algébriques } \subsetneq C \\ &\Leftrightarrow \text{tout fermé algébrique contenu strictement dans } C \text{ est fini.} \end{aligned}$$

Voici un tableau résumant la correspondance entre fermés algébriques et idéaux de polynômes, dans le cas du plan projectif.

Fermés algébriques de $\mathbf{P}^2$	Idéaux homogènes de $k[X, Y, Z]$
$\mathbf{P}^2$	$\{0\}$
$C = V(F)$ (F homogène irréductible)	$I(C) = (F)$
$\{(x_0 : y_0 : z_0)\}$	(si $x_0 \neq 0$) $(Y - \frac{y_0}{x_0}X, Z - \frac{z_0}{x_0}X)$
$\emptyset$	(X, Y, Z)

Remarque 2.4.8. — Attention, contrairement au cas affine, l'idéal associé à un point de $\mathbf{P}^2(k)$ n'est pas un idéal maximal de $k[X, Y, Z]$.

Nous verrons que tout fermé algébrique de $\mathbf{P}^2$ est soit $\mathbf{P}^2$, soit une réunion finie de courbes projectives et de points.

Remarque 2.4.9. — Nous ne traitons dans ce cours que des courbes projectives planes. Donnons cependant la définition générale des courbes projectives. Une courbe projective (irréductible) est un fermé algébrique C de $\mathbf{P}^n$ tel que :

(1) l'idéal $I(C)$ est premier (on dit alors que C est irréductible) ;

(2) la k-algèbre $A(C) := k[X_0, \ldots, X_n]/I(C)$ est de degré de transcendance 2 sur k : il existe $f, g \in A(C)$ algébriquement indépendants sur k tels que $A(C)$ soit algébrique sur $k[f, g]$.

Par exemple $\mathbf{P}^1$ lui-même est une courbe projective irréductible (on vérifiera que $A(\mathbf{P}^1) = k[X_0, X_1]$). Attention, contrairement au cas affine les éléments de $A(C)$ ne définissent pas des fonctions sur C, mais seulement des fonctions sur $\pi^{-1}(C)$, avec $\pi : \mathbf{A}^{n+1} - \{0\} \to \mathbf{P}^n$.

Pour $n = 2$, on retrouve exactement la définition vue plus haut. Lorsque $n = 3$, on parle de *courbe gauche*. On peut montrer que si $C \subset \mathbf{P}^n$ est une courbe algébrique, alors il faut au moins $n - 1$ polynômes pour engendrer l'idéal $I(C)$, mais attention, pour $n \geq 3$ il arrive que $n - 1$ éléments ne suffisent pas. C'est un problème ouvert que de savoir si toute courbe gauche de $\mathbf{P}^3$ peut être définie ensemblistement par deux polynômes homogènes.

2.5. Lien entre courbes affines et courbes projectives

Identifions $\mathbf{A}^n$ à une partie de $\mathbf{P}^n$ via l'application $(x_1, \ldots, x_n) \mapsto (1 : x_1 : \ldots : x_n)$. Remarquons que $\mathbf{A}^n$ est le complémentaire d'un hyperplan de $\mathbf{P}^n$, en particulier $\mathbf{A}^n$ est un ouvert de $\mathbf{P}^n$ pour la topologie de Zariski.

Lemme 2.5.1. — *Soit $F = V(P_1, \ldots, P_r)$ un fermé algébrique de $\mathbf{P}^n$, avec les $P_i \in k[X_0, \ldots, X_n]$ homogènes. Alors $F \cap \mathbf{A}^n = V(\widetilde{P_1}, \ldots, \widetilde{P_r})$ avec $\widetilde{P_i} = P_i(1, X_1, \ldots, X_n)$.*

Si $P \in k[X_0, \ldots, X_n]$ est homogène, le polynôme $\widetilde{P} = P(1, X_1, \ldots, X_n)$ est le *déshomogénéisé de P par rapport à X_0*. Remarquons que $\deg \widetilde{P} \leq \deg P$, avec égalité si et seulement si P n'est pas divisible par X_0. Remarquons que le choix de la variable X_0 correspond à choisir $V(X_0)$ comme hyperplan à l'infini de $\mathbf{A}^n$.

À partir de maintenant, on suppose $n = 2$. On note $(x : y : z)$ les coordonnées homogènes dans $\mathbf{P}^2$ et on identifie $\mathbf{A}^2$ à un ouvert de $\mathbf{P}^2$ via l'application $(x, y) \mapsto (x : y : 1)$.

Définition 2.5.2. — Soit $F \in k[X, Y]$ un polynôme homogène non nul de degré d. Le polynôme *homogénéisé* de F est le polynôme $\overline{F}(X, Y, Z) = Z^d F(\frac{X}{Z}, \frac{Y}{Z})$.

On vérifie que $\overline{F} \in k[X, Y, Z]$ et que $\overline{F}$ est homogène de degré d. De manière explicite, l'homogénéisé de $F = \sum_{i,j} a_{i,j} X^i Y^j$ est $\overline{F} = \sum_{i,j} a_{i,j} X^i Y^j Z^{d-i-j}$.

Propriétés :

- Pour tout $F \in k[X, Y]$ non nul, on a $F = \overline{F}(X, Y, 1)$.
- Pour tous $F_1, F_2 \in k[X, Y]$ non nuls, on a $\overline{F_1 F_2} = \overline{F_1} \cdot \overline{F_2}$.
- Si $H \in k[X, Y, Z]$ est homogène non divisible par Z, alors $H = \overline{H(X, Y, 1)}$.

Proposition 2.5.3. — *Si $C = V(F)$ est une courbe affine plane, alors $V(\overline{F})$ est l'adhérence de C dans $\mathbf{P}^2$ pour la topologie de Zariski. En particulier $V(\overline{F})$ est la plus petite courbe projective plane contenant C.*

Démonstration. — Notons $\overline{C}$ l'adhérence de C dans $\mathbf{P}^2$ pour la topologie de Zariski. On vérifie que F est le déshomogénéisé de $\overline{F}$. D'après le lemme 2.5.1, on a donc $C = V(\overline{F}) \cap \mathbf{A}^2$. En particulier $V(\overline{F})$ contient C, et comme $V(\overline{F})$ est un fermé algébrique, on en déduit que $V(\overline{F})$ contient $\overline{C}$. Réciproquement, posons $\overline{C} = V(P_1, \ldots, P_r)$ où les P_i sont homogènes. Pour chaque i, le polynôme $P_i(X, Y, 1)$ s'annule sur $C = V(F)$. D'après le Nullstellensatz affine, il existe $m \geq 1$ tel que $P_i(X, Y, 1)^m = FG$ avec $G \in k[X, Y]$. Posons $P_i = Z^e Q_i$ avec Q_i non divisible par Z. Alors l'homogénéisé de $P_i(X, Y, 1) = Q_i(X, Y, 1)$ est égal à Q_i. Comme l'homogénéisé d'un produit est le produit des homogénéisés, on obtient $Q_i^m = \overline{F} \cdot \overline{G}$, donc $\overline{F}$ divise Q_i^m. Par suite $\overline{F} | P_i^m$ et donc $V(\overline{F}) \subset V(P_i)$. Ceci étant vrai pour tout i, on en déduit $V(\overline{F}) \subset \overline{C}$. □

Définition 2.5.4. — Soit $C = V(F)$ une courbe affine plane, avec $F \in k[X, Y]$ non constant. On appelle *complétion projective de C*, et on note $\overline{C}$, la courbe projective $V(\overline{F})$.

D'après la proposition 2.5.3, la complétion projective de $C = V(F)$ ne dépend que de C, et pas du choix de F.

Définition 2.5.5. — Soit C une courbe affine plane. Les *points à l'infini* de C sont les points de $\overline{C} - C$.

Lemme 2.5.6. — *Si $F \in k[X, Y]$ est de degré $d \geq 1$, alors la courbe $C = V(F)$ possède au plus d points à l'infini.*

Démonstration. — On a $\overline{C} = V(H)$ où $H = \overline{F}$ est l'homogénéisé de F. On a $(x : y : 0) \in \overline{C}$ si et seulement si $H(x, y, 0) = 0$. Or le polynôme $H(X, Y, 0)$ est homogène de degré d, et non nul (puisque $\deg F = d$). On en déduit que $H(X, Y, 0)$ possède au plus d zéros dans $\mathbf{P}^1(k)$, et donc $\overline{C} - C$ est de cardinal $\leq d$. □

Les points à l'infini de la courbe C correspondent intuitivement aux « directions asymptotiques » de C (il faut utiliser ce terme avec prudence puisque k n'est pas a priori muni d'une topologie).

Nous pouvons maintenant énoncer la correspondance entre courbes affines et courbes projectives.

Théorème 2.5.7. — *Si l'on fixe une carte affine de $\mathbf{P}^2$, on a une bijection entre :*

(1) *les courbes affines planes ;*

(2) *les courbes projectives planes ne contenant pas la droite à l'infini.*

Cette bijection associe à une courbe affine plane sa complétion projective ; réciproquement, elle associe à une courbe projective plane son intersection avec la carte affine.

De plus, cette bijection préserve l'irréductibilité.

Démonstration. — On a vu que si $C = V(F)$ est une courbe affine plane, alors $\overline{C}$ est une courbe projective plane (prop. 2.5.3) et $\overline{C}$ ne contient pas la droite à l'infini (lemme 2.5.6). De plus $\overline{C} \cap \mathbf{A}^2 = V(\overline{F}) \cap \mathbf{A}^2 = V(\overline{F}(X, Y, 1)) = V(F) = C$.

Réciproquement, si $C = V(H)$ est une courbe projective plane ne contenant pas la droite à l'infini, alors $C \cap \mathbf{A}^2 = V(F)$ avec $F = H(X, Y, 1)$. Comme H n'est pas divisible par Z, on a $\deg F = \deg H \geq 1$ et donc $C \cap \mathbf{A}^2$ est une courbe affine plane. De plus la complétion projective de $C \cap \mathbf{A}^2$ est $V(\overline{F}) = V(\overline{H(X, Y, 1)}) = V(H) = C$ puisque H n'est pas divisible par Z. D'où la bijection annoncée.

Montrons l'assertion concernant l'irréductibilité. Supposons $C = V(F)$ avec $F \in k[X, Y]$ irréductible. Alors $\overline{C} = V(\overline{F})$. Si le polynôme $\overline{F}$ était réductible, on aurait $\overline{F} = H_1 H_2$ avec H_i homogène non constant (lemme 2.4.2) non divisible par Z (car $\overline{F}$ n'est pas divisible par Z), d'où $F = H_1(X, Y, 1)H_2(X, Y, 1)$ avec $\deg H_i(X, Y, 1) \geq 1$, absurde.

Réciproquement, soit $C = V(H)$ avec $H \in k[X, Y, Z]$ homogène irréductible non divisible par Z. Montrons que $F = H(X, Y, 1)$ est irréductible. On a $\deg F = \deg H$ donc F est non constant. Par l'absurde, si $F = F_1 F_2$ avec $\deg F_i \geq 1$ alors $H = \overline{F} = \overline{F_1} \cdot \overline{F_2}$ avec $\deg \overline{F_i} = \deg F_i \geq 1$, ce qui contredit l'irréductibilité de H. □

Remarque 2.5.8. — Attention, deux courbes affines planes C_1 et C_2 distinctes peuvent donner lieu à des complétions $\overline{C_1}$ et $\overline{C_2}$ projectivement équivalentes (dans le sens où il existe $g \in \mathrm{PGL}_3(\mathbf{C})$ tel que $C_2 = g(C_1)$). De manière équivalente, si l'on part d'une courbe projective plane C, alors deux cartes affines de $\mathbf{P}^2$ peuvent donner lieu à deux courbes affines planes distinctes. Un exemple est donné par les coniques affines (voir la fin de la section §2.1).

Exercice. — (1) Trouver deux courbes affines planes C_1 et C_2 non isomorphes telles que $\overline{C_1}$ et $\overline{C_2}$ sont projectivement équivalentes.

(2) Trouver deux courbes affines planes C_1 et C_2 isomorphes telles que $\overline{C_1}$ et $\overline{C_2}$ ne sont pas projectivement équivalentes.

Exercice. — Soit C une courbe affine plane. Montrer que si $I(C) = (F)$ alors $I(\overline{C}) = (\overline{F})$.

2.6. Points lisses et fonctions rationnelles

Soit C une courbe projective plane. D'après le lemme 2.4.3, l'idéal $I(C)$ est engendré par un polynôme $H \in k[X, Y, Z]$ homogène non constant.

Définition 2.6.1. — Soit $P = (x_0 : y_0 : z_0) \in C$. On dit que P est un *point lisse* de C si $(\frac{\partial H}{\partial X}, \frac{\partial H}{\partial Y}, \frac{\partial H}{\partial Z})(x_0, y_0, z_0) \neq (0, 0, 0)$. Un point non lisse de C est aussi appelé *point singulier* de C. On dit que C est lisse si tous ses points sont lisses.

Remarque 2.6.2. — Si H est homogène de degré $d \geq 1$, alors $\frac{\partial H}{\partial X}$, $\frac{\partial H}{\partial Y}$ et $\frac{\partial H}{\partial Z}$ sont homogènes de degré $d-1$, et donc la condition $(\frac{\partial H}{\partial X}, \frac{\partial H}{\partial Y}, \frac{\partial H}{\partial Z})(x_0, y_0, z_0) \neq (0, 0, 0)$ ne dépend pas du choix des coordonnées homogènes de P. De plus H est bien déterminé

à multiplication près par un élément de k^*, et donc la lissité de P ne dépend pas du choix de H.

Pour tout polynôme $H \in k[X,Y,Z]_d$, on a l'identité d'Euler

$$X\frac{\partial H}{\partial X} + Y\frac{\partial H}{\partial Y} + Z\frac{\partial H}{\partial Z} = d \cdot H.$$

On en déduit que si $(x_0, y_0, z_0) \in k^3 - \{0\}$ annule les dérivées partielles de H et si $d \neq 0$ dans k, alors le point $(x_0 : y_0 : z_0) \in \mathbf{P}^2(k)$ est automatiquement sur C. On en déduit le critère suivant pour trouver les points singuliers de C.

Proposition 2.6.3. — *Supposons que d n'est pas divisible par la caractéristique de k et que $H \in k[X,Y,Z]_d$ est sans facteur carré. Alors les points singuliers de $V(H)$ sont donnés par $V(H)^{sing} = V(\frac{\partial H}{\partial X}, \frac{\partial H}{\partial Y}, \frac{\partial H}{\partial Z})$.*

Définition 2.6.4. — Soit $P = (x_0 : y_0 : z_0)$ un point lisse de C. La tangente de C en P, notée $T_P C$ est la droite projective

$$\frac{\partial H}{\partial X}(x_0,y_0,z_0) \cdot X + \frac{\partial H}{\partial Y}(x_0,y_0,z_0) \cdot Y + \frac{\partial H}{\partial Z}(x_0,y_0,z_0) \cdot Z = 0. \tag{14}$$

Comme P est lisse, l'équation précédente est bien celle d'une droite projective. On vérifie comme précédemment que la droite $T_P C$ ne dépend ni du choix du représentant (x_0, y_0, z_0) de P, ni du choix du polynôme H.

La proposition suivante montre qu'il y a équivalence entre lissité « affine » et lissité « projective ».

Proposition 2.6.5. — *Soit C une courbe affine plane et P un point de C. Alors P est un point lisse de C si et seulement si P est un point lisse de $\overline{C}$.*

Démonstration. — Soit F un générateur de $I(C)$ et $H = \overline{F}$. Posons $P = (x_0, y_0) \in C$. Comme $F(X,Y) = H(X,Y,1)$, il vient $\frac{\partial F}{\partial X}(x_0,y_0) = \frac{\partial H}{\partial X}(x_0,y_0,1)$ et $\frac{\partial F}{\partial Y}(x_0,y_0) = \frac{\partial H}{\partial Y}(x_0,y_0,1)$.

Si C est lisse en P, alors l'une de ces deux quantités est non nulle et donc $(x_0 : y_0 : 1)$ est un point lisse de $\overline{C}$.

Réciproquement, supposons que $\overline{C}$ est lisse en $(x_0 : y_0 : 1)$. Supposons par l'absurde que $\frac{\partial F}{\partial X}$ et $\frac{\partial F}{\partial Y}$ s'annulent en (x_0, y_0). Alors $\frac{\partial H}{\partial X}$ et $\frac{\partial H}{\partial Y}$ s'annulent en $(x_0, y_0, 1)$ et grâce à l'identité d'Euler (14) évaluée au point $(x_0, y_0, 1)$, on a également $\frac{\partial H}{\partial Z}(x_0, y_0, 1) = 0$, ce qui contredit l'hypothèse. □

Une conséquence de la proposition précédente est qu'on peut tester la lissité d'un point d'une courbe projective en se plaçant dans une carte affine qui contient ce point. Dans la pratique, cela peut permettre de simplifier les calculs, comme le montre l'exemple suivant.

Exemple 2.6.6. — Prenons $C = V(Y^2 - F(X))$ avec $F \in k[X]$ unitaire de degré $d \geq 3$. On suppose que F n'est pas un carré dans $k[X]$, de sorte que $Y^2 - F(X)$ est irréductible dans $k[X,Y]$. La complétion projective de C est $\overline{C} = V(H)$ avec $H = Y^2 Z^{d-2} - \overline{F}(X,Z)$ où $\overline{F}$ est l'homogénéisé de F. Cherchons les points à l'infini

de C. On a $(x : y : 0) \in C$ si et seulement si $\overline{F}(x, 0) = 0$. Comme $\overline{F}(X, 0) = X^d$, on en déduit que l'unique point à l'infini de C est $P_\infty = (0 : 1 : 0)$. Étudions la lissité de P_∞. Comme P_∞ n'appartient pas (par définition) à C, on cherche une carte affine qui contient P_∞. Prenons la carte affine $\mathbf{A}^2 \hookrightarrow \mathbf{P}^2$ définie par $(u, v) \mapsto (u : 1 : v)$. L'équation de $\overline{C}$ dans cette carte affine s'écrit $v^{d-2} = \overline{F}(u, v)$, et dans cette carte on a $P_\infty = (0, 0)$. Posons $G = V^{d-2} - \overline{F}(U, V)$. Le polynôme G est irréductible dans $k[U, V]$ puisque H l'est. On vérifie que $\frac{\partial G}{\partial U} = -\frac{\partial \overline{F}}{\partial U}$ est homogène de degré $d-1$, donc s'annule en P_∞. De plus $\frac{\partial G}{\partial V} = (d-2)V^{d-3} - \frac{\partial \overline{F}}{\partial V}$ est non nul en P_∞ si et seulement si $d = 3$ (car dans ce cas $d - 2 = 1 \neq 0$ dans k). En conclusion P_∞ est un point lisse de $\overline{C}$ si et seulement si $d = 3$.

Exercice. — Soit C une courbe affine plane et P un point lisse de C. Montrer que $T_P\overline{C}$ est la complétion projective de $T_P C$.

Introduisons maintenant la notion de fonction sur une courbe projective. Soit C une courbe projective plane. Il importe de remarquer que contrairement au cas affine, un polynôme de $k[X, Y, Z]$, même homogène, ne définit pas de fonction sur C. Dans le cadre projectif, il n'y a donc pas de « k-algèbre des fonctions régulières sur C ». On peut en revanche définir les fonctions rationnelles sur C. Pour cela, on considère l'intersection de C avec une carte affine de $\mathbf{P}^2$.

Définition 2.6.7. — Soit C une courbe projective plane irréductible. On se donne une carte affine de $\mathbf{P}^2$ rencontrant C, et on note C_1 l'intersection de C avec cette carte affine. On définit alors le *corps des fonctions rationelles sur* C, noté $k(C)$, par $k(C) = k(C_1)$.

Remarque 2.6.8. — La définition précédente est un peu bancale, car elle dépend a priori du choix de la carte affine. Plus précisément, il faut expliquer comment on identifie les corps $k(C_1)$ et $k(C_2)$ lorsque C_1 et C_2 sont deux cartes affines de C. Nous le ferons ci-dessous sur un exemple. En fait, le bon point de vue (que nous ne développerons pas dans ce cours) est de considérer le cône $\widehat{C} = \pi^{-1}(C) \cup \{0\}$ au-dessus de C dans $\mathbf{A}^3$. Ce cône est une surface affine irréductible dans $\mathbf{A}^3$, de sorte que l'on peut considérer le corps $k(\widehat{C})$ des fonctions rationnelles sur $\widehat{C}$. Ce corps est trop gros (son degré de transcendance sur k est égal à 2), mais on peut définir $k(C)$ comme le sous-corps de $k(\widehat{C})$ formé des quotients $\frac{f}{g}$ avec $f, g \in k[\widehat{C}] = k[X, Y, Z]/I(C)$ homogènes de même degré et $g \neq 0$. En appliquant ce point de vue à la courbe $\mathbf{P}^1$, on est amenés à définir le corps $k(\mathbf{P}^1)$ des fonctions rationnelles sur $\mathbf{P}^1$ comme le sous-corps de $k(X, Y)$ formé des fractions rationnelles « homogènes de degré 0 », c'est-à-dire de la forme $\frac{F}{G}$ avec $F, G \in k[X, Y]$ homogènes de même degré et $G \neq 0$. Ce corps n'est autre que le sous-corps de $k(X, Y)$ engendré par $\frac{X}{Y}$. Dans ce cas, on a donc $k(\mathbf{P}^1) = k(\frac{X}{Y})$ et ce corps coïncide bien, en posant $T = \frac{X}{Y}$, avec le corps des fonctions rationnelles sur $\mathbf{A}^1$.

Exemple 2.6.9. — Prenons $C = V(Y^2Z - X^3 - Z^3)$. Dans la carte affine $(x, y) \mapsto (x : y : 1)$, la courbe s'écrit $C_1 : y^2 = x^3 + 1$. Dans la carte affine $(u, v) \mapsto (u : 1 : v)$, elle s'écrit $C_2 : v = u^3 + v^3$. Montrons que $k(C_1)$ et $k(C_2)$ sont canoniquement

isomorphes. Calculons les nouvelles coordonnées affines u, v en termes des anciennes coordonnées x, y. Dans $\mathbf{P}^2(k)$, on a

$$(x : y : 1) = (\frac{x}{y} : 1 : \frac{1}{y}) \qquad (x, y \in k; y \neq 0).$$

On a donc $u = \frac{x}{y}$ et $v = \frac{1}{y}$. Bien sûr, on obtient des dénominateurs car certains points de la première carte affine se retrouvent à l'infini dans la nouvelle carte. Toujours est-il que $\frac{x}{y}$ et $\frac{1}{y}$ ont un sens dans $k(C_1)$. On considère donc le morphisme « changement de cartes »

$$\begin{aligned} \varphi : k[U, V] &\to k(C_1) \\ U &\mapsto x/y \\ V &\mapsto 1/y. \end{aligned}$$

On a $C_2 = V(G)$ avec $G = V - U^3 - V^3$ et on vérifie que $G \in \ker \varphi$:

$$\varphi(G) = \frac{1}{y} - \frac{x^3}{y^3} - \frac{1}{y^3} = \frac{y^2 - x^3 - 1}{x^3} = 0$$

L'idéal $\ker \varphi$ est premier, contient $(G) = I(C_2)$ et correspond donc à un fermé algébrique contenu dans C_2. Comme C_2 est irréductible et $\ker \varphi$ n'est pas un idéal maximal (l'image de φ n'est pas réduite à k), on a nécessairement $\ker \varphi = I(C_2)$. Donc φ induit un morphisme injectif

$$\overline{\varphi} : k[C_2] \to k(C_1)$$

qui induit à son tour, par passage au corps des fractions, un k-morphisme

$$\widetilde{\varphi} : k(C_2) \to k(C_1).$$

Le morphisme $\widetilde{\varphi}$ est surjectif puisque $k(C_1) = k(x, y)$ et $\frac{x}{y}, \frac{1}{y} \in \mathrm{im}(\widetilde{\varphi})$. Les corps $k(C_1)$ et $k(C_2)$ sont donc (naturellement) k-isomorphes. On a $\widetilde{\varphi}(u) = \frac{x}{y}$ et $\widetilde{\varphi}(v) = \frac{1}{y}$ et donc aussi $x = \widetilde{\varphi}(\frac{u}{v})$ et $y = \widetilde{\varphi}(\frac{1}{v})$.

Dans la pratique, on omet d'écrire $\widetilde{\varphi}$ et on considère simplement x, y, u, v comme des éléments de $k(C)$ vérifiant $u = \frac{x}{y}$ et $v = \frac{1}{y}$ (et donc aussi $x = \frac{u}{v}$ et $y = \frac{1}{v}$).

Remarque 2.6.10. — Il n'est pas nécessaire de refaire le raisonnement ci-dessus pour chaque courbe : on admet que l'on peut travailler dans le corps des fonctions rationnelles d'une courbe projective irréductible en se plaçant dans la carte affine que l'on veut (en revanche, on fera attention à bien écrire le changement de cartes et à bien distinguer les anciennes coordonnées des nouvelles).

Définition 2.6.11. — Soit C une courbe projective plane irréductible et $P \in C$. Une fonction rationnelle $f \in k(C)$ est dite régulière en P si elle l'est dans une carte affine contenant P.

On admet que cette définition ne dépend pas de la carte affine choisie.

Notation 2.6.12. — Si C est une courbe projective plane irréductible et $P \in C$, on note $\mathcal{O}_{C,P}$ la sous-k-algèbre de $k(C)$ formée des fonctions qui sont régulières en P.

On peut toujours évaluer un élément de $\mathcal{O}_{C,P}$ en P, ce qui fournit un morphisme de k-algèbres $\mathcal{O}_{C,P} \to k$, de noyau $\mathfrak{m}_{C,P} = \{f \in \mathcal{O}_{C,P} : f(P) = 0\}$.

Vue la définition de la régularité en un point, si C est une courbe affine plane irréductible et $P \in C$, alors on a des isomorphismes canoniques $\mathcal{O}_{C,P} \cong \mathcal{O}_{\overline{C},P}$ et $\mathfrak{m}_{C,P} \cong \mathfrak{m}_{\overline{C},P}$. En d'autres termes, l'anneau local d'une courbe en un point ne dépend pas du fait que la courbe soit affine ou projective.

Toutes les propriétés vues dans les sections 1.8 et 1.9 restent vraies ; nous pouvons les résumer dans les équivalences suivantes, valables pour toute courbe projective plane irréductible C et tout point $P \in C$:

$$\begin{aligned} P \text{ est lisse } &\Leftrightarrow \dim_k \mathfrak{m}_{C,P}/\mathfrak{m}_{C,P}^2 = 1 \\ &\Leftrightarrow \mathfrak{m}_{C,P} \text{ est un idéal principal de } \mathcal{O}_{C,P} \\ &\Leftrightarrow \mathcal{O}_{C,P} \text{ est principal} \\ &\Leftrightarrow \mathcal{O}_{C,P} \text{ est intégralement clos} \\ &\Leftrightarrow \mathcal{O}_{C,P} \text{ est un anneau de valuation discrète.} \end{aligned}$$

En particulier, en tout point lisse d'une courbe projective, on dispose de la notion d'uniformisante en ce point et de la notion d'ordre d'annulation d'une fonction rationnelle. Plus précisément, si C est une courbe projective plane irréductible et P est un point *lisse* de C, on dispose comme d'habitude de la valuation discrète ord_P sur $k(C)$, et une uniformisante de C en P est une fonction rationnelle $f \in k(C)$ telle que $\mathrm{ord}_P(f) = 1$. Enfin, on dispose encore de la notion de développement limité en un point lisse.

2.7. Applications rationnelles entre courbes projectives

Soit $C = V(H)$ et $C' = V(H')$ des courbes projectives planes irréductibles.

Définition 2.7.1. — Une application rationnelle φ de C dans C' est un triplet (f_0, f_1, f_2) d'éléments de $k(C)$, non tous nuls, telles que $H'(f_0, f_1, f_2) = 0$. On identifie deux triplets (f_0, f_1, f_2) et (g_0, g_1, g_2) lorsque $(f_0 : f_1 : f_2) = (g_0 : g_1 : g_2)$ dans $\mathbf{P}^2(k(C))$, c'est-à-dire lorsqu'il existe $h \in k(C)^*$ telle que $g_i = hf_i$ pour tout $i \in \{0, 1, 2\}$.

Notation 2.7.2. — Si (f_0, f_1, f_2) est un triplet vérifiant les conditions de la définition précédente, on note $\varphi = (f_0 : f_1 : f_2) : C \dashrightarrow C'$.

Montrons qu'une telle application rationnelle définit une (vraie) application de $C - S$ dans C', où S est une partie finie de C. Notons S' l'ensemble (fini) des pôles des f_i, et $S'' = \{P \in C - S' : f_0(P) = f_1(P) = f_2(P) = 0\}$. Comme $(f_0, f_1, f_2) \neq (0, 0, 0)$, l'ensemble S'' est fini. Alors $S = S' \cup S''$ est fini et pour

tout $P \notin S$, on peut poser $\varphi(P) = (f_0(P) : f_1(P) : f_2(P)) \in \mathbf{P}^2(k)$. Comme $H'(f_0, f_1, f_2) = 0$, on a en fait $\varphi(P) \in C'$, de sorte que φ définit une application de $C - S$ vers C'.

Définition 2.7.3. — Soit $\varphi = (f_0 : f_1 : f_2) : C - - \succ C'$. On dit que φ est *définie* en $P \in C$ s'il existe une fonction rationnelle $h \in k(C)^*$ telle que :

(i) pour tout $i \in \{0, 1, 2\}$, la fonction hf_i est régulière en P ;

(ii) il existe $i \in \{0, 1, 2\}$ tel que $hf_i(P) \neq 0$.

On pose alors $\varphi(P) = (hf_0(P) : hf_1(P) : hf_2(P))$. Le *domaine de définition* de φ est l'ensemble des points de C en lesquels φ est définie. On dit que φ est un *morphisme* si son domaine de définition est C tout entier ; on note alors $\varphi : C \to C'$.

Notons que si φ est régulière en P alors $\varphi(P) \in C'$ puisque $H'(hf_0, hf_1, hf_2) = h^{\deg H'} H'(f_0, f_1, f_2) = 0$. De plus $\varphi(P)$ ne dépend pas du choix de la fonction h vérifiant (i) et (ii).

Théorème 2.7.4. — *Soit $\varphi : C - - \succ C'$. Si P est un point lisse de C, alors φ est définie en P. En particulier, si C est lisse alors φ est un morphisme.*

Démonstration. — Soit P un point lisse de C et $t \in k(C)$ une uniformisante en P. Notons $\varphi = (f_0 : f_1 : f_2)$ et posons $m = \min_{i \in \{0,1,2\}}(\mathrm{ord}_P(f_i))$. Comme $(f_0, f_1, f_2) \neq (0, 0, 0)$, on a $m \in \mathbf{Z}$. En prenant $h = t^{-m}$, on vérifie alors que les conditions (i) et (ii) sont vérifiées, de sorte que φ est régulière en P. □

Mentionnons également, sans démonstration, quelques compléments sur les applications rationnelles.

– Si $\varphi_1 : C - - \succ C'$ et $\varphi_2 : C - - \succ C'$ sont définies et coïncident sur une partie infinie de C, alors $\varphi_1 = \varphi_2$.

– Si $\varphi : C - - \succ C'$ est non constante, alors on peut définir un k-morphisme de corps $\varphi^* : k(C') \to k(C)$ en posant $\varphi^*(f) = f \circ \varphi$.

– L'application $\varphi \mapsto \varphi^*$ est une bijection entre l'ensemble des applications rationnelles non constantes $C - - \succ C'$ et les k-morphismes de corps de $k(C')$ dans $k(C)$.

– Si $\varphi : C - - \succ C'$ et $\psi : C' - - \succ C''$ sont non constantes, alors on peut définir $\psi \circ \varphi : C - - \succ C''$ et l'on a $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$.

– Deux courbes projectives irréductibles C et C' sont dites *birationnelles* s'il existe $\varphi : C - - \succ C'$ et $\psi : C' - - \succ C$ telles que $\psi \circ \varphi = \mathrm{id}_C$ et $\varphi \circ \psi = \mathrm{id}_{C'}$. Cela équivaut à dire que les corps $k(C)$ et $k(C')$ sont k-isomorphes.

– Une courbe projective irréductible C est dite *rationnelle* si C et $\mathbf{P}^1$ sont birationnelles, c'est-à-dire si le corps $k(C)$ est k-isomorphe à $k(T)$. D'après le théorème de Lüroth, cela revient à dire qu'il existe une application rationnelle non constante $\varphi : \mathbf{P}^1 - - \succ C$ (qui est alors nécessairement un morphisme, puisque $\mathbf{P}^1$ est lisse).

Pour terminer cette section, énonçons deux résultats importants dans l'étude des courbes algébriques.

***Théorème 2.7.5* (Résolution des singularités pour les courbes)**
Toute courbe algébrique irréductible est birationnelle à une courbe projective lisse (non nécessairement plane).

On peut faire remonter la démonstration de ce théorème à Newton (1676), qui établit qu'au voisinage de tout point singulier, une courbe peut toujours être paramétrée par des séries de Puiseux.

Remarque 2.7.6. — La courbe projective lisse fournie par le théorème est unique (à isomorphisme près). En effet, si C_1 et C_2 sont deux courbes projectives lisses qui conviennent, alors il existe des applications rationnelles $\varphi : C_1 - - \succ C_2$ et $\psi : C_2 - - \succ C_1$ telles que $\psi \circ \varphi = \mathrm{id}_{C_1}$ et $\varphi \circ \psi = \mathrm{id}_{C_2}$, et comme C_1 et C_2 sont lisses, φ et ψ sont des morphismes, et donc C_1 et C_2 sont isomorphes.

Remarque 2.7.7. — On peut reformuler le théorème de résolution des singularités de la manière suivante : pour toute extension K/k de degré de transcendance 1, il existe une courbe projective lisse C (non nécessairement plane) telle que les corps K et $k(C)$ soient k-isomorphes. De plus C est unique à isomorphisme près. On a donc une bijection entre les courbes projectives lisses (à isomorphisme près) et les extensions de degré de transcendance 1 de k (à k-isomorphisme près).

Si l'on se restreint aux courbes planes, on ne peut pas toujours espérer résoudre les singularités d'une courbe. On a cependant le résultat suivant.

***Théorème 2.7.8* (Noether, Bertini)**. — *Toute courbe algébrique irréductible est birationnelle à une courbe projective plane dont tous les points singuliers sont des points doubles ordinaires.*

2.8. Coniques et courbes rationnelles

Rappelons qu'une *conique* (projective) est une courbe de la forme $C = V(H)$ où $H \in k[X, Y, Z]$ est un polynôme homogène non nul de degré 2.

On dit que C est une *conique irréductible* (ou *non dégénérée*) lorsque C est définie par un polynôme H irréductible. Remarquons que si H est réductible, alors $H = H_1 H_2$ avec H_i homogène non nul de degré 1, et donc $C = V(H)$ est réunion de deux droites (éventuellement confondues). Il y a donc un léger abus de langage : même si H est réductible, la conique $C = V(H)$ peut être irréductible au sens usuel. Dans la suite, nous réserverons cependant le terme *conique irréductible* aux courbes de la forme $V(H)$ avec H homogène de degré 2 et irréductible. De même, une *courbe irréductible de degré d* sera une courbe définie par un polynôme homogène irréductible de degré d.

Proposition 2.8.1. — *Toute conique projective irréductible est lisse.*

Démonstration. — Soit $H \in k[X, Y, Z]_2$ irréductible et $C = V(H)$. Par l'absurde, supposons $P \in C$ singulier. Quitte à faire un changement projectif de coordonnées, on peut supposer $P = (0 : 0 : 1)$. Posons $F(X, Y) = H(X, Y, 1)$. On a $\deg F = 2$ (sinon H est divisible par Z). Dans la carte affine standard, on a $P = (0, 0)$ et donc

$F(0,0) = 0$. Comme P est singulier, on a de plus $\frac{\partial F}{\partial X}(0,0) = \frac{\partial F}{\partial Y}(0,0) = 0$ et donc $F = \alpha X^2 + \beta XY + \gamma Y^2$ avec $\alpha, \beta, \gamma \in k$, ce qui contredit l'irréductibilité de F. □

Proposition 2.8.2. — *Soit C une conique projective irréductible. Pour tout $P \in C$, on a $C \cap T_P C = \{P\}$.*

Démonstration. — Quitte à faire un changement projectif de coordonnées, on peut supposer $P = (0 : 0 : 1)$ et $T_P C : Y = 0$. Posons $C = V(H)$ et $F(X,Y) = H(X,Y,1)$. Comme $T_P C$ est la droite $Y = 0$, on a $\frac{\partial F}{\partial X}(0,0) = 0$ et donc $F = \alpha Y + \beta X^2 + \gamma XY + \delta Y^2$ avec $\alpha \neq 0$. On en déduit $H = \alpha YZ + \beta X^2 + \gamma XY + \delta Y^2$. On a $\beta \neq 0$ (sinon H serait divisible par Y). On vérifie alors directement que $V(H,Y) = \{P\}$. □

Lemme 2.8.3. — *Le groupe* $\mathrm{PGL}_3(k)$ *agit transitivement sur les triplets de points non alignés de* $\mathbf{P}^2(k)$.

Démonstration. — Il suffit de montrer que pour tous points $a, b, c \in \mathbf{P}^2(k)$ non alignés, il existe $g \in \mathrm{PGL}_3(k)$ envoyant a, b, c sur $(1:0:0), (0:1:0), (0:0:1)$. Posons $a = \mathbf{P}(\widetilde{a})$, $b = \mathbf{P}(\widetilde{b})$, $c = \mathbf{P}(\widetilde{c})$ avec $\widetilde{a}$, $\widetilde{b}$, $\widetilde{c}$ droites de k^3. Comme a, b, c ne sont pas alignés, on a une décomposition en somme directe $k^3 = \widetilde{a} \oplus \widetilde{b} \oplus \widetilde{c}$. Soit $\widetilde{g} \in \mathrm{GL}_3(k)$ envoyant $\widetilde{a}$ (resp. $\widetilde{b}$, $\widetilde{c}$) sur la droite engendrée par $(1,0,0)$ (resp. $(0,1,0)$, $(0,0,1)$). On vérifie alors que $g = [\widetilde{g}] \in \mathrm{PGL}_3(k)$ convient. □

Théorème 2.8.4. — *Toute conique projective irréductible est projectivement équivalente à la conique $V(YZ - X^2)$.*

Démonstration. — Comme C est infinie, on peut choisir $P_1, P_2 \in C$ distincts. Soit $T_i = T_{P_i} C$ (qui existe d'après la proposition 2.8.1). Comme $T_i \cap C = \{P_i\}$, on a $T_1 \neq T_2$ et donc $T_1 \cap T_2 = \{P_3\}$ avec $P_3 \in \mathbf{P}^2$ (et $P_3 \notin C$).

Grâce au lemme 2.8.3, on peut, quitte à faire un changement projectif de coordonnées, supposer que

$$P_1 = (0:0:1) \qquad P_2 = (0:1:0) \qquad P_3 = (1:0:0).$$

Comme $T_i = (P_i P_3)$, il vient $T_1 : Y = 0$ et $T_2 : Z = 0$. Posons $C = V(H)$ avec $H \in k[X,Y,Z]_2$ irréductible. Comme dans la démonstration de la proposition 2.8.2, on a $H = \alpha YZ + \beta X^2 + \gamma XY + \delta Y^2$ avec $\alpha, \beta \neq 0$. Puisque $P_2 \in C$, il vient $\delta = 0$. De plus $\frac{\partial H}{\partial X} = 2\beta X + \gamma Y$ et comme $T_{P_2} C$ est la droite $Z = 0$, il vient $\gamma = 0$. D'où $H = \alpha YZ + \beta X^2$. Comme k est algébriquement clos, un changement de coordonnées de la forme $(X' : Y' : Z') = (\lambda X : \mu Y : Z)$ avec $\lambda, \mu \in k^*$ montre que C est projectivement équivalente à $V(YZ - X^2)$. □

Proposition 2.8.5. — *Soit C une conique projective irréductible. Si* $\mathrm{car}(k) = 2$, *alors il existe un point $Q \in \mathbf{P}^2(k)$ tel que toutes les tangentes de C passent par Q.*

Démonstration. — Grâce au théorème 2.8.4, on peut supposer $C = V(H)$ avec $H = YZ - X^2$. On a

$$\frac{\partial H}{\partial X} = 0 \qquad \frac{\partial H}{\partial Y} = Z \qquad \frac{\partial H}{\partial Z} = Y.$$

Soit $P = (x : y : z) \in C$. Alors $T_P C$ est la droite $zY + yZ = 0$, qui passe par le point $Q = (1 : 0 : 0)$. □

Remarque 2.8.6. — On peut aussi expliquer ainsi la proposition précédente : en affine, on a $C : y = x^2$. La fonction polynomiale $x \mapsto x^2$ étant de dérivée nulle, toutes les tangentes de C sont horizontales et passent donc par le point à l'infini dans la direction horizontale.

Exercice. — Soit C une conique projective irréductible, avec $\mathrm{car}(k) \neq 2$.

(1) Montrer qu'aucun point de $\mathbf{P}^2(k)$ ne passe par toutes les tangentes de C.

(2) Montrer qu'un point hors de C passe par exactement deux tangentes de C.

Théorème 2.8.7. — *Toute conique projective irréductible est isomorphe à* $\mathbf{P}^1$. *En particulier, toute conique irréductible est rationnelle.*

Démonstration. — Vu le théorème 2.8.4, on peut supposer $C = V(YZ - X^2)$. Construisons un morphisme de $\mathbf{P}^1$ dans C. Dans la carte affine standard, la courbe $C_0 = C \cap \mathbf{A}^2$ admet l'équation $y = x^2$, d'où un isomorphisme $\varphi_0 : \mathbf{A}^1 \xrightarrow{\cong} C_0$ donné par $\varphi_0(t) = (t, t^2)$. On souhaite prolonger φ_0 en un morphisme $\varphi : \mathbf{P}^1 \to C$. On peut voir t comme un élément de $k(\mathbf{P}^1)$ et définir l'application rationnelle $\varphi = (t : t^2 : 1) : \mathbf{P}^1 \dashrightarrow C$. Le domaine de définition de φ contient $\mathbf{A}^1$, et comme $\varphi = (\frac{1}{t} : 1 : \frac{1}{t^2})$ on voit que φ est également définie en ∞ (avec $\varphi(\infty) = (0 : 1 : 0)$), de sorte que φ est un morphisme.

On définit de même l'application rationnelle $\psi : C \dashrightarrow \mathbf{P}^1$ par $\psi = (x : 1)$. Comme C est lisse, ψ est un morphisme (on vérifie que $\psi((0 : 1 : 0)) = \infty$). Enfin, on vérifie que $\psi \circ \varphi = \mathrm{id}_{\mathbf{P}^1}$ et $\varphi \circ \psi = \mathrm{id}_C$. □

Remarque 2.8.8. — Dans la pratique, pour trouver un paramétrage rationnel d'une conique irréductible C, on fixe un point $p_0 \in C$ et on considère l'ensemble p_0^* des droites de $\mathbf{P}^2$ passant par p_0. On a vu dans la proposition 2.1.10 que p_0^* est de manière naturelle une droite projective. On considère alors l'application $\varphi : p_0^* \to C$ qui à une droite D passant par p_0 associe le second point d'intersection de D avec C (on convient que $\varphi(T_{p_0} C) = p_0$). L'application φ est alors bijective, et fournit un paramétrage rationnel de C.

On s'intéresse maintenant aux courbes de degré $d \geq 3$. Nous allons donner des conditions suffisantes pour la rationalité de telles courbes.

Proposition 2.8.9. — *Si C est une courbe projective plane irréductible de degré $d \geq 3$, alors tout point singulier de C est de multiplicité $\leq d - 1$.*

Démonstration. — La démonstration est la même que la proposition 2.8.1. Soit $H \in k[X, Y, Z]_d$ irréductible et $C = V(H)$. Soit P un point singulier de C. Quitte à faire un changement projectif de coordonnées, on peut supposer $P = (0 : 0 : 1)$. Posons $F(X, Y) = H(X, Y, 1)$, de sorte que $F(0, 0) = 0$. On a $\deg F = d$ (sinon

H est divisible par Z). Par l'absurde, supposons que la multiplicité de P est $\geq d$. Alors F est combinaison linéaire des monômes $X^d, X^{d-1}Y, \ldots, Y^d$, ce qui contredit l'irréductibilité de F. □

Proposition 2.8.10. — *Soit C une courbe projective plane irréductible de degré $d \geq 3$. Si C admet un point singulier de multiplicité $d-1$, alors C est rationnelle.*

Démonstration. — Grâce à un changement projectif de coordonnées, on peut supposer que $P = (0 : 0 : 1)$ est singulier de multiplicité $d-1$. Posons $C = V(H)$ avec $H \in k[X,Y,Z]_d$ irréductible, et $F(X,Y) = H(X,Y,1)$. Par définition de la multiplicité, on a $F = F_{d-1} + F_d$ avec $F_i \in k[X,Y]_i$ et $F_{d-1}, F_d \neq 0$. Pour $t \in k$, calculons l'intersection de C avec la droite $D_t : y = tx$. On a

$$\begin{aligned}(x : tx : 1) \in C &\Leftrightarrow F_{d-1}(x,tx) + F_d(x,tx) = 0 \\ &\Leftrightarrow x^{d-1}F_{d-1}(1,t) + x^d F_d(1,t) = 0 \\ &\Leftrightarrow x = 0 \text{ ou } F_{d-1}(1,t) + xF_d(1,t) = 0.\end{aligned}$$

On voit alors que x et y s'expriment rationnellement en fonction de t. Plus précisément, on définit l'application rationnelle $\varphi : \mathbf{P}^1 \dashrightarrow C$ par

$$\varphi = (-\frac{F_{d-1}(1,t)}{F_d(1,t)} : -t\frac{F_{d-1}(1,t)}{F_d(1,t)} : 1),$$

où l'on voit t comme élément de $k(\mathbf{P}^1) = k(t)$. La définition de φ est licite car $F_d(1,t) \in k(t)^*$ et on vérifie que $F(-\frac{F_{d-1}(1,t)}{F_d(1,t)}, -t\frac{F_{d-1}(1,t)}{F_d(1,t)}) = 0$ dans $k(t)$. De plus φ est non constante car l'une au moins des composantes de φ est une fonction rationnelle non constante. Ainsi C est rationnelle. □

Remarque 2.8.11. — Dans la situation de la proposition 2.8.10, la courbe C, bien que rationnelle, n'est pas isomorphe à $\mathbf{P}^1$. En effet $\mathbf{P}^1$ est lisse, tandis que C ne l'est pas. On a seulement une application rationnelle $\varphi : \mathbf{P}^1 \dashrightarrow C$, qui est automatiquement un morphisme puisque $\mathbf{P}^1$ est lisse. On peut montrer que $\varphi : \mathbf{P}^1 \to C$ est surjectif (c'est une conséquence du théorème de l'élimination projective). En revanche φ n'est pas nécessairement injectif (et même s'il l'est, l'application rationnelle $\varphi^{-1} : C \dashrightarrow \mathbf{P}^1$ n'est pas définie au point singulier P).

Dans le cas des cubiques, la proposition 2.8.10 entraîne le résultat suivant.

Proposition 2.8.12. — *Toute cubique projective irréductible admettant un point singulier est rationnelle.*

En effet, d'après la proposition 2.8.9, le point singulier est nécessairement de multiplicité 2 ; on peut donc appliquer la proposition 2.8.10.

Exercice. — Trouver un paramétrage rationnel de la cubique $C : x^3 - 2x^2y - xy^2 + 2y^3 + xy = 0$.

Pour les quartiques (courbes de degré 4), on a également le résultat suivant.

Proposition 2.8.13. — *Toute quartique projective irréductible admettant* 3 *points singuliers est rationnelle.*

Démonstration. — Si l'un des points singuliers est de multiplicité 3, alors on peut appliquer la proposition 2.8.10. On peut donc supposer que les trois points singuliers sont de multiplicité 2. Ces trois points ne peuvent être alignés, sinon la droite qui les contient intersecterait la courbe en 6 points comptés avec multiplicité, donc serait contenue dans la quartique, ce qui contredit son irréductibilité.

En utilisant le lemme 2.8.3 et quitte à faire un changement projectif de coordonnées, on peut supposer que les points singuliers sont $(1:0:0)$, $(0:1:0)$ et $(0:0:1)$. Posons $C = V(H)$ avec $H \in k[X,Y,Z]_4$ irréductible. Comme $(0:0:1)$ est un point singulier de C, le polynôme H ne contient aucun terme en Z^4, en Z^3X ou en Z^3Y. En raisonnant de même pour les autres points singuliers, on voit que toutes les indéterminées interviennent dans H avec un degré ≤ 2. En posant $F(X,Y) = H(X,Y,1)$, on a donc

$$F = \alpha X^2Y^2 + \beta X^2 + \gamma Y^2 + \delta XY + \epsilon XY^2 + \zeta X^2Y.$$

On considère alors l'application rationnelle φ sur C définie par $\varphi = (\frac{1}{x} : \frac{1}{y} : 1)$. On vérifie que φ définit une application rationnelle $C \dashrightarrow C'$, où C' est la conique définie par

$$C' : \alpha Z'^2 + \beta X'^2 + \gamma Y'^2 + \delta X'Y' + \epsilon Y'Z' + \zeta X'Z' = 0.$$

Mais réciproquement, on a également une application rationnelle $\psi : C' \dashrightarrow C$ définie par $\psi = (\frac{1}{x'} : \frac{1}{y'} : 1)$. Comme $\psi \circ \varphi = \mathrm{id}_C$ et $\varphi \circ \psi = \mathrm{id}_{C'}$, les courbes C et C' sont birationnelles, et comme C' est rationnelle, il en va de même pour C. □

Exercice. — (1) Montrer qu'une cubique projective possédant au moins 2 points singuliers est réunion d'une droite et d'une conique.

(2) Montrer qu'une quartique projective possédant au moins 4 points singuliers est réunion de deux coniques.

2.9. Le théorème de Bézout

On souhaite donner un sens précis à l'énoncé suivant : *si C et C' sont des courbes planes de degrés respectifs d et d', alors C et C' s'intersectent en dd' points.*

Pour qu'un tel énoncé soit correct, il est nécessaire de prendre des précautions. Par exemple, si $C \subset \mathbf{R}^2$ est le cercle d'équation $x^2 + y^2 = 1$, on voit qu'une droite affine $D \subset \mathbf{R}^2$ peut couper C en 0, 1 ou 2 points.

Voici la liste des points auxquels il faut faire attention :

(1) On doit travailler sur un corps *algébriquement clos*. Par exemple, la droite $D : x = 2$ n'intersecte pas C dans $\mathbf{R}^2$, mais si en se plaçant dans $\mathbf{C}^2$, il y a bien 2 points d'intersection.

(2) On doit compter les points d'intersection *avec multiplicité*. Par exemple, la droite affine $D : x = 1$ intersecte C seulement en $P = (1, 0)$. Ceci est lié au fait que D est la tangente de C en P ; le point P doit être compté « avec multiplicité 2 ».

(3) On doit tenir compte des *points à l'infini*. Prenons par exemple la conique $C : xy = 1$ et la droite $D : x = 1$. Dans $\mathbf{C}^2$, l'intersection $C \cap D$ est réduite au point $P = (1, 1)$, et pourtant D n'est pas tangente à C en P. Ceci est lié au fait que C et D s'intersectent à l'infini : on vérifie en effet que $(0 : 1 : 0) \in \overline{C} \cap \overline{D}$. La droite projective $\overline{D}$ intersecte bien $\overline{C}$ en 2 points. Un autre exemple est donné par la droite $D' : x = 0$. On a $C \cap D' = \emptyset$ dans $\mathbf{C}^2$, et $\overline{C} \cap \overline{D'} = \{(0 : 1 : 0)\}$. Dans ce cas, la droite projective $\overline{D'}$ est tangente à $\overline{C}$ au point à l'infini.

(4) Les courbes considérées doivent être *sans composante commune*. En effet, si C et C' contiennent une même courbe, alors leur intersection $C \cap C'$ contient cette courbe, et donc est infinie.

Nous nous plaçons donc dans le cadre suivant : C et C' sont des courbes projectives planes, définies sur un corps k algébriquement clos. On pose $I(C) = (H)$ et $I(C') = (H')$ avec H (resp. H') polynôme homogène de $k[X, Y, Z]$ de degré d (resp. d'). On fait l'hypothèse que C et C' n'ont pas de composante commune, c'est-à-dire que les polynômes H et H' sont étrangers dans l'anneau factoriel $k[X, Y, Z]$.

Lemme 2.9.1. — *L'intersection $C \cap C'$ est finie.*

Démonstration. — En décomposant H en irréductibles, on se ramène au cas où H est irréductible. Alors C est irréductible et n'est pas contenue dans C' (sinon H diviserait H'). On conclut en utilisant la proposition 1.5.6 (ou plutôt sa version projective). □

On va d'abord définir la notion d'*intersection transversale* en un point.

Définition 2.9.2. — Soit $P \in C \cap C'$. On dit que *C et C' s'intersectent transversalement en P* si les deux conditions suivantes sont vérifiées :

(1) P est un point lisse de C et de C' ;

(2) les tangentes de C en P et de C' en P sont distinctes.

On note alors $C \pitchfork_P C'$. On dit que *C et C' s'intersectent transversalement* (notation $C \pitchfork C'$) si elles s'intersectent transversalement en tout point de $C \cap C'$.

Remarque 2.9.3. — La condition (2) dit intuitivement que les courbes C et C' « ne sont pas tangentes en P ».

Remarque 2.9.4. — Pour tester si C et C' s'intersectent transversalement en un point P, il suffit de se placer dans une carte affine contenant P et de vérifier si les conditions (1) et (2) sont réalisées.

On a envie de dire que lorsque C et C' s'intersectement transversalement en un point P, les courbes C et C' s'intersectent en P *avec multiplicité* 1. L'idée est que si on bouge légèrement la courbe C (ou la courbe C'), alors il n'y a toujours qu'un seul point d'intersection au voisinage de P (contrairement par exemple au

cas de l'intersection d'une courbe avec l'une de ses tangentes). Plus précisément, on va définir, pour tout point P du plan projectif, un entier $m_P(C, C') \in \mathbf{N}$, appelé *multiplicité d'intersection* de C et C' en P, qui vérifie les propriétés suivantes :

(1) $m_P(C, C') \geq 1 \Leftrightarrow P \in C \cap C'$;

(2) $m_P(C, C') = 1 \Leftrightarrow C \pitchfork_P C'$;

(3) $m_P(C, C') = m_P(C', C)$.

Il est bien entendu que ces propriétés ne suffisent pas à caractériser $m_P(C, C')$. Nous allons d'abord donner une définition (presque) intrinsèque de $m_P(C, C')$, puis nous expliquerons comment la calculer en pratique (dans les cas favorables).

On commence par choisir une carte affine de $\mathbf{P}^2$ contenant P. Les intersections respectives de C et C' avec cette carte affine seront encore notées (abusivement) C et C'. Les courbes C et C' sont donc des courbes affines planes, sans composante commune, et P est un point de $\mathbf{A}^2$.

Définition 2.9.5. — L'anneau local de $\mathbf{A}^2$ en P, noté $\mathcal{O}_{\mathbf{A}^2,P}$, est le localisé de $k[\mathbf{A}^2]$ en l'idéal maximal $\mathfrak{m}_P \subset k[\mathbf{A}^2]$ associé à P.

Remarque 2.9.6. — Explicitement, on a $k[\mathbf{A}^2] = k[X, Y]$ et en notant $P = (x_0, y_0)$, on a

$$\mathcal{O}_{\mathbf{A}^2,P} = \Big\{ \frac{F}{G} \in k(X, Y); F, G \in k[X, Y] \text{ et } G(x_0, y_0) \neq 0 \Big\}.$$

En particulier $\mathcal{O}_{\mathbf{A}^2,P}$ est une sous-k-algèbre de $k(X, Y)$ qui contient $k[X, Y]$. Par construction $\mathcal{O}_{\mathbf{A}^2,P}$ est un anneau local. Son idéal maximal $\mathfrak{m}_{\mathbf{A}^2,P}$ est donné par $\mathfrak{m}_{\mathbf{A}^2,P} = \mathfrak{m}_P \cdot \mathcal{O}_{\mathbf{A}^2,P}$, et on a explicitement

$$\mathfrak{m}_{\mathbf{A}^2,P} = \Big\{ \frac{F}{G} \in k(X, Y); F, G \in k[X, Y], F(x_0, y_0) = 0 \text{ et } G(x_0, y_0) \neq 0 \Big\}.$$

L'évaluation en P fournit un morphisme de k-algèbres $\mathcal{O}_{\mathbf{A}^2,P} \to k$, de noyau $\mathfrak{m}_{\mathbf{A}^2,P}$, d'où un isomorphisme canonique $\mathcal{O}_{\mathbf{A}^2,P}/\mathfrak{m}_{\mathbf{A}^2,P} \cong k$.

Remarque 2.9.7. — Attention, contrairement au cas des courbes, l'anneau $\mathcal{O}_{\mathbf{A}^2,P}$ n'est pas un anneau de valuation discrète. Une manière de le voir est de montrer que l'idéal $\mathfrak{m}_{\mathbf{A}^2,P}$ n'est pas principal. Si $\mathfrak{m}_{\mathbf{A}^2,P}$ était principal, alors le k-espace vectoriel $\mathfrak{m}_{\mathbf{A}^2,P}/\mathfrak{m}^2_{\mathbf{A}^2,P}$ serait de dimension ≤ 1. Or la théorie de la localisation fournit un isomorphisme $\mathfrak{m}_{\mathbf{A}^2,P}/\mathfrak{m}^2_{\mathbf{A}^2,P} \cong \mathfrak{m}_P/\mathfrak{m}^2_P$, et le k-espace vectoriel $\mathfrak{m}_P/\mathfrak{m}^2_P$ est de dimension 2, engendré par les classes de $X - x_0$ et de $Y - y_0$, ce qui permet de conclure.

Définition 2.9.8. — La *multiplicité d'intersection de C et C' en P*, notée $m_P(C, C')$, est définie par

$$m_P(C, C') = \dim_k \Big(\frac{\mathcal{O}_{\mathbf{A}^2,P}}{(I(C) + I(C')) \cdot \mathcal{O}_{\mathbf{A}^2,P}} \Big). \tag{15}$$

Il n'est pas évident, au vu de cette définition, que la multiplicité d'intersection est finie (nous le montrerons plus tard). Par ailleurs, nous admettons que si l'on part de deux courbes *projectives*, la multiplicité d'intersection, définie en ayant recours à une carte affine, ne dépend pas du choix de cette carte affine.

Expliquons d'où vient cette définition. Les idéaux $I(C)$ et $I(C')$ de $k[X,Y]$ définissent respectivement les courbes C et C'. Le lieu des zéros de $I(C)+I(C')$ dans $\mathbf{A}^2$ est donc

$$V(I(C)+I(C')) = V(I(C)) \cap V(I(C')) = C \cap C'.$$

Pourquoi alors considérer $I(C)+I(C')$ au lieu de $I(C\cap C')$? La réponse est donnée par l'exemple suivant. Considérons les courbes $C : y = x^2$ et $C' : y = 0$, qui vérifient $C\cap C' = \{(0,0)\}$. On a $I(C) = (Y - X^2)$ et $I(C') = (Y)$ de sorte que $I(C)+I(C') = (Y - X^2, Y) = (X^2, Y)$. Remarquons que $k[X,Y]/(X^2,Y) \cong k[X]/(X^2)$ est un k-espace vectoriel de dimension 2. Par conséquent $I(C) + I(C')$ est de codimension 2 dans $k[X,Y]$, tandis que $I(C \cap C') = (X,Y)$ est de codimension 1. En utilisant seulement l'intersection ensembliste $C \cap C'$, on ne peut plus retrouver la nature de l'intersection de C et C' au point $(0,0)$, tandis qu'en utilisant $I(C) + I(C')$, on a gardé l'information que C' est tangente à C au point $(0,0)$.

Montrons maintenant la finitude de $m_P(C,C')$.

Lemme 2.9.9. — *Si $P \notin C \cap C'$, alors $m_P(C,C') = 0$.*

Démonstration. — Supposons par exemple $P \notin C$ (le raisonnement est le même si $P \notin C'$). L'idéal $I(C)$ n'est pas inclus dans $\mathfrak{m}_P$ (sinon on aurait $C = V(I(C)) \supset V(\mathfrak{m}_P) = \{P\}$). Donc $I(C)$ contient un polynôme de $k[X,Y]$ qui est inversible dans $\mathcal{O}_{\mathbf{A}^2,P}$, d'où $I(C)\cdot\mathcal{O}_{\mathbf{A}^2,P} = \mathcal{O}_{\mathbf{A}^2,P}$ et $m_P(C,C') = 0$. □

Lemme 2.9.10. — *Il existe un entier $N \geq 1$ tel que pour tout point $P \in C \cap C'$, on ait $\mathfrak{m}_{\mathbf{A}^2,P}^N \subset (I(C)+I(C'))\cdot\mathcal{O}_{\mathbf{A}^2,P}$.*

Démonstration. — Posons $I = I(C)+I(C')$, de sorte que $V(I) = C\cap C'$. Posons $J = \prod_{P\in C\cap C'} \mathfrak{m}_P$, de sorte que $V(J) = \cup_{P\in C\cap C'} V(\mathfrak{m}_P) = C\cap C'$. Par noethérianité de $k[X,Y]$, l'idéal J est engendré par des polynômes $Q_1,\dots,Q_r \in k[X,Y]$. Pour tout i, le polynôme Q_i s'annule sur $V(I)$. Par le Nullstellensatz, il existe donc un entier $N_i \geq 1$ tel que $Q_i^{N_i} \in I$. Posons $N = \sum_{i=1}^r N_i$. L'idéal J^N est engendré par les $Q_1^{\alpha_1}\cdots Q_r^{\alpha_r}$, où $\alpha_1,\dots,\alpha_r$ sont des entiers naturels vérifiant $\alpha_1+\cdots+\alpha_r = N$. Pour tout tel r-uplet $(\alpha_1,\dots,\alpha_r)$, il existe i tel que $\alpha_i \geq N_i$ et donc $Q_1^{\alpha_1}\cdots Q_r^{\alpha_r} \in I$. Par suite $J^N \subset I$.

Donnons-nous maintenant un point $P \in C\cap C'$, et localisons en P. On a $(J^N)\cdot\mathcal{O}_{\mathbf{A}^2,P} = (J\cdot\mathcal{O}_{\mathbf{A}^2,P})^N = (\prod_{R\in C\cap C'} \mathfrak{m}_R\cdot\mathcal{O}_{\mathbf{A}^2,P})^N$. Comme

$$\mathfrak{m}_R\cdot\mathcal{O}_{\mathbf{A}^2,P} = \begin{cases} \mathfrak{m}_{\mathbf{A}^2,P} & \text{si } R = P, \\ \mathcal{O}_{\mathbf{A}^2,P} & \text{si } R \neq P, \end{cases}$$

il vient $\mathfrak{m}_{\mathbf{A}^2,P}^N \subset I\cdot\mathcal{O}_{\mathbf{A}^2,P}$. □

Proposition 2.9.11. — *On a $m_P(C,C') < +\infty$.*

Démonstration. — D'après le lemme 2.9.9, on peut supposer $P \in C \cap C'$. D'après le lemme 2.9.10, il suffit de montrer que $\dim_k(\mathcal{O}_{\mathbf{A}^2,P}/\mathfrak{m}^N_{\mathbf{A}^2,P}) < +\infty$. L'anneau $\mathcal{O}_{\mathbf{A}^2,P}$ étant noethérien, l'idéal $\mathfrak{m}^i_{\mathbf{A}^2,P}$ est de type fini pour tout $0 \leq i \leq N-1$. Par suite $\mathfrak{m}^i_{\mathbf{A}^2,P}/\mathfrak{m}^{i+1}_{\mathbf{A}^2,P}$ est un $\mathcal{O}_{\mathbf{A}^2,P}/\mathfrak{m}_{\mathbf{A}^2,P}$-module de type fini, c'est-à-dire un k-espace vectoriel de dimension finie, d'où la proposition. □

Montrons maintenant les propriétés (1) à (3) de la multiplicité d'intersection

(1) Le sens direct résulte du lemme 2.9.9. Réciproquement, supposons $P \in C \cap C'$. Alors $I(C)$ et $I(C')$ sont inclus dans $\mathfrak{m}_P$, d'où l'on tire $(I(C)+I(C'))\cdot\mathcal{O}_{\mathbf{A}^2,P} \subset \mathfrak{m}_{\mathbf{A}^2,P}$ et donc $m_P(C,C') \geq 1$.

(2) Supposons $m_P(C,C') = 1$. D'après (1), on a $P \in C \cap C'$. Posons $I(C) = (F)$ et $I(C') = (F')$. Comme $(F,F')\cdot\mathcal{O}_{\mathbf{A}^2,P} \subset \mathfrak{m}_{\mathbf{A}^2,P}$ et que $\mathfrak{m}_{\mathbf{A}^2,P}$ est de codimension 1 dans $\mathcal{O}_{\mathbf{A}^2,P}$, on a nécessairement $\mathfrak{m}_{\mathbf{A}^2,P} = (F,F')$ et donc le k-espace vectoriel $\mathfrak{m}_{\mathbf{A}^2,P}/\mathfrak{m}^2_{\mathbf{A}^2,P}$ est engendré par les classes de F et F'. Quitte à translater, supposons $P = (0,0)$. Posons $F = aX + bY + H$ et $F' = a'X + b'Y + H'$ avec $a,b,a',b' \in k$ et $H, H' \in \mathfrak{m}_P^2$. Dans $\mathfrak{m}_{\mathbf{A}^2,P}/\mathfrak{m}^2_{\mathbf{A}^2,P}$, on a $\overline{F} = a\overline{X} + b\overline{Y}$ et $\overline{F'} = a'\overline{X} + b'\overline{Y}$. Comme $(\overline{X},\overline{Y})$ est une base de $\mathfrak{m}_{\mathbf{A}^2,P}/\mathfrak{m}^2_{\mathbf{A}^2,P}$, on en déduit $\begin{pmatrix} a & b \\ a' & b' \end{pmatrix} \in \mathrm{GL}_2(k)$. En particulier $(a,b) \neq (0,0)$ (resp. $(a',b') \neq (0,0)$) donc P est un point lisse de C (resp. C'). De plus (a,b) n'est pas proportionnel à (a',b'), ce qui montre que les tangentes de C et C' en P sont distinctes, et donc $C \pitchfork_P C'$.

Réciproquement, supposons $C \pitchfork_P C'$. En gardant les notations précédentes et en raisonnant comme ci-dessus, on a $\begin{pmatrix} a & b \\ a' & b' \end{pmatrix} \in \mathrm{GL}_2(k)$. Posons $F = AX + BY$ et $F' = A'X + B'Y$ avec $A,B,A',B' \in k[X,Y]$ (une telle écriture n'est pas unique). Remarquons que $A(P) = a$, $A'(P) = a'$, $B(P) = b$ et $B'(P) = b'$. Considérons la matrice $M = \begin{pmatrix} A & B \\ A' & B' \end{pmatrix}$, à coefficients dans $k[X,Y]$. On a $\det(M) = AB' - A'B$ et donc $\det(M)(P) \in k^*$. Par suite $\det(M) \in \mathcal{O}^\times_{\mathbf{A}^2,P}$ et donc $M \in \mathrm{GL}_2(\mathcal{O}_{\mathbf{A}^2,P})$. Comme $\begin{pmatrix} F \\ F' \end{pmatrix} = M \begin{pmatrix} X \\ Y \end{pmatrix}$, il vient $\begin{pmatrix} X \\ Y \end{pmatrix} = M^{-1} \begin{pmatrix} F \\ F' \end{pmatrix}$ et donc $X, Y \in (F,F')\cdot\mathcal{O}_{\mathbf{A}^2,P}$. Par suite $\mathfrak{m}_{\mathbf{A}^2,P} = (X,Y) \subset (F,F')\cdot\mathcal{O}_{\mathbf{A}^2,P}$. D'autre part on sait déjà que $(F,F')\cdot\mathcal{O}_{\mathbf{A}^2,P} \subset \mathfrak{m}_{\mathbf{A}^2,P}$. On a donc $(I(C)+I(C'))\cdot\mathcal{O}_{\mathbf{A}^2,P} = \mathfrak{m}_{\mathbf{A}^2,P}$ et $m_P(C,C') = 1$.

(3) L'égalité $m_P(C,C') = m_P(C',C)$ résulte immédiatement de la définition.

Indiquons maintenant comment, dans la pratique, on peut calculer $m_P(C,C')$.

Proposition 2.9.12. — *Soit C, C' des courbes affines planes sans composante commune. Posons $I(C) = (F)$ et $I(C') = (F')$. Notons f l'image canonique de F dans $k[C']$, et f' l'image canonique de F' dans $k[C]$.*

Si P est un point lisse de C, alors $m_P(C,C') = \mathrm{ord}_{P\in C}(f')$. De même, si P est un point lisse de C', alors $m_P(C,C') = \mathrm{ord}_{P\in C'}(f)$.

Remarque 2.9.13. — La notation $\mathrm{ord}_{P\in C}$ signifie que l'on calcule l'ordre d'annulation en P sur la courbe C.

Démonstration. — Par symétrie, il suffit de prouver la première assertion. Par définition, on a $m_P(C,C') = \dim_k \mathcal{O}_{\mathbf{A}^2,P}/(F,F')$. Écrivons $\mathcal{O}_{\mathbf{A}^2,P}/(F,F')$ comme le quotient successif $(\mathcal{O}_{\mathbf{A}^2,P}/(F))/(\overline{F'})$, où $\overline{F'}$ désigne l'image canonique de F' dans $\mathcal{O}_{\mathbf{A}^2,P}/(F)$.

D'après la théorie de la localisation, l'anneau quotient $\mathcal{O}_{\mathbf{A}^2,P}/(F)$ s'identifie au localisé de $k[X,Y]/(F)$ en l'idéal maximal image de $\mathfrak{m}_P$ dans $k[X,Y]/(F)$. Comme $k[X,Y]/(F) \cong k[C]$, on en déduit que $\mathcal{O}_{\mathbf{A}^2,P}/(F)$ s'identifie à $\mathcal{O}_{C,P}$. De plus $\overline{F'} \in \mathcal{O}_{\mathbf{A}^2,P}/(F)$ s'identifie à $f' \in \mathcal{O}_{C',P}$, d'où l'on déduit $\mathcal{O}_{\mathbf{A}^2,P}/(F,F') \cong \mathcal{O}_{C,P}/(f')$.

Soit t une uniformisante de C en P. On peut écrire $f' = t^m u$ avec $m = \mathrm{ord}_P(f')$ et $u \in \mathcal{O}_{C,P}^\times$. Dans $\mathcal{O}_{C,P}$ on a donc $(f') = (t^m) = \mathfrak{m}_{C,P}^m$. Il vient alors

$$m_P(C,C') = \dim_k \mathcal{O}_{\mathbf{A}^2,P}/(F,F') = \dim_k(\mathcal{O}_{C,P}/\mathfrak{m}_{C,P}^m) = m$$

puisque $\dim_k(\mathfrak{m}_{C,P}^i/\mathfrak{m}_{C,P}^{i+1}) = 1$ pour tout $i \in \{0,\dots,m-1\}$. □

Exemple 2.9.14. — Soit $C : y = x^2$; $C' : y = x^3$ et $P = (0,0)$. Les polynômes $F = Y - X^2$ et $F' = Y - X^3$ sont irréductibles. On a $k[C] = k[X,Y]/(F) = k[x]$. Le point P est lisse dans C et comme $\frac{\partial F}{\partial Y}(P) \neq 0$, la fonction x est une uniformisante de C en P. On a $f' = y - x^3 = x^2 - x^3 \in k[C]$ d'où l'on tire $\mathrm{ord}_{P\in C}(f') = 2$ et donc $m_P(C,C') = 2$.

Cas particulier : intersection d'une courbe et d'une droite. Une droite étant lisse, il est toujours possible de calculer la multiplicité d'intersection par la méthode ci-dessus. Plus précisément, considérons l'intersection d'une courbe affine plane C avec la droite $D : y = ax + b$. Posons $I(C) = (F)$. On a $(x,y) \in C \cap D$ si et seulement si $y = ax + b$ et $F(x, ax+b) = 0$. L'ensemble $C \cap D$ est donc en bijection avec l'ensemble des racines du polynôme $R(X) = F(X, aX+b)$. On a alors la proposition utile suivante :

Proposition 2.9.15. — *Pour tout $P = (x_0, y_0) \in C \cap D$, l'entier $m_P(C,D)$ est égal à la multiplicité de la racine x_0 de R.*

Démonstration. — On a $k[D] = k[x]$ et en notant f l'image de F dans $k[D]$, on a $f = F(x, ax+b) = R(x)$. D'après la proposition 2.9.12, on a donc

$$m_P(C,D) = \mathrm{ord}_{P\in D}\, F(x, ax+b) = \mathrm{ord}_{P\in D}\, R(x).$$

Posons $R = (X - x_0)^m S$ avec $S \in k[X]$ tel que $S(x_0) \neq 0$, de sorte que m est la multiplicité de x_0 comme racine de R. Alors $R(x) = (x - x_0)^m S(x)$ et comme $x - x_0$ est une uniformisante de D en P, on obtient $\mathrm{ord}_{P\in D}\, R(x) = m$. □

Nous pouvons maintenant énoncer le théorème de Bézout.

Théorème 2.9.16. — *Soient C_1 et C_2 des courbes projectives planes sans composante commune. On note d_i le degré d'un générateur de $I(C_i)$. Alors*

$$\sum_{P \in C_1 \cap C_2} m_P(C_1, C_2) = d_1 d_2. \tag{16}$$

Remarque 2.9.17. — Une conséquence immédiate du théorème est que $C_1 \cap C_2$ est non vide : deux courbes projectives planes s'intersectent toujours. Cela généralise le fait que deux droites projectives s'intersectent toujours.

Remarque 2.9.18. — Une autre conséquence du théorème est que le cardinal de $C_1 \cap C_2$ est toujours $\leq d_1 d_2$, avec égalité si et seulement si $C_1 \pitchfork C_2$.

Pour la démonstration du théorème de Bézout, nous procédons en plusieurs étapes.

Première étape. On commence par choisir une droite projective D_∞ ne rencontrant pas $C_1 \cap C_2$. C'est possible car $C_1 \cap C_2$ est fini (lemme 2.9.1) et k est infini. Montrons que la droite D_∞ n'est pas une composante de C_1 ou de C_2. Supposons par exemple que $D_\infty \subset C_1$. Comme toute courbe affine plane possède au moins un point à l'infini, l'ensemble $C_2 \cap D_\infty$ est non vide, et donc $C_1 \cap C_2 \cap D_\infty \neq \emptyset$, en contradiction avec le choix de D_∞.

En considérant D_∞ comme la droite à l'infini, et comme aucune des courbes C_1 et C_2 ne contient D_∞, on peut voir ces courbes comme les complétions projectives de deux courbes affines planes. Nous noterons encore abusivement C_1 et C_2 ces courbes affines, et nous noterons $F_i \in k[X,Y]$ un générateur de $I(C_i)$. Remarquons que $\deg F_i = \deg \overline{F_i} = d_i$. De plus les courbes affines C_1 et C_2 n'ont pas de composante commune. Puisque les courbes affines C_1 et C_2 ne s'intersectent pas à l'infini, nous sommes ramenés à montrer l'identité suivante :

$$\sum_{P \in C_1 \cap C_2} m_P(C_1, C_2) = d_1 d_2. \tag{17}$$

Deuxième étape. Nous allons montrer l'identité suivante ;

$$\sum_{P \in C_1 \cap C_2} m_P(C_1, C_2) = \dim_k(k[X,Y]/(F_1, F_2)). \tag{18}$$

Posons $I = (F_1, F_2) \subset k[X,Y]$ et pour tout $P \in \mathbf{A}^2$, posons $I_P = I \cdot \mathcal{O}_{\mathbf{A}^2,P} \subset \mathcal{O}_{\mathbf{A}^2,P}$. Notons ϕ_P le morphisme canonique de k-algèbres $\phi_P : k[X,Y]/I \to \mathcal{O}_{\mathbf{A}^2,P}/I_P$.

Lemme 2.9.19. — *Pour tout $P \in C_1 \cap C_2$, le morphisme ϕ_P est surjectif.*

Démonstration. — Soit $F/G \in \mathcal{O}_{\mathbf{A}^2,P}$, avec $F, G \in k[X,Y]$ et $G(P) \neq 0$. D'après le lemme 2.9.10, il existe $N \geq 1$ tel que $\mathfrak{m}_P^N \subset I$. Puisque $V(\mathfrak{m}_P^N) = \{P\}$, l'anneau $k[X,Y]/\mathfrak{m}_P^N$ est local (son unique idéal maximal est $\mathfrak{m}_P/\mathfrak{m}_P^N$). Comme $G \notin \mathfrak{m}_P$, la classe $\overline{G}$ de G dans $k[X,Y]/\mathfrak{m}_P^N$ est inversible, d'où l'existence d'un polynôme $H \in k[X,Y]$ tel que $GH \equiv 1 \pmod{\mathfrak{m}_P^N}$. En particulier $GH \equiv 1 \pmod{I}$, d'où l'on tire la congruence $\frac{1}{G} \equiv H \pmod{I_P}$ dans $\mathcal{O}_{\mathbf{A}^2,P}$. On en déduit $F/G \equiv FH \pmod{I_P}$ et donc $\overline{F/G} = \phi_P(\overline{FH})$. □

Considérons maintenant le morphisme $\phi : k[X,Y]/I \to \prod_{P \in C_1 \cap C_2} \mathcal{O}_{\mathbf{A}^2,P}/I_P$ donné par le produit des ϕ_P. Pour établir (18), il suffit de montrer que ϕ est un isomorphisme.

Lemme 2.9.20. — *Le morphisme ϕ est injectif.*

Démonstration. — Soit $F \in k[X,Y]$ tel que pour tout $P \in C_1 \cap C_2$, on ait $F \in I_P$. Alors $J = \{H \in k[X,Y] : HF \in I\}$ est un idéal de $k[X,Y]$ et on veut $J = k[X,Y]$. Par l'absurde, si $J \neq k[X,Y]$, alors il existe $P \in \mathbf{A}^2$ tel que $J \subset \mathfrak{m}_P$. Comme J contient I, il vient $I \subset \mathfrak{m}_P$ et donc $P \in C_1 \cap C_2$. En utilisant l'hypothèse $F \in I_P$, on peut écrire $F = G/H$ avec $G \in I$ et $H(P) \neq 0$. On a alors $H \in J$ et $H \notin \mathfrak{m}_P$, une contradiction. □

Lemme 2.9.21. — *Le morphisme ϕ est surjectif.*

Démonstration. — D'après le lemme 2.9.19, le morphisme ϕ est surjectif sur chaque composante. Comme ϕ est un morphisme de k-algèbres, il suffit de montrer que pour tout $P \in C_1 \cap C_2$, il existe $F \in k[X,Y]$ tel que $F \in \mathcal{O}^{\times}_{\mathbf{A}^2,P}$ et $\phi_Q(F) = 0$ pour tout $Q \neq P$ (on aura alors $\phi(F) = (0,\ldots,0,*,0,\ldots,0)$ où $*$ est la composante en P et est inversible).

Soit $\lambda : k^2 \to k$ une forme linéaire qui sépare les points de $C_1 \cap C_2$ (c'est possible car $C_1 \cap C_2$ est fini et k est infini). On peut voir λ comme un polynôme de $k[X,Y]$ homogène de degré 1. Posons

$$f_P = \prod_{\substack{Q \in C_1 \cap C_2 \\ Q \neq P}} \lambda - \lambda(Q).$$

On a $f_P(P) \neq 0$ et pour tout $Q \in C_1 \cap C_2$ tel que $Q \neq P$, on a $f_P(Q) = 0$. En posant $F = f_P^N$, on a donc $F \in \mathcal{O}^{\times}_{\mathbf{A}^2,P}$ et pour tout $Q \in C_1 \cap C_2$ tel que $Q \neq P$, on a $F \in \mathfrak{m}_Q^N$ et donc $F \in I_Q$ grâce au lemme 2.9.10. Le polynôme F vérifie donc les conditions demandées. □

Cela achève la démonstration de (18).

Troisième étape. Nous allons montrer l'inégalité suivante :

$$\sum_{P \in C_1 \cap C_2} m_P(C_1, C_2) \leq d_1 d_2. \tag{19}$$

D'après (18), il suffit de montrer $\dim_k(k[X,Y]/I) \leq d_1 d_2$. Pour tout $d \geq 0$, notons $k[X,Y]_{\leq d}$ le k-espace vectoriel des polynômes de degré $\leq d$, et posons $\alpha(d) = \dim_k k[X,Y]_{\leq d}$. On a

$$\alpha(d) = \sum_{e=0}^{d} k[X,Y]_e = \sum_{e=0}^{d} (e+1) = \frac{(d+1)(d+2)}{2}.$$

Posons $I_{\leq d} = I \cap k[X,Y]_{\leq d}$. Considérons l'application k-linéaire

$$\begin{aligned} \psi_d : k[X,Y]_{\leq d-d_1} \oplus k[X,Y]_{\leq d-d_2} &\to k[X,Y]_{\leq d} \\ (A,B) &\mapsto AF_1 + BF_2. \end{aligned}$$

Remarquons que $\mathrm{im}(\psi_d) \subset I_{\leq d}$. Comme F_1 et F_2 sont premiers entre eux dans $k[X,Y]$, on a

$$\ker(\psi_d) = \{(CF_2, -CF_1); C \in k[X,Y]_{\leq d-d_1-d_2}\}.$$

Pour $d \geq d_1+d_2$, on a donc $\dim\ker(\psi_d) = \alpha(d-d_1-d_2)$ et par le théorème du rang, on en déduit $\dim\mathrm{im}(\psi_d) = \alpha(d-d_1)+\alpha(d-d_2)-\alpha(d-d_1-d_2)$. Pour $d \geq d_1+d_2$, on a donc

$$\dim_k\Big(\frac{k[X,Y]_{\leq d}}{I_{\leq d}}\Big) = \alpha(d) - \dim I_{\leq d} \leq \alpha(d) - \dim\mathrm{im}(\psi_d).$$

Un calcul explicite montre que cette dernière quantité vaut d_1d_2. Comme $k[X,Y]/I$ est un k-espace vectoriel de dimension finie, on a $k[X,Y]/I \cong k[X,Y]_{\leq d}/I_{\leq d}$ pour d assez grand, d'où l'on conclut $\dim_k(k[X,Y]/I) \leq d_1d_2$.

Quatrième et dernière étape. Il reste à montrer l'égalité dans (19). Un examen de la troisième étape révèle qu'il suffit de montrer $\mathrm{im}(\psi_d) = I_{\leq d}$ pour d assez grand. C'est ici que l'on va utiliser l'hypothèse que C_1 et C_2 ne s'intersectent pas à l'infini (si tel n'était pas le cas, on ne pourrait de toute façon pas espérer l'égalité dans (19)). Nous allons montrer que pour tout $d \geq d_1+d_2$, on a $I_{\leq d} \subset \mathrm{im}(\psi_d)$. Soit $d \geq d_1+d_2$ et $F \in I_{\leq d}$. Posons $F = A_1F_1 + A_2F_2$ avec $\deg(A_1)$ minimal. Nous allons montrer que $\deg(A_1) \leq d-d_1$ (cela entraînera $\deg A_2 \leq d-d_2$ et $F = \psi_d(A_1,A_2)$). Par l'absurde, supposons $\deg(A_1) > d-d_1$. Pour tout polynôme $B \in k[X,Y]$, notons B^* la composante homogène de plus haut degré de B (on a $\deg B^* = \deg B$). En posant $e = \deg(A_1)+d_1$ et en prenant la composante homogène de degré e de l'identité $F = A_1F_1 + A_2F_2$, on obtient

$$0 = A_1^*F_1^* + A_2^*F_2^*.$$

Les points à l'infini de C_i sont en bijection avec les racines de $F_i^* = \overline{F_i}(X,Y,0)$ dans $\mathbf{P}^1(k)$. Comme C_1 et C_2 ne s'intersectent pas à l'infini, on en déduit que F_1^* et F_2^* n'ont pas de racine commune dans $\mathbf{P}^1(k)$, et donc sont premiers entre eux dans $k[X,Y]$. On en déduit l'existence d'un polynôme $B \in k[X,Y]$ homogène tel que $A_1^* = F_2^*B$ et $A_2^* = -F_1^*B$. En posant $A_1' = A_1 - F_2B$ et $A_2' = A_2 + F_1B$, on vérifie que $F = A_1'F_1 + A_2'F_2$ avec $\deg(A_1') < \deg(A_1)$, ce qui contredit la minimalité de $\deg(A_1)$.

Cela achève la démonstration du théorème de Bézout.

2.10. Applications du théorème de Bézout

Théorème 2.10.1. — *Toute courbe projective plane lisse est irréductible.*

Démonstration. — Soit C une courbe projective plane lisse, et $H \in k[X,Y,Z]$ un générateur de $I(C)$. Supposons par l'absurde H réductible. On a alors $H = H_1H_2$ avec $H_i \in k[X,Y,Z]$ homogène non constant, et comme H est sans facteur carré, les polynômes H_1 et H_2 n'ont pas de facteur commun. D'après le théorème de Bézout, les courbes $C_1 = V(H_1)$ et $C_2 = V(H_2)$ s'intersectent, donc il existe $(x,y,z) \in k^3 - \{0\}$ tel que $H_1(x,y,z) = H_2(x,y,z) = 0$. On a alors $H(x,y,z) = 0$ et toutes les dérivées

partielles de H s'annulent en (x, y, z), de sorte que $(x : y : z)$ est un point singulier de C, ce qui contredit l'hypothèse. □

Remarque 2.10.2. — Attention, ce résultat est faux pour les courbes affines : par exemple, la réunion de deux droites affines parallèles est lisse, mais n'est pas irréductible.

Remarque 2.10.3. — Le théorème 2.10.1 admet la reformulation algébrique suivante : si $H \in k[X, Y, Z]$ est un polynôme homogène qui vérifie $V(H, \frac{\partial H}{\partial X}, \frac{\partial H}{\partial Y}, \frac{\partial H}{\partial Z}) = \emptyset$, alors H est irréductible (noter que la réciproque est fausse).

Théorème 2.10.4. — *Soit C une courbe projective plane lisse. Alors pour toute fonction rationnelle $f \in k(C)^\times$, on a*

$$\sum_{P \in C} \mathrm{ord}_P(f) = 0. \tag{20}$$

Remarque 2.10.5. — Ce théorème dit que sur une courbe projective, une fonction rationnelle admet autant de zéros que de pôles, comptés avec multiplicité. On peut le voir comme une généralisation du fait bien connu que sur un corps algébriquement clos, un polynôme admet autant de racines que son degré (dans le théorème précédent, cela correspond au cas où $C = \mathbf{P}^1$ et f est un polynôme).

Démonstration. — Notons d'abord que C est irréductible d'après le théorème 2.10.1. Quitte à faire un changement projectif de coordonnées, on peut supposer que C est la complétion projective d'une courbe affine plane irréductible $C_0 \subset \mathbf{A}^2$, de sorte que $k(C) = k(C_0)$. Comme $f \mapsto \mathrm{ord}_P(f)$ est un morphisme de groupes, il suffit de montrer le résultat pour $f \in k[C_0] - \{0\}$. Posons $I(C_0) = (F)$ et $f = A(x, y)$ avec $A \in k[X, Y]$ non divisible par F. On peut supposer que A est de degré $d \geq 1$.

Pour tout point $P \in C_0$, on a $\mathrm{ord}_P(f) = m_P(C_0, V(A))$ d'après la proposition 2.9.12, et donc $\mathrm{ord}_P(f) = m_P(C, C')$ où C' est la complétion projective de $V(A)$.

Soit maintenant $P \in C - C_0$. Notons $D_\infty = \mathbf{P}^2 - \mathbf{A}^2$ la droite à l'infini. On a $C' = V(\overline{A})$ avec $\overline{A}(X, Y, Z) = Z^d A(\frac{X}{Z}, \frac{Y}{Z})$. Posons $P = (x_P : y_P : 0)$ et supposons par exemple $x_P \neq 0$ (le raisonnement est le même si $y_P \neq 0$). Considérons la carte affine $(u, v) \mapsto (1 : u : v)$. Dans $k(C)$ on a $x = 1/v$ et $y = u/v$ de sorte que $f = A(1/v, u/v) = v^{-d}\overline{A}(1, u, v)$. En calculant dans cette carte, on a par définition $m_P(C, C') = \mathrm{ord}_P(\overline{A}(1, u, v))$ d'où $\mathrm{ord}_P(f) = m_P(C, C') - d\,\mathrm{ord}_P(v)$. Toujours dans cette carte affine, la droite D_∞ a pour équation $v = 0$, ce qui entraîne $\mathrm{ord}_P(v) = m_P(C, D_\infty)$.

On en déduit l'identité $\mathrm{ord}_P(f) = m_P(C, C') - d m_P(C, D_\infty)$, qui est en fait valable pour tout point $P \in C$. En prenant la somme sur P et en utilisant le théorème de Bézout, il vient

$$\sum_{P \in C} \mathrm{ord}_P(f) = \deg(C) \cdot d - d \cdot \deg(C) = 0.$$

□

Nous passons maintenant au théorème $AF + BG$ de Max Noether. Comme nous le verrons, ce théorème contient comme cas particuliers des théorèmes classiques comme le théorème de Pascal, de Pappus, etc.

Théorème 2.10.6 **(Théorème $AF + BG$ de Max Noether)**
Soit $F, G \in k[X, Y, Z]$ des polynômes homogènes sans facteur carré, de degrés respectifs $d, e \geq 1$. On suppose que les courbes $V(F)$ et $V(G)$ s'intersectent transversalement. Si $P \in k[X, Y, Z]_n$ vérifie $V(P) \supset V(F, G)$, alors il existe des polynômes $A \in k[X, Y, Z]_{n-d}$ et $B \in k[X, Y, Z]_{n-e}$ tels que $P = AF + BG$.

Démonstration. — **Premier cas** : $n \geq de - 1$.

Posons $S = V(F, G)$. Pour chaque $x \in S$, choisissons un représentant $\widetilde{x} \in k^3 - \{0\}$. Considérons l'application linéaire

$$\begin{aligned} \varphi : k[X, Y, Z]_n &\to k^S \\ P &\mapsto (P(\widetilde{x}))_{x \in S}. \end{aligned}$$

Montrons que φ est surjective. Pour tout $x \in S$, on choisit une droite projective D_x telle que $D_x \cap S = \{x\}$ (c'est possible car k est infini). On choisit également une droite D telle que $D \cap S = \emptyset$. Posons $D_x = V(\lambda_x)$ et $D = V(\lambda)$ avec $\lambda_x, \lambda \in k[X, Y, Z]_1$. D'après le théorème de Bézout, on a $\mathrm{card}(S) = de$. En posant $P_x = \lambda^{n-de+1} \prod_{y \in S - \{x\}} \lambda_y$, on a $P_x \in k[X, Y, Z]_n$ et $\varphi(P_x)$ est de la forme $(0, \ldots, 0, *, 0, \ldots, 0)$ où seule la composante en x est non nulle. On en déduit la surjectivité de φ. Par suite

$$\dim \ker \varphi = \dim k[X, Y, Z]_n - de = \frac{(n+1)(n+2)}{2} - de.$$

D'autre part $\ker \varphi$ contient l'espace vectoriel $V = k[X, Y, Z]_{n-d} \cdot F + k[X, Y, Z]_{n-e} \cdot G$ et par un calcul analogue à celui de la démonstration du théorème de Bézout, on trouve $\dim V = \frac{(n+1)(n+2)}{2} - de$, ce qui montre que $\ker \varphi = V$ et permet de conclure.

Deuxième cas : $n \geq d + e - 1$. On fait une récurrence descendante sur n. Supposons donc le résultat vrai pour un entier donné $n \geq d + e$, et montrons-le pour l'entier $n - 1$. Soit $P \in k[X, Y, Z]_{n-1}$ tel que $V(P) \supset V(F, G)$.

Pour toute forme linéaire non nulle λ sur k^3, on a $V(\lambda P) = V(\lambda) \cup V(P) \supset V(F, G)$ et par l'hypothèse de récurrence, il existe des polynômes homogènes A_λ et B_λ tels que $\lambda P = A_\lambda F + B_\lambda G$. Choisissons une droite projective D qui vérifie les deux conditions suivantes :

(1) D intersecte transversalement $V(F)$;

(2) D est disjointe de S.

C'est toujours possible car l'espace des droites projectives est de dimension 2 (c'est le plan projectif dual), tandis que l'ensemble des droites qui passent par un point donné p est de dimension 1 (c'est la droite projective duale p^*) ; de même l'ensemble des droites qui n'intersectent pas transversalement $V(F)$ est la réunion des droites passant par les points singuliers de $V(F)$ et des droites tangentes à $V(F)$, chacune

de ces conditions définissant un fermé algébrique strict du plan projectif dual. Par irréductibilité de $\mathbf{P}^2$, on en déduit que l'ensemble des droites qui ne vérifient pas (1) ou (2) est un fermé algébrique strict, d'où l'existence de D.

Posons $E = D \cap V(F)$ et donnons-nous une partie $E' \subset D$, disjointe de E et de cardinal $n - d - e + 1$ (en particulier E' est non vide). Posons $D = V(\lambda)$ avec λ forme linéaire non nulle sur k^3.

Lemme 2.10.7. — *Il existe des polynômes homogènes A et B tels que $\lambda P = AF + BG$ et $V(B) \supset E'$.*

Démonstration. — On cherche A et B sous la forme $A = A_\lambda + GQ$ et $B = B_\lambda - FQ$ avec $Q \in k[X,Y,Z]_{n-d-e}$. Pour tout $x \in E'$, choisissons un représentant $\widetilde{x}$ dans $k^3 - \{0\}$. On a l'équivalence

$$x \in V(B) \Leftrightarrow Q(\widetilde{x}) = \frac{B_\lambda(\widetilde{x})}{F(\widetilde{x})} \qquad (x \in E').$$

Notons qu'on a bien $F(\widetilde{x}) \neq 0$ car E' est disjoint de $V(F)$. Par interpolation, il est possible de trouver $Q \in k[X,Y,Z]_{n-d-e}$ vérifiant la condition ci-dessus pour tout $x \in E'$ (les points de E' étant alignés, on interpole « sur une droite »). □

En prenant A et B comme dans le lemme 2.10.7, on voit que BG s'annule sur $V(\lambda, F) = E$ et comme $E \cap V(G) = \emptyset$ (condition (2)), on en déduit que B s'annule sur E. Donc B s'annule sur $E \cup E'$ qui est une partie de cardinal $n - e + 1 > \deg(B)$. Par le théorème de Bézout, la droite D est nécessairement une composante de $V(B)$, ce qui entraîne $\lambda | B$ et donc $\lambda | AF$. Comme λ ne divise pas F d'après la condition (1), on en déduit $\lambda | A$ d'où le résultat pour P.

Troisième cas : n quelconque. On procède encore par récurrence descendante. Supposons le résultat vrai pour un entier donné $n \leq d + e - 1$, et montrons-le pour l'entier $n - 1$. Soit $P \in k[X,Y,Z]_{n-1}$ tel que $V(P) \supset V(F,G)$. On utilise la même méthode que dans le deuxième cas : on choisit une forme linéaire λ sur k^3 telle que la droite $D = V(\lambda)$ vérifie $\#(D \cap V(F)) = d$ et $D \cap V(F,G) = \emptyset$. Par l'hypothèse de récurrence, il existe des polynômes homogènes A et B tels que $\lambda P = AF + BG$. Les conditions sur D entraînent que B s'annule sur $D \cap V(F)$, qui est de cardinal $d \geq n - e + 1 > \deg(B)$. Par le théorème de Bézout, la droite D est nécessairement une composante de $V(B)$ et on conclut comme dans le deuxième cas. □

Théorème 2.10.8 **(Théorème de Cayley)**. — *On suppose* $\mathrm{car}(k) = 0$. *Soit $F, G \in k[X,Y,Z]$ des polynômes homogènes sans facteur carré, de degrés respectifs $d, e \geq 1$. On suppose que les courbes $V(F)$ et $V(G)$ s'intersectent transversalement. Soit C une courbe projective plane définie par un polynôme homogène de degré $d + e - 3$. Si C passe par $(de - 1)$ points de $V(F,G)$, alors C contient $V(F,G)$.*

Démonstration. — Soit $P \in k[X,Y,Z]_{d+e-3}$ non nul et $x \in V(F,G)$ le point « oublié » par $C = V(P)$. Choisissons une droite projective D passant par x et vérifiant les deux conditions suivantes :

(1) D intersecte transversalement $V(G)$;

(2) $D \cap V(F,G) = \{x\}$.

Noter que la condition (2) est vérifiée pour toute droite passant par x sauf un nombre fini. Quant à l'existence d'une droite D passant par x et vérifiant (1), on utilise l'hypothèse $\mathrm{car}(k) = 0$ et le fait que x est un point lisse de $V(G)$ (puisque $V(F) \pitchfork V(G)$).

Posons comme précédemment $D = V(\lambda)$. Alors le polynôme λP s'annule sur $V(F,G)$ et d'après le théorème de Max Noether, on peut écrire $\lambda P = AF + BG$ avec A et B homogènes de degrés respectifs $e-2$ et $d-2$ (si $d = 1$ resp. $e = 1$, alors $B = 0$ resp. $A = 0$). Posons $E = D \cap V(G)$, de sorte que $\#E = e$. Alors AF s'annule sur E et d'après la condition (2), on en déduit que A s'annule sur $E - \{x\}$ qui est de cardinal $e - 1 > \deg(A)$. Par le théorème de Bézout, la droite D est une composante de $V(A)$ et donc $\lambda | A$, ce qui permet d'écrire $P = \frac{A}{\lambda}F + \frac{B}{\lambda}G$ et de conclure. □

Théorème 2.10.9 **(Théorème de Pascal).** — *Soit $C \subset \mathbf{P}^2(k)$ une conique, que l'on suppose non réduite à une droite. Soit $P_1, P_2, \ldots, P_6$ des points de C, deux à deux distincts. On suppose que les droites $(P_1P_2), (P_2P_3), \ldots, (P_5P_6), (P_6P_1)$ sont deux à deux distinctes et ne sont pas incluses dans C (c'est automatique si C est irréductible). Alors les points de concours respectifs des droites (P_1P_2) et (P_4P_5), des droites (P_2P_3) et (P_5P_6), et des droites (P_3P_4) et (P_6P_1), sont alignés.*

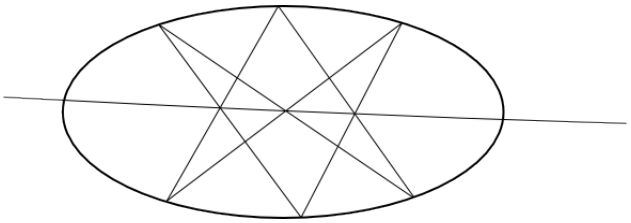

FIGURE 1. L'hexagramme mystique de Pascal

Démonstration. — Posons $C = V(F)$ avec $F \in k[X,Y,Z]_2$ sans facteur carré. Pour tout $1 \leq i \leq 6$, choisissons une forme linéaire λ_i sur k^3 telle que $V(\lambda_i) = (P_iP_{i+1})$ (avec la convention $P_7 = P_1$). Posons

$$G = \lambda_1\lambda_3\lambda_5,$$
$$P = \lambda_2\lambda_4\lambda_6.$$

Par hypothèse, les courbes C et $V(G)$ n'ont pas de composante commune et comme $C \cap V(G)$ contient les points $P_1, \ldots, P_6$, le théorème de Bézout entraîne que C et $V(G)$ s'intersectent transversalement, avec $C \cap V(G) = V(F,G) = \{P_1, \ldots, P_6\}$.

Le polynôme P vérifie $V(P) \supset V(F,G)$. En appliquant le théorème de Max Noether, on trouve $P = AF + BG$ avec A homogène de degré 1 et $B \in k$.

Pour tout $1 \leq i \leq 3$, notons M_i le point d'intersection de (P_iP_{i+1}) et $(P_{i+3}P_{i+4})$. Les points M_1, M_2, M_3 appartiennent à $V(P,G)$ et donc à $V(AF)$. Par ailleurs M_i est distinct des points P_i et P_{i+1} (si l'on avait par exemple $M_i = P_i$ alors les points P_i, P_{i+3} et P_{i+4} seraient alignés, donc la droite les contenant serait incluse dans C,

contre l'hypothèse). Il en résulte que $M_i \notin C$ (sinon la droite $(M_iP_iP_{i+1})$ serait incluse dans C, contre l'hypothèse). Il en découle que les points M_1, M_2 et M_3 sont alignés sur la droite $V(A)$. □

Remarque 2.10.10. — Dans le cas où la conique C est réunion de deux droites, le théorème de Pascal devient le théorème de Pappus.

Enfin, nous allons montrer que le théorème de Bézout entraîne l'existence d'une *loi de groupe* sur toute cubique plane lisse.

Introduisons d'abord la notion de *diviseur*. Étant donnée une courbe C, un *diviseur* sur C est une somme formelle finie de points de C, à coefficients dans $\mathbf{Z}$. Un diviseur sur C s'écrit sous la forme $\sum_{i=1}^{r} n_i[P_i]$ avec $n_i \in \mathbf{Z}$ et $P_i \in C$. Autrement dit, un diviseur sur C est un élément du groupe abélien libre de base C. Le groupe des diviseurs sur C est noté $\mathrm{Div}(C)$. On dispose d'une application *degré* sur $\mathrm{Div}(C)$, à valeurs dans $\mathbf{Z}$, définie par

$$\deg(\sum_{i=1}^{r} n_i[P_i]) = \sum_{i=1}^{r} n_i.$$

L'application $\deg : \mathrm{Div}(C) \to \mathbf{Z}$ est un morphisme de groupes. On dit qu'un diviseur $D \in \mathrm{Div}(C)$ est *effectif* si les coefficients de D sont positifs, autrement dit si $D = \sum_{i=1}^{r} n_i[P_i]$ avec $n_i \geq 0$ pour tout $1 \leq i \leq r$. On note alors $D \geq 0$. Enfin, étant donnés deux diviseurs $D, D' \in \mathrm{Div}(C)$, on dit que $D \geq D'$ lorsque $D - D' \geq 0$.

Étant données deux courbes projectives planes C_1, C_2, sans composante commune, on peut considérer la somme formelle $C_1 \cdot C_2$ définie par

$$C_1 \cdot C_2 := \sum_{P \in C_1 \cap C_2} m_P(C_1, C_2)[P]$$

On peut penser à $C_1 \cdot C_2$ comme à une version améliorée de $C_1 \cap C_2$, qui tient compte des multiplicités. C'est un diviseur (effectif) sur C_1 ou C_2. Le théorème de Bézout s'énonce alors très simplement : on a $\deg(C_1 \cdot C_2) = \deg(C_1) \cdot \deg(C_2)$.

Soit maintenant C une cubique projective plane lisse (donc irréductible, d'après le théorème 2.10.1). Fixons un point $O \in C$. Nous allons définir une loi de groupe sur C d'élément neutre O.

Remarquons d'abord que C ne contient aucune droite projective (par irréductibilité de C) et donc toute droite projective D intersecte C en trois points, comptés avec multiplicité. Autrement dit, pour toute droite projective D, on a $\deg(C \cdot D) = 3$. Donnons-nous maintenant deux points $P, Q \in C$. Il existe alors une unique droite projective D telle que $C \cdot D \geq [P] + [Q]$. En effet, si $P \neq Q$, alors D est simplement la droite (PQ), tandis que si $P = Q$, alors D est la tangente de C en P (bien définie puisque C est supposée lisse). Comme $C \cdot D$ est de degré 3, il existe un unique point $\varphi(P, Q) \in C$ tel que

$$C \cdot D = [P] + [Q] + [\varphi(P, Q)] \tag{21}$$

Remarquons qu'on peut très bien avoir $\varphi(P,Q) = P$ ou $\varphi(P,Q) = Q$ dans le cas où D est une tangente de C (on peut même avoir $P = Q = \varphi(P,Q)$, auquel cas $C \cap D = \{P\}$; on dit alors que P est un *point d'inflexion* de C).

Nous avons donc défini une application $\varphi : C \times C \to C$. Définissons maintenant une loi de composition interne $\oplus$ sur C par

$$P \oplus Q := \varphi(O, \varphi(P,Q)) \qquad (P,Q \in C). \tag{22}$$

Remarque 2.10.11. — Contrairement à φ, la loi $\oplus$ dépend du choix de O.

Théorème 2.10.12. — *L'ensemble C muni de la loi $\oplus$ est un groupe abélien d'élément neutre O.*

Démonstration. — Comme $\varphi(P,Q) = \varphi(Q,P)$ pour tout $P,Q \in C$, la loi $\oplus$ est commutative.

Montrons que O est élément neutre. Soit $P \in C$ et D l'unique droite telle que $C \cdot D \geq [O] + [P]$. Alors $C \cdot D = [O] + [P] + [\varphi(O,P)]$ et donc $\varphi(O, \varphi(O,P)) = P$, ce qui montre que $O \oplus P = P$, d'où le fait que O est élement neutre.

Donnons-nous $P \in C$ et montrons l'existence d'un inverse de P. Soit D_0 la tangente de C en O, de sorte que $C \cdot D_0 = 2[O] + [O']$ avec $O' = \varphi(O,O)$. Posons $P' = \varphi(O', P) \in C$. Par définition, il existe une droite D telle que $C \cdot D = [O'] + [P] + [P']$. En particulier $\varphi(P,P') = O'$ et donc $P \oplus P' = \varphi(O,O') = O$.

Le point le plus délicat est l'associativité de $\oplus$, qui va résulter du théorème $AF + BG$. Soit $P,Q,R \in C$. Pour montrer $P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$, il suffit de montrer

$$\varphi(P, Q \oplus R) = \varphi(P \oplus Q, R).$$

Soit $D_1, D_2, D_3, D_1', D_2', D_3'$ les droites définies par

$$\begin{aligned}
C \cdot D_1 &= [P] + [Q] + [\varphi(P,Q)] \\
C \cdot D_2 &= [P \oplus Q] + [R] + [\varphi(P \oplus Q, R)] \\
C \cdot D_3 &= [Q \oplus R] + [O] + [\varphi(Q,R)] \\
C \cdot D_1' &= [P \oplus Q] + [O] + [\varphi(P,Q)] \\
C \cdot D_2' &= [Q] + [R] + [\varphi(Q,R)] \\
C \cdot D_3' &= [P] + [Q \oplus R] + [\varphi(P, Q \oplus R)]
\end{aligned}$$

Considérons les cubiques (réductibles) $C' = D_1 \cup D_2 \cup D_3$ et $C'' = D_1' \cup D_2' \cup D_3'$. Comme C' (resp. C'') est une réunion de droites, les courbes C et C' (resp. C et C'') n'ont pas de composante commune. Les diviseurs $C \cdot C'$ et $C \cdot C''$ sont de degré 9 et on a $C \cdot C' = \sum_{i=1}^{3} C \cdot D_i$ et $C \cdot C'' = \sum_{i=1}^{3} C \cdot D_i'$. On remarque que ces diviseurs sont de la forme

$$C \cdot C' = \sum_{i=1}^{8} [P_i] + [P_9]$$
$$C \cdot C'' = \sum_{i=1}^{8} [P_i] + [P'_9]$$

et il s'agit de montrer $P_9 = P'_9$.

Faisons l'hypothèse que les points $P_1, \ldots, P_9$ sont deux à deux distincts (et donc $C \pitchfork C'$). Posons $C = V(F)$, $C' = V(G)$ et $C'' = V(H)$, de sorte que $V(F,G) = \{P_1, \ldots, P_9\}$. On veut appliquer le théorème de Max Noether à H pour pouvoir conclure que $P_9 \in C''$ et donc $P_9 = P'_9$. On sait seulement a priori que H s'annule sur $\{P_1, \ldots, P_8\}$. Choisissons donc une droite projective $D = V(\lambda)$ passant par P_9, et posons $C \cdot D = [P_9] + [S] + [T]$, de sorte que $P_9 = \varphi(S,T)$. On peut alors appliquer le théorème de Max Noether au polynôme λH, qui s'annule sur $\{P_1, \ldots, P_9\}$: il vient $\lambda H = AF + BG$ avec $A, B \in k[X,Y,Z]_1$. Posons $D' = V(B)$ (on a $B \neq 0$ car sinon F serait réductible). On peut alors faire le calcul suivant en théorie de l'intersection :

$$\begin{aligned} C \cdot (D \cup C'') &= V(F) \cdot V(\lambda H) \\ &= V(F) \cdot V(AF + BG) \\ &= V(F) \cdot V(BG) \\ &= C \cdot (D' \cup C'). \end{aligned}$$

En utilisant la bilinéarité du produit d'intersection $\cdot$ et en comparant les diviseurs, il vient $C \cdot D' = [P'_9] + [S] + [T]$ ce qui fait que $P'_9 = \varphi(S,T) = P_9$.

Nous ne détaillons pas la preuve lorsque certains des points $P_1, \ldots, P_9$ sont confondus. Une manière de faire est d'utiliser une version « avec multiplicités » du théorème $AF + BG$. Une autre manière est d'utiliser un argument de densité : si le résultat est vrai pour (P,Q,R) appartenant à un ouvert Zariski dense de $C \times C \times C$, alors il est vrai pour tout (P,Q,R) car les applications $(P,Q,R) \mapsto P \oplus (Q \oplus R)$ et $(P,Q,R) \mapsto (P \oplus Q) \oplus R$ sont régulières sur $C \times C \times C$. □