COURBES ALGÉBRIQUES

par

Vincent Sécherre

Quelques références bibliographiques

1. Alain Chenciner, *Courbes algébriques planes*, Springer, 2008.
2. Jean Dieudonné, *Cours de géométrie algébrique*, PUF, 1974.
3. William Fulton, *Algebraic curves*, disponible à :
   `http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf`
4. Keith Kendig, *Elementary algebraic geometry*, Springer, 1977.
5. Daniel Perrin, *Géométrie algébrique : une introduction*, CNRS Editions, 1995.
6. Henning Stichtenoth, *Algebraic function fields and codes*, GTM 254, Springer, 2009.

Laboratoire de mathématiques de Versailles, UVSQ, CNRS, Université Paris-Saclay, 78035 Versailles, France
`vincent.secherre@math.uvsq.fr`

Chapitre 1. Ensembles algébriques affines

Dans tout ce cours, on fixe une fois pour toutes un corps k.

1.1. Ensembles algébriques affines

Soit un entier $n \geqslant 1$. On note $\mathbf{A}^n(k)$, ou bien $\mathbf{A}^n$ si aucune confusion n'est possible, l'ensemble k^n vu comme espace affine. On l'appelle l'*espace affine de dimension n sur k*.

Notons $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ la k-algèbre des polynômes en n indéterminées à coefficients dans k. Si S est une partie de $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, on pose :

$$\mathbf{V}(\mathrm{S}) = \{x \in \mathbf{A}^n \mid \mathrm{P}(x) = 0 \text{ pour tout } \mathrm{P} \in \mathrm{S}\}. \tag{1.1}$$

C'est l'ensemble des zéros communs à tous les éléments de S. Si S est fini et égal à $\{\mathrm{P}_1, \ldots, \mathrm{P}_r\}$, on écrit $\mathbf{V}(\mathrm{P}_1, \ldots, \mathrm{P}_r)$ plutôt que $\mathbf{V}(\{\mathrm{P}_1, \ldots, \mathrm{P}_r\})$.

Exemple 1.1. — (1) On a $\mathbf{V}(\varnothing) = \mathbf{A}^n$ et $\mathbf{V}(1) = \varnothing$.

(2) Si $n = 2$, l'ensemble $\mathbf{V}(\mathrm{X}^2 + \mathrm{Y}^2 - 1)$ est le cercle $\{(x, y) \in k^2 \mid x^2 + y^2 = 1\}$ dans $\mathbf{A}^2$.

(3) Si $n = 3$, l'ensemble $\mathbf{V}(\mathrm{XYZ})$ est la réunion des plans $\mathrm{X} = 0$, $\mathrm{Y} = 0$ et $\mathrm{Z} = 0$.

(4) Pour $i \in \{1, \ldots, r\}$, soit $\mathrm{P}_i = a_{i,1}\mathrm{X}_1 + \cdots + a_{i,n}\mathrm{X}_n - b_i$ avec les $a_{i,j}$ et les b_i dans k. Alors $\mathbf{V}(\mathrm{P}_1, \ldots, \mathrm{P}_r)$ est l'ensemble des solutions du système linéaire :

$$\sum_{j=1}^{n} a_{ij} x_j = b_i, \quad i = 1, \ldots, r.$$

C'est ou bien l'ensemble vide, ou bien un sous-espace affine de dimension $\geqslant n - r$.

(5) Si $n = 1$ et si $\mathrm{S} \subseteq k[\mathrm{X}]$, alors $\mathbf{V}(\mathrm{S})$ est ou bien $\mathbf{A}^1$, ou bien une partie finie de $\mathbf{A}^1$.

Définition 1.2. — Une partie de $\mathbf{A}^n$ de la forme $\mathbf{V}(\mathrm{S})$ avec $\mathrm{S} \subseteq k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ est appelée un *ensemble algébrique affine*.

Proposition 1.3. — *On a les propriétés suivantes :*

(1) *Si* $\mathrm{P}, \mathrm{Q} \in k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, *alors* $\mathbf{V}(\mathrm{PQ}) = \mathbf{V}(\mathrm{P}) \cup \mathbf{V}(\mathrm{Q})$.

(2) *Pour tout* $\mathrm{S} \subseteq k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, *on a :*

$$\mathbf{V}(\mathrm{S}) = \bigcap_{\mathrm{P} \in \mathrm{S}} \mathbf{V}(\mathrm{P}).$$

(3) *Si* $\mathrm{S} \subseteq \mathrm{S}' \subseteq k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, *alors* $\mathbf{V}(\mathrm{S}) \supseteq \mathbf{V}(\mathrm{S}')$.

(4) *Si* I *est l'idéal engendré par* $\mathrm{S} \subseteq k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, *alors* $\mathbf{V}(\mathrm{S}) = \mathbf{V}(\mathrm{I})$.

1.2. L'idéal associé à une partie de $\mathbf{A}^n$

Soit E une partie de $\mathbf{A}^n$. On pose :

$$\mathbf{I}(\mathrm{E}) = \{\mathrm{P} \in k[\mathrm{X}_1, \ldots, \mathrm{X}_n] \mid \mathrm{P}(x) = 0 \text{ pour tout } x \in \mathrm{E}\}. \tag{1.2}$$

C'est l'ensemble des polynômes qui s'annulent sur E. C'est un idéal de $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$.

Proposition 1.4. — *Etant données* E, E' *des parties de* $\mathbf{A}^n$, *on a les propriétés suivantes :*

(1) *On a* $\mathbf{I}(\mathrm{E} \cup \mathrm{E}') = \mathbf{I}(\mathrm{E}) \cap \mathbf{I}(\mathrm{E}')$.

(2) *Si* $\mathrm{E} \subseteq \mathrm{E}'$, *alors* $\mathbf{I}(\mathrm{E}) \supseteq \mathbf{I}(\mathrm{E}')$.

(3) *Si* $\mathrm{V} = \mathbf{V}(\mathbf{I}(\mathrm{E}))$, *alors* $\mathbf{I}(\mathrm{E}) = \mathbf{I}(\mathrm{V})$.

(4) *Si* E *est un ensemble algébrique affine, alors* $\mathbf{V}(\mathbf{I}(\mathrm{E})) = \mathrm{E}$.

Démonstration. — Si $V = \mathbf{V}(\mathbf{I}(E))$, on a $V \supseteq E$ donc $\mathbf{I}(V) \subseteq \mathbf{I}(E)$. Inversement, si $P \in \mathbf{I}(E)$, il s'annule par définition sur $\mathbf{V}(\mathbf{I}(E)) = V$ et appartient donc à $\mathbf{I}(V)$.

Si en outre E est de la forme $\mathbf{V}(S)$ avec $S \subseteq k[X_1, \dots, X_n]$, montrons que $V = E$. Etant donné $x \in V$, pour que x appartienne à E, il faut et il suffit que $P(x) = 0$ pour tout $P \in S$. Comme $x \in V$, on a $P(x) = 0$ pour tout $P \in \mathbf{I}(E)$, donc en particulier pour tout $P \in S$. □

La dernière propriété implique que la restriction de $\mathbf{I}$ aux ensembles algébriques affines de $\mathbf{A}^n$ est injective. On a donc une correspondance injective :

$$\{\text{ensembles algébriques affines de } \mathbf{A}^n\} \to \{\text{idéaux de } k[X_1, \dots, X_n]\}.$$

Quelle est l'image de cette correspondance ? L'important théorème des zéros de Hilbert (théorème 1.14 ci-dessous) répondra à cette question lorsque k est algébriquement clos.

Exemple 1.5. — (1) On a $\mathbf{I}(\varnothing) = k[X_1, \dots, X_n]$.
(2) Si k est infini, on a $\mathbf{I}(\mathbf{A}^n) = \{0\}$.
(3) Si k est fini de cardinal q, on a $\mathbf{I}(\mathbf{A}^1) = (X^q - X)$.
(4) Si $n = 1$ et $a \in \mathbf{A}^1$, on a $\mathbf{I}(\{a\}) = (X - a)$.
(5) Lorsque $n \geqslant 2$, l'anneau $k[X_1, \dots, X_n]$ n'est plus principal. Fixons $a = (a_1, \dots, a_n) \in \mathbf{A}^n$ et posons :

$$\mathfrak{m}_a = (X_1 - a_1, \dots, X_n - a_n). \tag{1.3}$$

Développant n'importe quel polynôme P de $k[X_1, \dots, X_n]$ dans la base des monômes de la forme $(X_1 - a_1)^{m_1} \dots (X_n - a_n)^{m_n}$, on voit que $\mathfrak{m}_a$ est un idéal maximal, égal au noyau du morphisme d'algèbres $P \mapsto P(a)$ de $k[X_1, \dots, X_n]$ dans k, c'est-à-dire $\mathbf{I}(\{a\})$. C'est un idéal non principal.

L'application $a \mapsto \mathfrak{m}_a$ permet donc d'interpréter tout point de $\mathbf{A}^n$ comme un idéal maximal de la k-algèbre $k[X_1, \dots, X_n]$. Les idéaux maximaux de $k[X_1, \dots, X_n]$ sont-ils tous de cette forme ? C'est à nouveau le théorème 1.14 qui répondra à cette question si k est algébriquement clos.

Exemple 1.6. — Considérons l'idéal I de $k[X, Y]$ engendré par le polynôme $Y^2 - X$. L'ensemble $V = \mathbf{V}(I)$ est la parabole d'équation $y^2 = x$. Calculons l'idéal $\mathbf{I}(V)$. Soit $F \in \mathbf{I}(V)$. En considérant les éléments de $k[X, Y]$ comme des polynômes en la variable X à coefficients dans $k[Y]$, on peut effectuer la division euclidienne de F par $Y^2 - X$. En effet, ce dernier est bien un polynôme unitaire de l'anneau $k[Y][X]$. On a donc $F = (Y^2 - X)Q + R$ où $Q, R \in k[X, Y]$ et le degré de R en X est $\leqslant 0$, c'est-à-dire que la variable X n'apparaît pas dans R. Or F et $Y^2 - X$, donc R lui aussi, s'annulent tous les deux sur V. Cela signifie que $R \in k[Y]$ est un polynôme s'annulant en toutes les ordonnées des points de V. Or, pour tout $y \in k$, on a $(y^2, y) \in V$, donc $R(y) = 0$. Si le corps k est infini, on en déduit que $R = 0$, ce qui prouve que F est divisible par $Y^2 - X$. On a donc prouvé que $\mathbf{I}(V)$ est inclus dans l'idéal (F). Par ailleurs, on sait que $(F) \subseteq \mathbf{I}(V)$. Ainsi on a l'égalité $\mathbf{I}(V) = (Y^2 - X)$.

Si le corps k est fini de cardinal q, le polynôme R est divisible par $Y^q - Y$. On en déduit que $\mathbf{I}(V)$ est égal à $(Y^2 - X, Y^q - Y)$.

Dans le cas où k est algébriquement clos, le théorème des zéros de Hilbert nous donnera une méthode beaucoup plus rapide et générale pour prouver ce genre de résultat.

1.3. Deux théorèmes de finitude

Les deux propriétés de finitude dont il est question dans cette section s'appuient sur le résultat important suivant, dû à Hilbert.

***Théorème 1.7* (Théorème de la base de Hilbert).** — *L'anneau $k[X_1, \dots, X_n]$ est noethérien, c'est-à-dire qu'on a les propriétés équivalentes suivantes :*

(1) *Tout idéal de $k[X_1, \dots, X_n]$ est engendré par un nombre fini d'éléments.*
(2) *Il n'existe pas de suite infinie strictement croissante d'idéaux dans $k[X_1, \dots, X_n]$.*

Nous allons montrer que tout ensemble algébrique affine de $\mathbf{A}^n$ peut être défini par un nombre *fini* d'équations.

Théorème 1.8. — *Pour tout ensemble algébrique affine $V \subseteq \mathbf{A}^n$, il existe un nombre fini de polynômes $P_1, \dots, P_r$ de $k[X_1, \dots, X_n]$ tels que $V = \mathbf{V}(P_1, \dots, P_r)$.*

Démonstration. — Soit $S \subseteq k[X_1, \dots, X_n]$ telle que $V = \mathbf{V}(S)$. Notant I l'idéal de $k[X_1, \dots, X_n]$ engendré par S, on a $V = \mathbf{V}(I)$. D'après le théorème de la base de Hilbert, l'idéal I est engendré par un nombre *fini* de polynômes $P_1, \dots, P_r$. On a donc $\mathbf{V}(P_1, \dots, P_r) = \mathbf{V}(I) = V$. □

Passons maintenant à la notion d'irréductibilité.

Définition 1.9. — Un ensemble algébrique affine $V \subseteq \mathbf{A}^n$ est *irréductible* si, pour toute décomposition $V = V_1 \cup V_2$ avec V_1, V_2 des ensembles algébriques affines, on a $V_1 = V$ ou $V_2 = V$.

Proposition 1.10. — *Soit V un ensemble algébrique affine de $\mathbf{A}^n$. Les assertions suivantes sont équivalentes.*

(1) *L'ensemble algébrique affine V est irréductible.*
(2) *L'idéal $\mathbf{I}(V)$ est un idéal premier.*
(3) *L'anneau-quotient $k[X_1, \dots, X_n]/\mathbf{I}(V)$ est intègre.*

Démonstration. — D'abord, soient $P, Q \in k[X_1, \dots, X_n]$ tels que $PQ \in \mathbf{I}(V)$. On a donc $P(x)Q(x) = 0$ pour tout $x \in V$. Comme k est un corps, pour chaque $x \in V$, on a soit $P(x) = 0$, soit $Q(x) = 0$, ce qui se traduit par l'égalité :

$$V = (V \cap \mathbf{V}(P)) \cup (V \cap \mathbf{V}(Q)).$$

Supposant V irréductible, cela donne par exemple $V \cap \mathbf{V}(P) = V$, c'est-à-dire $V \subseteq \mathbf{V}(P)$, donc $P(x) = 0$ pour tout $x \in V$, ce qui implique que $P \in \mathbf{I}(V)$. L'idéal $\mathbf{I}(V)$ est donc premier.

Inversement, supposons que V n'est pas irréductible et écrivons $V = V_1 \cup V_2$ avec V_1, V_2 des ensembles algébriques affines strictement inclus dans V. Comme $V \mapsto \mathbf{I}(V)$ est injective, on obtient que $\mathbf{I}(V_i) \supsetneq \mathbf{I}(V)$ pour chaque $i \in \{1, 2\}$. On peut donc choisir $P_i \in \mathbf{I}(V_i)$ n'appartenant pas à $\mathbf{I}(V)$, pour chaque i. L'égalité $V = V_1 \cup V_2$ implique que $P_1P_2 \in \mathbf{I}(V)$, et ainsi l'idéal $\mathbf{I}(V)$ n'est pas premier. □

Théorème 1.11. — *Soit $V \subseteq \mathbf{A}^n$ un ensemble algébrique affine. Il existe des ensembles algébriques affines irréductibles $V_1, \dots, V_m$ tels que :*

(1) $V = V_1 \cup \dots \cup V_m$;
(2) *pour tous $i \neq j$, on a $V_i \not\subseteq V_j$.*

Les V_i sont uniques à l'ordre près et s'appellent les composantes irréductibles de V.

Démonstration. — On raisonne par l'absurde, en supposant l'existence d'un ensemble algébrique affine V indécomposable, c'est-à-dire qui ne se décompose pas ainsi. On peut le choisir tel que $\mathbf{I}(V)$ soit maximal parmi les idéaux de la forme $\mathbf{I}(W)$ où W décrit les ensembles algébriques affines indécomposables : si un tel choix n'existait pas, on pourrait créer une suite strictement croissante d'idéaux $\mathbf{I}(W_0) \subsetneq \mathbf{I}(W_1) \subsetneq \dots$ avec les W_i indécomposables, ce qui contredirait le fait que $k[X_1, \dots, X_n]$ est noethérien.

Puisqu'un tel V n'est pas irréductible (sans quoi il ne serait pas indécomposable), on peut l'écrire sous la forme $V = W_1 \cup W_2$ avec W_1, W_2 des ensembles algébriques affines strictement inclus dans V. Comme

$\mathbf{I}$ est injective, on a $\mathbf{I}(\mathrm{W}_i) \supsetneq \mathbf{I}(\mathrm{V})$ pour chaque $i \in \{1,2\}$. Par la propriété de maximalité de $\mathbf{I}(\mathrm{V})$, les W_i ne sont pas indécomposables, donc V non plus : contradiction.

Pour l'unicité, écrivons $\mathrm{V} = \mathrm{V}_1 \cup \cdots \cup \mathrm{V}_m = \mathrm{W}_1 \cup \cdots \cup \mathrm{W}_p$. Pour chaque $i \in \{1,\dots,m\}$, on a :

$$\mathrm{V}_i = \mathrm{V} \cap \mathrm{V}_i = (\mathrm{W}_1 \cap \mathrm{V}_i) \cup \cdots \cup (\mathrm{W}_p \cap \mathrm{V}_i)$$

et l'irréductibilité de V_i implique qu'il existe un $j \in \{1,\dots,p\}$ tel que $\mathrm{V}_i = \mathrm{W}_j \cap \mathrm{V}_i$, c'est-à-dire $\mathrm{V}_i \subseteq \mathrm{W}_j$. En raisonnant de façon analogue avec la composante irréductible W_j, on trouve un $l \in \{1,\dots,m\}$ tel que $\mathrm{W}_j \subseteq \mathrm{V}_l$. On a donc $\mathrm{V}_i \subseteq \mathrm{V}_l$, ce qui implique $l = i$, puis $\mathrm{V}_i = \mathrm{W}_j$. Par conséquent, j est déterminé par i, et l'application $i \mapsto j$ ainsi définie est bijective. □

En conclusion, on a deux descriptions possibles d'un ensemble algébrique affine $\mathrm{V} \subseteq \mathbf{A}^n$: ou bien comme une intersection :

$$\mathrm{V} = \mathbf{V}(\mathrm{P}_1) \cap \cdots \cap \mathbf{V}(\mathrm{P}_r), \quad \mathrm{P}_1,\dots,\mathrm{P}_r \in k[\mathrm{X}_1,\dots,\mathrm{X}_n],$$

ou bien comme une réunion :

$$\mathrm{V} = \mathrm{V}_1 \cup \cdots \cup \mathrm{V}_m$$

avec $\mathbf{I}(\mathrm{V}_1),\dots,\mathbf{I}(\mathrm{V}_m)$ des idéaux premiers (uniquement déterminés) de $k[\mathrm{X}_1,\dots,\mathrm{X}_n]$.

1.4. Le théorème des zéros de Hilbert

Désormais, on suppose que le corps k est algébriquement clos.

On a vu que l'application $\mathrm{V} \mapsto \mathbf{I}(\mathrm{V})$ est injective lorsque restreinte aux ensembles algébriques affines. En revanche, l'application $\mathrm{I} \mapsto \mathbf{V}(\mathrm{I})$ n'est pas injective : étant donné $\mathrm{P} \in k[\mathrm{X}_1,\dots,\mathrm{X}_n]$, on a $\mathbf{V}(\mathrm{P}^m) = \mathbf{V}(\mathrm{P})$ pour tout entier $m \geqslant 1$.

Intéressons-nous à l'image de $\mathrm{V} \mapsto \mathbf{I}(\mathrm{V})$. Il existe des idéaux de $k[\mathrm{X}_1,\dots,\mathrm{X}_n]$ qui ne sont pas de la forme $\mathbf{I}(\mathrm{V})$, avec V un ensemble algébrique affine de $\mathbf{A}^n$. En effet, si P est un polynôme tel que $\mathrm{P}^m \in \mathbf{I}(\mathrm{V})$ pour un certain entier $m \geqslant 1$, alors on a $\mathrm{P} \in \mathbf{I}(\mathrm{V})$. Ainsi par exemple, l'idéal (X_1^2) n'est pas de la forme $\mathbf{I}(\mathrm{V})$ pour $\mathrm{V} \subseteq \mathbf{A}^n$.

Définition 1.12. — (1) Un idéal I de $k[\mathrm{X}_1,\dots,\mathrm{X}_n]$ est dit *radical* si, pour tout polynôme $\mathrm{P} \in k[\mathrm{X}_1,\dots,\mathrm{X}_n]$ et tout entier $m \geqslant 1$ tels que $\mathrm{P}^m \in \mathrm{I}$, on a $\mathrm{P} \in \mathrm{I}$.

(2) Soit I un idéal de $k[\mathrm{X}_1,\dots,\mathrm{X}_n]$. L'ensemble :

$$\sqrt{\mathrm{I}} = \{\mathrm{P} \in k[\mathrm{X}_1,\dots,\mathrm{X}_n] \mid \text{il existe un } m \geqslant 1 \text{ tel que } \mathrm{P}^m \in \mathrm{I}\}$$

est un idéal radical de $k[\mathrm{X}_1,\dots,\mathrm{X}_n]$, appelé le *radical* de I.

Remarque 1.13. — (1) L'idéal $\sqrt{\mathrm{I}}$ est l'image réciproque par le morphisme de k-algèbres :

$$k[\mathrm{X}_1,\dots,\mathrm{X}_n] \to k[\mathrm{X}_1,\dots,\mathrm{X}_n]/\mathrm{I}$$

de l'ensemble des éléments nilpotents de la k-algèbre $k[\mathrm{X}_1,\dots,\mathrm{X}_n]/\mathrm{I}$.

(2) Tout idéal premier est radical.

On peut maintenant énoncer le théorème des zéros de Hilbert.

***Théorème 1.14* (Théorème des zéros de Hilbert)**. — *Si* I *est un idéal de* $k[\mathrm{X}_1,\dots,\mathrm{X}_n]$, *l'idéal* $\mathbf{I}(\mathbf{V}(\mathrm{I}))$ *est égal au radical de* I.

Remarque 1.15. — En d'autres termes, si I est engendré par $\mathrm{P}_1,\dots,\mathrm{P}_r$ et si un polynôme Q s'annule sur $\mathrm{V} = \mathbf{V}(\mathrm{P}_1,\dots,\mathrm{P}_r)$, alors il y a des polynômes $\mathrm{A}_1,\dots,\mathrm{A}_r$ et un entier $m \geqslant 1$ tels que $\mathrm{Q}^m = \mathrm{A}_1\mathrm{P}_1 + \cdots + \mathrm{A}_r\mathrm{P}_r$.

Exemple 1.16. — Si $n = 1$, l'idéal I est engendré par un seul polynôme $\mathrm{P} \in k[\mathrm{X}]$. Si Q s'annule sur $\mathbf{V}(\mathrm{P})$, c'est-à-dire en chacune des racines de P dans k, alors il y a un $\mathrm{A} \in k[\mathrm{X}]$ et $m \geqslant 1$ tels que $\mathrm{Q}^m = \mathrm{AP}$.

Théorème 1.17. — **(Première variante du théorème des zéros de Hilbert)**. *Si* I *est un idéal propre de* $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$*, alors* $\mathbf{V}(\mathrm{I})$ *est non vide.*

Proposition 1.18. — *Les théorèmes 1.17 et 1.14 sont équivalents.*

Démonstration. — Soit I un idéal propre de $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, et écrivons $\mathbf{I}(\mathbf{V}(\mathrm{I})) = \sqrt{\mathrm{I}}$. Si $\mathbf{V}(\mathrm{I})$ était vide, on obtiendrait $\sqrt{\mathrm{I}} = k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, ce qui impliquerait $1 \in \mathrm{I}$: contradiction.

Inversement, soit I un idéal de $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. Alors $\sqrt{\mathrm{I}}$ est inclus dans $\mathbf{I}(\mathbf{V}(\mathrm{I}))$, car ce dernier contient I et est radical. Soient $\mathrm{P}_1, \ldots, \mathrm{P}_r$ des polynômes engendrant I, et soit un polynôme $\mathrm{G} \in \mathbf{I}(\mathbf{V}(\mathrm{I}))$. Notons J l'idéal $(\mathrm{P}_1, \ldots, \mathrm{P}_r, \mathrm{YG} - 1)$ de $k[\mathrm{X}_1, \ldots, \mathrm{X}_n, \mathrm{Y}]$. Supposons que $\mathbf{V}(\mathrm{J})$ est non vide et fixons un point $(x_1, \ldots, x_n, y) \in \mathbf{V}(\mathrm{J}) \subseteq \mathbf{A}^{n+1}$. On a :

$$\mathrm{P}_1(x_1, \ldots, x_n) = \cdots = \mathrm{P}_r(x_1, \ldots, x_n) = 0, \quad y\mathrm{G}(x_1, \ldots, x_n) = 1.$$

Ainsi on a $x = (x_1, \ldots, x_n) \in \mathbf{V}(\mathrm{I})$ et donc $\mathrm{G}(x) = 0$, ce qui contredit la dernière égalité. Par conséquent $\mathbf{V}(\mathrm{J})$ est vide, ce dont on déduit par hypothèse que J est égal à $k[\mathrm{X}_1, \ldots, \mathrm{X}_n, \mathrm{Y}]$ tout entier. Il y a donc des polynômes $\mathrm{A}_1, \ldots, \mathrm{A}_r, \mathrm{B} \in k[\mathrm{X}_1, \ldots, \mathrm{X}_n, \mathrm{Y}]$ tels que :

$$1 = \sum_{i=1}^{r} \mathrm{A}_i(\mathrm{X}_1, \ldots, \mathrm{X}_n, \mathrm{Y})\mathrm{P}_i + \mathrm{B}(\mathrm{X}_1, \ldots, \mathrm{X}_n, \mathrm{Y})(\mathrm{YG} - 1).$$

En remplaçant Y par $1/\mathrm{G}$ et en chassant les dénominateurs, on trouve :

$$\mathrm{G}^m = \sum_{i=1}^{r} \widetilde{\mathrm{A}}_i \mathrm{P}_i$$

pour un entier $m \geqslant 1$ assez grand, avec $\widetilde{\mathrm{A}}_1, \ldots, \widetilde{\mathrm{A}}_r \in k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. □

On introduit une seconde variante.

Théorème 1.19. — **(Seconde variante du théorème des zéros de Hilbert)**. *Soit* L *une extension de* k *qui est de type fini comme* k*-algèbre. Alors* L *est de degré* 1 *sur* k*.*

Proposition 1.20. — *Les théorèmes 1.19 et 1.17 sont équivalents.*

Démonstration. — Soit L une extension de k de type fini comme k-algèbre. Il y a un entier $n \geqslant 1$ et un idéal maximal I de $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ tel que L soit isomorphe comme k-algèbre au quotient de $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ par I. D'après le théorème 1.17, on a $\mathbf{V}(\mathrm{I}) \neq \varnothing$. Soit $a = (a_1, \ldots, a_n) \in \mathbf{V}(\mathrm{I})$ et soit $\mathfrak{m}_a$ l'idéal maximal de $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ qui lui est associé par (1.3). On a :

$$\mathrm{I} \subseteq \mathbf{I}(\mathbf{V}(\mathrm{I})) \subseteq \mathrm{I}(\{a\}) = \mathfrak{m}_a.$$

Donc $\mathrm{I} = \mathfrak{m}_a$, et par conséquent L est isomorphe à $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]/\mathfrak{m}_a \simeq k$.

Inversement, soit I un idéal propre de $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. Comme $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ est noethérien, il y a un idéal maximal $\mathfrak{m}$ contenant I. Quitte à remplacer I par $\mathfrak{m}$, on peut supposer I maximal. Alors la k-algèbre de type fini $\mathrm{L} = k[\mathrm{X}_1, \ldots, \mathrm{X}_n]/\mathrm{I}$ est un corps qui, d'après le théorème 1.19, est isomorphe à k. Pour chaque $i \in \{1, \ldots, n\}$, notons a_i l'image de X_i dans k, et écrivons $a = (a_1, \ldots, a_n)$ et $\mathfrak{m}_a = (\mathrm{X}_1 - a_1, \ldots, \mathrm{X}_n - a_n)$, qui est un idéal maximal de $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. On a $\mathfrak{m}_a \subseteq \mathrm{I}$, donc $\mathfrak{m}_a = \mathrm{I}$ et $a \in \mathbf{V}(\mathrm{I})$. □

Corollaire 1.21. — *Les applications* $\mathbf{V}$ *et* $\mathbf{I}$ *induisent des correspondances bijectives :*

(1) *entre ensembles algébriques affines de* $\mathbf{A}^n$ *et idéaux radicaux de* $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ *;*
(2) *entre ensembles algébriques affines irréductibles de* $\mathbf{A}^n$ *et idéaux premiers de* $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ *;*

(3) *entre points de* $\mathbf{A}^n$ *et idéaux maximaux de* $k[\mathrm{X}_1, \dots, \mathrm{X}_n]$.

Remarque 1.22. — Jusqu'à présent, on n'a pas utilisé le fait que le corps k est algébriquement clos. C'est pour prouver le théorème 1.19 qu'on en a besoin. Plus précisément, la proposition 1.23 jointe au fait que k est algébriquement clos entraînent le théorème 1.19.

Proposition 1.23. — *Soit* K *un corps, et soit* L *une extension de* K *qui est de type fini comme* K*-algèbre. Alors* L *est finie sur* K.

Démonstration. — On écrit $\mathrm{L} = \mathrm{K}[v_1, \dots, v_n]$, avec $v_1, \dots, v_n \in \mathrm{L}$, et on raisonne par récurrence sur n.

Si $n = 1$, on a $\mathrm{L} = \mathrm{K}[v]$. Comme L est un corps, v est algébrique sur K donc L est finie sur K.

Supposons maintenant que $n \geqslant 2$ et posons $\mathrm{F} = \mathrm{K}(v_n)$, de sorte que $\mathrm{L} = \mathrm{F}[v_1, \dots, v_{n-1}]$. Par hypothèse de récurrence, L est finie sur F, et il reste à prouver que F est finie sur K, c'est-à-dire que $v = v_n$ est algébrique sur K. Supposons le contraire. Pour tout $i \in \{1, \dots, n-1\}$, il y a un polynôme $\mathrm{P}_i \in \mathrm{F}[\mathrm{T}]$ non nul tel que $\mathrm{P}_i(v_i) = 0$. Soit $a \in \mathrm{K}[v]$ un dénominateur commun à tous les coefficients non nuls des P_i. Alors av_i est *entier* sur $\mathrm{K}[v]$ pour tout $i \leqslant n-1$, c'est-à-dire racine d'un polynôme Q_i unitaire à coefficients dans $\mathrm{K}[v]$. On en déduit que, pour tout $f \in \mathrm{F} \subseteq \mathrm{L} = \mathrm{K}[v_1, \dots, v_{n-1}, v]$, il existe un entier $m \geqslant 1$ tel que $a^m f$ soit entier sur $\mathrm{K}[v]$. Or $\mathrm{K}[v]$ est intégralement clos dans F, donc $a^m f \in \mathrm{K}[v]$. On en déduit que $\mathrm{F} = \mathrm{K}[v, a^{-1}]$.

Soit $b \in \mathrm{K}[v]$ premier à a. Choisissant $f = 1/b$, il y a un $m \geqslant 1$ tel que $a^m/b \in \mathrm{K}[v]$. Ecrivant $a^m = bc$ pour un $c \in \mathrm{K}[v]$, on contredit le fait que b est premier à a. □

Remarque 1.24. — Pour une autre preuve du théorème des zéros de Hilbert, voir ici :

`http://www.math.tau.ac.il/~bernstei/Unpublished_texts/Unpublished_list.html`

Voici une première application du théorème des zéros de Hilbert pour prouver qu'un ensemble algébrique affine est irréductible.

Proposition 1.25. — *Soit* P *un polynôme irréductible de* $k[\mathrm{X}_1, \dots, \mathrm{X}_n]$. *L'ensemble algébrique affine* $\mathbf{V}(\mathrm{P})$ *est irréductible.*

Démonstration. — Il suffit de montrer que l'idéal (P) est premier. Une fois que ce sera fait, on en déduira que $\mathbf{I}(\mathbf{V}(\mathrm{P})) = \sqrt{(\mathrm{P})} = (\mathrm{P})$ est premier, donc que $\mathbf{V}(\mathrm{P})$ est irréductible.

Supposons que (P) n'est pas premier, et soient F et G deux polynômes qui ne sont pas dans (P) mais tels que $\mathrm{FG} \in (\mathrm{P})$. Le produit FG est divisible par P, et comme $k[\mathrm{X}_1, \dots, \mathrm{X}_n]$ est factoriel et que P est irréductible, on en déduit que P divise soit F, soit G : contradiction. □

Exemple 1.26. — Pour un contre-exemple à cette proposition lorsque k est le corps des nombres réels, voir la feuille d'exercices.

1.5. L'algèbre des fonctions régulières

Ici encore, le corps k est supposé algébriquement clos. Si V est un ensemble algébrique affine de $\mathbf{A}^n$, on pose :

$$k[\mathrm{V}] = k[\mathrm{X}_1, \dots, \mathrm{X}_n]/\mathbf{I}(\mathrm{V})$$

qu'on appelle l'*algèbre des fonctions régulières* sur V. Comme l'idéal $\mathbf{I}(\mathrm{V})$ est radical, $k[\mathrm{V}]$ est une k-algèbre de type fini *réduite*, c'est-à-dire sans élément nilpotent autre que 0.

Exemple 1.27. — On a $k[\mathbf{A}^n] = k[\mathrm{X}_1, \dots, \mathrm{X}_n]$.

Proposition 1.28. — *Soit* A *une* k*-algèbre de type fini réduite. Il existe un entier* $n \geqslant 1$ *et un ensemble algébrique affine* $\mathrm{V} \subseteq \mathbf{A}^n$ *tels que* $\mathrm{A} \simeq k[\mathrm{V}]$.

Démonstration. — Comme A est de type fini, il y a un $n \geqslant 1$ et un morphisme surjectif de k-algèbres :

$$\varphi : k[\mathrm{X}_1, \ldots, \mathrm{X}_n] \to \mathrm{A}.$$

Son noyau I est un idéal, qui est radical parce que A est réduite. Posons $\mathrm{V} = \mathbf{V}(\mathrm{I}) \subseteq \mathbf{A}^n$. Alors $\mathbf{I}(\mathrm{V}) = \mathrm{I}$ d'après le théorème des zéros de Hilbert, et donc $k[\mathrm{V}] \simeq \mathrm{A}$. □

Définition 1.29. — Une *fonction régulière* sur V est une fonction φ de V dans k telle qu'il y ait un polynôme $\mathrm{P} \in k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ pour lequel $\varphi(a) = \mathrm{P}(a)$ pour tout $a \in \mathrm{V}$.

Etant donné $\mathrm{P} \in k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, on note $\widetilde{\mathrm{P}}$ la fonction régulière $a \mapsto \mathrm{P}(a)$ sur V. L'application $\mathrm{P} \mapsto \widetilde{\mathrm{P}}$ induit un morphisme injectif de k-algèbres de $k[\mathrm{V}]$ dans la k-algèbre des fonctions de V dans k, permettant d'identifier un élément de $k[\mathrm{V}]$ à une fonction de V dans k.

1.6. Applications régulières entre ensembles algébriques affines

Soient de entiers $n, m \geqslant 1$ et soient $\mathrm{V} \subseteq \mathbf{A}^n$ et $\mathrm{W} \subseteq \mathbf{A}^m$ des ensembles algébriques affines.

Définition 1.30. — Une *application régulière* (ou *morphisme d'ensembles algébriques affines*) de V dans W est une application $\varphi : \mathrm{V} \to \mathrm{W}$ telle que chaque fonction coordonnée $\varphi_j : \mathrm{V} \to \mathbf{A}^1$, $j \in \{1, \ldots, m\}$, soit une fonction régulière sur V. On note $\mathrm{Hom}(\mathrm{V}, \mathrm{W})$ l'ensemble des morphismes de V dans W.

Exemple 1.31. — (1) Soit $\mathrm{V} = \mathbf{A}^1$ et soit $\mathrm{W} = \mathbf{V}(\mathrm{Y} - \mathrm{X}^2) \subseteq \mathbf{A}^2$. Alors $t \mapsto (t, t^2)$ est une application régulière de V vers W.

(2) Les applications affines de $\mathbf{A}^n$ dans $\mathbf{A}^m$ sont des applications régulières.

(3) En particulier, les projections sont des applications régulières.

(4) L'application $\varphi : t \mapsto (t^2 - 1, t(t^2 - 1))$ de $\mathbf{A}^1$ dans $\mathbf{V}(\mathrm{Y}^2 - \mathrm{X}^3 - \mathrm{X}^2)$ est une application régulière (non injective).

(5) La composée de deux applications régulières est une application régulière.

Etant donné une application régulière $\varphi \in \mathrm{Hom}(\mathrm{V}, \mathrm{W})$, on note φ^* l'application de $k[\mathrm{W}]$ dans $k[\mathrm{V}]$ définie par $f \mapsto f \circ \varphi$. C'est un morphisme de k-algèbres.

Théorème 1.32. — *L'application $\varphi \mapsto \varphi^*$ est une bijection de* $\mathrm{Hom}(\mathrm{V}, \mathrm{W})$ *dans l'ensemble :*

$$\mathrm{Hom}_k(k[\mathrm{W}], k[\mathrm{V}])$$

des morphismes de k-algèbre de $k[\mathrm{W}]$ dans $k[\mathrm{V}]$.

Démonstration. — Soit $\alpha : k[\mathrm{W}] \to k[\mathrm{V}]$ un morphisme de k-algèbres. Si $a \in \mathrm{V}$, on lui associe l'idéal maximal $\mathfrak{m}_a \supseteq \mathbf{I}(\mathrm{V})$. Ecrivons le diagramme :

$$\begin{array}{ccc} k[\mathrm{Y}_1, \ldots, \mathrm{Y}_m] & & k[\mathrm{X}_1, \ldots, \mathrm{X}_n] \\ {\scriptstyle \pi_{\mathrm{W}}}\downarrow & & \downarrow{\scriptstyle \pi_{\mathrm{V}}} \\ k[\mathrm{W}] & \xrightarrow[\alpha]{} & k[\mathrm{V}] \end{array}$$

où π_{V} désigne le morphisme surjectif naturel de $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ dans $k[\mathrm{V}]$. L'idéal $\mathrm{J} = \pi_{\mathrm{W}}^{-1}(\alpha^{-1}(\pi_{\mathrm{V}}(\mathfrak{m}_a)))$ de $k[\mathrm{Y}_1, \ldots, \mathrm{Y}_m]$ contient $\mathbf{I}(\mathrm{W})$. Montrons qu'il est maximal. D'abord, $\pi_{\mathrm{V}}(\mathfrak{m}_a)$ est maximal dans $k[\mathrm{V}]$. L'idéal J est le noyau de la composée $\mathrm{ev}_a \circ \alpha \circ \pi_{\mathrm{W}}$, où ev_a désigne le morphisme d'évaluation au point a. L'image de ce morphisme étant un corps, son noyau est un idéal maximal.

D'après le théorème des zéros de Hilbert, il existe un unique point $b = (b_1, \ldots, b_m) \in \mathrm{W}$ tel que J soit égal à l'idéal maximal $\mathfrak{m}_b = (\mathrm{Y}_1 - b_1, \ldots, \mathrm{Y}_m - b_m)$. L'application $a \mapsto b$ ainsi définie est notée φ. On va montrer qu'elle est régulière.

Pour chaque $j \in \{1, \dots, m\}$, notons φ_j la fonction $a \mapsto b_j$. Le morphisme π_{V} étant surjectif, on choisit un polynôme F_j tel que $\alpha(\pi_{\mathrm{W}}(\mathrm{Y}_j)) = \pi_{\mathrm{V}}(\mathrm{F}_j)$. Montrons que φ_j est la fonction régulière associée à F_j, c'est-à-dire que b_j est égal à $\mathrm{F}_j(a)$. Le point b est caractérisé par la propriété :

$$\mathrm{P}(b) = 0 \quad \Leftrightarrow \quad \alpha \circ \pi_{\mathrm{W}}(\mathrm{P})(a) = 0 \tag{1.4}$$

pour tout $\mathrm{P} \in k[\mathrm{Y}_1, \dots, \mathrm{Y}_m]$. Choisissons $\mathrm{P} = \mathrm{Y}_j - b_j$. Alors on a $\mathrm{P}(b) = 0$ donc $\alpha \circ \pi_{\mathrm{W}}(\mathrm{Y}_j - b_j)(a) = 0$, ce qui s'écrit $\mathrm{F}_j(a) = b_j$. Finalement, on a bien $\varphi^* = \alpha$.

Pour l'injectivité, supposons qu'il y ait des applications régulières φ, ψ telles que $\varphi^* = \psi^*$. On a donc $\varphi^*(\pi_{\mathrm{W}}(\mathrm{Y}_j)) = \psi^*(\pi_{\mathrm{W}}(\mathrm{Y}_j))$ pour tout $j \in \{1, \dots, m\}$. Mais, d'après ce qui précède, on a $\varphi^*(\pi_{\mathrm{W}}(\mathrm{Y}_j)) = \varphi_j \in k[\mathrm{V}]$. Donc φ et ψ ont les mêmes fonctions coordonnées, ce qui entraîne $\varphi = \psi$. □

Remarque 1.33. — On traduit ce résultat en disant que $\mathrm{V} \mapsto k[\mathrm{V}]$ est une *anti-équivalence* entre la catégorie des ensembles algébriques affines et la catégorie des k-algèbres de type fini réduites. Cela signifie que l'étude des uns équivaut à celle des autres : les propriétés géométriques des ensembles algébriques affines se traduisent en des propriétés algébriques des k-algèbres de type fini réduites, et inversement.

Définition 1.34. — Des ensembles algébriques affines $\mathrm{V} \subseteq \mathbf{A}^n$ et $\mathrm{W} \subseteq \mathbf{A}^m$ sont dits *isomorphes* s'il y a des applications régulières $\varphi \in \mathrm{Hom}(\mathrm{V}, \mathrm{W})$ et $\psi \in \mathrm{Hom}(\mathrm{W}, \mathrm{V})$ telles que $\varphi \circ \psi = \mathrm{id}_{\mathrm{W}}$ et $\psi \circ \varphi = \mathrm{id}_{\mathrm{V}}$. On dit alors que φ est un *isomorphisme* de V vers W.

Attention : un isomorphisme n'est pas la même chose qu'un morphisme bijectif : il y a des morphismes bijectifs qui ne sont pas des isomorphismes parce que leur réciproque n'est pas une application régulière.

Proposition 1.35. — *Une application régulière $\varphi : \mathrm{V} \to \mathrm{W}$ est un isomorphisme si et seulement si φ^* est un isomorphisme de k-algèbres. En particulier, deux ensembles algébriques affines* V *et* W *sont isomorphes si et seulement si $k[\mathrm{V}]$ et $k[\mathrm{W}]$ sont des k-algèbres isomorphes.*

Exemple 1.36. — (1) On pose $\mathrm{V} = \mathbf{V}(\mathrm{Y} - \mathrm{X}^2) \subseteq \mathbf{A}^2$. Alors $\varphi : t \mapsto (t, t^2)$ est un isomorphisme de $\mathbf{A}^1$ vers V, dont la réciproque est la projection $(x, y) \mapsto x$.

(2) Soit $\mathrm{V} = \mathbf{V}(\mathrm{Y}^2 - \mathrm{X}^3) \subseteq \mathbf{A}^2$. Alors $\varphi : t \mapsto (t^2, t^3)$ est un morphisme bijectif de $\mathbf{A}^1$ vers V. Mais ce n'est pas un isomorphisme, car φ^* a pour image $k[\mathrm{T}^2, \mathrm{T}^3] \subsetneq k[\mathrm{T}]$ et n'est donc pas bijective.

Si E est une partie de $\mathbf{A}^n$, on note $\overline{\mathrm{E}}$ l'ensemble algébrique affine $\mathbf{V}(\mathbf{I}(\mathrm{E}))$. (Il s'agit de l'adhérence de E dans $\mathbf{A}^n$ au sens de la topologie de Zariski.)

Proposition 1.37. — *Soit $\mathrm{V} \subseteq \mathbf{A}^n$ un ensemble algébrique affine, et soit $\varphi : \mathrm{V} \to \mathbf{A}^m$ une application régulière. Si* V *est irréductible, alors $\overline{\varphi(\mathrm{V})}$ est irréductible.*

Démonstration. — Posons $\mathrm{W} = \overline{\varphi(\mathrm{V})}$ et soit $f \in \mathrm{Ker}(\varphi^*)$, où φ^* désigne le morphisme de k-algèbres de $k[\mathrm{W}]$ dans $k[\mathrm{V}]$. Ecrivant $f = \mathrm{F} \bmod \mathbf{I}(\mathrm{W})$ pour un $\mathrm{F} \in k[\mathrm{Y}_1, \dots, \mathrm{Y}_m]$, le polynôme F s'annule en tout point de $\varphi(\mathrm{V})$, donc en tout point de W. Aussi le morphisme φ^* est-il injectif, et la k-algèbre $k[\mathrm{W}]$, se plongeant dans une k-algèbre intègre, est elle-même intègre. Par conséquent, W est irréductible. □

Chapitre 2. Dimension et points singuliers

Désormais, nous appellerons *variété affine* un ensemble algébrique affine irréductible.

2.1. Dimension

Soit $\mathrm{V} \subseteq \mathbf{A}^n$ une variété affine. Comme l'anneau $k[\mathrm{V}]$ est intègre, on peut former son corps de fractions, noté $k(\mathrm{V})$. En tant qu'extension de k, il est engendré par un nombre fini d'éléments : les images x_i des X_i par le morphisme :

$$\pi_{\mathrm{V}} : k[\mathrm{X}_1, \ldots, \mathrm{X}_n] \to k[\mathrm{V}] \subseteq k(\mathrm{V}).$$

En général, l'extension $k(\mathrm{V})$ est transcendante sur k. (En revanche, les x_i ne sont pas forcément tous transcendants sur k : penser par exemple à $\mathbf{V}(\mathrm{Y} - \mathrm{X}^2, \mathrm{Z})$ dans $\mathbf{A}^3$.)

Définition 2.1. — Soit K une extension de k.

(1) Une partie S de K est *algébriquement libre sur* k si, pour tout $m \geqslant 1$, tous $s_1, \ldots, s_m \in \mathrm{S}$ et tout $\mathrm{P} \in k[\mathrm{X}_1, \ldots, \mathrm{X}_m]$, on a $\mathrm{P}(s_1, \ldots, s_m) = 0$ si et seulement si $\mathrm{P} = 0$.

(2) Une *base de transcendance* de K sur k est une partie $\mathrm{B} \subseteq \mathrm{K}$ algébriquement libre et telle que K soit algébrique sur $k(\mathrm{B})$.

Remarque 2.2. — Contrairement aux bases d'espaces vectoriels, une base de transcendance B n'est pas toujours génératrice, c'est-à-dire que $k(\mathrm{B})$ n'est pas toujours égale à K. Si K admet une base de transcendance B telle que $k(\mathrm{B}) = \mathrm{K}$, on dit que K est *purement transcendante* sur k.

Proposition 2.3. — *Soit* S *une partie de* K *telle que* K *soit algébrique sur* $k(\mathrm{S})$.

(1) *Les bases de transcendance de* K/k *incluses dans* S *sont les parties de* S *algébriquement libres maximales.*

(2) *Supposons que* S *soit finie. Alors toutes les bases de transcendance de* K/k *sont finies et de même cardinal, appelé le* degré de transcendance *de* K/k *et noté* $\mathrm{degtr}(\mathrm{K}/k)$.

Définition 2.4. — On appelle *dimension* d'une variété affine $\mathrm{V} \subseteq \mathbf{A}^n$ le degré de transcendance de $k(\mathrm{V})$ sur k.

Exemple 2.5. — Soit $\mathrm{V} = \mathbf{V}(\mathrm{X}^2 + \mathrm{Y}^2 - 1) \subseteq \mathbf{A}^2$. Alors $k(\mathrm{V})$ est engendré par x, y sur k. Si x et y étaient tous deux algébriques sur k, alors $k(\mathrm{V})$ serait algébrique sur k, donc isomorphe à k, et V serait réduite à un point, ce qui n'est pas le cas. Ainsi x est transcendant sur k et y est une racine du polynôme $\mathrm{T}^2 + x^2 - 1$ à coefficients dans $k(x)$. Donc $\{x\}$ est une base de transcendance et le degré de transcendance de $k(\mathrm{V})$ sur k est égal à 1.

Exemple 2.6. — (1) On a $k(\mathbf{A}^n) = k(\mathrm{X}_1, \ldots, \mathrm{X}_n)$ donc $\dim(\mathbf{A}^n) = n$.

(2) Si $\mathrm{P} \in k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ est irréductible, alors $\mathbf{V}(\mathrm{P})$ est une variété affine de dimension $n-1$. En effet, quitte à renuméroter les variables, on peut supposer que X_n apparaît dans P. Si Q est un polynôme de $k[\mathrm{X}_1, \ldots, \mathrm{X}_{n-1}]$ tel que $\mathrm{Q}(x_1, \ldots, x_{n-1}) = 0$ dans $k(\mathbf{V}(\mathrm{P}))$, alors $\mathrm{Q}(a)$ est égal à $\mathrm{Q}(x_1, \ldots, x_{n-1})(a) = 0$ pour tout $a \in \mathbf{V}(\mathrm{P})$, donc $\mathrm{Q} \in \mathbf{I}(\mathbf{V}(\mathrm{P})) = (\mathrm{P})$. Ainsi P, de degré $\geqslant 1$ en X_n, divise Q, de degré $\leqslant 0$ en X_n, donc $\mathrm{Q} = 0$. Par conséquent $\{x_1, \ldots, x_{n-1}\}$ est algébriquement libre sur k, et x_n est algébrique sur $k(x_1, \ldots, x_{n-1})$ puisque $\mathrm{P}(x_1, \ldots, x_n) = 0$.

Proposition 2.7. — *Une variété affine* $\mathrm{V} \subseteq \mathbf{A}^n$ *est de dimension* 1 *si et seulement s'il existe* $f \in k(\mathrm{V})$ *transcendante sur* k *telle que* $k(\mathrm{V})$ *soit algébrique sur* $k(f)$.

Si tel est le cas, comme k est algébriquement clos, il suffit de choisir n'importe quel $f \notin k$.

2.2. Singularités

Soit $\mathrm{V} \subseteq \mathbf{A}^n$ une variété affine de dimension d. Choisissons des polynômes $\mathrm{F}_1, \dots, \mathrm{F}_r$ engendrant l'idéal $\mathbf{I}(\mathrm{V})$ dans $k[\mathrm{X}_1, \dots, \mathrm{X}_n]$. Soit F l'application régulière de $\mathbf{A}^n$ dans $\mathbf{A}^r$ définie par $\mathrm{F}(a) = (\mathrm{F}_1(a), \dots, \mathrm{F}_r(a))$ pour $a \in \mathbf{A}^n$. L'ensemble des points où elle s'annule est V. On fixe un point $a \in \mathrm{V}$ et l'on forme la matrice :

$$\mathrm{J}_a\mathrm{F} = \begin{pmatrix} \frac{\partial \mathrm{F}_1}{\partial \mathrm{X}_1}(a) & \dots & \frac{\partial \mathrm{F}_1}{\partial \mathrm{X}_n}(a) \\ \vdots & & \vdots \\ \frac{\partial \mathrm{F}_r}{\partial \mathrm{X}_1}(a) & \dots & \frac{\partial \mathrm{F}_r}{\partial \mathrm{X}_n}(a) \end{pmatrix}$$

de $\mathrm{M}_{r,n}(k)$, appelée *matrice jacobienne* de F en a.

Définition 2.8. — Le point $a \in \mathrm{V}$ est dit *régulier* si le rang de $\mathrm{J}_a\mathrm{F}$ est égal à $n - d$. Dans le cas contraire, il est dit *singulier*. Une variété affine sans point singulier est dite *lisse*.

Exemple 2.9. — (1) La variété affine $\mathbf{V}(\mathrm{X}^2 + \mathrm{Y}^2 - 1)$ est lisse.
(2) La variété affine $\mathbf{V}(\mathrm{Y}^2 - \mathrm{X}^3)$ admet le point $(0, 0)$ comme unique point singulier.
(3) La variété affine $\mathbf{V}(\mathrm{X} - \mathrm{YZ}, \mathrm{Y}^2 - \mathrm{XZ}, \mathrm{Z}^2 - \mathrm{Y}) \subseteq \mathbf{A}^3$ est lisse.
(4) Etudier la lissité de $\mathbf{V}(\mathrm{Y}^2 - \mathrm{X}(\mathrm{X} - 1)(\mathrm{X} - \lambda))$ suivant les valeurs de $\lambda \in k$.

Remarque 2.10. — On peut prouver que, en général, le rang de $\mathrm{J}_a\mathrm{F}$ est $\leqslant n - d$ quel que soit le point $a \in \mathrm{V}$. Voir le théorème 2.15 et la remarque 2.18.

L'inconvénient de cette définition est qu'elle dépend *a priori* du choix des $\mathrm{F}_1, \dots, \mathrm{F}_r$. Nous allons donner une autre définition (équivalente) qui ne dépendra pas du choix des $\mathrm{F}_1, \dots, \mathrm{F}_r$.

2.3. Anneau local en un point

Soit $\mathrm{V} \subseteq \mathbf{A}^n$ une variété affine, et soit $a \in \mathrm{V}$. Tout élément $f \in k(\mathrm{V})$ peut s'écrire comme un quotient p/q, avec $p, q \in k[\mathrm{V}]$ et $q \neq 0$. Bien sûr, p et q ne sont pas uniques.

Définition 2.11. — (1) On dit que $f \in k(\mathrm{V})$ est *défini* au point $a \in \mathrm{V}$ s'il existe $p, q \in k[\mathrm{V}]$ tels que $f = p/q$ et $q(a) \neq 0$.
(2) La *valeur* de f en a, notée $f(a)$, est le quotient $p(a)q(a)^{-1} \in k$, qui est indépendant du choix de p et q.

L'ensemble :

$$\mathcal{O}_a = \{f \in k(\mathrm{V}) \mid f \text{ est défini en } a\}$$

est un sous-anneau (et même une sous-k-algèbre) de $k(\mathrm{V})$ contenant $k[\mathrm{V}]$. Si V n'est pas réduite à un point, c'est-à-dire si sa dimension est non nulle, ce n'est pas un corps et, comme k-algèbre, elle n'est pas de type fini. L'anneau $\mathcal{O}_a$ a toutefois une propriété remarquable.

Définition 2.12. — Un anneau A est dit *local* s'il n'a qu'un seul idéal maximal $\mathfrak{m}$. Le quotient $\mathrm{A}/\mathfrak{m}$ est un corps, appelé le *corps résiduel* de A.

On remarque que le complémentaire de $\mathfrak{m}$ dans A est formé des éléments inversibles de A.

Proposition 2.13. — *L'anneau $\mathcal{O}_a$ est un anneau local noethérien intègre. Son idéal maximal est l'idéal M_a formé des éléments nuls en a, et son corps résiduel est isomorphe à k.*

Démonstration. — Posons $\mathrm{A} = \mathcal{O}_a$ pour alléger les notations. L'application $f \mapsto f(a)$ est un morphisme surjectif de k-algèbres de A dans k, de noyau M_a, qui est donc un idéal maximal. On voit que les éléments du complémentaire de M_a dans A sont inversibles. Ainsi M_a est le seul idéal maximal de A, qui est donc local.

Ensuite A est intègre, car c'est un sous-anneau d'un corps. Il reste à prouver qu'il est noethérien. Soit I un idéal de A et soit $\mathrm{J} = \mathrm{I} \cap k[\mathrm{V}]$. Comme $k[\mathrm{V}]$ est noethérien (car quotient de $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ qui l'est), il existe $p_1, \ldots, p_r \in \mathrm{J}$ engendrant J. Soit maintenant $f \in \mathrm{I}$. Il y a $q \in k[\mathrm{V}]$ tel que $qf \in k[\mathrm{V}]$ et $q(a) \neq 0$. Ainsi $qf \in \mathrm{J}$ et l'on peut écrire :

$$qf = c_1 p_1 + \cdots + c_r p_r$$

avec $c_1, \ldots, c_r \in k[\mathrm{V}]$, donc $f = b_1 p_1 + \cdots + b_r p_r$ avec $b_i = c_i q^{-1} \in \mathrm{A}$ pour chaque i. Ainsi $p_1, \ldots, p_r$ engendrent l'idéal I, qui est donc de type fini. □

Corollaire 2.14. — *Pour tout $i \geqslant 0$, le quotient $\mathsf{M}_a^i/\mathsf{M}_a^{i+1}$ est un k-espace vectoriel de dimension finie.*

Démonstration. — L'idéal M_a^i est de type fini, engendré par des éléments $p_1, \ldots, p_r$. Donc $\mathsf{M}_a^i/\mathsf{M}_a^{i+1}$ est de dimension finie $\leqslant r$, engendré par les images de $p_1, \ldots, p_r$ modulo M_a^{i+1}. □

Théorème 2.15. — *Pour tout $a \in \mathrm{V}$, la dimension du k-espace vectoriel $\mathsf{M}_a/\mathsf{M}_a^2$ est supérieure ou égale à $\dim(\mathrm{V})$, avec égalité si et seulement si a est régulier.*

Remarque 2.16. — Comme en géométrie différentielle, le dual algébrique de $\mathsf{M}_a/\mathsf{M}_a^2$ s'appelle l'*espace tangent* à V en a. On le note $\mathrm{T}_a\mathrm{V}$.

Démonstration. — On va montrer que $\mathrm{T}_a\mathrm{V}$ est isomorphe au noyau de $\mathrm{J}_a\mathrm{F}$. Ceci prouvera que le rang de $\mathrm{J}_a\mathrm{F}$ ne dépend pas du choix de $\mathrm{F}_1, \ldots, \mathrm{F}_r$ et que $\dim(\mathsf{M}_a/\mathsf{M}_a^2) = \dim(\mathrm{V})$ si et seulement si a est régulier. Ce noyau est le sous-espace vectoriel de k^n formé des $b = (b_1, \ldots, b_n)$ tels que :

$$\sum_{i=1}^{n} b_i \frac{\partial \mathrm{F}_j}{\partial \mathrm{X}_i}(a) = 0, \quad j \in \{1, \ldots, r\}. \tag{2.1}$$

Etant donnés un tel b et $f \in \mathcal{O}_a$, qu'on écrit $f = p/q$ avec $p, q \in k[\mathrm{V}]$ et $q(a) \neq 0$, on pose :

$$\mathrm{D}_b(f) = \mathrm{J}_a \left(\frac{\mathrm{P}}{\mathrm{Q}} \right)(b) \tag{2.2}$$

où P et Q sont n'importe quels polynômes de $k[\mathrm{X}_1, \cdots, \mathrm{X}_n]$ tels que $p = \mathrm{P} \bmod \mathbf{I}(\mathrm{V})$ et $q = \mathrm{Q} \bmod \mathbf{I}(\mathrm{V})$. Vérifions que la quantité (2.2) ne dépend pas du choix de P et Q. Il suffit pour cela de montrer que, pour tout $\mathrm{R} \in \mathbf{I}(\mathrm{V})$, on a $\mathrm{J}_a\mathrm{R}(b) = 0$. En effet, si l'on écrit $\mathrm{R} = \mathrm{F}_1\mathrm{A}_1 + \cdots + \mathrm{F}_r\mathrm{A}_r$, on a :

$$\mathrm{J}_a\mathrm{R}(b) = \sum_{i=1}^{n} \sum_{j=1}^{r} b_i \left(\mathrm{F}_j(a) \frac{\partial \mathrm{A}_j}{\partial \mathrm{X}_i}(a) + \frac{\partial \mathrm{F}_j}{\partial \mathrm{X}_i}(a) \mathrm{A}_j(a) \right)$$

qui est bien égal à 0 grâce à (2.1) et au fait que $\mathrm{F}_1(a) = \cdots = \mathrm{F}_r(a) = 0$. Ceci définit une forme linéaire D_b sur $\mathcal{O}_a$, et on vérifie qu'elle s'annule sur M_a^2 du fait que $\mathrm{D}_b(fg) = g(a)\mathrm{D}_b(f) + f(a)\mathrm{D}_b(g)$ pour tous $f, g \in \mathcal{O}_a$. Ainsi l'application :

$$t_b : f \bmod \mathsf{M}_a^2 \mapsto \mathrm{D}_b(f)$$

est une forme linéaire sur $\mathsf{M}_a/\mathsf{M}_a^2$. Il ne reste plus qu'à vérifier que $b \mapsto t_b$ est un isomorphisme de k-espaces vectoriels de $\mathrm{Ker}\ \mathrm{J}_a\mathrm{F}$ vers $\mathrm{T}_a\mathrm{V}$, ce qui se déduit de la formule $b_i = t_b(x_i - a_i)$, où $a = (a_1, \ldots, a_n)$ et x_i est l'image de X_i dans $\mathcal{O}_a$. Pour l'inégalité $\dim(\mathrm{T}_a\mathrm{V}) \geqslant \dim(\mathrm{V})$, voir la remarque 2.18. □

Remarque 2.17. — Une *dérivation en a* sur V est une application k-linéaire $\mathrm{D} : \mathcal{O}_a \to k$ telle que, pour tous $f, g \in \mathcal{O}_a$, on ait $\mathrm{D}(fg) = f(a)\mathrm{D}(g) + g(a)\mathrm{D}(f)$. On note $\mathrm{D}_a\mathrm{V}$ le k-espace vectoriel des dérivations en a sur V. Si $\mathrm{D} \in \mathrm{D}_a\mathrm{V}$, l'application $f \bmod \mathsf{M}_a^2 \mapsto \mathrm{D}(f)$ est une forme linéaire sur $\mathsf{M}_a/\mathsf{M}_a^2$. Inversement, si $\xi \in \mathrm{T}_a\mathrm{V}$, l'application $f \mapsto \xi(f - f(a) \bmod \mathsf{M}_a^2)$ est une dérivation en a sur V. Ces deux opérations sont des isomorphismes de k-espaces vectoriels réciproques l'un de l'autre entre $\mathrm{D}_a\mathrm{V}$ et $\mathrm{T}_a\mathrm{V}$.

Remarque 2.18. — Posons $\mathrm{K} = k(\mathrm{V})$ pour alléger les notations. Une *dérivation* sur V est une application k-linéaire $\Delta : \mathrm{K} \to \mathrm{K}$ telle qu'on ait $\Delta(fg) = f\Delta(g) + g\Delta(f)$ pour tous $f, g \in \mathrm{K}$. En s'inspirant des arguments ci-dessus, on démontre que le k-espace vectoriel $\mathrm{Der}(\mathrm{V})$ des dérivations sur V est isomorphe au noyau de la matrice :

$$\mathrm{JF} = \left(\frac{\partial \mathrm{F}_i}{\partial \mathrm{X}_j}(x_1, \dots, x_n)\right)_{1 \leqslant i \leqslant r, 1 \leqslant j \leqslant n} \in \mathrm{M}_{r,n}(k[\mathrm{V}]) \subseteq \mathrm{M}_{r,n}(\mathrm{K}).$$

Soit $a \in \mathrm{V}$, et soit s le rang de $\mathrm{J}_a\mathrm{F}$. Quitte à réordonner les lignes et les colonnes de $\mathrm{J}_a\mathrm{F}$, on peut supposer que le déterminant de la matrice :

$$\left(\frac{\partial \mathrm{F}_i}{\partial \mathrm{X}_j}(a)\right)_{1 \leqslant i,j \leqslant s} \in \mathrm{M}_s(k)$$

est non nul. Le déterminant de la matrice :

$$\left(\frac{\partial \mathrm{F}_i}{\partial \mathrm{X}_j}(x_1, \dots, x_n)\right)_{1 \leqslant i,j \leqslant s} \in \mathrm{M}_s(\mathrm{K})$$

est donc lui aussi non nul, ce qui entraîne que le rang t de JF est $\geqslant s$. On a donc :

$$\dim(\mathrm{Der}(\mathrm{V})) = n - t \leqslant n - s.$$

Il ne reste plus qu'à prouver l'égalité $\dim(\mathrm{Der}(\mathrm{V})) = \dim(\mathrm{V})$, qui provient de la théorie générale des dérivations. (Voir par exemple Morandi, *Field and Galois theory*, Theorem 23.12.)

Exemple 2.19. — Soit V la variété affine $\mathbf{V}(\mathrm{Y}^2 - \mathrm{X}^3) \subseteq \mathbf{A}^2$, et soit $(a, b) \in \mathbf{A}^2$. Au moyen de la formule de Taylor, on écrit :

$$\mathrm{X}^3 - \mathrm{Y}^2 = a^3 - b^2 + 3a^2(\mathrm{X} - a) - 2b(\mathrm{Y} - b) + 3a(\mathrm{X} - a)^2 - (\mathrm{Y} - b)^2 + (\mathrm{X} - a)^3.$$

Notons x, y les images de X, Y dans $k[\mathrm{V}]$ et supposons que $(a, b) \in \mathrm{V}$. On trouve :

$$3a^2(x - a) - 2b(y - b) = (y - b)^2 - 3a(x - a)^2 - (x - a)^3 \in \mathsf{M}_{(a,b)}^2.$$

Si $(a, b) \neq (0, 0)$, les générateurs $x - a$, $y - b$ de $\mathsf{M}_{(a,b)}$ ont donc des images liées dans $\mathsf{M}_{(a,b)}/\mathsf{M}_{(a,b)}^2$.

Supposons maintenant que $(a, b) = (0, 0)$, et supposons qu'il y a des scalaires $u, v \in k$ tels qu'on ait $ux + vy \in \mathsf{M}_{(0,0)}^2$. L'idéal $\mathsf{M}_{(0,0)}^2$ est engendré par x^2, xy, y^2, et comme y^2 est égal à x^3 il suffit de prendre x^2 et xy. Ecrivons :

$$ux + vy = x^2 f + xyg, \quad f, g \in \mathcal{O}_{(0,0)}.$$

Cela donne $v^2x^3 = (-ux + x^2f + xyg)^2$ donc $v^2x = (-u + xf + yg)^2$, et en évaluant en $(0, 0)$ on trouve $u = 0$. Par conséquent, on a $y(v - xg) = x^2 f$, donc $x^3(v - xg)^2 = x^4 f^2$. En simplifiant par x^3 et en évaluant en $(0, 0)$, on trouve $v = 0$. Ainsi $\mathsf{M}_{(0,0)}/\mathsf{M}_{(0,0)}^2$ est de dimension 2.

Remarque 2.20. — Une fonction rationnelle sur V définie en tout point de V est régulière. En effet, pour une telle fonction $f \in k(\mathrm{V})$, l'ensemble $\mathrm{J} = \{q \in k[\mathrm{V}] \mid qf \in k[\mathrm{V}]\}$ est un idéal, et cet idéal contient 1 si et seulement si f est régulière. Supposons que ce ne soit pas le cas ; J est donc inclus dans un idéal maximal $\mathfrak{m}_a$ pour un $a \in \mathrm{V}$. La fonction f étant définie en a, elle s'écrit p/q avec $p, q \in k[\mathrm{V}]$ et $q(a) \neq 0$, c'est-à-dire que $q \in \mathrm{J}$ mais $q \notin \mathfrak{m}_a$: contradiction.

2.4. Courbes algébriques affines

Une *courbe* (algébrique affine) de $\mathbf{A}^n$ est une variété affine de $\mathbf{A}^n$ de dimension 1.

Proposition 2.21. — *Soit* C *une courbe. Un point* $x \in \mathrm{C}$ *est régulier si et seulement si* $\mathsf{M}_a/\mathsf{M}_a^2$ *est un* k*-espace vectoriel de dimension* 1.

Exemple 2.22. — Si $\mathrm{C} = \mathbf{A}^1$, alors $k[\mathrm{C}] = k[\mathrm{X}]$. Pour $a \in \mathrm{C}$, l'anneau local $\mathcal{O}_a$ des $f \in k(\mathrm{C})$ définis en a est formé des fractions dans $k(\mathrm{X})$ dont le dénominateur ne s'annule pas en a. L'idéal M_a est engendré par $\mathrm{X} - a$ et M_a^2 est engendré par $(\mathrm{X} - a)^2$, donc $\mathsf{M}_a/\mathsf{M}_a^2$ est de dimension 1 sur k. Par conséquent, $\mathbf{A}^1$ est lisse.

Proposition 2.23. — *L'ensemble des points singuliers d'une courbe est fini.*

Démonstration. — Voir D. Perrin, Problème IV. □

Dans le cas des courbes, on a une autre caractérisation des points réguliers.

Définition 2.24. — Un *anneau de valuation discrète* est un anneau intègre à la fois principal et local.

Si A est un anneau de valuation discrète, on note $\mathfrak{m}$ son idéal maximal. Tout élément $t \in \mathrm{A}$ engendrant $\mathfrak{m}$ s'appelle une *uniformisante* de A.

Proposition 2.25. — (1) *Les idéaux de* A *sont exactement* (0) *et les* $\mathfrak{m}^i$, $i \geqslant 0$.
(2) *Si* t *est une uniformisante de* A, *alors* $\mathfrak{m}^i$ *est engendré par* t^i, *pour tout* $i \geqslant 0$.
(3) *L'intersection des* $\mathfrak{m}^i$, $i \geqslant 0$, *est égale à* (0).

Démonstration. — Le point (2) est immédiat. Prouvons le point (3). Soit $a \in \mathrm{A}$ appartenant à l'intersection des $\mathfrak{m}^i$, $i \geqslant 0$, et supposons que $a \neq 0$. Comme A est noethérien, la suite croissante d'idéaux $(at^{-i})_{i \geqslant 0}$ est stationnaire, c'est-à-dire qu'il existe un entier i_0 tel que, pour tout $i \geqslant i_0$, on ait $at^{-i} = at^{-i_0}u_i$ avec $u_i \in \mathrm{A}^\times$. L'anneau A étant intègre (car principal), on en déduit que t^{i-i_0} est une unité, ce qui est faux dès que $i \geqslant i_0 + 1$. Par conséquent, a est nul.

Soit maintenant I un idéal non nul de A, et soit $i \geqslant 0$ le plus grand entier tel que I soit inclus dans $\mathfrak{m}^i$. Alors $t^{-i}\mathrm{I}$ est un idéal de A qui n'est pas inclus dans l'idéal maximal $\mathfrak{m}$: on a donc $t^{-i}\mathrm{I} = \mathrm{A}$, et ainsi $\mathrm{I} = \mathfrak{m}^i$. □

Etant donné $a \in \mathrm{A}$ non nul, l'unique entier $i \geqslant 0$ tel que $(a) = \mathfrak{m}^i$ s'appelle la *valuation* de a. On la note $v(a)$.

Proposition 2.26. — *Pour tous* $a, b \in \mathrm{A}$, *on a* $v(ab) = v(a) + v(b)$ *et* $v(a+b) \geqslant \min(v(a), v(b))$.

On a le résultat suivant.

Théorème 2.27. — *Soit* C *une courbe. Un point* $a \in \mathrm{C}$ *est régulier si et seulement si l'anneau local* $\mathcal{O}_a$ *est un anneau de valuation discrète.*

Démonstration. — Notons A l'anneau $\mathcal{O}_a$ et $\mathfrak{m}$ son idéal maximal. Si A est de valuation discrète, alors $\mathfrak{m}/\mathfrak{m}^2$ est de dimension 1 (car engendré par l'image d'une uniformisante modulo $\mathfrak{m}^2$), donc a est régulier.

Inversement, supposons que a est régulier. Alors pour tout $t \in \mathfrak{m}$ qui n'est pas dans $\mathfrak{m}^2$, la classe de t modulo $\mathfrak{m}^2$ engendre $\mathfrak{m}/\mathfrak{m}^2$, de sorte qu'on a $\mathfrak{m} = kt \oplus \mathfrak{m}^2$. Quitte à effectuer un changement de variable affine, on peut supposer que a est le point $(0, \dots, 0)$ pour alléger les notations, et donc que $\mathfrak{m}$ est engendré par $x_1, \dots, x_n$, où x_i est l'image de X_i dans A. Pour chaque i, on écrit donc :

$$x_i = \lambda_i t + \sum_{j=1}^{n} a_{ij} x_j$$

avec les $\lambda_i \in k$ et les $a_{ij} \in \mathsf{M}_a$, ce qu'on peut écrire sous forme matricielle :

$$(\mathrm{I} - \mathrm{B})\mathrm{X} = t\Lambda$$

avec I la matrice identité, B la matrice des a_{ij} et Λ la matrice colonne des λ_i (et X celle des x_i). Comme B est nulle modulo $\mathfrak{m}$, le déterminant de $\mathrm{I} - \mathrm{B}$ est congru à 1 mod $\mathfrak{m}$ et donc $\mathrm{I} - \mathrm{B}$ est inversible dans $\mathrm{M}_n(\mathrm{A})$. On obtient donc :

$$\mathrm{X} = t(\mathrm{I} - \mathrm{B})^{-1}\Lambda,$$

ce qui prouve que $x_i \in (t)$ pour tout i, et donc que $\mathfrak{m}$ est principal, engendré par t.

Pour prouver que tout idéal de A est principal, on suit l'argument de la preuve de la proposition 2.25, en s'appuyant sur le fait que A est noethérien et intègre et que $\mathfrak{m}$ est principal. □

Remarque 2.28. — Il existe des anneaux locaux dont l'idéal maximal est principal mais qui ne sont pas noethériens. Par exemple, le sous-anneau A de $k(\!(y)\!)[\![x]\!]$ formé des séries formelles :

$$f(x,y) = \sum_{i \geqslant 0} x^i h_i(y), \quad h_0(y) \in k[\![y]\!], \quad h_i(y) \in k(\!(y)\!), \quad i \geqslant 1,$$

est un anneau local dont l'idéal maximal $\mathfrak{m}$, le noyau de $f \mapsto h_0(0)$, est engendré par y ; il n'est pas noethérien car l'intersection des $\mathfrak{m}^i$, $i \geqslant 0$, est l'idéal principal engendré par x. Cet exemple m'a été fourni par Olivier Piltant, que je remercie.

Lemme 2.29. — *Soit* C *une courbe, et soit a un point régulier de* C.

(1) *Pour tout élément $f \in k(\mathrm{C})$ non nul, on a soit $f \in \mathcal{O}_a$, soit $1/f \in \mathcal{O}_a$.*
(2) *Si* A *est un sous-anneau de $k(\mathrm{C})$ tel que $\mathcal{O}_a \subseteq \mathrm{A} \subsetneq k(\mathrm{C})$, alors $\mathrm{A} = \mathcal{O}_a$.*

Démonstration. — Ecrivons $f = p/q$ avec $p, q \in k[\mathrm{C}]$ et $q(a) \neq 0$. Le point a étant régulier, l'anneau $\mathcal{O}_a$ est de valuation discrète : fixons-en une uniformisante t. Ecrivons $p = t^a u$ où $a \geqslant 0$ est la valuation de p dans $\mathcal{O}_a$ et où $u \in \mathcal{O}_a$ est inversible. Comme $q(a) \neq 0$, l'élément q est inversible dans $\mathcal{O}_a$. Si $f \notin \mathcal{O}_a$, alors $a \leqslant -1$, ce dont on déduit que $1/f = t^{-a}(qu^{-1}) \in \mathsf{M}_a$.

Supposons qu'il existe $f \in \mathrm{A}$ telle que $f \notin \mathcal{O}_a$. Alors $1/f \in \mathsf{M}_a$ donc :

$$1 = f \cdot (1/f) \in \mathrm{A}\mathsf{M}_a = \mathrm{A}t.$$

On a donc $t^{-1} \in \mathrm{A}$, puis $t^{-n} \in \mathrm{A}$ pour tout $n \geqslant 1$. Pour contredire le fait que $\mathrm{A} \subsetneq k(\mathrm{C})$, il ne nous reste qu'à prouver que $k(\mathrm{C})$ est la réunion des $t^{-n}\mathcal{O}_a$ pour $n \geqslant 1$, ce qui est une conséquence du point 1. □

Remarque 2.30. — (1) Si $a \in \mathrm{C}$ n'est pas régulier, l'anneau $\mathcal{O}_a$ ne vérifie pas les propriétés du lemme 2.29. Par exemple, si C est la courbe singulière $\mathbf{V}(\mathrm{Y}^2 - \mathrm{X}^3)$, la fonction $f = x/y$ n'est pas définie en $(0,0)$ et son inverse non plus. On a $f^2 = x$, de sorte que $\mathcal{O}_{(0,0)} \subsetneq \mathcal{O}_{(0,0)}[f] \subsetneq k(\mathrm{C})$.

(2) Il y a des sous-anneaux propres maximaux de $k(\mathrm{C})$ qui ne sont de la forme $\mathcal{O}_a$ pour aucun point $a \in \mathrm{C}$; si C est la droite affine $\mathbf{A}^1$, la sous-k-algèbre de $k(\mathrm{X})$ formée des fractions P/Q telles que $\deg(\mathrm{P}) \leqslant \deg(\mathrm{Q})$ en est un exemple. Ce problème sera résolu par la géométrie projective.

2.5. Compléments sur les courbes

Terminons ce chapitre par quelques résultats complémentaires sur les courbes, qui ne seront pas nécessaires pour les chapitres suivants.

Théorème 2.31. — *Une courbe* C *est lisse si et seulement si* $k[\mathrm{C}]$ *est intégralement clos, c'est-à-dire si tout* $f \in k(\mathrm{C})$ *entier sur* $k[\mathrm{C}]$ *appartient à* $k[\mathrm{C}]$.

Remarque 2.32. — Ainsi, si C est une courbe lisse, l'anneau $k[\mathrm{C}]$ est noethérien, intègre, intégralement clos et de dimension 1. Un anneau commutatif vérifiant toutes ces conditions s'appelle un *anneau de Dedekind*. De tels anneaux apparaissent en théorie des nombres : l'anneau des entiers d'un corps de nombres est un anneau de Dedekind. Cette structure commune permet d'unifier la théorie des nombres et la théorie des courbes.

Le résultat suivant est intuitivement simple mais pas si facile à prouver.

Proposition 2.33. — *Soit* C *une courbe. Les sous-ensembles algébriques affines propres de* C *sont finis.*

Démonstration. — Soit V un sous-ensemble algébrique affine propre, que l'on peut supposer irréductible, dans $\mathrm{C} \subseteq \mathbf{A}^n$. L'idéal $\mathrm{J} = \mathbf{I}(\mathrm{V}) \subseteq k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ contient strictement $\mathbf{I}(\mathrm{C})$. Soit $\mathrm{F} \in \mathrm{J}$ n'appartenant pas à $\mathbf{I}(\mathrm{C})$, et soit f son image dans $k(\mathrm{C})$.

Si f est algébrique sur k, alors $f \in k$ car k est algébriquement clos, c'est-à-dire que f vue comme fonction sur C est constante. Comme $f \notin \mathbf{I}(\mathrm{C})$, cette constante est non nulle. Il y a donc un $\lambda \in k$ non nul tel que $\mathrm{F} \in \lambda + \mathbf{I}(\mathrm{C})$. Par conséquent on a $\lambda \in \mathrm{J}$, ce qui implique que $\mathrm{J} = k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$, donc que V est vide.

Si f est transcendante sur k, alors $k(\mathrm{C})$ est algébrique sur $k(f)$. On note x_i l'image de X_i dans $k(\mathrm{C})$ pour $i \in \{1, \ldots, n\}$. Il y a un polynôme non nul $\mathrm{P}_i(\mathrm{U}, \mathrm{T}) \in k[\mathrm{U}, \mathrm{T}]$ tel que $\mathrm{P}_i(f, x_i) = 0$. On peut supposer que les coefficients de $\mathrm{P}_i(\mathrm{U}, \mathrm{T})$ dans $k[\mathrm{U}]$ sont premiers entre eux dans leur ensemble. Ecrivons :

$$\mathrm{P}_i(\mathrm{U}, \mathrm{T}) = \mathrm{P}_i(0, \mathrm{T}) + \mathrm{U}\mathrm{Q}_i(\mathrm{U}, \mathrm{T}).$$

Remplaçant U par f et T par x_i, on trouve que $\mathrm{P}_i(0, x_i) = -f\mathrm{Q}_i(f, x_i)$ appartient à $\mathcal{J}$, l'idéal image de J dans $k[\mathrm{C}]$. Si $\mathrm{P}_i(0, \mathrm{T})$ était nul, on aurait $\mathrm{P}_i(f, \mathrm{T}) = f\mathrm{Q}_i(f, \mathrm{T})$, qui contredirait le fait que ses coefficients dans $k[f]$ sont premiers entre eux dans leur ensemble. Donc $\mathrm{P}_i(0, \mathrm{T})$ est non nul, ce qui entraîne que x_i est algébrique sur k dans $k[\mathrm{C}]/\mathcal{J} \simeq k[\mathrm{X}_1, \ldots, \mathrm{X}_n]/\mathrm{J} = k[\mathrm{V}]$.

L'anneau $k[\mathrm{V}]$ étant formé d'éléments algébriques sur k, on a $k[\mathrm{V}] = k$, c'est-à-dire que J est maximal. Ainsi, la variété V est réduite à un point. □

Chapitre 3. Ensembles algébriques projectifs

Dans un premier temps, on suppose que k est un corps quelconque. On le supposera algébriquement clos à partir du paragraphe 3.3, lorsqu'on arrivera au théorème des zéros projectif.

3.1. L'espace projectif

Soit E un k-espace vectoriel de dimension finie $\geqslant 1$.

Définition 3.1. — L'*espace projectif* $\mathbf{P}(\mathrm{E})$ est l'ensemble des droites (vectorielles) de E.

Tout automorphisme $u \in \mathrm{GL}(\mathrm{E})$ envoie bijectivement droites de E sur droites de E. La bijection $\overline{u}$ de $\mathbf{P}(\mathrm{E})$ sur lui-même qui en résulte s'appelle une *homographie*. Les homographies forment un groupe, noté $\mathrm{PGL}(\mathrm{E})$, canoniquement isomorphe au quotient de $\mathrm{GL}(\mathrm{E})$ par son centre $k^\times$.

Si $\mathrm{E} = k^{n+1}$, $n \geqslant 0$, alors l'espace projectif $\mathbf{P}(k^{n+1})$ est noté $\mathbf{P}^n(k)$, ou $\mathbf{P}^n$ si aucune confusion n'en résulte. Si $(x_0, x_1, \ldots, x_n) \in k^{n+1}$ est un vecteur non nul, la droite qu'il engendre, donc le point de $\mathbf{P}^n$ lui correspondant, est noté $[x_0 : x_1 : \ldots : x_n]$. Les scalaires $x_0, x_1, \ldots, x_n$ sont des *coordonnées homogènes* pour ce point. Elles ne sont pas uniques, puisque :

$$[\lambda x_0 : \lambda x_1 : \ldots : \lambda x_n] = [x_0 : x_1 : \ldots : x_n]$$

pour tout scalaire non nul $\lambda \in k^\times$.

Exemple 3.2. — Dans $\mathbf{P}^1 = \mathbf{P}(k^2)$, les points sont les $[x_0 : x_1]$ avec $(x_0, x_1) \in k^2$ et $(x_0, x_1) \neq (0, 0)$. Si $x_1 \neq 0$, on a $[x_0 : x_1] = [x_0/x_1 : 1]$ et si $x_1 = 0$, on a $[x_0 : x_1] = [1 : 0]$. On a ainsi :

$$\mathbf{P}^1 = \{[\lambda : 1] \mid \lambda \in k\} \cup \{[1 : 0]\}$$

ce que l'on va écrire $\mathbf{P}^1 = \mathbf{A}^1 \cup \{\infty\}$. On dit que $\mathbf{P}^1$ est obtenu à partir de $\mathbf{A}^1$ en lui ajoutant un "point à l'infini" $\infty = [1 : 0]$. Soit maintenant $u \in \mathrm{GL}_2(k)$ qu'on écrit :

$$u = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad a, b, c, d \in k, \quad ad - bc \neq 0.$$

Soit $x \in \mathbf{P}^1$ un point de coordonnées homogènes x_0, x_1. Alors on a $\overline{u}(x) = [ax_0 + bx_1 : cx_0 + dx_1]$. Si $cx_0 + dx_1$ est non nul, on peut écrire :

$$\overline{u}(x) = \left[\frac{ax_0 + bx_1}{cx_0 + dx_1} : 1\right]$$

et sinon, on obtient $\overline{u}(x) = \infty$. On commet habituellement l'abus de notation :

$$\overline{u}(x) = \frac{ax + b}{cx + d} \in \mathbf{P}^1$$

avec les conventions habituelles $\overline{u}(-d/c) = \infty$ et $\overline{u}(\infty) = a/c$, où un élément $\lambda \in k$ est assimilé au point $[\lambda : 1] \in \mathbf{P}^1$.

Exemple 3.3. — Le jeu de Dobble est le plan projectif $\mathbf{P}^2$ sur un corps à 7 éléments.

3.2. Cartes

Pour chaque $i \in \{0, \ldots, n\}$, on a une application $u_i : \mathbf{A}^n \to \mathbf{P}^n$ définie par :

$$u_i(x_1, \ldots, x_n) = [x_1 : \ldots : 1 : \ldots : x_n]$$

où le 1 apparaît à la $i$ème place. C'est une application injective, et son image est notée U_i. C'est l'ensemble des points de $\mathbf{P}^n$ dont la $i$ème coordonnée homogène est non nulle. Sa réciproque de U_i vers $\mathbf{A}^n$ est notée φ_i.

Définition 3.4. — Le couple $(\mathrm{U}_i, \varphi_i)$ s'appelle une *carte standard* de $\mathbf{P}^n$.

Exemple 3.5. — (1) Pour $n = 1$, on a $u_1 : \mathbf{A}^1 \to \mathbf{P}^1$, $x \mapsto [x : 1]$, et le complémentaire de $\mathrm{U}_1 = \varphi_1(\mathbf{A}^1)$ dans $\mathbf{P}^1$ est le "point à l'infini" $\infty = [1 : 0]$.

(2) Pour $n = 2$, on a $u_2 : \mathbf{A}^2 \to \mathbf{P}^2$, $(x, y) \mapsto [x : y : 1]$ et le complémentaire de $\mathrm{U}_2 = u_2(\mathbf{A}^2)$ dans $\mathbf{P}^2$ est l'ensemble $\{[x : y : 0] \mid (x, y) \neq (0, 0)\}$ qui s'identifie à $\mathbf{P}^1$ via la bijection :

$$[x : y] \mapsto [x : y : 0].$$

On appelle le complémentaire $\mathbf{P}^2 \backslash \mathrm{U}_2$ la "droite à l'infini". On peut la décomposer à son tour :

$$\mathbf{P}^2 \backslash \mathrm{U}_2 = \{[x : 1 : 0] \mid x \in k\} \cup \{[1 : 0 : 0]\},$$

le premier morceau s'identifiant à $\mathbf{A}^1$ et le second à un point.

(3) Plus généralement, $\mathbf{P}^n$ peut être décomposé en l'union disjointe :

$$\mathbf{P}^n = \mathrm{X}_n \cup \mathrm{X}_{n-1} \cup \cdots \cup \mathrm{X}_1 \cup \mathrm{X}_0$$

où chaque X_i est en bijection avec l'espace affine $\mathbf{A}^i$. Plus précisément, on a :

$$\mathrm{X}_n = \mathrm{U}_n, \quad \mathrm{X}_i = (\mathbf{P}^n \backslash (\mathrm{U}_n \cup \cdots \cup \mathrm{U}_{i+1})) \cap \mathrm{U}_i, \quad i \in \{0, \ldots, n-1\}.$$

La partie $\mathrm{X}_i \cup \mathrm{X}_{i-1} \cup \cdots \cup \mathrm{X}_0$ est en bijection avec $\mathbf{P}^i$, pour $i \in \{0, \ldots, n\}$. Habituellement, on appelle $\mathrm{X}_{n-1} \cup \cdots \cup \mathrm{X}_0 \simeq \mathbf{P}^{n-1}$ l'*hyperplan à l'infini* dans $\mathbf{P}^n$.

Malgré le vocabulaire employé ci-dessus, il faut comprendre que ces décompositions, donc la notion d'objet à l'infini, ne sont pas canoniques mais relatives au choix d'une base de k^{n+1}. Par exemple, pour $n = 1$, aucun point de $\mathbf{P}^1$ n'est privilégié *a priori* pour servir de point à l'infini. Ce n'est qu'après avoir choisi une base de k^2 qu'on a des coordonnées homogènes et qu'on peut définir un point à l'infini.

3.3. Ensembles algébriques projectifs

A partir de maintenant, on suppose que le corps k est algébriquement clos.

Sur l'espace projectif $\mathbf{P}^n$, on ne peut pas définir la valeur d'un polynôme $\mathrm{F} \in k[\mathrm{X}_0, \ldots, \mathrm{X}_n]$ en un point $a \in \mathbf{P}^n$, car la quantité $\mathrm{F}(a_0, \ldots, a_n) \in k$ dépend du choix des coordonnées homogènes $a_0, \ldots, a_n$ choisies pour le point a. En revanche, on peut définir l'annulation d'un polynôme en un point de $\mathbf{P}^n$.

Définition 3.6. — (1) Si $\mathrm{F} \in k[\mathrm{X}_0, \ldots, \mathrm{X}_n]$ est homogène de degré $d \geqslant 0$, on dit qu'il *s'annule* en $a \in \mathbf{P}^n$ si $\mathrm{F}(a_0, \ldots, a_n) = 0$ pour un choix de coordonnées homogènes pour a. Ceci ne dépend pas de ce choix, puisque :

$$\mathrm{F}(\lambda a_0, \ldots, \lambda a_n) = \lambda^d \cdot \mathrm{F}(a_0, \ldots, a_n)$$

pour tout $\lambda \in k^\times$.

(2) Si $F \in k[X_0, \dots, X_n]$, on peut le décomposer de façon unique en :

$$F = F_0 + F_1 + \cdots + F_d$$

avec F_i homogène de degré i. On dit que F *s'annule* en $a \in \mathbf{P}^n$ si chacun des F_i s'annule en a.

Définition 3.7. — (1) Etant donnée une partie $S \subseteq k[X_0, \dots, X_n]$, on note $\mathbf{V}(S)$ l'ensemble des points $a \in \mathbf{P}^n$ tels que $F(a) = 0$ pour tout $F \in S$.

(2) Si E est une partie de $\mathbf{P}^n$, on note $\mathbf{I}(E)$ l'idéal des polynômes de $k[X_0, \dots, X_n]$ s'annulant en tout $a \in E$.

Un ensemble de la forme $\mathbf{V}(S)$ s'appelle un *ensemble algébrique projectif*. Comme dans le cas affine, il ne dépend que de l'idéal engendré par S. De façon analogue au cas affine :

(1) un ensemble algébrique projectif V dans $\mathbf{P}^n$ est dit *irréductible* s'il ne peut être décomposé en une union de deux ensembles algébriques projectifs strictement plus petits ;

(2) un ensemble algébrique projectif V est irréductible si et seulement si $\mathbf{I}(V)$ est un idéal premier ;

(3) un ensemble algébrique projectif irréductible est appelé une *variété projective*.

Remarque 3.8. — (1) Comme $k[X_0, \dots, X_n]$ est noethérien, il suffit de considérer les parties S qui sont finies. Par définition de l'annulation d'un polynôme en un point, il suffit même de ne considérer les parties finies S qui sont constituées de polynômes homogènes.

(2) Un idéal de la forme $\mathbf{I}(E)$ est non seulement radical, mais il est aussi *homogène*, c'est-à-dire engendré par des polynômes homogènes.

(3) Les opérations $\mathbf{V}$ et $\mathbf{I}$ sont décroissantes.

(4) Les ensembles algébriques projectifs sont stables par union finie et intersection quelconque. En outre, $\mathbf{P}^n$ et l'ensemble vide sont des ensembles algébriques projectifs. Par conséquent, ils forment les fermés d'une topologie sur $\mathbf{P}^n$, appelée *topologie de Zariski*.

On note $\mathfrak{m}_\varnothing$ l'idéal maximal de $k[X_0, \dots, X_n]$ engendré par $X_0, \dots, X_n$. Alors $\mathbf{V}(\mathfrak{m}_\varnothing) = \varnothing$.

Théorème 3.9 **(Théorème des zéros projectif)**. — *Soit un entier $n \geqslant 1$.*

(1) *Si* V *est un ensemble algébrique projectif de $\mathbf{P}^n$, on a $\mathbf{V}(\mathbf{I}(V)) = V$.*

(2) *Si* I *est un idéal homogène de $k[X_0, \dots, X_n]$ et si $\mathbf{V}(I)$ n'est pas vide, alors $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$.*

(3) *Si* I *est un idéal homogène, alors $\mathbf{V}(I)$ est vide si et seulement si $\sqrt{I}$ contient $\mathfrak{m}_\varnothing$.*

Corollaire 3.10. — *Les opérations $\mathbf{V}$ et $\mathbf{I}$ induisent une correspondance bijective :*

(1) *entre ensembles algébriques projectifs non vides et idéaux radicaux homogènes propres distincts de $\mathfrak{m}_\varnothing$,*

(2) *entre variétés projectives non vides et idéaux premiers homogènes distincts de $\mathfrak{m}_\varnothing$.*

3.4. Lien entre affine et projectif

Rappelons que, pour tout $i \in \{0, \dots, n\}$, on a une carte standard $\varphi_i : U_i \to \mathbf{A}^n$ définie par :

$$[x_0 : x_1 : \cdots : x_n] \mapsto \left(\frac{x_0}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i} \right).$$

Les U_i sont ouverts dans $\mathbf{P}^n$ pour la topologie de Zariski, car le complémentaire de U_i dans $\mathbf{P}^n$ est le fermé $\mathbf{V}(X_i)$. Ils forment un recouvrement fini de $\mathbf{P}^n$.

Proposition 3.11. — *L'application $\varphi_i : U_i \to \mathbf{A}^n$ est un homéomorphisme.*

Démonstration. — Prouvons-le pour $i = 0$. Pour $\mathrm{P} \in k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ de degré $d \geqslant 0$, on pose :

$$\mathrm{P}^*(\mathrm{X}_0, \ldots, \mathrm{X}_n) = \mathrm{X}_0^d \cdot \mathrm{P}\left(\frac{\mathrm{X}_1}{\mathrm{X}_0}, \ldots, \frac{\mathrm{X}_n}{\mathrm{X}_0}\right)$$

qui est homogène de degré d. A l'inverse, si $\mathrm{F} \in k[\mathrm{X}_0, \ldots, \mathrm{X}_n]$ est homogène de degré $d \geqslant 0$, on pose :

$$\mathrm{F}_*(\mathrm{X}_1, \ldots, \mathrm{X}_n) = \mathrm{F}(1, \mathrm{X}_1, \ldots, \mathrm{X}_n)$$

qui est de degré $\leqslant d$. On vérifie que $(\mathrm{P}^*)_* = \mathrm{P}$. En revanche, $(\mathrm{F}_*)^*$ n'est pas toujours égal à F. Si X_0^m est la plus grande puissance de X_0 divisant F, on a $\mathrm{F} = \mathrm{X}_0^m \cdot (\mathrm{F}_*)^*$.

Pour prouver que φ_0 est un homéomorphisme, il suffit de vérifier que :

$$\varphi_0(\mathrm{U}_0 \cap \mathbf{V}(\mathrm{F})) = \mathbf{V}(\mathrm{F}_*)$$

pour tout polynôme $\mathrm{F} \in k[\mathrm{X}_0, \ldots, \mathrm{X}_n]$ homogène, et que :

$$\varphi_0^{-1}(\mathbf{V}(\mathrm{P})) = \mathrm{U}_0 \cap \mathbf{V}(\mathrm{P}^*)$$

pour tout polynôme $\mathrm{P} \in k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$. La vérification en est laissée au lecteur. □

Lemme 3.12. — *Soit* V *un ensemble algébrique affine dans* $\mathbf{A}^n$*, et soit* V^* *l'ensemble algébrique projectif* $\mathbf{V}(\{\mathrm{P}^* \mid \mathrm{P} \in \mathbf{I}(\mathrm{V})\})$ *dans* $\mathbf{P}^n$*.*

(1) *L'adhérence de* $\varphi_0^{-1}(\mathrm{V})$ *dans* $\mathbf{P}^n$ *est égale à* V^**, et* $\mathrm{U}_0 \cap \mathrm{V}^*$ *est égal à* $\varphi_0^{-1}(\mathrm{V})$*.*

(2) *Si* V *est irréductible, alors* V^* *est irréductible.*

(3) *Si* $\mathrm{V}_1, \ldots, \mathrm{V}_m$ *sont les composantes irréductibles de* V*, alors les composantes irréductibles de* V^* *sont* $\mathrm{V}_1^*, \ldots, \mathrm{V}_m^*$*.*

Démonstration. — L'égalité $\varphi_0^{-1}(\mathrm{V}) = \mathrm{U}_0 \cap \mathrm{V}^*$ se déduit immédiatement de ce que $(\mathrm{P}^*)_* = \mathrm{P}$ pour tout polynôme $\mathrm{P} \in k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$.

Pour prouver la seconde assertion, on va supposer que l'idéal $\mathrm{I} = \mathbf{I}(\mathrm{V})$ de $k[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ est premier et montrer que l'idéal homogène I^* de $k[\mathrm{X}_0, \ldots, \mathrm{X}_n]$ engendré par les P^*, $\mathrm{P} \in \mathrm{I}$, est premier lui aussi. Soient donc $\mathrm{F}, \mathrm{G} \in k[\mathrm{X}_0, \ldots, \mathrm{X}_n]$ tels que $\mathrm{FG} \in \mathrm{I}^*$. On peut écrire :

$$\mathrm{FG} = \mathrm{A}_1\mathrm{P}_1^* + \cdots + \mathrm{A}_r\mathrm{P}_r^*$$

avec $\mathrm{P}_1, \ldots, \mathrm{P}_r \in \mathrm{I}$ et $\mathrm{A}_1, \ldots, \mathrm{A}_r \in k[\mathrm{X}_0, \ldots, \mathrm{X}_n]$. Remplaçant X_0 par 1, on trouve :

$$\mathrm{F}_*\mathrm{G}_* = (\mathrm{A}_1)_*\mathrm{P}_1 + \cdots + (\mathrm{A}_r)_*\mathrm{P}_r$$

qui appartient donc à I. Celui-ci étant premier, on en déduit que $\mathrm{F}_* \in \mathrm{I}$ ou $\mathrm{G}_* \in \mathrm{I}$. Supposant que $\mathrm{F}_* \in \mathrm{I}$, on trouve $(\mathrm{F}_*)^* \in \mathrm{I}^*$, ce qui entraîne que $\mathrm{F} = \mathrm{X}_0^m \cdot (\mathrm{F}_*)^* \in \mathrm{I}^*$, où X_0^m est la plus grande puissance de X_0 divisant F.

Complétons maintenant la preuve de la première assertion. Soit W un ensemble algébrique projectif de $\mathbf{P}^n$ contenant $\varphi_0^{-1}(\mathrm{V})$. Si $\mathrm{F} \in \mathbf{I}(\mathrm{W})$, alors F_* appartient à I, donc $\mathrm{F} = \mathrm{X}_0^m \cdot (\mathrm{F}_*)^* \in \mathrm{I}^*$. On en déduit que $\mathbf{I}(\mathrm{W}) \subseteq \mathrm{I}^*$, donc que $\mathrm{V}^* \subseteq \mathbf{V}(\mathbf{I}(\mathrm{W})) = \mathrm{W}$.

Prouvons enfin la troisième et dernière assertion. L'égalité $\mathrm{V} = \mathrm{V}_1 \cup \cdots \cup \mathrm{V}_m$ équivaut à l'égalité :

$$\mathrm{I} = \mathrm{I}_1 \cap \cdots \cap \mathrm{I}_m$$

où chaque idéal $\mathrm{I}_i = \mathbf{I}(\mathrm{V}_i)$ est premier. Si $\mathrm{P} \in \mathrm{I}$, on a $\mathrm{P}^* \in \mathrm{I}_i^*$ pour chaque i, donc $\mathrm{I}^* \subseteq \mathrm{I}_1^* \cap \cdots \cap \mathrm{I}_m^*$, ce dont on déduit que $\mathrm{V}_1^* \cup \cdots \cup \mathrm{V}_m^* \subseteq \mathbf{V}(\mathrm{I}_1^* \cap \cdots \cap \mathrm{I}_m^*) \subseteq \mathrm{V}^*$, la première inclusion venant du fait que $\mathrm{I}_1^* \cap \cdots \cap \mathrm{I}_m^* \subseteq \mathrm{I}_i^*$, donc que $\mathrm{V}_i^* \subseteq \mathbf{V}(\mathrm{I}_1^* \cap \cdots \cap \mathrm{I}_m^*)$, pour tout $i \in \{1, \ldots, m\}$. Inversement, on a :

$$\varphi_0^{-1}(\mathrm{V}) = \varphi_0^{-1}(\mathrm{V}_1) \cup \cdots \cup \varphi_0^{-1}(\mathrm{V}_m) \subseteq \mathrm{V}_1^* \cup \cdots \cup \mathrm{V}_m^*$$

ce qui, prenant l'adhérence compte tenu de la première assertion, entraîne que $\mathrm{V}^* \subseteq \mathrm{V}_1^* \cup \cdots \cup \mathrm{V}_m^*$. Les V_i^* sont irréductibles d'après la seconde assertion. Enfin, si $\mathrm{V}_i^* \subseteq \mathrm{V}_j^*$, intersectant avec U_0 et appliquant φ_0, on trouve $\mathrm{V}_i \subseteq \mathrm{V}_j$, ce qui entraîne $i = j$. On obtient le résultat voulu. □

Corollaire 3.13. — *Un ensemble algébrique affine de $\mathbf{A}^n$ est irréductible si et seulement si son adhérence dans $\mathbf{P}^n$ est un ensemble algébrique projectif irréductible.*

Remarque 3.14. — L'ensemble algébrique projectif $\mathrm{W} \subseteq \mathbf{P}^2$ d'équation $\mathrm{XZ} = 0$ est la réunion de deux droites projectives. L'ensemble algébrique affine $\varphi_{\mathrm{Y}}(\mathrm{W} \cap \mathrm{U}_{\mathrm{Y}})$ de $\mathbf{A}^2$ est la réunion de deux droites affines, et son adhérence dans $\mathbf{P}^n$ est égale à W.

En revanche, l'ensemble algébrique affine $\mathrm{V} = \varphi_{\mathrm{X}}(\mathrm{W} \cap \mathrm{U}_{\mathrm{X}})$ de $\mathbf{A}^2$ est la droite affine d'équation $\mathrm{Z} = 0$. Son adhérence $\overline{\mathrm{V}}$ dans $\mathbf{P}^2$ est incluse dans W, mais ne peut pas lui être égale puisque W n'est pas irréductible. En l'occurrence, $\overline{\mathrm{V}}$ est la droite *projective* d'équation $\mathrm{Z} = 0$.

Remarque 3.15. — Si V est un ensemble algébrique affine de $\mathbf{A}^n$, il n'est pas toujours suffisant d'homogénéïser n'importe quels polynômes définissant V pour obtenir des polynômes homogènes définissant son adhérence $\overline{\mathrm{V}}$ dans $\mathbf{P}^n$.

Par exemple, si $\mathrm{V} = \mathbf{V}(\mathrm{Y} - \mathrm{X}^2, \mathrm{Z} - \mathrm{X}^2) \subseteq \mathbf{A}^3$, alors $\mathrm{W} = \mathbf{V}(\mathrm{YT} - \mathrm{X}^2, \mathrm{ZT} - \mathrm{X}^2) \subseteq \mathbf{P}^3$ contient strictement $\overline{\mathrm{V}}$ puisque W contient tous les points de la forme $[0 : y : z : 0]$ alors que V, et donc $\overline{\mathrm{V}}$, est inclus dans l'hyperplan d'équation $\mathrm{Y} = \mathrm{Z}$.

3.5. Fonctions régulières et fonctions rationnelles

Etant donnée une variété affine $\mathrm{V} \subseteq \mathbf{A}^n$, nous avons défini son anneau de fonctions régulières $k[\mathrm{V}]$, puis son corps de fonctions rationnelles $k(\mathrm{V})$ comme le corps des fractions de $k[\mathrm{V}]$.

Nous ne pouvons pas procéder de même pour une variété projective $\mathrm{V} \subseteq \mathbf{P}^n$ car, comme nous le verrons, l'anneau des fonctions régulières sur V tout entier peut être très (trop) petit (penser au théorème de Liouville en analyse complexe). Nous allons d'abord définir un anneau de fonctions régulières pour tout ouvert de V, puis nous définirons le corps des fonctions rationnelles.

Définition 3.16. — Soit V une variété projective, et soit U un ouvert de V. Une application $f : \mathrm{U} \to k$ est dite *régulière* si, pour tout point $a \in \mathrm{U}$, il existe un voisinage Ω_a de a dans U et deux polynômes homogènes G et H de même degré tels que H ne s'annule pas sur Ω_a et, pour tout $x = [x_0 : \ldots : x_n] \in \Omega_a$, on ait :

$$f(x) = \mathrm{G}(x_0, \ldots, x_n)/\mathrm{H}(x_0, \ldots, x_n). \tag{3.1}$$

On note $\mathcal{O}_{\mathrm{V}}(\mathrm{U})$ l'anneau des fonctions régulières sur U.

Remarque 3.17. — La quantité (3.1) ne dépend pas du choix des coordonnées homogènes car G et H sont homogènes de même degré.

Proposition 3.18. — *Une fonction régulière est continue pour la topologie de Zariski.*

Démonstration. — Ceci se vérifie localement, et localement c'est immédiat puisqu'un quotient de polynômes est continu pour la topologie de Zariski. □

Exemple 3.19. — On a $\mathcal{O}_{\mathbf{P}^1}(\mathbf{P}^1) = k$, c'est-à-dire que toute fonction régulière sur $\mathbf{P}^1$ est constante.

Soit V une variété projective. Notons $\mathscr{K}(\mathrm{V})$ l'ensemble des couples (U, f) formés d'un ouvert non vide $\mathrm{U} \subseteq \mathrm{V}$ et d'une fonction régulière $f \in \mathcal{O}_{\mathrm{V}}(\mathrm{U})$. Deux couples (U, f), (U', f') sont dits équivalents si les fonctions f et f' coïncident sur $\mathrm{U} \cap \mathrm{U}'$. Ceci définit une relation d'équivalence, notée $\sim$.

Remarque 3.20. — Tout ouvert non vide de V est dense. En effet, si U est un tel ouvert, alors la décomposition $\mathrm{V} = \overline{\mathrm{U}} \cup (\mathrm{V} \backslash \mathrm{U})$ et le fait que V est irréductible impliquent que U est dense.

Si U, U′ sont des ouverts non vides de V, alors $\mathrm{U} \cap \mathrm{U}' \neq \varnothing$ car V est irréductible.

Définition 3.21. — L'ensemble-quotient de $\mathscr{K}(\mathrm{V})$ par la relation $\sim$ est noté $k(\mathrm{V})$. Il est naturellement muni d'une structure de k-algèbre en faisant un corps, qu'on appelle le corps des *fonctions rationnelles* sur V.

Démonstration. — Etant donné $(\mathrm{U}, f) \in \mathscr{K}(\mathrm{V})$, notons $[\mathrm{U}, f]$ sa classe d'équivalence dans $k(\mathrm{V})$. Supposons que $[\mathrm{U}, f]$ n'est pas nulle. Alors f n'est pas la fonction nulle sur U. Par continuité de f, l'ensemble $\mathrm{D}(f)$ des points de U où f ne s'annule pas est un ouvert non vide, et quitte à remplacer U par $\mathrm{D}(f)$ on peut supposer que f ne s'annule en aucun point de U. Ainsi $[\mathrm{U}, f]$ est inversible, d'inverse $[\mathrm{U}, 1/f]$. □

Définition 3.22. — La *dimension* d'une variété projective $\mathrm{V} \subseteq \mathbf{P}^n$ est le degré de transcendance de $k(\mathrm{V})$ sur k.

Définition 3.23. — Un point $x \in \mathrm{V} \subseteq \mathbf{P}^n$ est dit *régulier* s'il existe un $i \in \{0, \ldots, n\}$ tel que $x \in \mathrm{U}_i$ et tel que $\varphi_i(x)$ soit un point régulier de $\varphi_i(\mathrm{V} \cap \mathrm{U}_i)$.

Ceci ne dépend pas de l'entier $i \in \{0, \ldots, n\}$ tel que $x \in \mathrm{U}_i$.

Proposition 3.24. — *Supposons que* $\mathrm{V} \cap \mathrm{U}_0$ *soit non vide et posons* $\mathrm{V}_0 = \varphi_0(\mathrm{V} \cap \mathrm{U}_0)$. *Alors* V_0 *est une variété affine, et les corps* $k(\mathrm{V})$ *et* $k(\mathrm{V}_0)$ *sont* k*-isomorphes.*

Démonstration. — L'ensemble algébrique affine V_0 est égal à $\mathbf{V}(\mathrm{F}_* \mid \mathrm{F} \in \mathbf{I}(\mathrm{V}))$. L'irréductibilité de V et l'égalité $\mathrm{V} = (\overline{\mathrm{V} \cap \mathrm{U}_0}) \cup (\mathrm{V} \backslash \mathrm{U}_0)$ entraînent que l'adhérence de V_0 dans $\mathbf{P}^n$ est égale à V. Par conséquent, V est irréductible. En outre, l'opération de déshomogénéïsation induit un isomorphisme de k-algèbres de $k(\mathrm{V})$ vers $k(\mathrm{V}_0)$. □

3.6. Applications régulières et applications rationnelles

Soient $\mathrm{V} \subseteq \mathbf{P}^n$ et $\mathrm{W} \subseteq \mathbf{P}^m$ des variétés projectives.

Définition 3.25. — Soit U un ouvert non vide de V. Une application $\varphi : \mathrm{U} \to \mathrm{W}$ est dite *régulière* si, pour tout point $a \in \mathrm{U}$, il y a un voisinage ouvert Ω de a dans U et des polynômes homogènes $\mathrm{G}_0, \mathrm{H}_0, \ldots, \mathrm{G}_m, \mathrm{H}_m$ tels que :

(1) G_i et H_i sont de même degré pour tout $i \in \{0, \ldots, m\}$;
(2) $\mathrm{H}_0, \ldots, \mathrm{H}_m$ ne s'annulent pas sur Ω ;
(3) il n'existe pas de $x \in \Omega$ tel que $\mathrm{G}_0(x) = \cdots = \mathrm{G}_m(x) = 0$;
(4) on a :

$$\varphi(x) = \left[\frac{\mathrm{G}_0(x_0, \ldots, x_n)}{\mathrm{H}_0(x_0, \ldots, x_n)} : \cdots : \frac{\mathrm{G}_m(x_0, \ldots, x_n)}{\mathrm{H}_m(x_0, \ldots, x_n)} \right]$$

pour tout $x = [x_0 : \cdots : x_m] \in \Omega$.

Il y a une définition équivalente, qui a l'avantage de fonctionner pour les variétés affines aussi bien que projectives. Soient V et W des variétés, affines ou projectives.

Définition 3.26. — Soit U un ouvert non vide de V. Une application continue $\varphi : \mathrm{U} \to \mathrm{W}$ est dite *régulière* si, pour tout ouvert $\Omega \subseteq \mathrm{W}$ et toute fonction régulière $f \in \mathcal{O}_{\mathrm{W}}(\Omega)$, la composée :

$$f \circ \varphi : \varphi^{-1}(\Omega) \to k$$

est une fonction régulière dans $\mathcal{O}_{\mathrm{V}}(\varphi^{-1}(\Omega))$.

Si V et W sont des variété affines, on peut vérifier qu'on retrouve la définition 1.30 en choisissant pour f la projection sur une coordonnée.

Si V est projective et W affine, on peut vérifier, là encore en choisissant pour f la projection sur une coordonnée, que φ est une application régulière si et seulement si ses fonctions coordonnées sont des fonctions régulières au sens de la définition 3.16.

Si W est une variété projective, il n'y a pas de notion canonique de fonction coordonnée car $\mathbf{P}^m$ ne se décompose pas en un produit de m copies de $\mathbf{P}^1$. On peut tout de même écrire :

$$\varphi(x) = [\varphi_0(x) : \ldots : \varphi_m(x)]$$

pour tout point $x \in \mathrm{U}$, mais les fonctions $\varphi_i : \mathrm{U} \to k$ ne sont pas uniquement déterminées.

Deux applications régulières $f : \mathrm{U} \to \mathrm{W}$ et $f' : \mathrm{U}' \to \mathrm{W}$ sont dites *équivalentes* si f et f' coïncident sur $\mathrm{U} \cap \mathrm{U}'$.

Définition 3.27. — Une *application rationnelle* de V dans W est une classe d'équivalence pour cette relation. On note $[\mathrm{U}, f]$ la classe d'équivalence de (U, f).

Une application rationnelle est *définie* en un point $x \in \mathrm{V}$ si elle est de la forme $[\mathrm{U}, f]$ pour un ouvert U contenant x. Le domaine de définition d'une application rationnelle est donc un ouvert de V.

Exemple 3.28. — L'application $\varphi_0 : \mathrm{U}_0 \to \mathbf{A}^1$ définie par $[x : y] \mapsto yx^{-1}$ définit une application rationnelle $[\mathrm{U}_0, \varphi_0]$ de $\mathbf{P}^1$ dans $\mathbf{A}^1$ dont le domaine de définition est U_0.

Pour prouver que cette application rationnelle φ n'est pas définie en $a = [0 : 1]$, supposons le contraire, c'est-à-dire qu'il existe un voisinage ouvert Ω de a sur lequel φ a une expression de la forme :

$$\varphi([x : y]) = \mathrm{G}(x, y)/\mathrm{H}(x, y)$$

avec G, H homogènes de même degré et H ne s'annulant pas sur Ω. Sur l'intersection $\Omega \cap \mathrm{U}_0$, cela donne :

$$\mathrm{G}(x, y)/\mathrm{H}(x, y) = yx^{-1}$$

c'est-à-dire que le polynôme homogène $\mathrm{XG} - \mathrm{YH}$ s'annule sur l'ouvert $\Omega \cap \mathrm{U}_0$, donc sur $\mathbf{P}^1$ tout entier car $\Omega \cap \mathrm{U}_0$ est dense. Au point a, cela donne $\mathrm{H}(0, 1) = 0$, ce qui contredit le fait que H ne doit pas s'annuler sur Ω.

Si une application rationnelle de V dans W est définie sur V tout entier, on dit que c'est un *morphisme* (de variétés projectives) de V dans W.

Exemple 3.29. — Soit $\mathrm{V} = \mathbf{V}(\mathrm{X}^2 + \mathrm{Y}^2 - \mathrm{Z}^2) \subseteq \mathbf{P}^2$ et soit $\mathrm{W} = \mathbf{P}^1$. On considère l'application rationnelle $\varphi : \mathrm{V} \to \mathbf{P}^1$ définie par l'application régulière :

$$[x : y : z] \mapsto [x + z : y]$$

sur l'ouvert U des points $[x : y : z]$ tels que $x+z$ et y ne sont pas nuls en même temps, c'est-à-dire l'ensemble V privé du point $a = [1 : 0 : -1]$. Nous allons voir que φ est un morphisme, c'est-à-dire qu'elle est également définie en a, pourvu que la caractéristique de k soit différente de 2. Pour cela, on remarque que l'application régulière $[-y : x - z]$ est définie sur le complémentaire U' de $a' = [1 : 0 : 1]$ dans V, et que sur l'intersection $\mathrm{U} \cap \mathrm{U}'$ on a :

$$[-y : x - z] = \left[\frac{x^2 - z^2}{y} : x - z\right] = [x + z : y]$$

c'est-à-dire que ces deux applications régulières sont équivalentes et la seconde est définie en a.

3.7. Courbes projectives

Une *courbe projective* est une variété projective de dimension 1.

Définition 3.30. — Soit C une courbe projective, soit un point $x \in \mathrm{C}$ et soit $i \in \{0, \ldots, n\}$ tel que $x \in \mathrm{U}_i$. D'après la proposition 3.24, il y a un isomorphisme naturel :

$$k(\mathrm{C}) \simeq k(\varphi_i(\mathrm{C} \cap \mathrm{U}_i)). \tag{3.2}$$

de k-algèbres, $\varphi_i(\mathrm{C} \cap \mathrm{U}_i)$ étant une courbe algébrique affine. On note $\mathcal{O}_x$, et on appelle *anneau local de* C *en* x, le sous-anneau de $k(\mathrm{C})$ image par (3.2) de l'anneau local de $\varphi_i(\mathrm{C} \cap \mathrm{U}_i)$ en $\varphi_i(x)$. Il ne dépend pas de l'entier i choisi.

Si x est un point régulier d'une courbe projective C, l'anneau local $\mathcal{O}_x$ est donc un anneau de valuation discrète d'après le théorème 2.27, et il vérifie les propriétés du lemme 2.29. Il possède une valuation v_x qui, en vertu du lemme 2.29, peut être étendue à tout le corps $k(\mathrm{C})$ en posant $v_x(f) = -v_x(1/f)$ pour tout $f \notin \mathcal{O}_x$.

Proposition 3.31. — *Soit* C *une courbe projective et soit* $\varphi : \mathrm{C} \to \mathbf{P}^m$ *une application rationnelle. Alors* φ *est définie en tout point régulier de* C.

Démonstration. — Ecrivons φ sous la forme $[f_0 : \ldots : f_m]$ avec $f_0, \ldots, f_m \in k(\mathrm{C})$. Soit $x \in \mathrm{C}$ un point régulier. Fixons une uniformisante t de $\mathcal{O}_x$, et soit r le minimum des entiers $v_x(f_0), \ldots, v_x(f_m)$. Alors les entiers $v_x(t^{-r} f_j)$ sont tous positifs, et l'un d'eux est nul. Les fonctions $g_j = t^{-r} f_j$ ne s'annulent donc pas toutes en x, et $[g_0 : \ldots : g_m]$ est équivalente à φ et définie en x. □

Corollaire 3.32. — *Si* C *est une courbe projective lisse, toute application rationnelle de* C *dans* $\mathbf{P}^m$ *est un morphisme.*

Remarque 3.33. — Si C est une courbe projective lisse, l'application $f \mapsto [f : 1]$ définit une bijection entre $k(\mathrm{C})$ et les morphismes de C dans $\mathbf{P}^1$ différents du morphisme constant $[1 : 0]$.

Exemple 3.34. — Soit $\mathrm{C} = \mathbf{V}(\mathrm{X}^3 + \mathrm{X}^2\mathrm{Z} - \mathrm{Y}^2\mathrm{Z})$. La fonction rationnelle $y/x \in k(\mathrm{C})$ correspond à l'application rationnelle $[x : y : z] \mapsto [y : x]$ de C dans $\mathbf{P}^1$. Ce n'est pas un morphisme, car elle n'est pas définie en $[0 : 0 : 1]$. Donc C n'est pas lisse. Vérifier que l'anneau local correspondant n'est pas principal.

Chapitre 4. Diviseurs sur une courbe

Soit C une courbe projective lisse. L'objectif de ce chapitre est d'associer à C un entier $g \geqslant 0$ appelé son genre.

4.1. Zéros et pôles

On a associé à tout point $x \in \mathrm{C}$ une application *valuation* :

$$v_x : k(\mathrm{C}) \to \mathbf{Z} \cup \{+\infty\}$$

associant à toute fonction $f \in k(\mathrm{C})$ sa *multiplicité* (ou son *ordre*) au point x. Rappelons que :

$$\mathcal{O}_x = \{f \in k(\mathrm{C}) \mid v_x(f) \geqslant 0\}$$

est un anneau de valuation discrète, d'idéal maximal $\mathsf{M}_x = \{f \in k(\mathrm{C}) \mid v_x(f) \geqslant 1\}$. On dit que x est un *zéro* de f si $v_x(f) \geqslant 1$, et que c'est un *pôle* de f si $v_x(f) \leqslant -1$, c'est-à-dire si x est un zéro de $1/f$. L'application $f \mapsto 1/f$ sur $k(\mathrm{C})^\times$ interchange zéros et pôles.

Commençons par établir une série de lemmes qui serviront dans la preuve du théorème d'approximation faible 4.4 ci-dessous.

Lemme 4.1. — *Etant donnés $x, y \in \mathrm{C}$, on a $\mathcal{O}_x = \mathcal{O}_y$ si et seulement si $x = y$.*

Démonstration. — Soient $x, y \in \mathrm{C}$ tels que $\mathcal{O}_x = \mathcal{O}_y$. En appliquant à C une homographie convenable, on peut supposer que $x, y \in \mathrm{U}_0$. Remplaçant C par $\varphi_0(\mathrm{C} \cap \mathrm{U}_0)$, on peut supposer que C est affine. Les anneaux locaux $\mathcal{O}_x$ et $\mathcal{O}_y$ étant égaux, ils ont le même idéal maximal, ce qui entraîne qu'une fonction sur C s'annule en x si et seulement si elle s'annule en y. Ecrivant $x = (x_1, \dots, x_n)$ et $y = (y_1, \dots, y_n)$, et appliquant ce principe aux polynômes $\mathrm{X}_i - x_i$ pour $i \in \{1, \dots, n\}$, on trouve que $x_i = y_i$ pour tout i. □

Lemme 4.2. — *Etant donnés deux points distincts $x, y \in \mathrm{C}$, il y a une fonction $f \in k(\mathrm{C})$ ayant x pour zéro et y pour pôle.*

Démonstration. — D'après le lemme 4.1, il y a une fonction $h \in \mathcal{O}_x$ qui n'est pas dans $\mathcal{O}_y$, et une fonction $k \in \mathcal{O}_y$ qui n'est pas dans $\mathcal{O}_x$. Alors la fonction $f = hk^{-1}$ convient. □

Lemme 4.3. — *Soient $x_1, \dots, x_n$ des points distincts de* C. *Il y a un $u \in k(\mathrm{C})$ ayant x_1 pour zéro et $x_2, \dots, x_n$ pour pôles.*

Démonstration. — Procédons par récurrence sur n, le cas $n = 2$ étant réglé par le lemme 4.2.

Supposons le résultat vrai pour $n - 1 \geqslant 2$ points. Il y a une fonction $h \in k(\mathrm{C})$ ayant x_1 pour zéro et $x_2, \dots, x_{n-1}$ pour pôles. Si en outre x_n est un pôle de h, on a ce que l'on souhaite. Dans le cas contraire, soit $v \in \mathsf{M}_{x_1}$ ayant x_n pour pôle, et posons $u = h + v^r$, avec $r \geqslant 1$ choisi de sorte que $r \cdot v_{x_i}(v) \neq v_{x_i}(h)$ pour tout $i \geqslant 2$. Alors une telle fonction u convient. □

***Théorème 4.4* (Théorème d'approximation faible).** — *Soit $n \geqslant 1$. Soient $x_1, \dots, x_n$ des points distincts de* C, *soient $r_1, \dots, r_n \in \mathbf{Z}$ et soient des fonctions $g_1, \dots, g_n \in k(\mathrm{C})$. Il y a une fonction $f \in k(\mathrm{C})$ telle que $v_{x_i}(f - g_i) \geqslant r_i$ pour tout $i \in \{1, \dots, n\}$.*

Remarque 4.5. — Ce théorème n'est pas sans lien avec le lemme chinois de l'arithmétique. Si l'on remplace les x_i par des nombres premiers p_i, les g_i par des entiers $a_i \in \mathbf{Z}$ et si l'on suppose que les r_i sont positifs, le lemme chinois dit qu'il existe un entier $b \in \mathbf{Z}$ congru à a_i mod $p_i^{r_i}$ pour chaque i, c'est-à-dire que la valuation p_i-adique de $b - a_i$ est $\geqslant r_i$.

Démonstration. — Prouvons qu'il existe une fonction $w \in k(\mathrm{C})$ telle que $v_{x_1}(w-1) > r_1$ et $v_{x_i}(w) > r_i$ pour $i \geqslant 2$. Soit u comme dans le lemme 4.3. Posons $w = (1+u^s)^{-1}$ pour un entier $s > \max\{r_1, \ldots, r_n\}$. Ainsi :

$$v_{x_1}(w-1) = v_{x_1}(u^s w) = s \cdot v_{x_1}(u) > r_1$$

tandis que :

$$v_{x_i}(w) = -v_{x_i}(1+u^s) = -s \cdot v_{x_i}(u) > r_i, \quad i \in \{2, \ldots, n\}.$$

Ainsi, étant donné $s \in \mathbf{Z}$ tel que $v_{x_i}(g_j) \geqslant s$ pour tous i, j, il y a une fonction $w_i \in k(\mathrm{C})$ telle que :

$$v_{x_i}(w_i - 1) > r_i - s \quad \text{et} \quad v_{x_j}(w_i) > r_j - s, \quad j \neq i.$$

Alors la fonction $f = w_1 g_1 + \cdots + w_n g_n$ convient. □

Proposition 4.6. — *Soit $f \in k(\mathrm{C})$ et soient $x_1, \ldots, x_n \in \mathrm{C}$ des zéros de f, avec $n \geqslant 0$. Alors :*

$$\sum_{i=1}^{n} v_{x_i}(f) \leqslant [k(\mathrm{C}) : k(f)].$$

Démonstration. — Pour tout $i \in \{1, \ldots, n\}$, on fixe une uniformisante $\varpi_i \in \mathcal{O}_{x_i}$. D'après le théorème d'approximation faible, pour chaque i, il y a une fonction $t_i \in k(\mathrm{C})$ telle que $v_{x_i}(t_i - \varpi_i) \geqslant 2$ et $v_{x_j}(t_i - 1) \geqslant 1$ pour tout $j \neq i$. Ainsi t_i est une uniformisante en x_i ne s'annulant pas en les x_j pour $j \neq i$.

Invoquant derechef le théorème d'approximation faible, il existe $h_i \in k(\mathrm{C})$ telle que $v_{x_i}(h_i - 1) \geqslant 1$ et $v_{x_j}(h_i) \geqslant v_{x_j}(f)$ pour $j \neq i$. On a donc $h_i(x_i) = 1$. Nous allons prouver que les $t_i^j h_i$, pour $i \in \{1, \ldots, n\}$ et $j \in \{0, \ldots, v_{x_i}(f) - 1\}$, sont linéairement indépendants sur $k(f)$. Raisonnant par l'absurde, écrivons :

$$\sum_{i=1}^{n} \sum_{j=0}^{v_{x_i}(f)-1} \mathrm{P}_{ij}(f) t_i^j h_i = 0 \tag{4.1}$$

avec les $\mathrm{P}_{ij}(f) \in k[f]$. Comme f est transcendante sur k, on peut supposer que les $\mathrm{P}_{ij}(f)$ sont premiers entre eux dans leur ensemble, et donc en particulier pas tous divisibles par f. Choisissons des indices a, b tels que f ne divise par P_{ab} mais divise P_{aj} pour tout $j < b$, et divisons (4.1) par t_a^b.

(1) Si $i \neq a$, alors $\mathrm{P}_{ij}(f) t_i^j h_i t_a^{-b}$ s'annule en x_a car h_i s'y annule à l'ordre $\geqslant v_{x_a}(f) > b$.
(2) Si $i = a$ et $j < b$, alors $\mathrm{P}_{aj}(f) t_a^{j-b} h_a$ s'annule en x_a car $\mathrm{P}_{aj}(f)$ s'y annule à l'ordre $\geqslant v_{x_a}(f) > b$.
(3) Si $i = a$ et $j > b$, alors $\mathrm{P}_{aj}(f) t_a^{j-b} h_a$ s'annule en x_a car t_a^{j-b} s'y annule.

Par conséquent, $\mathrm{P}_{ab}(f) h_a$ s'annule en x_a. Mais $h_a(x_a) = 1$ et, f s'annulant en x_a, la valeur de $\mathrm{P}_{ab}(f)$ en x_a est égale au terme constant de P_{ab}, qui est non nul car on a supposé que f ne divise pas P_{ab}. On en déduit une contradiction. □

Corollaire 4.7. — *Une fonction $f \in k(\mathrm{C})$ non nulle n'a qu'un nombre fini de zéros et de pôles.*

4.2. Le théorème d'existence

Venons-en au théorème important suivant.

Théorème 4.8. — *Toute fonction $f \in k(\mathrm{C})$ non constante a au moins un zéro et un pôle.*

Démonstration. — Quitte à remplacer f par $1/f$, il suffit de prouver que toute fonction f non constante a au moins un zéro. La preuve ci-dessous est inspirée de J. Dieudonné, t. 2, §3.3.

On considère C comme une courbe projective de $\mathbf{P}^n$ avec $n \geqslant 1$. Soit $f \in k(\mathrm{C})$ sans zéro. On pose :

$$\mathrm{F} = \{(x, f(x)) \mid x \in \mathrm{C} \text{ n'est pas un pôle de } f\} \subseteq \mathbf{P}^n \times \mathbf{A}^1$$

et on note $\mathrm{Z} \subseteq \mathbf{A}^1$ l'ensemble des $f(x)$ où x décrit les points de C qui ne sont pas pôles de f. Par hypothèse, on a $0 \notin \mathrm{Z}$. On va montrer que Z est une partie finie de $\mathbf{A}^1$, en prouvant l'existence d'un polynôme non nul $\mathrm{P} \in k[\mathrm{Y}]$ s'annulant sur Z.

On note A la k-algèbre $k[\mathrm{Y}][\mathrm{X}_0, \dots, \mathrm{X}_n]$, et $\mathfrak{a}$ l'idéal de A engendré par les polynômes homogènes (en les X_i) de la forme :

$$h = \sum_{\alpha} h_\alpha(\mathrm{Y})\mathrm{X}^\alpha$$

tels que $h(x, y) = 0$ pour tout point $(x, y) \in \mathrm{F}$, où $\alpha = (\alpha_0, \dots, \alpha_n)$ décrit $\mathbf{N}^{n+1}$ et où X^α désigne le monôme $\mathrm{X}_0^{\alpha_0} \dots \mathrm{X}_n^{\alpha_n}$. Pour tout entier $i \in \{0, \dots, n\}$, notons $(\mathrm{U}_i, \varphi_i)$ la carte standard de $\mathbf{P}^n$ lui correspondant et assimilons $\mathrm{U}_i \times \mathbf{A}^1$ à l'espace affine $\mathbf{A}^{n+1}$.

Lemme 4.9. — *L'intersection* $\mathrm{F}_i = \mathrm{F} \cap (\mathrm{U}_i \times \mathbf{A}^1)$ *est un fermé de* $\mathrm{U}_i \times \mathbf{A}^1$.

Démonstration. — Soit C_i la courbe algébrique affine $\varphi_i(\mathrm{C} \cap \mathrm{U}_i)$ et soit $f_i \in k(\mathrm{C}_i)$ la fonction rationnelle correspondant à f par l'intermédiaire de l'isomorphisme de la proposition 3.24. La fonction $1/f_i$ étant définie en tout point de C_i, elle est régulière d'après la remarque 2.20. On a donc $f_i = 1/q$ pour $q \in k[\mathrm{C}_i]$. Choisissant un polynôme $\mathrm{Q} \in k[\mathrm{X}_0, \dots, \mathrm{X}_{i-1}, \mathrm{X}_{i+1}, \dots, \mathrm{X}_n]$ dont l'image dans $k[\mathrm{C}_i]$ soit q, on en déduit l'égalité $\mathrm{F}_i = (\mathrm{C}_i \times \mathbf{A}^1) \cap \mathbf{V}(1 - \mathrm{YQ})$. □

Les ensembles F_i et $\mathrm{U}_i \times \{0\}$ sont des fermés disjoints de $\mathrm{U}_i \times \mathbf{A}^1$. L'ensemble algébrique correspondant à la somme des idéaux $\mathbf{I}(\mathrm{F}_i)$ et $\mathbf{I}(\mathrm{U}_i \times \{0\})$ dans $k[\mathrm{U}_i \times \mathbf{A}^1] = k[\mathrm{Y}][\mathrm{X}_0, \dots, \mathrm{X}_{i-1}, \mathrm{X}_{i+1}, \dots, \mathrm{X}_n]$ est donc vide. Par le théorème des zéros de Hilbert, il existe un $g_i \in \mathbf{I}(\mathrm{F}_i)$ et un $h_i \in k[\mathrm{X}_0, \dots, \mathrm{X}_{i-1}, \mathrm{X}_{i+1}, \dots, \mathrm{X}_n]$ tel que :

$$1 = g_i + \mathrm{Y}h_i. \tag{4.2}$$

Homogénéïsant et multipliant par X_i^r pour un entier r strictement supérieur au degré de g_i, on obtient :

$$\mathrm{X}_i^r = \mathrm{X}_i^r g_i\left(\frac{\mathrm{X}_0}{\mathrm{X}_i}, \dots, \frac{\mathrm{X}_{i-1}}{\mathrm{X}_i}, \frac{\mathrm{X}_{i+1}}{\mathrm{X}_i}, \dots, \frac{\mathrm{X}_n}{\mathrm{X}_i}\right) + \mathrm{YX}_i^r h_i\left(\frac{\mathrm{X}_0}{\mathrm{X}_i}, \dots, \frac{\mathrm{X}_{i-1}}{\mathrm{X}_i}, \frac{\mathrm{X}_{i+1}}{\mathrm{X}_i}, \dots, \frac{\mathrm{X}_n}{\mathrm{X}_i}\right)$$

ce qui s'écrit $\mathrm{G}_{i,r} + \mathrm{YH}_{i,r}$ avec $\mathrm{G}_{i,r} \in \mathfrak{a}$ et $\mathrm{H}_{i,r} \in k[\mathrm{X}_0, \dots, \mathrm{X}_{i-1}, \mathrm{X}_{i+1}, \dots, \mathrm{X}_n]$ homogènes de degré r. Il existe donc un entier R tel que, pour tout $r \geqslant \mathrm{R}$ et tout $\alpha \in \mathbf{N}^{n+1}$ de somme r, on ait :

$$\mathrm{X}^\alpha = \mathrm{G}_\alpha + \sum_{\beta} h_{\alpha\beta}\mathrm{YX}^\beta$$

avec $\mathrm{G}_\alpha \in \mathfrak{a}$ et $h_{\alpha\beta} \in k[\mathrm{Y}]$ pour tout $\beta \in \mathbf{N}^{n+1}$ de somme r. Ceci s'écrit sous forme matricielle :

$$(\mathrm{I} - \mathrm{YH})\mathrm{X} = \mathrm{G}$$

avec I la matrice identité, H la matrice des $h_{\alpha\beta}$, et X, G les matrices colonnes des X^α et des G_α respectivement. Résolvant ce système linéaire et posant $\mathrm{P}(\mathrm{Y}) = \det(\mathrm{I} - \mathrm{YH}) \in k[\mathrm{Y}]$, on a $\mathrm{P}(0) = 1$ et $\mathrm{P}(\mathrm{Y})\mathrm{X}_i^r \in \mathfrak{a}$ pour tout $r \geqslant \mathrm{R}$ et tout $i \in \{0, \dots, n\}$.

Soit maintenant $y \in \mathrm{Z}$. Soit $x = [x_0 : \cdots : x_n] \in \mathrm{C}$ tel que $y = f(x)$ et soit $i \in \{0, \dots, n\}$ tel que $x \in \mathrm{U}_i$. Comme $\mathrm{P}(\mathrm{Y})\mathrm{X}_i^r \in \mathfrak{a}$ et $x_i \neq 0$, on a $\mathrm{P}(y) = 0$. On en déduit que P vérifie les conditions voulues. Ainsi f ne prend qu'un nombre fini de valeurs. La courbe C étant irréductible, f est constante. □

4.3. Diviseurs

Nous abordons maintenant le sujet central de ce chapitre, qui va être formalisé au moyen de la notion de diviseur.

Définition 4.10. — Un *diviseur* sur C est une somme finie formelle :

$$\mathrm{D} = \sum_{x \in \mathrm{C}} n_x \cdot x \tag{4.3}$$

où les $n_x \in \mathbf{Z}$ sont nuls à l'exception d'un nombre fini d'entre eux.

En d'autres termes, un diviseur sur C est une application de C dans $\mathbf{Z}$ à support fini. Les diviseurs sur C forment un groupe abélien noté $\mathrm{Div}(\mathrm{C})$.

Définition 4.11. — Si $f \in k(\mathrm{C})$ est non nulle, on lui associe le diviseur :

$$\mathrm{div}(f) = \sum_{x \in \mathrm{C}} v_x(f) \cdot x$$

qui est bien défini car f n'a qu'un nombre fini de zéros et de pôles. Un diviseur de cette forme est dit *principal*.

On a $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$ et $\mathrm{div}(1/f) = -\mathrm{div}(f)$ pour toutes fonctions $f, g \in k(\mathrm{C})$ non nulles. Les diviseurs principaux forment donc un sous-groupe $\mathrm{Pr}(\mathrm{C}) \subseteq \mathrm{Div}(\mathrm{C})$, et div induit un morphisme surjectif de groupes de $k(\mathrm{C})^\times$ dans $\mathrm{Pr}(\mathrm{C})$.

Le résultat suivant est un corollaire de l'important théorème 4.8.

Proposition 4.12. — *Le noyau de* div *est égal à* $k^\times$.

Définissons un morphisme de groupes deg de $\mathrm{Div}(\mathrm{C})$ dans $\mathbf{Z}$ en posant :

$$\deg\left(\sum_{x \in \mathrm{C}} n_x \cdot x\right) = \sum_{x \in \mathrm{C}} n_x.$$

Il est surjectif, et on note $\mathrm{Div}^0(\mathrm{C})$ son noyau. On verra plus tard que tout diviseur principal est de degré 0. Le groupe-quotient $\mathrm{Div}^0(\mathrm{C})/\mathrm{Pr}(\mathrm{C})$, appelé *groupe de Picard* de C, est un invariant important de C. On le note $\mathrm{Pic}^0(\mathrm{C})$.

Remarque 4.13. — On verra que $\mathrm{Pic}^0(\mathrm{C})$ est trivial si et seulement si C est isomorphe à $\mathbf{P}^1$. En général, le groupe de Picard n'est pas trivial. Si C est une courbe elliptique (c'est-à-dire une courbe de genre 1), il y a une bijection de $\mathrm{Pic}^0(\mathrm{C})$ sur C, permettant de munir C d'une structure de groupe abélien.

Exemple 4.14. — Vérifier que le groupe de Picard de $\mathbf{P}^1$ est trivial.

4.4. Les espaces $\mathscr{L}(\mathrm{D})$

Un diviseur D sur C est *positif* (ou *effectif*) si tous ses coefficients n_x sont $\geqslant 0$. Ceci définit une relation d'ordre partiel sur $\mathrm{Div}(\mathrm{C})$:

$$\mathrm{D}' \geqslant \mathrm{D} \quad \Leftrightarrow \quad \mathrm{D}' - \mathrm{D} \text{ est positif.}$$

Si $\mathrm{D} \in \mathrm{Div}(\mathrm{C})$, on pose :

$$\mathscr{L}(\mathrm{D}) = \{0\} \cup \{f \in k(\mathrm{C}) \text{ non nulles} \mid \mathrm{div}(f) + \mathrm{D} \geqslant 0\}.$$

On a le lemme suivant.

Lemme 4.15. — *Une fonction $f \in k(\mathrm{C})$ appartient à $\mathscr{L}(0)$ si et seulement si elle est constante.*

Démonstration. — $\mathscr{L}(0)$ contient toutes les fonctions constantes car toute fonction constante non nulle a un diviseur nul. S'il y a $f \in \mathscr{L}(0)$ non constante, alors elle a au moins un pôle, ce qui contredit l'inégalité $\mathrm{div}(f) \geqslant 0$. □

Proposition 4.16. — *Soient* D, D' *des diviseurs de* C.

(1) $\mathscr{L}(\mathrm{D})$ *est un sous-k-espace vectoriel de* $k(\mathrm{C})$.
(2) *Si* $\mathrm{D} \leqslant \mathrm{D}'$, *alors* $\mathscr{L}(\mathrm{D}) \subseteq \mathscr{L}(\mathrm{D}')$ *et* $\dim \mathscr{L}(\mathrm{D}')/\mathscr{L}(\mathrm{D}) \leqslant \deg(\mathrm{D}' - \mathrm{D})$.

(3) *L'espace* $\mathscr{L}(\mathrm{D})$ *est de dimension finie.*

Démonstration. — Le point 1 est une conséquence du fait que, pour tous $f, g \in k(\mathrm{C})$, $\lambda \in k^\times$ et $x \in \mathrm{C}$, on a $\mathrm{div}(\lambda f) = \mathrm{div}(f)$ et $v_x(f+g) \geqslant \min(v_x(f), v_x(g))$.

Pour le point 2, il suffit de traiter le cas où $\mathrm{D}' = \mathrm{D} + y$ avec $y \in \mathrm{C}$. Fixons une uniformisante t en y, et définissons une forme linéaire φ sur $\mathscr{L}(\mathrm{D}')$ en posant :

$$\varphi(f) = (t^{n_y+1} f)(y).$$

Elle est bien définie car $v_y(f) + n_y + 1 \geqslant 0$ pour toute $f \in \mathscr{L}(\mathrm{D}')$, et son noyau est égal à $\mathscr{L}(\mathrm{D})$. On en déduit le résultat voulu.

Pour le dernier point, supposons d'abord que D est effectif. D'après le point 2, on a $\mathscr{L}(0) \subseteq \mathscr{L}(\mathrm{D})$ et $\dim \mathscr{L}(\mathrm{D})/\mathscr{L}(0) \leqslant \deg(\mathrm{D})$. On déduit du lemme 4.15 que $\dim \mathscr{L}(\mathrm{D}) \leqslant 1 + \deg(\mathrm{D})$. Dans le cas général, soit D' un diviseur effectif tel que $\mathrm{D} \leqslant \mathrm{D}'$. D'après le point 2, on trouve que $\mathscr{L}(\mathrm{D}) \subseteq \mathscr{L}(\mathrm{D}')$, et ce dernier est de dimension finie d'après ce qui précède. □

Pour tout diviseur D, on note $\dim(\mathrm{D})$ la dimension de $\mathscr{L}(\mathrm{D})$. Il ressort de la preuve du lemme précédent que, si D est effectif, on a $\dim(\mathrm{D}) \leqslant 1 + \deg(\mathrm{D})$.

Nous voici prêts à prouver que tout diviseur principal est de degré 0. Pour toute fonction non nulle $f \in k(\mathrm{C})$, on pose :

$$\begin{aligned} \mathrm{div}_0(f) &= \sum_{x \text{ zéro de } f} v_x(f) \cdot x, \\ \mathrm{div}_\infty(f) &= \sum_{x \text{ pôle de } f} (-v_x(f)) \cdot x. \end{aligned}$$

Ce sont deux diviseurs effectifs, et on a $\mathrm{div}(f) = \mathrm{div}_0(f) - \mathrm{div}_\infty(f)$. Remarquons également que $\mathrm{div}_\infty(f) = \mathrm{div}_0(1/f)$.

Théorème 4.17. — *Soit $f \in k(\mathrm{C})$ non constante, et soit n le degré de $k(\mathrm{C})$ sur $k(f)$. Alors :*

$$\deg(\mathrm{div}_0(f)) = \deg(\mathrm{div}_\infty(f)) = n.$$

Démonstration. — Quitte à changer f en $1/f$, il suffit de prouver que $\deg \mathrm{div}_\infty(f) = n$. Soit m le degré de $\mathrm{div}_\infty(f)$. D'après la proposition 4.6, on a $m \leqslant n$. Soit $(h_1, \dots, h_n)$ une base de $k(\mathrm{C})$ sur $k(f)$. Pour tout $r \geqslant 1$, les fonctions $h_i f^j$, avec $i \in \{1, \dots, n\}$ et $j \in \{0, \dots, r\}$, sont linéairement indépendantes sur k. Choisissons un diviseur $\mathrm{E} \geqslant 0$ tel que $h_1, \dots, h_n$ appartiennent à $\mathscr{L}(\mathrm{E})$, ce qui est possible car les zéros et pôles des h_i sont en nombre fini. Alors les $h_i f^j$ appartiennent toutes à $\mathscr{L}(\mathrm{E} + r \cdot \mathrm{div}_\infty(f))$ car :

$$\mathrm{div}(h_i f^j) + \mathrm{E} + r \cdot \mathrm{div}_\infty(f) = (\mathrm{div}(h_i) + \mathrm{E}) + (r - j) \cdot \mathrm{div}_\infty(f) + j \cdot \mathrm{div}_0(f)$$

est une somme de trois diviseurs effectifs. Posons $\mathrm{F} = \mathrm{E} + r \cdot \mathrm{div}_0(f)$. C'est un diviseur effectif et on a :

$$n(r+1) \leqslant \dim(\mathrm{F}) \leqslant 1 + \deg(\mathrm{F}) = 1 + mr + \deg(\mathrm{E}),$$

l'inégalité de gauche provenant de ce que les fonctions $h_i f^j$, avec $i \in \{1, \dots, n\}$ et $j \in \{0, \dots, r\}$, sont linéairement indépendantes sur k. Faisant tendre r vers l'infini, on trouve que $m \geqslant n$. □

Corollaire 4.18. — *Tout diviseur principal est de degré* 0.

Corollaire 4.19. — *On a* $\dim(\mathrm{D}) = 0$ *pour tout diviseur* D *de degré* < 0.

Corollaire 4.20. — *Soit* $\mathrm{D} \in \mathrm{Div}(\mathrm{C})$ *de degré* 0. *Les conditions suivantes sont équivalentes :*

(1) D *est principal.*
(2) $\dim(\mathrm{D}) \geqslant 1$.
(3) $\dim(\mathrm{D}) = 1$.

Démonstration. — Si $\mathrm{D} = \mathrm{div}(f)$, alors l'application $g \mapsto fg$ est un isomorphisme de k-espaces vectoriels de $\mathscr{L}(\mathrm{D})$ vers $\mathscr{L}(0)$, qui est de dimension 1

Si $\dim(\mathrm{D}) \geqslant 1$, soit $f \in \mathscr{L}(\mathrm{D})$ non nulle et posons $\mathrm{E} = \mathrm{D} + \mathrm{div}(f) \geqslant 0$. Mais le degré de E est égal à $\deg(\mathrm{D}) = 0$, donc E est nul. Par conséquent, D est le diviseur principal $\mathrm{div}(1/f)$. □

4.5. Le théorème de Riemann

Le théorème suivant définit le genre de C.

Théorème 4.21. — *L'ensemble des entiers* $\deg(\mathrm{D}) - \dim(\mathrm{D}) + 1$*, lorsque* D *décrit* $\mathrm{Div}(\mathrm{C})$*, est majoré. Sa borne supérieure est un entier* $g \geqslant 0$*, qu'on appelle le genre de* C*.*

Démonstration. — Pour tout diviseur D, on pose :

$$i(\mathrm{D}) = \deg(\mathrm{D}) - \dim(\mathrm{D}) + 1.$$

On remarque que :

(1) on a $i(\mathrm{D}) \geqslant 0$ pour tout diviseur effectif D,
(2) on a $i(0) = 0$, et
(3) si $\mathrm{D} \leqslant \mathrm{D}'$, alors $i(\mathrm{D}) \leqslant i(\mathrm{D}')$, c'est-à-dire que la fonction i est croissante sur $\mathrm{Div}(\mathrm{D})$.

(Les deux dernières conditions impliquent la première.) Soit $f \in k(\mathrm{C})$ non constante, et soit $\mathrm{B} = \mathrm{div}_\infty(f)$.

Lemme 4.22. — *Il existe un entier* $m \geqslant 0$ *tel que* $i(r \cdot \mathrm{B}) \leqslant m$ *pour tout entier* $r \geqslant 0$*.*

Démonstration. — Comme on l'a fait dans la preuve du théorème 4.17, on montre qu'il existe un diviseur $\mathrm{E} \geqslant 0$, dépendant de f, tel que $(r+1)\deg(\mathrm{B}) \leqslant \dim(\mathrm{E} + r \cdot \mathrm{B})$ pour tout $r \geqslant 0$. Mais :

$$\dim(\mathrm{E} + r \cdot \mathrm{B}) - \dim(r \cdot \mathrm{B}) \leqslant \deg(\mathrm{E})$$

de sorte que $(r+1)\deg(\mathrm{B}) \leqslant \deg(\mathrm{E}) + \dim(r \cdot \mathrm{B})$. Cela donne $i(r \cdot \mathrm{B}) \leqslant \deg(\mathrm{E} - \mathrm{B}) + 1$. □

Etant donné un diviseur D, il y a un diviseur effectif E tel que $\mathrm{D} \leqslant \mathrm{E}$, donc $i(\mathrm{D}) \leqslant i(\mathrm{E})$. Il suffit donc de majorer $i(\mathrm{E})$ pour E effectif. D'après le lemme 4.22, il existe un $m \geqslant 0$ indépendant de r et E tel que $i(r \cdot \mathrm{B} - \mathrm{E}) \leqslant i(r \cdot \mathrm{B}) \leqslant m$ pour tout $r \geqslant 1$. Pour r assez grand, on a :

$$\dim(r \cdot \mathrm{B} - \mathrm{E}) \geqslant r \cdot \deg(\mathrm{B}) - \deg(\mathrm{E}) + 1 - m \geqslant 1$$

car $\deg(\mathrm{B}) \geqslant 1$. Fixons un tel $r \geqslant 1$ et choisissons une fonction $h \in \mathscr{L}(r \cdot \mathrm{B} - \mathrm{E})$ non nulle. Alors on a $\mathrm{E} - \mathrm{div}(h) \leqslant r \cdot \mathrm{B}$, ce qui donne $i(\mathrm{E}) = i(\mathrm{E} - \mathrm{div}(h)) \leqslant i(r \cdot \mathrm{B}) \leqslant m$. Le théorème 4.21 est prouvé. □

Proposition 4.23. — *Il existe un entier* $c \geqslant 0$*, dépendant uniquement de* C*, tel que :*

$$\deg(\mathrm{D}) - \dim(\mathrm{D}) + 1 = g$$

pour tout diviseur D *de degré* $\geqslant c$*.*

Démonstration. — Soit G un diviseur tel que $i(\mathrm{G}) = g$, et posons $c = \deg(\mathrm{G}) + g$. Si D est un diviseur tel que $\deg(\mathrm{D}) \geqslant c$, alors :

$$g \geqslant i(\mathrm{D} - \mathrm{G}) = \deg(\mathrm{D} - \mathrm{G}) - \dim(\mathrm{D} - \mathrm{G}) + 1 \geqslant g - \dim(\mathrm{D} - \mathrm{G}) + 1.$$

Il y a donc une fonction non nulle $f \in \mathscr{L}(\mathrm{D} - \mathrm{G})$, c'est-à-dire qu'on a $\mathrm{D} + \mathrm{div}(f) \geqslant \mathrm{G}$. L'entier $i(\mathrm{D}) \leqslant g$ est égal à $i(\mathrm{D} + \mathrm{div}(f)) \geqslant i(\mathrm{G}) = g$, ce qui entraîne que $i(\mathrm{D}) = g$ comme voulu. □

Exemple 4.24. — Considérons la courbe projective $\mathrm{C} = \mathbf{V}(\mathrm{Y}^2\mathrm{Z} - \mathrm{X}^3 - \mathrm{XZ}^2)$ dans $\mathbf{P}^2$. Si k est de caractéristique différente de 2, ce que nous supposons, elle est lisse. Le corps $k(\mathrm{C})$ est engendré sur k par les fonctions rationnelles $u = x/z$ et $v = y/z$. Il est quadratique sur $k(u)$, et on a la relation $v^2 = u^3 + u$. Une fonction rationnelle f sur C s'écrit donc de façon unique $\mathrm{A}(u) + v\mathrm{B}(u)$ avec $\mathrm{A}(u), \mathrm{B}(u) \in k(u)$. Posons $\infty = [0 : 1 : 0] \in \mathrm{C}$ et calculons la dimension de l'espace vectoriel $\mathscr{L}(\mathrm{D})$ associé au diviseur effectif $\mathrm{D} = 2n \cdot \infty$ pour n assez grand. On en déduira le genre de C grâce à la proposition 4.23. L'espace $\mathscr{L}(\mathrm{D})$ est formé des fonctions f dont le seul pôle est ∞, et dont l'ordre en ce pôle est supérieur ou égal à $-2n$.

D'abord, si $f = \mathrm{A}(u) + v\mathrm{B}(u)$ n'a aucun pôle sur $\mathrm{C} - \{\infty\} = \mathrm{C} \cap \mathrm{U}_\mathrm{Z}$, elle induit par déshomogénéïsation par rapport à Z une fonction rationnelle $f_\mathrm{Z} = \mathrm{A}(x) + y\mathrm{B}(x)$ sur la courbe algébrique affine $\mathrm{C}_\mathrm{Z} = \varphi_\mathrm{Z}(\mathrm{C} \cap \mathrm{U}_\mathrm{Z}) = \mathbf{V}(\mathrm{Y}^2 - \mathrm{X}^3 - \mathrm{X})$, définie en tout point de celle-ci. D'après la remarque 2.20, il s'ensuit que $f_\mathrm{Z} \in k[\mathrm{C}_\mathrm{Z}] = k[x, y]$, donc que A et B sont des polynômes.

Ensuite, l'idéal maximal M_∞ de l'anneau local $\mathcal{O}_\infty$ des fonctions rationnelles sur C définies en ∞ est engendré par $t = x/y = u/v$ et $z/y = v^{-1}$. Comme $v^{-1} = t^3 + tv^{-2} \in \mathsf{M}_\infty^3$, on en déduit que t est une uniformisante en ∞. Ainsi $f = \mathrm{A}(u) + v\mathrm{B}(u)$, avec $\mathrm{A}(u), \mathrm{B}(u) \in k[u]$, a un pôle en ∞ d'ordre $\geqslant -2n$ si et seulement si $t^{2n} f \in \mathcal{O}_\infty$. Comme $t^2 = u^{-1}/(1 + u^{-2})$ et $1 + u^{-2} \in \mathcal{O}_\infty^\times$, on trouve $v_\infty(u) = -2$ et :

$$t^{2n} f \in \mathcal{O}_\infty \quad \Leftrightarrow \quad u^{-n}\mathrm{A}(u) + vu^{-n}\mathrm{B}(u) \in \mathcal{O}_\infty. \tag{4.4}$$

On a $v_\infty(u^{-n}\mathrm{A}(u)) = 2n - 2\deg(\mathrm{A})$ et :

$$\begin{aligned} v_\infty(vu^{-n}\mathrm{B}(u)) &= \frac{1}{2} \cdot v_\infty((vu^{-n}\mathrm{B}(u))^2) \\ &= \frac{1}{2} \cdot (-6 + 4n - 4\deg(\mathrm{B})) \\ &= 2n - 3 - 2\deg(\mathrm{B}). \end{aligned}$$

Ces deux valuations n'étant jamais égales car de parités différentes, la somme des termes $u^{-n}\mathrm{A}(u)$ et $vu^{-n}\mathrm{B}(u)$ est dans $\mathcal{O}_\infty$ si et seulement si chacun des deux l'est, c'est-à-dire si $\deg(\mathrm{A}) \leqslant n$ et $\deg(\mathrm{B}) \leqslant n - 2$. On en déduit que $\dim(\mathrm{D}) = 2n$ dès que $n \geqslant 2$, et par conséquent que :

$$\deg(\mathrm{D}) - \dim(\mathrm{D}) + 1 = 1$$

dès que $n \geqslant 2$. On déduit de la proposition 4.23 que C est de genre 1.

4.6. Le théorème de Riemann-Roch

Pour finir ce chapitre, nous allons préciser le théorème 4.21, en déterminant la différence entre g et $i(\mathrm{D}) = \deg(\mathrm{D}) - \dim(\mathrm{D}) + 1$ pour tout diviseur D.

Dans tout ce paragraphe, on pose $\mathrm{F} = k(\mathrm{C})$ et on note g le genre de C.

Définition 4.25. — Une *adèle* de F est une application $a : \mathrm{C} \to \mathrm{F}$ telle qu'existe une partie finie $\mathrm{S} \subseteq \mathrm{C}$ telle que $a_x \in \mathcal{O}_x$ pour tout $x \notin \mathrm{S}$.

L'ensemble $\mathbb{A}$ des adèles de F est une sous-F-algèbre de l'algèbre des fonctions de C dans F, un élément $f \in \mathrm{F}$ s'identifiant à l'adèle constante $x \mapsto f$.

Si D est un diviseur sur C, qu'on écrit comme en (4.3), on pose :

$$\mathscr{A}(\mathrm{D}) = \{a \in \mathbb{A} \mid v_x(a_x) \geqslant -n_x \text{ pour tout } x \in \mathrm{C}\}.$$

C'est un sous-k-espace vectoriel de $\mathbb{A}$, et on a $\mathscr{A}(\mathrm{D}) \cap \mathrm{F} = \mathscr{L}(\mathrm{D})$.

Proposition 4.26. — *Soient* $\mathrm{D} \leqslant \mathrm{D}'$ *des diviseurs de* C. *Alors* $\mathscr{A}(\mathrm{D}) \subseteq \mathscr{A}(\mathrm{D}')$ *et :*

$$\dim \mathscr{A}(\mathrm{D}')/\mathscr{A}(\mathrm{D}) = \deg(\mathrm{D}' - \mathrm{D}).$$

Démonstration. — La preuve est identique à celle de la proposition 4.16. La seule différence est que, pour $\mathrm{D}' = \mathrm{D} + y$, la forme linéaire φ n'est pas nulle, car on a $\varphi(a) \neq 0$ pour n'importe quelle adèle $a \in \mathscr{A}(\mathrm{D}')$ telle que $v_y(a_y) = -n_y - 1$. □

Proposition 4.27. — *Pour tout diviseur* D *de* C, *l'espace* $\mathbb{A}/(\mathscr{A}(\mathrm{D})+\mathrm{F})$ *est de dimension finie, égale à* $g - i(\mathrm{D})$.

Démonstration. — Soient D, D' des diviseurs de C tels que $\mathrm{D} \leqslant \mathrm{D}'$. On va montrer que :

$$\dim((\mathscr{A}(\mathrm{D}') + \mathrm{F})/(\mathscr{A}(\mathrm{D}) + \mathrm{F})) = i(\mathrm{D}') - i(\mathrm{D}). \tag{4.5}$$

Pour cela, on considère l'application k-linéaire :

$$u : \mathscr{A}(\mathrm{D}')/\mathscr{A}(\mathrm{D}) \to (\mathscr{A}(\mathrm{D}') + \mathrm{F})/(\mathscr{A}(\mathrm{D}) + \mathrm{F})$$

définie par $u(a+\mathscr{A}(\mathrm{D})) = a+(\mathscr{A}(\mathrm{D})+\mathrm{F})$. Elle est surjective car un élément de la forme $a+f+(\mathscr{A}(\mathrm{D})+\mathrm{F})$ avec $a \in \mathscr{A}(\mathrm{D}')$ et $f \in \mathrm{F}$ a pour antécédent $a+\mathscr{A}(\mathrm{D})$. Son noyau est formé des $a+\mathscr{A}(\mathrm{D})$, avec $a \in \mathscr{A}(\mathrm{D}')$, tels que $a \in \mathscr{A}(\mathrm{D}) + \mathrm{F}$. Pour de tels éléments, il y a un $b \in \mathscr{A}(\mathrm{D})$ et un $f \in \mathrm{F}$ tels que $a = b + f$, ce qui entraîne que $f = a - b \in \mathscr{A}(\mathrm{D}') \cap \mathrm{F} = \mathscr{L}(\mathrm{D}')$. Par conséquent, on a :

$$\mathrm{Ker}(u) = (\mathscr{L}(\mathrm{D}') + \mathscr{A}(\mathrm{D}))/\mathscr{A}(\mathrm{D}) \simeq \mathscr{L}(\mathrm{D}')/\mathscr{L}(\mathrm{D})$$

ce dont on déduit (4.5). Soit maintenant G un diviseur tel que $i(\mathrm{G}) = g$. Montrons que :

$$\mathbb{A} = \mathscr{A}(\mathrm{G}) + \mathrm{F}. \tag{4.6}$$

Si $\mathrm{G}' \geqslant \mathrm{G}$, on a $i(\mathrm{G}') \geqslant i(\mathrm{G}) = g$ donc $i(\mathrm{G}') = i(\mathrm{G})$. Soit $a \in \mathbb{A}$, et soit $\mathrm{G}' \geqslant \mathrm{G}$ tel que $a \in \mathscr{A}(\mathrm{G}')$. La formule (4.5) implique que $\mathscr{A}(\mathrm{G}') \subseteq \mathscr{A}(\mathrm{G}) + \mathrm{F}$, ce qui prouve (4.6).

Soit D un diviseur de C, et soit $\mathrm{D}' \geqslant \mathrm{D}$ tel que $i(\mathrm{D}') = g$ (dont l'existence est assurée par la proposition 4.23). D'après (4.5), l'espace $\mathbb{A}/(\mathscr{A}(\mathrm{D}) + \mathrm{F})$ est de dimension finie $g - i(\mathrm{D})$, comme voulu. □

L'espace $\mathbb{A}/(\mathscr{A}(\mathrm{D}) + \mathrm{F})$ est parfois noté $\mathrm{H}^1(\mathrm{D})$, en référence à la théorie cohomologique sous-jacente (que nous n'aborderons pas dans ce cours).

Définition 4.28. — On appelle *différentielle de Weil* une forme k-linéaire ω sur $\mathbb{A}$ telle qu'il y ait un diviseur D pour lequel le noyau de ω contienne $\mathscr{A}(\mathrm{D}) + \mathrm{F}$.

On note Ω le k-espace vectoriel des différentielles de Weil. Il est muni d'une structure d'espace vectoriel sur F par la formule :

$$\omega f : a \mapsto \omega(fa)$$

définissant une différentielle de Weil ωf à partir de $\omega \in \mathbb{A}$ et de $f \in \mathrm{F}$. Pour tout diviseur D, on note $\Omega(\mathrm{D})$ le sous-espace de Ω formé des différentielles de Weil nulles sur $\mathscr{A}(\mathrm{D}) + \mathrm{F}$, c'est-à-dire le dual de $\mathrm{H}^1(\mathrm{D})$. Si $\omega \in \Omega(\mathrm{D})$ et $f \in \mathrm{F}$, on a $\omega f \in \Omega(\mathrm{D} + \mathrm{div}(f))$.

Proposition 4.29. — *Le* F*-espace vectoriel* Ω *est de dimension* 1.

Démonstration. — Soient ω_1 et ω_2 des différentielles de Weil non nulles, et soient D_1 et D_2 des diviseurs de C tels que $\omega_i \in \Omega(\mathrm{D}_i)$ pour $i = 1, 2$. Etant donné un diviseur B, on a des applications k-linéaires injectives :

$$u_i : \mathscr{L}(\mathrm{D}_i + \mathrm{B}) \to \Omega(-\mathrm{B})$$

définies par $f \mapsto \omega_i f$. On va montrer qu'il existe un diviseur B tel que $\mathrm{Im}(u_1) \cap \mathrm{Im}(u_2)$ ne soit pas réduit à $\{0\}$. Cela prouvera la proposition.

D'après la proposition 4.23, si le degré de B est assez grand, on a $i(\mathrm{D}_i + \mathrm{B}) = g$ pour $i = 1, 2$. D'après la proposition 4.27, l'espace $\Omega(-\mathrm{B})$ est de dimension $g - i(-\mathrm{B}) = g - 1 + \deg(\mathrm{B})$ car $\dim(-\mathrm{B}) = 0$. On écrit :

$$\begin{aligned}\dim(\mathrm{Im}(u_1) \cap \mathrm{Im}(u_2)) &= \dim \mathrm{Im}(u_1) + \dim \mathrm{Im}(u_2) - \dim(\mathrm{Im}(u_1) + \mathrm{Im}(u_2)) \\ &\geqslant \dim(\mathrm{D}_1 + \mathrm{B}) + \dim(\mathrm{D}_2 + \mathrm{B}) - \dim \Omega(-\mathrm{B}) \\ &\geqslant \deg(\mathrm{D}_1 + \mathrm{B}) + \deg(\mathrm{D}_2 + \mathrm{B}) - i(\mathrm{D}_1 + \mathrm{B}) - i(\mathrm{D}_2 + \mathrm{B}) - \deg(\mathrm{B}) + 3 - g\end{aligned}$$

ce qui est $\geqslant \deg(\mathrm{B}) + \deg(\mathrm{D}_1 + \mathrm{D}_2) + 3 - 3g$. Si l'on choisit le degré de B de sorte que ce minorant soit strictement positif, on obtient le résultat voulu. □

Lemme 4.30. — *Soit $\omega \in \Omega$ une différentielle de Weil non nulle. L'ensemble :*

$$\mathrm{Div}(\omega) = \{\mathrm{D} \in \mathrm{Div}(\mathrm{C}) \mid \omega \text{ s'annule sur } \mathscr{A}(\mathrm{D}) + \mathrm{F}\}$$

a un (unique) plus grand élément, noté $\mathrm{div}(\omega)$.

Démonstration. — D'après la proposition 4.23, il existe une constante c ne dépendant que de C telle que $i(\mathrm{D}) = g$ pour tout diviseur D de degré $\geqslant c$. Comme $\dim \Omega(\mathrm{D}) = g - i(\mathrm{D})$ d'après la proposition 4.27, on a $\deg(\mathrm{D}) \leqslant c - 1$ pour tout $\mathrm{D} \in \mathrm{Div}(\omega)$. On peut donc choisir un diviseur $\mathrm{W} \in \mathrm{Div}(\omega)$ de degré maximal.

Soit $\mathrm{D} \in \mathrm{Div}(\omega)$ et supposons que $\mathrm{D} \not\leqslant \mathrm{W}$. Il y a donc un point $y \in \mathrm{C}$ en lequel on ait $v_y(\mathrm{D}) > v_y(\mathrm{W})$. On va montrer que $\mathrm{W}' = \mathrm{W} + y \in \mathrm{Div}(\omega)$, ce qui contredira la maximalité de W. Pour cela, il s'agit de montrer que ω s'annule sur $\mathscr{A}(\mathrm{W}') + \mathrm{F}$.

Toute adèle $a \in \mathscr{A}(\mathrm{W}')$ se décompose de façon unique sous la forme $a' + a''$, où a' est nulle en y et a'' est nulle sur le complémentaire de y dans C. On a donc $a' \in \mathscr{A}(\mathrm{W})$ et $a'' \in \mathscr{A}(\mathrm{D})$, ce qui entraîne l'égalité $\omega(a) = \omega(a') + \omega(a'') = 0$ comme voulu. □

Un diviseur de la forme $\mathrm{div}(\omega)$ pour un $\omega \in \Omega$ non nul s'appelle un *diviseur canonique* de C.

Remarque 4.31. — (1) Deux diviseurs canoniques de C sont équivalents modulo $\mathrm{Pr}(\mathrm{C})$.
(2) Pour tout diviseur D, on a $\Omega(\mathrm{D}) = \{0\} \cup \{\omega \in \Omega \text{ non nulles} \mid \mathrm{div}(\omega) - \mathrm{D} \geqslant 0\}$.

Voici enfin le théorème de Riemann-Roch, qui conclut ce chapitre et ce cours.

Théorème 4.32. — *Soit* W *un diviseur canonique de* C. *Pour tout diviseur* D, *on a :*

$$\deg(\mathrm{D}) - \dim(\mathrm{D}) + 1 = g - \dim(\mathrm{W} - \mathrm{D}).$$

Démonstration. — Il suffit de montrer que les espaces $\Omega(\mathrm{D})$ et $\mathscr{L}(\mathrm{W} - \mathrm{D})$ sont isomorphes. Pour cela, on écrit $\mathrm{W} = \mathrm{div}(\omega)$ et on considère l'application linéaire $\varphi : f \mapsto \omega f$ de $\mathscr{L}(\mathrm{W} - \mathrm{D})$ dans $\Omega(\mathrm{D})$. D'abord, elle est injective d'après la proposition 4.29. Ensuite, toujours d'après la proposition 4.29, toute différentielle de Weil $\omega' \in \Omega(\mathrm{D})$ s'écrit sous la forme ωg pour un unique $g \in \mathrm{F}$. On a :

$$\mathrm{div}(g) + \mathrm{W} - \mathrm{D} = \mathrm{div}(g) + \mathrm{div}(\omega) - \mathrm{D} = \mathrm{div}(\omega g) - \mathrm{D} = \mathrm{div}(\omega') - \mathrm{D} \geqslant 0$$

donc $g \in \mathscr{L}(\mathrm{W} - \mathrm{D})$. □

VINCENT SÉCHERRE, Université de Versailles Saint-Quentin, Bâtiment Fermat, 45 avenue des États-Unis, 78035 Versailles cedex • *E-mail :* vincent.secherre@math.uvsq.fr