Géométrie algébrique

David A. Madore

9 avril 2016

MDI349

Introduction / motivations

Qu'est-ce que la géométrie algébrique ? En condensé :

— **But :** Étudier les solutions de systèmes d'équations polynomiales dans un corps ou un anneau commutatif quelconque, ou des objets apparentés. (Étudier = étudier leur existence, les compter, les paramétrer, les relier, définir une structure dessus, etc.)

— **Géométrie :** Voir de tels systèmes d'équations comme des objets géométriques, soit plongés dans un espace ambiant (espace affine, espace projectif), soit intrinsèques ; leur appliquer des concepts de géométrie (espace tangent, étude locale de singularités, etc.).

— **Moyens :** L'étude locale de ces objets passe par les fonctions définies dessus, qui sont des anneaux commutatifs tout à fait généraux, donc l'*algèbre commutative* (étude des anneaux commutatifs et de leurs idéaux).

Problèmes *géométriques* = étude de solutions sur des corps algébriquement clos (e.g., $\mathbb{C}$: géométrie algébrique complexe ; $\bar{\mathbb{F}}_p$) ou « presque » (e.g., $\mathbb{R}$: géométrie algébrique réelle). Problèmes *arithmétiques* = sur des corps loin d'être algébriquement clos (e.g., $\mathbb{Q}$: géométrie arithmétique), ou des anneaux commutatifs plus généraux (e.g., $\mathbb{Z}$: idem, « équations diophantiennes »).

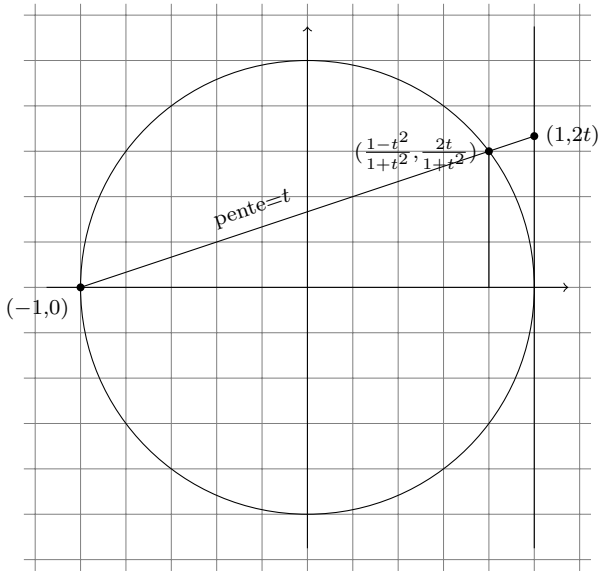
Applications : cryptographie et codage (géométrie sur $\mathbb{F}_q$), calcul formel, robotique (géométrie sur $\mathbb{R}$), analyse complexe (géométrie sur $\mathbb{C}$), théorie des nombres (sur $\mathbb{Q}$, corps de nombres...), etc.

Un exemple : Pour tout anneau commutatif k, on définit $C(k) = \{(x, y) \in k^2 : x^2 + y^2 = 1\}$. Interprétation géométrique : ceci est un cercle ! Il est plongé dans le « plan affine » $\mathbb{A}^2$ défini par $\mathbb{A}^2(k) = k^2$ pour tout anneau k.

— Sur $\mathbb{R}$, les solutions forment effectivement un cercle, au sens naïf.

— (Sur $\mathbb{C}$, les solutions dans $\mathbb{C}^2$ forment une surface, qui ressemblerait plutôt à une sphère privée de deux points.)
— Sur $\mathbb{F}_q$, on peut compter les solutions : on peut montrer qu'il y en a $q-1$ ou $q+1$ selon que $q \equiv 1 \pmod 4$ ou $q \equiv 3 \pmod 4$ (ou encore q pour $q = 2^r$).
— Sur $\mathbb{Q}$, il n'est pas complètement évident de trouver des solutions autres que $(\pm 1, 0)$ et $(0, \pm 1)$. Un exemple : $(\frac{4}{5}, \frac{3}{5})$ (Pythagore, Euclide...).

Paramétrage des solutions :



Un petit calcul géométrique (cf. les formules exprimant $\cos\theta, \sin\theta$ en fonction de $\tan\frac{\theta}{2}$), valable sur tout corps k de caractéristique $\neq 2$ (ou en fait tout anneau commutatif dans lequel 2 est inversible [1]), permet de montrer que toute solution $(x, y) \in C(k)$ autre que $(-1, 0)$ peut s'écrire de la forme $(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$ avec $t \in k$ (uniquement défini, et vérifiant $t^2 \neq -1$).

Remarques : (a) ceci correspond à un point $(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}) \in C(k(t))$ où $k(t)$ est le corps des fonctions rationnelles à une indéterminée sur k ; (b) ceci permet, par exemple, de trouver de nombreuses solutions sur $\mathbb{Q}$, ou d'en trouver rapidement sur $\mathbb{F}_q$ (q impair) ; (c) on a, en fait, défini un « morphisme » d'objets géométriques de la droite affine $\mathbb{A}^1$ vers le cercle C (privé du point $(-1, 0)$).

On peut aussi définir une structure de *groupe* (abélien) sur les points de $C(k)$ pour n'importe quel anneau commutatif k : si $(x, y) \in C(k)$ et $(x', y') \in C(k)$, on définit leur composée $(x, y) \star (x', y') = (x'', y'')$ par

$$\begin{cases} x'' = xx' - yy' \\ y'' = xy' + yx' \end{cases}$$

1. C'est-à-dire, une $\mathbb{Z}[\frac{1}{2}]$-algèbre, où $\mathbb{Z}[\frac{1}{2}] = \{\frac{a}{2^r} : a \in \mathbb{Z}, r \in \mathbb{N}\}$.

(cf. les formules exprimant $\cos(\theta+\theta'), \sin(\theta+\theta')$ en fonction de $\cos\theta, \sin\theta$ et $\cos\theta', \sin\theta'$). Élément neutre : $(1,0)$; inverse de (x,y) : $(x,-y)$.

(Les fonctions trigonométriques, "transcendantes", servent à motiver ces formules, mais les formules sont parfaitement valables sur $\mathbb{F}_q$ bien que $\cos\theta, \sin\theta$ n'aient pas de sens !)

Remarque : Tout élément f de l'anneau commutatif $\mathbb{R}[x,y]/(x^2+y^2-1)$ définit une fonction réelle sur le cercle $C(\mathbb{R})$: ces fonctions s'appellent « polynômes trigonométriques ». Tout élément de l'anneau commutatif $\mathbb{Z}[x,y]/(x^2+y^2-1)$ définit une fonction (à valeurs dans k) sur *n'importe quel* $C(k)$. On verra aussi plus loin qu'un élément de $C(k)$ peut se voir comme un morphisme d'anneaux commutatifs $\mathbb{Z}[x,y]/(x^2+y^2-1) \to k$.

1 Prolégomènes d'algèbre commutative

1.1 Anneaux réduits, intègres

Sauf précision expresse du contraire, tous les anneaux considérés sont commutatifs et ont un élément unité (noté 1). Il existe un unique anneau dans lequel $0=1$, c'est l'anneau réduit à un seul élément, appelé l'**anneau nul**.

Si k est un anneau, une **k-algèbre** (là aussi : implicitement commutative) est la donnée d'un morphisme d'anneaux $k \xrightarrow{\varphi} A$ (appelé *morphisme structural* de l'algèbre). On peut multiplier un élément de A par un élément de k avec : $c \cdot x = \varphi(c)\, x \in A$ (pour $c \in k$ et $x \in A$).

Anneau **réduit** = anneau dans lequel $x^n = 0$ implique $x = 0$. En général, un x (dans un anneau A) tel que $x^n = 0$ pour un certain $n \in \mathbb{N}$ s'appelle un élément **nilpotent**.

Anneau **intègre** = anneau non nul dans lequel $xy = 0$ implique $x = 0$ ou $y = 0$ (remarque : la réciproque vaut dans tout anneau). En général, un x (dans un anneau A) tel qu'il existe $y \neq 0$ tel que $xy = 0$ s'appelle un **diviseur de zéro**.

Élément **inversible** (ou *unité*) d'un anneau A = élément x tel qu'il existe y vérifiant $xy = 1$. L'ensemble $A^\times$ ou $\mathbb{G}_m(A)$ des tels éléments forme un *groupe*, appelé groupe multiplicatif des inversibles de A. Un **corps** est un anneau tel que $A^\times = A \setminus \{0\}$.

Tout corps est un anneau intègre. Tout anneau intègre est un anneau réduit.

On rappelle qu'un **idéal** d'un anneau est un sous-groupe additif I de A tel que $AI \subseteq I$. Si $(x_i)_{i\in\Lambda}$ sont des éléments de A, l'intersection de tous les idéaux contenant les x_i est un idéal et s'appelle l'idéal **engendré** par les x_i : c'est l'ensemble des toutes les combinaisons linéaires $a_1 x_{i_1} + \cdots + a_n x_{i_n}$ avec $a_1, \ldots, a_n \in A$ et $i_1, \ldots, i_n \in \Lambda$. Lorsque Λ est fini : l'idéal I engendré par $x_1, \ldots, x_n$ est l'ensemble des toutes les combinaisons linéaires $a_1 x_1 + \cdots + a_n x_n$ et il peut se noter

$Ax_1 + \cdots + Ax_n$ ou parfois $(x_1, \ldots, x_n)$: on dit que I est un idéal **de type fini**. Si I peut être engendré par un seul élément, $I = Ax$ (aussi noté (x)), on dit que I est un idéal **principal**.

Idéal nul $(0) = \{0\}$. Idéal plein ou idéal unité A : un élément x est inversible ssi l'idéal (x) qu'il engendre est l'idéal unité.

Idéal **maximal** d'un anneau A = un idéal $\mathfrak{m} \neq A$ tel que si $\mathfrak{m} \subseteq \mathfrak{m}'$ (avec $\mathfrak{m}'$ un autre idéal) alors soit $\mathfrak{m}' = \mathfrak{m}$ soit $\mathfrak{m}' = A$). Propriété équivalente : c'est un idéal $\mathfrak{m}$ tel que $A/\mathfrak{m}$ soit un corps.

Idéal **premier** d'un anneau A = un idéal $\mathfrak{p} \neq A$ tel que si $x, y \notin \mathfrak{p}$ alors $xy \notin \mathfrak{p}$. Propriété équivalente : c'est un idéal $\mathfrak{p}$ tel que $A/\mathfrak{p}$ soit intègre.

Idéal **radical** d'un anneau A = un idéal $\mathfrak{r}$ tel que si $x^n \in \mathfrak{r}$ alors $x \in \mathfrak{r}$. Propriété équivalente : c'est un idéal $\mathfrak{r}$ tel que $A/\mathfrak{r}$ soit réduit.

Exemples : L'idéal $7\mathbb{Z}$ de $\mathbb{Z}$ est maximal (le quotient $\mathbb{Z}/7\mathbb{Z}$ est un corps), donc *a fortiori* premier et radical. L'idéal 0 de $\mathbb{Z}$ est premier mais non maximal (le quotient $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$ est un anneau intègre mais non un corps). L'idéal $6\mathbb{Z}$ de $\mathbb{Z}$ est radical mais n'est pas premier. L'idéal $9\mathbb{Z}$ de $\mathbb{Z}$ n'est pas radical.

Un anneau est un corps ssi son idéal (0) est maximal. Un anneau est intègre ssi son idéal (0) est premier. Un anneau est réduit ssi son idéal (0) est radical.

Un anneau est dit **local** lorsqu'il a un unique idéal maximal. (En particulier, un corps est un anneau local.) Le quotient d'un anneau local par son idéal maximal s'appelle son *corps résiduel*. *Exercice :* l'anneau A des rationnels de la forme $\frac{a}{b}$ avec $a, b \in \mathbb{Z}$ et b impair est un anneau local dont l'idéal maximal $\mathfrak{m}$ est formé des $\frac{a}{b}$ avec a pair. (Quel est le corps résiduel ?)

On admet le résultat ensembliste suivant :

Lemme 1.1.1 (principe maximal de Hausdorff)**.** Soit $\mathscr{F}$ un ensemble de parties d'un ensemble A. On suppose que $\mathscr{F}$ est non vide et que pour toute partie non vide $\mathscr{T}$ de $\mathscr{F}$ totalement ordonnée par l'inclusion (c'est-à-dire telle que pour $I, I' \in \mathscr{T}$ on a soit $I \subseteq I'$ soit $I \supseteq I'$) la réunion $\bigcup_{I \in \mathscr{T}} I$ soit contenue dans un élément de $\mathscr{F}$. Alors il existe dans $\mathscr{F}$ un élément $\mathfrak{M}$ maximal pour l'inclusion (c'est-à-dire que si $I \supseteq \mathfrak{M}$ avec $I \in \mathscr{F}$ alors $I = \mathfrak{M}$).

Proposition 1.1.2. Dans un anneau A, tout idéal strict (=autre que A) est inclus dans un idéal maximal.

Démonstration. Si I est un idéal strict de A, on applique le principe maximal de Hausdorff à $\mathscr{F}$ l'ensemble des idéaux stricts de A contenant I. Si $\mathscr{T}$ est une chaîne (=partie totalement ordonnée pour l'inclusion) de tels idéaux, la réunion $\bigcup_{I \in \mathscr{T}} I$ en est encore un [2] (pour voir que la réunion est encore un idéal strict, remarquer que 1 n'y appartient pas). Le principe maximal de Hausdorff permet de conclure. ☺

2. La réunion de deux idéaux n'est généralement pas un idéal, car si $x \in I$ et $x' \in I'$, la

Proposition 1.1.3. Dans un anneau, l'ensemble des éléments nilpotents est un idéal : c'est le plus petit idéal radical (intersection des idéaux radicaux). Cet idéal est aussi l'intersection des idéaux premiers de l'anneau. On l'appelle le **nilradical** de l'anneau.

Démonstration. L'ensemble des nilpotents est un idéal car si $x^n = 0$ et $y^n = 0$ alors $(x+y)^{2n} = 0$ en développant. Il est inclus dans tout idéal radical, et il est visiblement lui-même radical : c'est donc le plus petit idéal radical. Étant inclus dans tout idéal radical, il est *a fortiori* inclus dans tout idéal premier. Reste à montrer que si z est inclus dans tout idéal premier, alors z est nilpotent.

Supposons que z n'est pas nilpotent. Considérons $\mathfrak{p}$ un idéal maximal pour l'inclusion parmi les idéaux ne contenant aucun z^n : un tel idéal existe d'après le principe maximal de Hausdorff (il existe un idéal ne contenant aucun z^n, à savoir $\{0\}$). Montrons qu'il est premier : si $x, y \notin \mathfrak{p}$, on veut voir que $xy \notin \mathfrak{p}$. Par maximalité de $\mathfrak{p}$, chacun des idéaux [3] $\mathfrak{p} + (x)$ et $\mathfrak{p} + (y)$ doit rencontrer $\{z^n\}$, c'est-à-dire qu'on doit pouvoir trouver deux éléments de la forme $f + ax$ et $g + by$ avec $f, g \in \mathfrak{p}$ et $a, b \in A$, qui soient des puissances de z ; leur produit est alors aussi une puissance de z, donc n'est pas dans $\mathfrak{p}$, donc $abxy \notin \mathfrak{p}$ (car les trois autres termes sont dans $\mathfrak{p}$), et a plus forte raison $xy \notin \mathfrak{p}$. ☺

En appliquant ce dernier résultat à A/I, on obtient :

Proposition 1.1.4. Si A est un anneau et I un idéal de A, l'ensemble des éléments tels que $z^n \in I$ pour un certain $n \in \mathbb{N}$ est un idéal : c'est le plus petit idéal radical contenant I. Cet idéal est précisément l'intersection des idéaux premiers de A contenant I. On l'appelle le **radical** de l'idéal I et on le note $\sqrt{I}$.

L'intersection des idéaux maximaux d'un anneau s'appelle le **radical de Jacobson** de cet anneau : il est, en général, strictement plus grand que le nilradical.

Notons aussi la conséquence facile suivante de la proposition 1.1.2.

Proposition 1.1.5. Dans un anneau A, l'ensemble des éléments non-inversibles est la réunion de tous les idéaux maximaux.

Démonstration. Dire que x est inversible signifie que x engendre l'idéal unité. Si c'est le cas, x n'appartient à aucun idéal strict de A, et en particulier aucun idéal

somme $x + x'$ n'a pas de raison d'appartenir à $I \cup I'$. En revanche, si $\mathscr{T}$ est une famille d'idéaux totalement ordonnée par l'inclusion, alors $\bigcup_{I \in \mathscr{T}} I$ est un idéal : si $x \in I$ et $x' \in I'$, où $I, I' \in \mathscr{T}$, on peut écrire soit $I \subseteq I'$ soit $I' \subseteq I$, et dans un cas comme dans l'autre on a $x + x' \in \bigcup_{I \in \mathscr{T}} I$.

3. On rappelle que si I, J sont deux idéaux d'un anneau, l'ensemble $I + J = \{u + v : u \in I, v \in J\}$ est un idéal, c'est l'idéal engendré par $I \cup J$, c'est-à-dire, le plus petit idéal contenant I et J ; on l'appelle idéal somme de I et J. Dans le cas particulier où $J = (x)$ est engendré par un élément, c'est donc l'idéal engendré par $I \cup \{x\}$.

maximal. Réciproquement, si x n'est pas inversible, l'idéal (x) qu'il engendre est strict, donc inclus dans un idéal maximal $\mathfrak{m}$ d'après 1.1.2, donc x est bien dans la réunion des idéaux maximaux. ☺

1.2 Anneaux noethériens

Anneau **noethérien** : c'est un anneau A vérifiant les proprités équivalentes suivantes :

— toute suite croissante pour l'inclusion $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ d'idéaux de A stationne (c'est-à-dire est constante à partir d'un certain rang) ;
— tout idéal I de A est de type fini : il existe une famille ***finie*** (x_i) d'éléments de I qui engendre I comme idéal ;
— plus précisément, si I est l'idéal engendré par une famille x_i d'éléments, on peut trouver une sous-famille finie des x_i qui engendre le même idéal I.

L'essentiel des anneaux utilisés en géométrie algébrique (en tout cas, auxquels on aura affaire) sont noethériens. L'anneau $\mathbb{Z}$ est noethérien. Tout corps est un anneau noethérien. Tout quotient d'un anneau noethérien est noethérien (attention : il n'est pas vrai qu'un sous-anneau d'un anneau noethérien soit toujours noethérien). Et surtout :

Proposition 1.2.1 (théorème de la base de Hilbert)**.** Si A est un anneau noethérien, alors l'anneau $A[t]$ des polynômes à une indéterminée sur A est noethérien.

Démonstration. Soit $I \subseteq A[t]$ un idéal. Supposons par l'absurde que I n'est pas de type fini. On construit par récurrence une suite $f_0, f_1, f_2, \ldots$ d'éléments de I comme suit. Si $f_0, \ldots, f_{r-1}$ ont déjà été choisis, comme l'idéal $(f_0, \ldots, f_{r-1})$ qu'ils engendrent n'est pas I, on peut choisir f_r de plus petit degré possible parmi les éléments de I non dans $(f_0, \ldots, f_{r-1})$.

Appelons c_i le coefficient dominant de f_i. Comme A est supposé noethérien, il existe m tel que $c_0, \ldots, c_{m-1}$ engendrent l'idéal J engendré par tous les c_i. Montrons qu'en fait $f_0, \ldots, f_{m-1}$ engendrent I (ce qui constitue une contradiction).

On peut écrire $c_m = a_0 c_0 + \cdots + a_{m-1} c_{m-1}$. Par ailleurs, le degré de f_m est supérieur ou égal au degré de chacun de $f_0, \ldots, f_{m-1}$ par minimalité de ces derniers. On peut donc construire le polynôme $g = \sum_{i=0}^{m-1} a_i f_i t^{\deg f_m - \deg f_i}$, qui a les mêmes degré et coefficient dominant que f_m, et qui appartient à $(f_0, \ldots, f_{m-1})$. Alors, $f_m - g$ est de degré strictement plus petit que f_m, il appartient à I mais pas à $(f_0, \ldots, f_{m-1})$: ceci contredit la minimalité dans le choix de f_m. ☺

En itérant ce résultat, on voit que si A est noethérien, alors $A[t_1, \ldots, t_d]$ l'est pour tout $d \in \mathbb{N}$. Comme un quotient d'un anneau noethérien est encore noethérien :

Définition 1.2.2. Une A-algèbre B est dite **de type fini** (comme A-algèbre) lorsqu'il existe $x_1, \ldots, x_d \in B$ (qu'on dit *engendrer* B comme A-algèbre) tel que tout élément de B s'écrive $f(x_1, \ldots, x_d)$ pour un certain polynôme $f \in A[t_1, \ldots, t_d]$.

Dire que B est une A-algèbre de type fini engendrée par $x_1, \ldots, x_d$ signifie donc que le morphisme $\xi\colon A[t_1, \ldots, t_d] \to B$ défini par $f \mapsto f(x_1, \ldots, x_d)$ est *surjectif*. Par conséquent, si I désigne le noyau de ce morphisme (c'est-à-dire l'ensemble des $f \in A[t_1, \ldots, t_d]$ qui s'annulent en $(x_1, \ldots, x_d)$) alors ξ définit un isomorphisme $A[t_1, \ldots, t_d]/I \xrightarrow{\sim} B$. On peut donc dire : une A-algèbre de type fini est un quotient de $A[t_1, \ldots, t_d]$ (pour un certain d).

Corollaire 1.2.3. Une algèbre de type fini sur un anneau noethérien, et en particulier sur un corps ou sur $\mathbb{Z}$, est un anneau noethérien.

1.3 Localisation

On dit qu'une partie S d'un anneau A est *multiplicative* lorsque $1 \in S$ et $s, s' \in S \Rightarrow ss' \in S$. Par exemple, le complémentaire d'un idéal premier est, par définition, multiplicative ; en particulier, dans un anneau intègre, l'ensemble des éléments non nuls est une partie multiplicative.

Dans ces conditions, on construit un anneau noté $A[S^{-1}]$ (ou $S^{-1}A$) de la façon suivante : ses éléments sont notés a/s avec $a \in A$ et $s \in S$, où on identifie [4] $a/s = a'/s'$ lorsqu'il existe $t \in S$ tel que $t(a's - as') = 0$. L'addition est définie par $(a/s) + (a'/s') = (a's + as')/(ss')$ (le zéro par $0/1$, l'opposé par $-(a/s) = (-a)/s$) et la multiplication par $(a/s) \cdot (a'/s') = (aa')/(ss')$ (l'unité par $1/1$). Cet anneau est muni d'un morphisme naturel $A \xrightarrow{\iota} A[S^{-1}]$ donné par $a \mapsto a/1$. On l'appelle le **localisé** de A inversant la partie multiplicative S. Si A est une k-algèbre (pour un certain anneau k) alors $A[S^{-1}]$ est une k-algèbre de façon évidente (en composant le morphisme structural $k \to A$ par le morphisme naturel $A \to A[S^{-1}]$).

Proposition 1.3.1.
- — Le morphisme naturel $A \xrightarrow{\iota} A[S^{-1}]$ est injectif si et seulement si S ne contient aucun diviseur de zéro. (Extrême inverse : si S contient 0, alors $A[S^{-1}]$ est l'anneau nul.)
- — Tout idéal J de $A[S^{-1}]$ est de la forme $J = I[S^{-1}] := \{a/s : a \in I, s \in S\}$ où I est l'image réciproque dans A (par le morphisme naturel $\iota\colon A \to A[S^{-1}]$) de l'idéal J considéré.

4. Ce racourci de langage signifie qu'on considère la relation d'équivalence $\sim$ sur $A \times S$ définie par $(a, s) \sim (a', s')$ lorsqu'il existe $t \in S$ tel que $t(a's - as') = 0$, on appelle $A[S^{-1}]$ le quotient $(A \times S)/\sim$, et on note a/s la classe de (a, s) pour cette relation ; il faudrait encore vérifier que toutes les opérations proposées ensuite sont bien définies.

— L'application $\mathfrak{p} \mapsto \iota^{-1}(\mathfrak{p})$ définit une bijection entre les idéaux premiers de $A[S^{-1}]$ et ceux de A ne rencontrant pas S.

Cas particuliers importants : si $\mathfrak{p}$ est premier et $S = A \setminus \mathfrak{p}$ est son complémentaire, on note $A_{\mathfrak{p}} = A[S^{-1}]$; c'est un anneau local (dont l'idéal maximal est $\mathfrak{p}[S^{-1}] = \{a/s : a \in \mathfrak{p}, s \notin \mathfrak{p}\}$) : on l'appelle le localisé de A **en** $\mathfrak{p}$. Si A est un anneau intègre et $S = A \setminus \{0\}$ l'ensemble des éléments non nuls de A, on note $\mathrm{Frac}(A) = A[S^{-1}]$: c'est un corps, appelé **corps des fractions** de A. Par exemple, $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$ et $\mathrm{Frac}(k[t]) = k(t)$ pour k un corps.

Toute partie Σ de A engendre une partie multiplicative S (c'est l'intersection de toutes les parties multiplicatives contenant Σ, ou simplement l'ensemble de tous les produits possibles d'éléments de Σ) : on note généralement $A[\Sigma^{-1}]$ pour $A[S^{-1}]$. En particulier, lorsque $\Sigma = \{\sigma_1, \dots, \sigma_n\}$, on note $A[\sigma_1^{-1}, \dots, \sigma_n^{-1}]$ ou $A[\frac{1}{\sigma_1}, \dots, \frac{1}{\sigma_n}]$.

Proposition 1.3.2. Si A est un anneau et $\sigma_1, \dots, \sigma_n \in A$, alors
— L'anneau $A[\frac{1}{\sigma_1}, \dots, \frac{1}{\sigma_n}]$ s'identifie à $A[\frac{1}{f}]$ où $f = \sigma_1 \cdots \sigma_n$.
— De plus, $A[\frac{1}{f}] \cong A[z]/(zf - 1)$ (ici, $A[z]$ est l'anneau des polynômes en une indéterminée), par un isomorphisme envoyant $\frac{a}{f^n}$ sur la classe de az^n

2 Variétés algébriques affines sur un corps algébriquement clos

Dans cette section, k sera un corps algébriquement clos.

On appelle **espace affine de dimension** d sur k l'ensemble k^d (on parle de droite ou plan affine lorsque $d = 1, 2$). Il sera aussi parfois noté $\mathbb{A}^d$ ou $\mathbb{A}^d(k)$ pour des raisons qui apparaîtront plus loin.

2.1 Correspondance entre fermés de Zariski et idéaux

Comment associer une partie de k^d à un idéal de $k[t_1, \dots, t_d]$?

Si $\mathscr{F}$ est une partie de $k[t_1, \dots, t_d]$, on définit un ensemble $Z(\mathscr{F}) = \{(x_1, \dots, x_d) \in k^d : (\forall f \in \mathscr{F})\, f(x_1, \dots, x_d) = 0\}$.

Remarques évidentes : si $\mathscr{F} \subseteq \mathscr{F}'$ alors $Z(\mathscr{F}) \supseteq Z(\mathscr{F}')$ (la fonction Z est « décroissante pour l'inclusion ») ; on a $Z(\mathscr{F}) = \bigcap_{f \in \mathscr{F}} Z(f)$ (où $Z(f)$ est un racourci de notation pour $Z(\{f\})$). Plus intéressant : si I est l'idéal engendré par $\mathscr{F}$ alors $Z(I) = Z(\mathscr{F})$. On peut donc se contenter de regarder les $Z(I)$ avec I idéal de $k[t_1, \dots, t_d]$. Encore un peu mieux : si $\sqrt{I} = \{f : (\exists n)\, f^n \in I\}$ désigne le radical de l'idéal I, on a $Z(\sqrt{I}) = Z(I)$; on peut donc se contenter de considérer les $Z(I)$ avec I idéal radical.

On appellera **fermé de Zariski** dans k^d une partie E de la forme $Z(\mathscr{F})$ pour une certaine partie $\mathscr{F}$ de $k[t_1, \ldots, t_d]$, dont on a vu qu'on pouvait supposer qu'il s'agit d'un idéal radical.

Le vide est un fermé de Zariski ($Z(1) = \varnothing$) ; l'ensemble k^d tout entier est un fermé de Zariski ($Z(0) = k^d$). Tout singleton est un fermé de Zariski : en effet, $Z(\mathfrak{m}_x) = \{x\}$, où $\mathfrak{m}_x$ est l'idéal $(t_1 - x_1, \ldots, t_d - x_d)$; remarquer que $\mathfrak{m}_x$ est un idéal maximal, le quotient $k[t_1, \ldots, t_d]/\mathfrak{m}_x$ s'identifiant à k par la fonction $f \mapsto f(x)$ d'évaluation en x.

Si $(E_i)_{i\in\Lambda}$ sont des fermés de Zariski, alors $\bigcap_{i\in\Lambda} E_i$ est un fermé de Zariski : plus précisément, si $(I_i)_{i\in\Lambda}$ sont des idéaux de $k[t_1, \ldots, t_d]$, alors $Z(\sum_{i\in\Lambda} I_i) = \bigcap_{i\in\Lambda} Z(I_i)$. Si E, E' sont des fermés de Zariski, alors $E \cup E'$ est un fermé de Zariski : plus précisément, si I, I' sont des idéaux de $k[t_1, \ldots, t_d]$, alors $Z(I \cap I') = Z(I) \cup Z(I')$ (l'inclusion $\supseteq$ est évidente ; pour l'autre inclusion, si $x \in Z(I \cap I')$ mais $x \notin Z(I)$, il existe $f \in I$ tel que $f(x) \neq 0$, et alors pour tout $f' \in I'$ on a $f(x)\, f'(x) = 0$ puisque $f f' \in I \cap I'$, donc $f'(x) = 0$, ce qui prouve $x \in Z(I')$).

Comment associer un idéal de $k[t_1, \ldots, t_d]$ à une partie de k^d ?

Réciproquement, si E est une partie de k^d, on note $\mathfrak{I}(E) = \{f \in k[t_1, \ldots, t_d] : (\forall (x_1, \ldots, x_d) \in E)\, f(x_1, \ldots, x_d) = 0\}$. Vérification facile : c'est un idéal de $k[t_1, \ldots, t_d]$, et même un idéal radical. Remarque évidente : si $E \subseteq E'$ alors $\mathfrak{I}(E) \supseteq \mathfrak{I}(E')$; on a $\mathfrak{I}(E) = \bigcap_{x\in E} \mathfrak{m}_x$ (où $\mathfrak{m}_x$ désigne l'idéal maximal $\mathfrak{I}(\{x\})$ des polynômes s'annulant en x), et en particulier $\mathfrak{I}(E) \neq k[t_1, \ldots, t_d]$ dès que $E \neq \varnothing$.

On a de façon triviale $\mathfrak{I}(\varnothing) = k[t_1, \ldots, t_d]$. De façon moins évidente, si k est infini (ce qui est en particulier le cas lorsque k est algébriquement clos), on a $\mathfrak{I}(k^d) = (0)$ (démonstration par récurrence sur d, laissée en exercice).

Sur un corps fini $\mathbb{F}_q$, on a $\mathfrak{I}({\mathbb{F}_q}^d) \neq (0)$. Par exemple, si t est une des indéterminées, le polynôme $t^q - t$ s'annule en tout point de ${\mathbb{F}_q}^d$.

Le rapport entre ces deux fonctions

On a $E \subseteq Z(\mathscr{F})$ ssi $\mathscr{F} \subseteq \mathfrak{I}(E)$, puisque les deux signifient « tout polynôme dans $\mathscr{F}$ s'annule en tout point de E ».

En particulier, en appliquant cette remarque à $\mathscr{F} = \mathfrak{I}(E)$, on a $E \subseteq Z(\mathfrak{I}(E))$ pour toute partie E de k^d ; et en appliquant la remarque à $E = Z(\mathscr{F})$, on a $\mathscr{F} \subseteq \mathfrak{I}(Z(\mathscr{F}))$. De $E \subseteq Z(\mathfrak{I}(E))$ on déduit $\mathfrak{I}(E) \supseteq \mathfrak{I}(Z(\mathfrak{I}(E)))$ (car $\mathfrak{I}$ est décroissante), mais par ailleurs $\mathfrak{I}(E) \subseteq \mathfrak{I}(Z(\mathfrak{I}(E)))$ en appliquant l'autre inclusion à $\mathfrak{I}(E)$: donc $\mathfrak{I}(E) = \mathfrak{I}(Z(\mathfrak{I}(E)))$ pour toute partie E de k^d ; de même, $Z(\mathscr{F}) = Z(\mathfrak{I}(Z(\mathscr{F})))$ pour tout ensemble $\mathscr{F}$ de polynômes. On a donc prouvé :

Proposition 2.1.1. Avec les notations ci-dessus :

— Une partie E de k^d vérifie $E = Z(\mathfrak{I}(E))$ si et seulement si elle est de la forme $Z(\mathscr{F})$ pour un certain $\mathscr{F}$ (= : c'est un fermé de Zariski), et dans ce cas on peut prendre $\mathscr{F} = \mathfrak{I}(E)$, qui est un idéal radical.
— Une partie I de $k[t_1, \ldots, t_d]$ vérifie $I = \mathfrak{I}(Z(I))$ si et seulement si elle est de la forme $\mathfrak{I}(E)$ pour un certain E, et dans ce cas on peut prendre $E = Z(I)$, et I est un idéal radical de $k[t_1, \ldots, t_d]$.
— Les fonctions $\mathfrak{I}$ et Z se restreignent en des bijections décroissantes réciproques entre l'ensemble des fermés de Zariski E de k^d et l'ensemble des idéaux (radicaux) I de $k[t_1, \ldots, t_d]$ tels que $I = \mathfrak{I}(Z(I))$.

On va voir ci-dessous que les idéaux tels que $I = \mathfrak{I}(Z(I))$ sont exactement (tous) les idéaux radicaux de $k[t_1, \ldots, t_d]$.

Fermés irréductibles et idéaux premiers

On dit qu'un fermé de Zariski $E \subseteq k^d$ non vide est **irréductible** lorsqu'on ne peut pas écrire $E = E' \cup E''$, où E', E'' sont deux fermés de Zariski (forcément contenus dans E...), sauf si $E' = E$ ou $E'' = E$.

Contre-exemple : $Z(xy)$ (dans le plan k^2 de coordonnées x, y) n'est pas irréductible, car $Z(xy) = \{(x, y) \in k^2 : xy = 0\} = \{(x, y) \in k^2 : x = 0 \text{ ou } y = 0\} = Z(x) \cup Z(y)$ est réunion de $Z(x)$ (l'axe des ordonnées) et $Z(y)$ (l'axe des abscisses) qui sont tous les deux strictement plus petits que $Z(xy)$.

Proposition 2.1.2. Un fermé de Zariski $E \subseteq k^d$ est irréductible si, et seulement si, l'idéal $\mathfrak{I}(E)$ est premier.

Démonstration. Supposons $\mathfrak{I}(E)$ premier : on veut montrer que E est irréductible. Supposons $E = E' \cup E''$ comme ci-dessus (on a vu que $E = Z(\mathfrak{I}(E))$, $E' = Z(\mathfrak{I}(E'))$ et $E'' = Z(\mathfrak{I}(E''))$) : on veut montrer que $E' = E$ ou $E'' = E$. Supposons le contraire, c'est-à-dire $\mathfrak{I}(E) \neq \mathfrak{I}(E')$ et $\mathfrak{I}(E) \neq \mathfrak{I}(E'')$. Il existe alors $f' \in \mathfrak{I}(E') \setminus \mathfrak{I}(E)$ et $f'' \in \mathfrak{I}(E'') \setminus \mathfrak{I}(E)$. On a alors $f'f'' \notin \mathfrak{I}(E)$ car $\mathfrak{I}(E)$ est premier, et pourtant $f'f''$ s'annule sur E' et E'' donc sur E, une contradiction.

Réciproquement, supposons E irréductible : on veut montrer que $\mathfrak{I}(E)$ est premier. Soient f', f'' tels que $f'f'' \in \mathfrak{I}(E)$: posons $E' = Z(\mathfrak{I}(E) + (f'))$ et $E'' = Z(\mathfrak{I}(E) + (f''))$. On a $E' \subseteq E$ et $E'' \subseteq E$ puisque $E = Z(\mathfrak{I}(E))$, et en fait $E' = E \cap Z(f')$ et $E'' = E \cap Z(f'')$; on a par ailleurs $E = E' \cup E''$ (car si $x \in E$ alors $f'(x)\, f''(x) = 0$ donc soit $f'(x) = 0$ soit $f''(x) = 0$, et dans le premier cas $x \in E'$ et dans le second $x \in E''$). Puisqu'on a supposé E irréductible, on a, disons, $E' = E$, c'est-à-dire $E \subseteq Z(f')$, ce qui signifie $f' \in \mathfrak{I}(E)$. Ceci montre bien que $\mathfrak{I}(E)$ est premier. ☺

2.2 Le Nullstellensatz

(Nullstellensatz, littéralement, « théorème du lieu d'annulation », ou « théorème des zéros de Hilbert ».)

On rappelle que k est algébriquement clos ! (Pour l'instant, cela n'a pas beaucoup servi.)

Proposition 2.2.1 (Nullstellensatz faible)**.** Soit k un corps algébriquement clos. Si I est un idéal de $k[t_1, \ldots, t_d]$ tel que $Z(I) = \varnothing$, alors $I = k[t_1, \ldots, t_d]$.

Démonstration dans le cas particulier où k est indénombrable. Supposons par contraposée $I \subsetneq k[t_1, \ldots, t_d]$. Alors il existe un idéal maximal $\mathfrak{m}$ tel que $I \subseteq \mathfrak{m}$, et on a $Z(\mathfrak{m}) \subseteq Z(I)$. On va montrer $Z(\mathfrak{m}) \neq \varnothing$.

Soit $K = k[t_1, \ldots, t_d]/\mathfrak{m}$. Il s'agit d'un corps, qui est de dimension au plus dénombrable (=il a une famille génératrice dénombrable, à savoir les images des monômes dans les t_i) sur k. Mais K ne peut pas contenir d'élément transcendant τ sur k car, k ayant été supposé indénombrable, la famille des $\frac{1}{\tau - x}$ pour $x \in k$ serait linéairement indépendante (par décomposition en élément simples) dans $k(\tau)$ donc dans K. Donc K est algébrique sur k. Comme k était supposé algébriquement clos, on a en fait $K = k$. Les classes des indéterminées $t_1, \ldots, t_d$ définissent alors des éléments $x_1, \ldots, x_d \in k$, et pour tout $f \in \mathfrak{m}$, on a $f(x_1, \ldots, x_d) = 0$. Autrement dit, $(x_1, \ldots, x_d) \in Z(\mathfrak{m})$, ce qui conclut. ☺

En fait, dans le cours de cette démonstration, on a montré (dans le cas particulier où on s'est placé, mais c'est vrai en général) :

Proposition 2.2.2 (idéaux maximaux de $k[t_1, \ldots, t_d]$)**.** Soit k un corps algébriquement clos. Tout idéal maximal $\mathfrak{m}$ de $k[t_1, \ldots, t_d]$ est de la forme $\mathfrak{m}_{(x_1,\ldots,x_d)} := \{f : f(x_1, \ldots, x_d) = 0\}$ pour un certain $(x_1, \ldots, x_d) \in k^d$.

Démonstration. En fait, on a prouvé que si $\mathfrak{m}$ est un idéal maximal, il existe $(x_1, \ldots, x_d) \in k^d$ tels que $(x_1, \ldots, x_d) \in Z(\mathfrak{m})$, ce qui donne $\mathfrak{m} \subseteq \mathfrak{I}(\{(x_1, \ldots, x_d)\})$, mais par maximalité de $\mathfrak{m}$ ceci est en fait une égalité. ☺

En particulier, le corps quotient $k[t_1, \ldots, t_d]/\mathfrak{m}$ est isomorphe à k, l'isomorphisme étant donnée par l'évaluation au point $(x_1, \ldots, x_d)$ tel que ci-dessus.

Théorème 2.2.3 (Nullstellensatz = théorème des zéros de Hilbert)**.** Soit I un idéal de $k[t_1, \ldots, t_d]$ (toujours avec k un corps algébriquement clos) : alors $\mathfrak{I}(Z(I)) = \sqrt{I}$ (le radical de I).

Démonstration. On sait que $\sqrt{I} \subseteq \mathfrak{I}(Z(I))$ et il s'agit de montrer la réciproque. Soit $f \in \mathfrak{I}(Z(I))$: on veut prouver $f \in \sqrt{I}$. On vérifie facilement que ceci revient à montrer que l'idéal $I[\frac{1}{f}]$ de $k[t_1, \ldots, t_d, \frac{1}{f}]$ est l'idéal unité. Or $k[t_1, \ldots, t_d, \frac{1}{f}] =$

$k[t_1, \ldots, t_d, z]/(zf - 1)$ d'après 1.3.2. Soit J l'idéal engendré par I et $zf - 1$ dans $k[t_1, \ldots, t_d, z]$: on voit que $Z(J) = \varnothing$ (dans k^{d+1}), car on ne peut pas avoir simultanément $f(x_1, \ldots, x_d) = 0$ et $z\, f(x_1, \ldots, x_d) = 1$, donc le Nullstellensatz faible entraîne $J = k[t_1, \ldots, t_d, z]$: ceci donne $I[\frac{1}{f}] = k[t_1, \ldots, t_d, \frac{1}{f}]$. ☺

Scholie 2.2.4. Si k est un corps algébriquement clos, les fonctions $I \mapsto Z(I)$ et $E \mapsto \mathfrak{I}(E)$ définissent des bijections réciproques, décroissantes pour l'inclusion, entre les idéaux radicaux de $k[t_1, \ldots, t_d]$ d'une part, et les fermés de Zariski de k^d d'autre part.

Ces bijections mettent les *points* (c'est-à-dire les singletons) de k^d en correspondance avec les idéaux maximaux de $k[t_1, \ldots, t_d]$ (ils ont tous pour quotient k), et les *fermés irréductibles* en correspondance avec les idéaux premiers.

2.3 L'anneau d'un fermé de Zariski

Si X est un fermé de Zariski dans k^d avec k algébriquement clos, on a vu qu'il existe un unique idéal radical I de $k[t_1, \ldots, t_d]$, à savoir l'idéal $I = \mathfrak{I}(X)$ des polynômes s'annulant sur X, tel que $X = Z(I)$. Le quotient $k[t_1, \ldots, t_d]/I$ (qui est donc un anneau réduit, et intègre ssi X est irréductible) s'appelle l'**anneau des fonctions régulières** sur X et se note $\mathcal{O}(X)$ (ou parfois $k[X]$).

Pourquoi fonctions régulières ? On peut considérer un élément $f \in \mathcal{O}(X)$ comme une fonction $X \to k$ de la façon suivante : si $\tilde{f} \in k[t_1, \ldots, t_d]$ est un représentant de f (modulo I) et si $x = (x_1, \ldots, x_d) \in X$, la valeur de $\tilde{f}(x_1, \ldots, x_d)$ ne dépend pas du choix de $\tilde{f}$ représentant f puisque tout élément de I s'annule en x ; on peut donc appeler $f(x)$ cette valeur. Inversement, un $f \in \mathcal{O}(X)$ est complètement déterminé par sa valeur sur chaque point x de X (rappel : k est algébriquement clos ici, et c'est important !) ; en effet, si f s'annule en tout $x \in X$, tout élément de $k[t_1, \ldots, t_d]$ représentant f s'annule en tout $x \in X$, c'est-à-dire appartient à $\mathfrak{I}(X)$, ce qui signifie justement $f = 0$ dans $\mathcal{O}(X)$. Moralité : on peut bien considérer les éléments de $\mathcal{O}(X)$ comme des fonctions. Ces fonctions sont, tout simplement, *les restrictions à X des fonctions polynomiales sur l'espace affine $\mathbb{A}^d$*.

Dans le cas où $X = \mathbb{A}^d = k^d$ tout entier (donc $I = (0)$), évidemment, $\mathcal{O}(\mathbb{A}^d) = k[t_1, \ldots, t_d]$.

On définit un **fermé de Zariski de** X comme un fermé de Zariski de k^d qui se trouve être inclus dans X. La bonne nouvelle est que la correspondance entre fermés de Zariski de k^d et idéaux de $k[t_1, \ldots, t_d]$ se généralise presque mot pour mot à une correspondance entre fermés de Zariski de X et idéaux de $\mathcal{O}(X)$:

Proposition 2.3.1. Avec les notations ci-dessus :

— Tout fermé de Zariski de X est de la forme $Z(\mathscr{F}) := \{x \in X : (\forall f \in \mathscr{F})\ f(x) = 0\}$ pour un certain ensemble $\mathscr{F}$ d'éléments de $\mathcal{O}(X)$.

— En posant $\mathfrak{I}(E) := \{f \in \mathcal{O}(X) : (\forall x \in E)\, f(x) = 0\}$, les fonctions $I \mapsto Z(I)$ et $E \mapsto \mathfrak{I}(E)$ définissent des bijections réciproques, décroissantes pour l'inclusion, entre les idéaux radicaux de $\mathcal{O}(X)$ d'une part, et les fermés de Zariski de X d'autre part : on a $\mathfrak{I}(Z(I)) = \sqrt{I}$ pour tout idéal I de $\mathcal{O}(X)$.
— Ces bijections mettent les *points* (c'est-à-dire les singletons) de X en correspondance avec les idéaux maximaux de $\mathcal{O}(X)$ (qui sont donc tous de la forme $\mathfrak{m}_x := \{f \in \mathcal{O}(X) : f(x) = 0\}$ pour un $x \in X$) ; et les *fermés irréductibles* en correspondance avec les idéaux premiers.

Soulignons en particulier que si X' est un fermé de Zariski de X (disons défini comme $X' = Z(I)$ où I est un idéal radical de $\mathcal{O}(X)$), alors la surjection canonique $\mathcal{O}(X) \to \mathcal{O}(X)/I$ est un morphisme d'anneaux $\mathcal{O}(X) \to \mathcal{O}(X')$ qu'il faut interpréter comme envoyant une fonction régulière f sur X sur sa *restriction* à X', parfois notée $f|_{X'}$.

2.4 Variétés algébriques affines, morphismes

On appelle provisoirement **variété algébrique affine** dans k^d (toujours avec k algébriquement clos) un fermé de Zariski X de k^d. Pourquoi cette double terminologie ? Le terme « fermé de Zariski » insiste sur X en tant que plongé dans l'espace affine $\mathbb{A}^d$. Le terme de « variété algébrique affine » insiste sur l'aspect intrinsèque de X, muni de ses propres fermés de Zariski et de ses propres fonctions régulières, qu'on va maintenant présenter. On a vu ci-dessus comment associer à X un anneau $\mathcal{O}(X)$ des fonctions régulières, qui coïncide avec l'ensemble des fonctions $X \to k$ qui sont restrictions de fonctions polynomiales sur k^d.

On appelle **morphisme de variétés algébriques affines** sur k entre un fermé de Zariski $X \subseteq k^d$ et un fermé de Zariski $Y \subseteq k^e$ une application $X \to Y$ telle que chacune des e coordonnées à l'arrivée soit une fonction régulière sur X. Autrement dit, il s'agit de la donnée de e éléments $f_1, \ldots, f_e$ de $\mathcal{O}(X)$ tels que $(f_1(x), \ldots, f_e(x)) \in Y$ pour tout $x \in X$.

Proposition 2.4.1. Si $X = Z(I) \subseteq k^d$ et $Y = Z(J) \subseteq k^e$, et si $(f_1, \ldots, f_e) \in \mathcal{O}(X)$, alors $f = (f_1, \ldots, f_e)$ définit un morphisme $X \to Y$ (autrement dit $(f_1(x), \ldots, f_e(x)) \in Y$ pour tout $x \in X$) *si et seulement si* $h(f_1, \ldots, f_e) = 0$ (vu comme élément de $\mathcal{O}(X)$) pour tout $h \in J$.

Démonstration. Il y a équivalence entre :
— $h(f_1, \ldots, f_e) = 0$ dans $\mathcal{O}(Y)$ pour tout $h \in J$,
— $h(f_1(x), \ldots, f_e(x)) = 0$ pour tout $h \in J$ et $x \in X$, et
— $(f_1(x), \ldots, f_e(x)) \in Y$ pour tout $x \in X$.

(L'équivalence entre les deux premières affirmations vient du fait que pour $g \in \mathcal{O}(X)$, ici $g = h(f_1, \ldots, f_e)$, on a $g = 0$ si et seulement si $g(x) = 0$ pour tout $x \in X$. L'équivalence entre les deux dernières vient du fait que $(y_1, \ldots, y_e) \in Y$ si et seulement si $h(y_1, \ldots, y_e) = 0$ pour tout $h \in J$ par définition de $Y = Z(J)$.) ☺

Remarquons en particulier que les fonctions régulières sur X (c'est-à-dire les éléments de $\mathcal{O}(X)$) peuvent se voir comme des morphismes $X \to \mathbb{A}^1$ de X vers la droite affine.

Remarquons par ailleurs que les morphismes de variétés algébriques se composent : donnés deux morphismes $X \to Y$ et $Y \to Z$, on peut définir un morphisme $X \to Z$ en composant les applications.

Lorsque $f\colon X \to Y$ est un morphisme comme ci-dessus, on définit $f^*\colon \mathcal{O}(Y) \to \mathcal{O}(X)$ de la façon suivante : si $h \in \mathcal{O}(Y)$ est une fonction régulière vue comme un morphisme $Y \to \mathbb{A}^1$, on définit $f^*(h) \in \mathcal{O}(X)$ comme la fonction régulière donnée par le morphisme composé $h \circ f\colon X \to \mathbb{A}^1$. (Autrement dit, f^* est l'application de composition à droite par f.)

Proposition 2.4.2. Si $X \subseteq \mathbb{A}^d$ et $Y \subseteq \mathbb{A}^e$ sont deux variétés algébriques affines, la correspondance $f \mapsto f^*$ définie ci-dessus définit une bijection entre les morphismes $X \to Y$ de variétés algébriques affines et les morphismes $\mathcal{O}(Y) \to \mathcal{O}(X)$ de k-algèbres.

Démonstration. Si les indéterminées $u_1, \ldots, u_e$ sont les e coordonnées sur $\mathbb{A}^e$, alors les classes de $u_1, \ldots, u_e$ définissent des éléments de $\mathcal{O}(Y)$: si $f\colon X \to Y$ est un morphisme de variétés algébriques, alors les fonctions $f_1, \ldots, f_e \in \mathcal{O}(X)$ le définissant sont simplement les images par f^* de ces éléments. Ceci montre que f^* permet de retrouver f (la correspondance $f \mapsto f^*$ est injective). Et si $\psi\colon \mathcal{O}(Y) \to \mathcal{O}(X)$ est un morphisme quelconque, alors en définissant $f_1, \ldots, f_e$ comme les images de $u_1, \ldots, u_e \in \mathcal{O}(Y)$ par ψ, on a $h(f_1, \ldots, f_e) = 0$ dans $\mathcal{O}(Y)$ pour tout $h \in J$ (puisque $h(u_1, \ldots, u_e) = 0$ dans $\mathcal{O}(Y)$) donc $f_1, \ldots, f_e$ définissent bien un morphisme $X \to Y$. ☺

Une fois qu'on dispose de cette notion de morphisme, on peut par exemple dire que deux variétés algébriques affines X, Y sont **isomorphes** lorsqu'il existe des morphismes $X \to Y$ et $Y \to X$ dont la composée chaque sens est l'identité. Ceci signifie, tout simplement, que les k-algèbres $\mathcal{O}(X)$ et $\mathcal{O}(Y)$ sont isomorphes.

Ceci justifie partiellement la différence de terminologie entre « fermé de Zariski » (dans k^d) et « variété algébrique affine » (sur k) : dans le premier cas, on insiste sur X en tant que partie de k^d, tandis que dans le second cas on la considère *à isomorphisme près* de variété algébrique affine (sur k).

Pour souligner qu'on parle de l'ensemble des points de X, plutôt que de X comme variété algébrique affine, on écrit parfois $X(k)$.

Exemples : Considérons la courbe d'équation $y^2 = x^3$, c'est-à-dire $C = Z(g)$ où $g = y^2 - x^3 \in k[x, y]$ (anneau des polynômes à deux indéterminées x, y sur un corps algébriquement clos k), et $\mathbb{A}^1$ la droite affine sur k. On a $\mathcal{O}(C) = k[x, y]/(y^2 - x^3)$ et $\mathcal{O}(\mathbb{A}^1) = k[t]$. On définit un morphisme $\mathbb{A}^1 \xrightarrow{f} C$ par $t \mapsto (t^2, t^3)$: ce morphisme correspond à un morphisme d'anneaux dans l'autre sens, $\mathcal{O}(C) \xrightarrow{f^*} \mathcal{O}(\mathbb{A}^1)$, donné par $x \mapsto t^2$ et $y \mapsto t^3$. Ce morphisme n'est pas un isomorphisme car t n'est pas dans l'image de f^*. Ceci, bien que $\mathbb{A}^1(k) \to C(k)$ soit une bijection au niveau des k-points.

Considérons la courbe $C^\sharp$ (la « cubique gauche » affine) d'équations $y = z^3$ et $x = z^2$, c'est-à-dire $C^\sharp = Z(x - z^2, y - z^3)$. On a un morphisme $\mathbb{A}^1 \to C^\sharp$ envoyant t sur (t^2, t^3, t) : cette fois, ce morphisme est un isomorphisme, et sa réciproque est donnée par $(x, y, z) \mapsto z$. L'anneau $\mathcal{O}(C^\sharp) = k[x, y, z]/(x - z^2, y - z^3)$ est isomorphe à $k[t]$. Par ailleurs, le morphisme $\mathbb{A}^1 \to C$ décrit au paragraphe précédent peut être vu comme la composée de l'isomorphisme $\mathbb{A}^1 \to C^\sharp$ et de la projection $C^\sharp \to C$ décrite par $(x, y, z) \mapsto (x, y)$.

Sur le cercle $C = Z(x^2+y^2-1)$ (pas le même C que dans les deux paragraphes précédents), si k est de caractéristique $\neq 5$, on peut définir le morphisme $C \to C$ de « rotation d'angle $\arctan \frac{3}{4}$ » (terminologie abusive si k n'est pas un corps contenant $\mathbb{R}$) ou « multiplication par le point $(\frac{4}{5}, \frac{3}{5})$ » par $(x, y) \mapsto (\frac{4}{5}x - \frac{3}{5}y, \frac{3}{5}x + \frac{4}{5}y)$. C'est un isomorphisme de C avec lui-même. On pourrait définir l'opération de composition $C \times C \to C$ par $((x, y), (x', y')) \mapsto (xx' - yy', xy' + yx')$ mais il faudrait pour cela avoir défini le produit de deux variétés (pour donner un sens à $C \times C$), ce qu'on n'a pas encore fait.

Variétés algébriques affines abstraites, et le spectre d'une algèbre.

Note : On considère que deux variétés algébriques (affines) sont « la même » lorsqu'elle sont isomorphes, alors que deux fermés de Zariski sont « le même » lorsqu'ils sont égaux dans le $\mathbb{A}^d$ dans lequel ils vivent. Par exemple, la cubique gauche $C^\sharp$ décrite ci-dessus, en tant que fermé de Zariski, n'est pas une droite, mais en tant que variété algébrique affine c'est juste $\mathbb{A}^1$ puisqu'on a montré qu'elle lui était isomorphe. Ou, si on préfère, un fermé de Zariski de $\mathbb{A}^d$ est la donnée d'une variété algébrique affine *plus* un plongement de celle-ci dans $\mathbb{A}^d$.

Dans cette optique, si R est une k-algèbre de type fini (on rappelle, cf. 1.2.2, que cela signifie que R est engendrée en tant qu'algèbre par un nombre fini d'éléments $x_1, \ldots, x_d$, autrement dit que R peut se voir comme le quotient de $k[t_1, \ldots, t_d]$ par un idéal $(f_1, \ldots, f_r)$ de ce dernier) et si R est réduite, alors on peut voir R comme l'anneau $\mathcal{O}(X)$ pour une certaine variété algébrique X, à savoir le $X = Z(f_1, \ldots, f_r)$ défini par les équations $f_1 = 0, \ldots, f_r = 0$ dans $\mathbb{A}^d$. Cette variété est unique en ce sens que toutes les variétés X telles que $\mathcal{O}(X) = R$ sont isomorphes (puisque leurs $\mathcal{O}(X)$ sont isomorphes, justement). On peut donc donner un nom à X : c'est le **spectre** de R, noté $\operatorname{Spec} R$. (Par

exemple, $\operatorname{Spec} k[t] = \mathbb{A}^1_k$ et plus généralement $\operatorname{Spec} k[t_1, \ldots, t_d] = \mathbb{A}^d_k$. Et bien sûr, $\operatorname{Spec} k$ est vu comme un point. Quant à l'ensemble vide, c'est $\operatorname{Spec} 0$ où 0 est l'anneau nul.)

Abstraitement, on peut donc dire que les variétés algébriques affines sont les $\operatorname{Spec} R$ pour R une k-algèbre réduite de type fini.

2.5 La topologie de Zariski

On appelle **ouvert de Zariski** dans k^d (toujours avec k un corps algébriquement clos) le complémentaire d'un fermé de Zariski. Autrement dit, si I est un idéal de $k[t_1, \ldots, t_d]$, on définit $U(I) = \{(x_1, \ldots, x_d) \in k^d : (\exists f \in I)\, f(x_1, \ldots, x_d) \neq 0\}$ le complémentaire de $Z(I)$: un ouvert de Zariski de k^d est un ensemble de la forme $U(I)$. Plus généralement, si X est une variété algébrique affine, si I est un idéal de $\mathcal{O}(X)$, on définit $U(I) = \{(x_1, \ldots, x_d) \in X : (\exists f \in I)\, f(x_1, \ldots, x_d) \neq 0\}$ le complémentaire de $Z(I)$: on appelle ces ensembles ouverts de Zariski de X.

Étant donné qu'une intersection quelconque ou une réunion finie de fermés sont des fermés, dualement, *une réunion quelconque ou une intersection finie d'ouverts sont des ouverts* (par ailleurs, l'ensemble vide et l'ensemble plein sont des ouverts) — ces propriétés sont constitutives de la notion de *topologie*, en l'occurrence la **topologie de Zariski** (sur l'ensemble k^d ou $X(k)$).

Si X' est un fermé de Zariski de X, alors les fermés et ouverts de Zariski de X' sont précisément les intersections avec X' des fermés et ouverts de Zariski de X. (On dit que la topologie de X' est *induite* par celle de X.)

Si I est engendré par les éléments $f_1, \ldots, f_r$, on peut écrire $U(I) = D(f_1) \cup \cdots \cup D(f_r)$ où $D(f_i) := U(\{f_i\})$ est l'ouvert où f_i ne s'annule pas. Les $D(f)$ s'appellent parfois *ouverts principaux*, on verra plus loin pourquoi il est utile de les distinguer ; ceci montre qu'ils forment une *base d'ouverts* (un ensemble d'ouverts stable par intersections finies est dit former une base d'ouverts pour une topologie lorsque tout ouvert est une réunion d'une sous-famille d'entre eux).

Proposition 2.5.1. Si X est une variété algébrique affine et $f_i \in \mathcal{O}(X)$ (pour $i \in \Lambda$ disons), alors $\bigcup_{i\in\Lambda} D(f_i) = X$ si et seulement si les f_i engendrent l'idéal unité dans $\mathcal{O}(X)$ (c'est-à-dire ssi il existe des g_i, tous nuls sauf un nombre fini, tels que $\sum_{i\in\Lambda} g_i f_i = 1$).

Démonstration. Dire $\bigcup_{i\in\Lambda} D(f_i) = X$ équivaut à $\bigcap_{i\in\Lambda} Z(f_i) = \varnothing$, c'est-à-dire encore $Z(\{f_i\}) = \varnothing$, soit encore $Z(I) = \varnothing$ où I est l'idéal engendré par les f_i, et l'énoncé découle du Nullstellensatz faible. ☺

On aura besoin pour la suite de remarquer que $D(f) \cap D(f') = D(ff')$.

Un peu de vocabulaire de topologie : dans ce qui suit, on suppose que X est un ensemble muni d'une topologie (c'est-à-dire un ensemble de parties de X dites « ouvertes » contenant $\varnothing$ et X et telles qu'une réunion quelconque ou une intersection finie d'ouverts sont des ouverts), sachant qu'on s'intéresse évidemment au cas de la topologie de Zariski.

Si $x \in U \subseteq V$ avec U ouvert (et V une partie quelconque de X), on dit que V est un **voisinage** de x. (Un voisinage ouvert de x est donc tout simplement la même chose qu'un ouvert contenant x.)

Si $E \subseteq X$ est une partie quelconque, l'intersection de tous les fermés (=complémentaires des ouverts) contenant E, c'est-à-dire le plus petit fermé contenant E, s'appelle **adhérence** de E, parfois notée $\overline{E}$. Il s'agit de l'ensemble des $x \in X$ tels que tout voisinage de x rencontre E. Lorsque l'adhérence de E est X tout entier, on dit que E est **dense** dans X.

On dit que X est **irréductible** lorsque toute écriture $X = F' \cup F''$ avec F', F'' fermés impose $F' = X$ ou $F'' = X$; de façon équivalente, cela signifie que tout ouvert non vide de X est dense.

On dit que X est **connexe** lorsque (X est non vide et que) $\varnothing$ et X sont les seuls ensembles à la fois ouverts et fermés dans X. (« Irréductible » est plus fort que « connexe », car si X est irréductible, tout ouvert non vide est dense, et en particulier le seul ouvert fermé non vide est X tout entier.)

Dans le cas de la topologie de Zariski sur une variété algébrique affine X sur un corps algébriquement clos k (c'est-à-dire, sur $X(k)$) :

— X est irréductible ssi $\mathcal{O}(X)$ est intègre (cf. 2.1.2),

— l'adhérence de Zariski d'une partie $E \subseteq X(k)$ est $Z(\mathfrak{I}(E))$ (en effet, ceci est un fermé de Zariski contenant E, et si $Z(J) \supseteq E$ est un autre fermé de Zariski contenant E alors on a vu $J \subseteq \mathfrak{I}(E)$ donc $Z(J) \supseteq Z(\mathfrak{I}(E))$ — ceci montre que $Z(\mathfrak{I}(E))$ est bien le plus petit pour l'inclusion fermé de Zariski contenant E).

Exemple (idiot) : On suppose k de caractéristique zéro, disons $k = \mathbb{C}$; quelle est l'adhérence de Zariski de $\mathbb{Z}$ dans $\mathbb{A}^1(k)$? Réponse : L'ensemble $\mathfrak{I}(\mathbb{Z})$ des polynômes s'annulant en chaque point de $\mathbb{Z}$ est réduit à (0) puisqu'un polynôme en une variable ne peut avoir qu'un nombre fini de racines ; donc l'adhérence de Zariski de $\mathbb{Z}$ est $Z(\mathfrak{I}(\mathbb{Z})) = \mathbb{A}^1(k)$ tout entier, c'est-à-dire que $\mathbb{Z}$ est dense dans la droite affine pour la topologie de Zariski. Plus généralement, on peut facilement montrer que les seuls fermés de Zariski de $\mathbb{A}^1(k)$ sont la droite $\mathbb{A}^1(k)$ tout entière et les parties *finies*.

Composantes connexes.

Proposition 2.5.2. Si X est une variété algébrique affine, alors X est connexe si et seulement si les seuls éléments $e \in \mathcal{O}(X)$ vérifiant $e^2 = e$ (appelés **idempotents**) sont 0 et 1.

Démonstration. Si $e^2 = e$ avec $e \neq 0, 1$, alors $e(1-e) = 0$. On a donc $X = Z(e) \cup Z(1-e)$; et $Z(e) \cap Z(1-e) = \varnothing$ (car $e, 1-e$ engendrent l'idéal unité, si on veut). Donc $Z(e)$ et $Z(1-e)$ sont deux fermés complémentaires l'un de l'autre, donc ils sont aussi ouverts. Comme e n'est pas nul, $Z(e)$ n'est pas X tout entier, et de même pour $Z(1-e)$ car $e \neq 1$; donc $Z(e)$ est un ouvert fermé autre que $\varnothing$ et X, et X n'est pas connexe.

Réciproquement, supposons que X' soit un ouvert fermé dans X autre que $\varnothing$ et X, et soit X'' son complémentaire, qui vérifie les mêmes conditions. On peut écrire $X' = Z(I')$ et $X'' = Z(I'')$ avec I', I'' deux idéaux radicaux stricts de $\mathcal{O}(X)$. Puisque $X' \cap X'' = \varnothing$, on a $I' + I'' = (1)$ (où (1) désigne l'idéal unité, c'est-à-dire $\mathcal{O}(X)$ tout entier) ; il existe donc $e \in I'$ tel que $1 - e \in I''$. Mais alors $e(1-e) \in I' \cap I''$, or $I' \cap I'' = (0)$ car $X' \cup X'' = X$. On a donc $e^2 = e$, et $e \neq 1$ car e appartient à un idéal strict, et $e \neq 0$ car $1 - e \neq 1$. ☺

Proposition 2.5.3. Toute variété algébrique affine X est réunion d'un nombre fini de fermés connexes. De plus, il existe une écriture $X = \bigcup_{i=1}^{n} X_i$ vérifiant $X_i \cap X_j = \varnothing$ pour $i \neq j$, et une telle écriture est unique (à l'ordre des facteurs près) : les X_i s'appellent les **composantes connexes** de X.

Composantes irréductibles.

Proposition 2.5.4. Toute variété algébrique affine X est réunion d'un nombre fini de fermés irréductibles. De plus, il existe une écriture $X = \bigcup_{i=1}^{n} X_i$ vérifie $X_i \not\subseteq X_j$ pour $i \neq j$, et une telle écriture est unique (à l'ordre des facteurs près) : les X_i s'appellent les **composantes irréductibles** de X.

Démonstration. Montrons par l'absurde que X est réunion d'un nombre fini de fermés irréductibles : comme X n'est pas lui-même irréductible, on peut écrire $X = X_1 \cup X_1'$ avec X_1, X_1' fermés stricts dans X, et l'un d'entre eux ne doit pas être irréductible, disons X_1, donc on peut écrire $X_1 = X_2 \cup X_2'$, et ainsi de suite. On obtient ainsi une suite de fermés strictement décroissante pour l'inclusion $X \supsetneq X_1 \supsetneq X_2 \supsetneq \cdots$, qui correspond à une suite strictement croissante d'idéaux (radicaux) dans $\mathcal{O}(X)$, ce qui est impossible car $\mathcal{O}(X)$ est noethérien (cf. 1.2.3).

On peut donc écrire $X = \bigcup_{i=1}^{n} X_i$, et quitte à jeter les X_i déjà inclus dans un autre X_j (et à répéter le processus si nécessaire), on peut supposer $X_i \not\subseteq X_j$ pour $i \neq j$.

Montrons enfin l'unicité. Si $X = \bigcup_{i=1}^{n} X_i = \bigcup_{j=1}^{p} Y_j$ sont deux telles écritures, on a $X_i = \bigcup_{j=1}^{p} (X_i \cap Y_j)$. Comme X_i est irréductible, l'un des $X_i \cap Y_j$ doit être égal à X_i, c'est-à-dire $X_i \subseteq Y_j$; par symétrie de l'argument, ce Y_j est lui-même inclus dans un $X_{i'}$, et comme $X_i \subseteq X_{i'}$, la condition sur la décomposition donne $i' = i$, donc $Y_j = X_i$ et on a bien montré que chaque X_i est un des Y_j et vice versa. ☺

Exemple : $Z(xy) \subseteq \mathbb{A}^2$ a pour composantes irréductibles $Z(x)$ et $Z(y)$. En revanche, il est connexe (=sa seule composante connexe est lui-même) : en effet, si U est un ouvert fermé de $Z(xy)$, quitte à remplacer U par son complémentaire on peut supposer que U contient $(0,0)$, et alors U est un ouvert fermé rencontrant $Z(x)$ et $Z(y)$ à la fois — mais comme ceux-ci sont irréductibles, et en particulier connexes, $U \cap Z(x) = Z(x)$ et $U \cap Z(y) = Z(y)$, ce qui montre $U = Z(xy)$.

2.6 Fonctions régulières sur un ouvert, morphismes

Soit X une variété algébrique affine sur k, et $f \in \mathcal{O}(X)$. On définira **l'anneau des fonctions régulières** sur l'ouvert principal $D(f) = X \setminus Z(f)$ comme le localisé $\mathcal{O}(X)[\frac{1}{f}]$ inversant f de l'anneau $\mathcal{O}(X)$ des fonctions régulières sur X. Autrement dit (cf. 1.3), les fonctions régulières sont $D(f)$ sont définies comme des fractions de fonctions régulières sur X admettant une puissance de f au dénominateur.

On peut bien les voir comme des fonctions : si $x \in D(f)$, cela signifie que $x \in X$ et que $f(x) \neq 0$, ce qui permet d'évaluer en x une fonction de la forme $\frac{g}{f^n}$.

Exemple : Les fonctions régulières sur $\mathbb{A}^1 \setminus \{0\}$ (la droite affine privée de l'origine, c'est-à-dire $D(t)$ dans $\mathbb{A}^1 = \operatorname{Spec} k[t]$) sont les fonctions rationnelles de la forme $\frac{g}{t^n}$ avec $n \geq 0$ (=les fonctions rationnelles n'ayant pas d'autre pôle qu'en zéro). Plus généralement, toute fonction rationnelle $h \in k(t)$ peut être considérée comme une fonction régulière sur un certain ouvert de $\mathbb{A}^1$, à savoir l'ouvert où le dénominateur de h ne s'annule pas.

Si $I = (f_1, \ldots, f_r)$ est un idéal de $\mathcal{O}(X)$, avec X une variété algébrique affine, on appelle **fonction régulière** sur $U := U(I) = D(f_1) \cup \cdots \cup D(f_r) = X \setminus Z(I)$ la donnée d'une fonction $h \colon U \to k$ telle que la restriction de h à chaque $D(f_i)$ soit une fonction régulière. *Fait :* Ceci ne dépend pas du choix des f_i engendrant l'idéal I. Ces fonctions régulières forment un anneau, noté $\mathcal{O}(U)$.

Si U est un ouvert de Zariski d'une variété algébrique affine X, et V un ouvert de Zariski d'une variété algébrique affine $Y \subseteq \mathbb{A}^e$, on appelle **morphisme** $U \to V$ une application $U \to V$ telle que chacune des e coordonnées à l'arrivée soit une fonction régulière sur U. Autrement dit, il s'agit de la donnée de e éléments $f_1, \ldots, f_e$ de $\mathcal{O}(U)$ tels que $(f_1(x), \ldots, f_e(x)) \in V$ pour tout $x \in U$. Comme précédemment, les fonctions régulières ne sont autres que les morphismes vers $\mathbb{A}^1$. On appellera **isomorphisme** entre U et V la donnée de morphismes $U \to V$ et $V \to U$ dont la composée chaque sens est l'identité.

On appelle **variété algébrique quasi-affine**, un ouvert d'une variété algébrique affine (considérée à isomorphisme près) comme on vient de le décrire.

Proposition 2.6.1. Si U est une variété algébrique *quasi-affine* et Y une variété algébrique *affine*, alors les morphismes $U \to Y$ sont en correspondance avec

les morphismes $\mathcal{O}(Y) \to \mathcal{O}(U)$ (de k-algèbres) en envoyant $f\colon U \to Y$ sur $f^*\colon \mathcal{O}(Y) \to \mathcal{O}(U)$ (défini comme le morphisme qui envoie une fonction régulière $h\colon Y \to \mathbb{A}^1$ sur $f^*(h) := h \circ f\colon U \to \mathbb{A}^1$).

Les ouverts *principaux* (les $D(f)$), en fait, n'apportent rien de nouveau :

Proposition 2.6.2. Si $f \in \mathcal{O}(X)$ avec X une variété algébrique affine, alors l'ouvert principal $D(f) = X \setminus Z(f)$ est isomorphe à la variété algébrique affine $\operatorname{Spec} \mathcal{O}(X)[\frac{1}{f}]$.

En revanche, pour un ouvert quelconque, on obtient véritablement des choses nouvelles.


La proposition 2.6.1 cesse d'être vraie si on considère des morphismes entre deux variétés algébriques quasi-affines quelconques. Par exemple, le plan affine $\mathbb{A}^2 = \operatorname{Spec} k[x, y]$ et le complémentaire $\mathbb{A}^2 \setminus \{(0, 0)\}$ de l'origine dans le plan affine ont exactement le même anneau des fonctions régulières, pourtant, ces deux variétés quasi-affines ne sont pas isomorphes.

Si U est une variété algébrique quasi-affine, il existe un morphisme naturel $\psi\colon U \to \operatorname{Spec} \mathcal{O}(U)$ d'après la proposition 2.6.1, à savoir celui qui correspond à l'identité sur $\mathcal{O}(U)$. On dit que la variété algébrique quasi-affine U est **affine** lorsque ψ est un isomorphisme (de façon équivalente, lorsque U est isomorphe à une variété algébrique affine telle qu'on l'a définie précédemment).

La proposition 2.6.2 a pour conséquence utile le fait que tout point d'une variété algébrique quasi-affine a un *voisinage* affine (autrement dit, « pour l'étude locale, les affines suffisent »).

3 L'espace projectif et les variétés quasiprojectives

3.1 L'espace projectif sur un corps

Si k est un corps, on note $\mathbb{P}^d(k)$ (ou juste $\mathbb{P}^d$ si k est algébriquement clos et sous-entendu) l'ensemble des $(d+1)$-uplets d'éléments *non tous nuls* de k modulo la relation d'équivalence $(x_0, \cdots, x_d) \sim (x'_0, \cdots, x'_d)$ ssi les vecteurs $(x_0, \cdots, x_d)$ et $(x'_0, \cdots, x'_d)$ sont colinéaires. On note $(x_0 : \cdots : x_d)$ (certains auteurs préfèrent $[x_0, \ldots, x_d]$) la classe de $(x_0, \ldots, x_d)$ pour cette relation d'équivalence. On peut voir $\mathbb{P}^d(k)$ comme l'ensemble des droites vectorielles (=passant par l'origine) de k^{d+1}.

Idée intuitive : tout point de $\mathbb{P}^d(k)$, selon que $x_0 \neq 0$ ou $x_0 = 0$, peut être mis sous la forme $(1 : x_1 : \cdots : x_d)$ (avec $x_1, \ldots, x_d$ quelconques) ou bien $(0 : x_1 : \cdots : x_d)$ (avec $x_1, \ldots, x_d$ non tous nuls). Le point $(x_1, \ldots, x_d)$ de $\mathbb{A}^d$ sera identifié au point $(1 : x_1 : \cdots : x_d)$ de $\mathbb{P}^d$, tandis que les points de la forme

$(0 : x_1 : \ldots : x_d)$ sont appelés « points à l'infini » (et collectivement, « hyperplan à l'infini »). On peut donc écrire $\mathbb{P}^d(k) = \mathbb{A}^d(k) \cup \mathbb{P}^{d-1}(k)$ (réunion disjointe de l'ensemble $Z(x_0)(k)$ des points où $x_0 \neq 0$ et de celui $D(x_0)(k)$ des points où $x_0 = 0$) ; moralement, on aura envie que $\mathbb{A}^d$ soit un ouvert dans $\mathbb{P}^d$ et $\mathbb{P}^{d-1}$ son fermé complémentaire. Noter que le choix de x_0 est arbitraire : on peut voir $\mathbb{P}^d$ comme réunion de $d+1$ espaces affines $\mathbb{A}^d$ (à savoir $D(x_0), \ldots, D(x_d)$).

3.2 Polynômes homogènes, fermés et ouverts de Zariski de $\mathbb{P}^d$, Nullstellensatz projectif

On veut voir $\mathbb{P}^d$ comme une variété algébrique (au moins pour k algébriquement clos pour le moment). Il faudra une notion d'ouverts et une notion de fonctions régulières.

On dit qu'un $f \in k[t_0, \ldots, t_d]$ est **homogène de degré** ℓ lorsque tous les monômes qui le constituent ont le même degré total ℓ. L'intérêt de cette remarque est que si $(x_0 : \cdots : x_d) \in \mathbb{P}^d(k)$ avec k un corps, et $f \in k[t_0, \ldots, t_d]$ est homogène, le fait que $f(x_0, \ldots, x_d) = 0$ ou $\neq 0$ ne dépend pas du choix du représentant choisi de $(x_0 : \cdots : x_d)$. On peut donc définir $Z(f) = \{(x_0 : \cdots : x_d) \in \mathbb{P}^d(k) : f(x_0, \ldots, x_d) = 0\}$ et $D(f)$ son complémentaire.

On apppelle **partie homogène de degré** ℓ d'un polynôme $f \in k[t_0, \ldots, t_d]$ la somme de tous ses monômes de degré total ℓ. Évidemment, tout polynôme est la somme de ses parties homogènes. Le produit de deux polynômes homogènes de degrés respectifs ℓ et ℓ' est homogène de degré $\ell + \ell'$.

On dit qu'un idéal I de $k[t_0, \ldots, t_d]$ est **homogène** lorsqu'il peut être engendré par des polynômes homogènes (cela ne signifie pas, évidemment, qu'il ne contient que des polynômes homogènes, ni même que *tout* ensemble de générateurs de I soit constitué de polynômes homogènes). De façon équivalente, il s'agit d'un idéal tel que pour tout $f \in I$, toute partie homogène de f est encore dans I. (Démonstration de l'équivalence : si toute partie homogène d'un élément de I appartient encore à I, en prenant un ensemble quelconque de générateurs de I, les parties homogènes de ceux-ci appartiennent encore à I et sont encore génératrices puisqu'elles engendrent les générateurs choisis, donc I admet bien un ensemble de générateurs homogènes ; réciproquement, si I est engendré par $f_1, \ldots, f_r$ homogènes de degrés $\ell_1, \ldots, \ell_r$ et si h appartient à I, disons $h = \sum_i g_i f_i$, alors pour tout ℓ, la partie homogène de degré ℓ de h est $h^{[\ell]} = \sum_i g_i^{[\ell-\ell_i]} f_i$ où $g_i^{[\ell-\ell_i]}$ désigne la partie homogène de degré $\ell - \ell_i$ de g_i, donc $h^{[\ell]}$ appartient aussi à I.)

(Concrètement, dire que I est homogène signifie — au moins lorsque I est radical et que k est algébriquement clos — que le fermé *affine* qu'il définit dans $\mathbb{A}^{d+1}$ est un *cône*, c'est-à-dire stable par homothéties. L'ensemble $Z(I)$ défini ci-dessus va être ce cône vu comme un ensemble de droites vectorielles donc comme

un objet géométrique dans $\mathbb{P}^d$.)

Pour I idéal homogène de $k[t_0, \ldots, t_d]$, on définit $Z(I)$ comme l'intersection des $Z(f)$ pour $f \in I$ homogène, ou simplement, d'après ce qui précède, l'intersection des $Z(f)$ pour f parcourant un ensemble de générateurs homogènes de I. Les $Z(I)$ s'appellent les fermés [de Zariski] de $\mathbb{P}^d$. Inversement, si E est une partie de $\mathbb{P}^d$, on appelle $\mathfrak{I}(E)$ l'idéal (par définition homogène) engendré par les polynômes homogènes f s'annulant en tout point de E (c'est-à-dire tels que $Z(f) \supseteq E$).

Théorème 3.2.1. Si k est un corps algébriquement clos :

- (Nullstellensatz faible projectif.) Pour I un idéal homogène de $k[t_0, \ldots, t_d]$, on a $Z(I) = \varnothing$ dans $\mathbb{P}^d$ ssi il existe un entier naturel ℓ tel que I contienne tous les monômes en $t_0, \ldots, t_d$ de degré total ℓ (et, par conséquent, de tout degré plus grand). Un tel idéal s'appelle **irrelevant** [avec un bel anglicisme].
- (Nullstellensatz projectif.) Les fonctions $I \mapsto Z(I)$ et $E \mapsto \mathfrak{I}(E)$ définissent des bijections réciproques, décroissantes pour l'inclusion, entre les idéaux homogènes radicaux de $k[t_0, \ldots, t_d]$ autres que $(t_0, \ldots, t_d)$ d'une part, et les fermés de Zariski de $\mathbb{P}^d(k)$ d'autre part.
- Ces bijections mettent en correspondance les idéaux homogènes premiers de $k[t_0, \ldots, t_d]$ avec les fermés irréductibles de $\mathbb{P}^d$.
- Si I est un idéal homogène de $k[t_0, \ldots, t_d]$ tel que $Z(I) \neq \varnothing$ (i.e., qui n'est pas irrelevant) alors $\mathfrak{I}(Z(I)) = \sqrt{I}$ (le radical de I).

Remarque 3.2.2. Pour qu'un idéal homogène I de $k[t_0, \ldots, t_d]$ contienne tous les monômes à partir d'un certain degré total ℓ (c'est-à-dire, qu'il soit irrelevant), il faut et il suffit qu'il contienne tous les t_i^n à partir d'un certain n. (En effet, un sens est trivial, et pour l'autre sens, si I contient tous les t_i^n, alors il contient tout monôme de degré $(d+1)n$, puisqu'un tel monôme contient au moins un t_i à la puissance n.) Comme il n'y a qu'un nombre fini des t_i, on peut aussi intervertir les quantificateurs : c'est encore la même chose que de dire que pour chaque i, l'idéal I contient une certaine puissance $t_i^{n_i}$ de t_i.

Les ouverts de Zariski de $\mathbb{P}^d$ sont bien sûr, par définition, les complémentaires $U(I)$ des fermés de Zariski $Z(I)$. Ils peuvent toujours s'écrire de la forme $D(f_1) \cup \cdots \cup D(f_r)$ où $f_1, \ldots, f_r$ sont des polynômes homogènes en $t_0, \ldots, t_d$.

3.3 Le lien affine-projectif

On a déjà signalé que $\mathbb{P}^d$ est la réunion des $d+1$ ouverts $D(t_0), \ldots, D(t_d)$, qu'on veut considérer comme $d+1$ espaces affines, ou $d+1$ copies de l'espace

affine $\mathbb{A}^d$. Il faut considérer que les coordonnées affines sur $D(t_i)$ sont les $\frac{t_j}{t_i}$ avec $j \neq i$ (ce qui fait d coordonnées).

Le lien affine-projectif est explicité par les affirmations suivantes :

— Si $f \in k[t_0, \ldots, t_d]$ est homogène de degré ℓ, l'intersection de $Z(f) \subseteq \mathbb{P}^d$ avec $D(t_i)$ est donnée par $Z(\frac{f}{t_i^\ell}) \subseteq \mathbb{A}^d$ en voyant $\frac{f}{t_i^\ell}$ comme un polynôme en les $\frac{t_j}{t_i}$.

— Plus généralement, si $X = Z(I) \subseteq \mathbb{P}^d$ est le fermé de Zariski défini par un idéal homogène I de $k[t_0, \ldots, t_d]$, l'intersection de X avec $D(t_i)$ est la variété affine $Z(I_{t_i}) \subseteq \mathbb{A}^d$ où I_{t_i} est l'idéal engendré par les $\frac{f_j}{t_i^{\ell_j}}$ pour f_j parcourant des générateurs homogènes de I et $\ell_j = \deg f_j$ (l'idéal I_{t_i} ne dépend pas du choix des f_j).

— Bon à savoir : si I est un idéal homogène de $k[t_0, \ldots, t_d]$, alors $k[\frac{t_0}{t_i}, \ldots, \frac{t_d}{t_i}]/I_{t_i}$, où I_{t_i} est défini ci-dessus, est l'ensemble des éléments homogènes de degré zéro de $(k[t_0, \ldots, t_d]/I)[\frac{1}{t_i}]$. L'un ou l'autre, donc, est vu comme l'ensemble des fonctions régulières sur $Z(I) \cap D(t_i)$.

— Inversement, donnée un fermé de Zariski $X = Z(I) \subseteq \mathbb{A}^d$ de l'espace affine, où I est un idéal radical de $k[\tau_1, \ldots, \tau_d]$, on peut définir une variété projective $X^+ = Z(I^+)$ dont l'idéal I^+ est engendré par les $f^+ := t_0^{\deg f} f(\frac{t_1}{t_0}, \ldots, \frac{t_d}{t_0}) \in k[t_0, \ldots, t_d]$ pour tous les $f \in I$ (c'est-à-dire les polynômes homogénéisés) : on peut montrer qu'il s'agit précisément de l'adhérence de X dans $\mathbb{P}^d$. Malheureusement, il ne suffit pas en général de prendre un ensemble de générateurs de I pour que leurs homogénéisés engendrent I^+ (penser à $I = (\tau_2 - \tau_1^2,\ \tau_3 - \tau_1^3)$ qui contient $\tau_3 - \tau_1\tau_2$ alors que $(t_0t_2 - t_1^2,\ t_0t_3 - t_1^3)$ ne contient pas $t_0t_3 - t_1t_2$, il faut le mettre explicitement dans I^+). Il y a cependant un cas favorable : lorsque $X = Z(f)$ est une hypersurface, alors $X^+ = Z(f^+)$.

3.4 Variétés projectives et quasiprojectives, morphismes

On appelle **variété algébrique projective**, resp. **variété algébrique quasi-projective**, un fermé de Zariski de l'espace projectif $\mathbb{P}^d$, resp. un ouvert de Zariski d'une telle variété (autrement dit, l'intersection d'un ouvert et d'un fermé de Zariski de $\mathbb{P}^d$).

Si X est une variété algébrique projective (resp. quasiprojective) dans $\mathbb{P}^d$ et qu'on note $D(t_0), \ldots, D(t_d)$ les $d+1$ ouverts $\{t_0 \neq 0\}, \ldots, \{t_d \neq 0\}$ chacun identifié à un espace affine $\mathbb{A}^d$, alors, comme expliqué en 3.3, chacun des $X \cap D(t_i)$ peut être considéré comme une variété algébrique affine (resp. quasi-affine).

Comment définir un morphisme entre variétés algébriques projectives ou quasiprojectives ? Moralement, on veut le définir comme une application qui est « localement » un morphisme entre variétés algébriques affines.

On peut par exemple définir une **fonction régulière** h sur une variété projective ou quasiprojective X comme une fonction $h\colon X \to \mathbb{A}^1$ telle que $h|_{X\cap D(t_i)}$ soit une fonction régulière sur $X \cap D(t_i)$ pour chaque i. Pour les morphismes, la situation est un peu plus compliquée car il faut considérer non seulement des recouvrements au départ mais aussi à l'arrivée.

Voici une première définition possible : si $X \subseteq \mathbb{P}^d$ et $Y \subseteq \mathbb{P}^e$ sont deux variétés quasiprojectives, un **morphisme** $X \to Y$ est une fonction $h\colon X \to Y$ telle qu'il existe un recouvrement $X = \bigcup_\lambda V_\lambda$ [qu'on peut toujours supposer fini] de X par des ouverts de Zariski V_λ, chacun complètement contenu dans un $D(t_{i_\lambda}) \cong \mathbb{A}^d$ (ce qui permet de considérer au moins V_λ ou $X\cap D(t_{i_\lambda})$ comme une variété quasi-affine) et tel que $h(V_\lambda)$ soit contenu dans un $D(u_{j_\lambda}) \cong \mathbb{A}^e$ de $\mathbb{P}^e$ où on a noté $(u_0 : \cdots : u_e)$ les coordonnées sur $\mathbb{P}^e$ (ceci permet de considérer $Y \cap D(u_{j_\lambda})$ comme une variété quasi-affine), avec $h|_{V_\lambda}\colon V_\lambda \to (Y \cap D(u_{j_\lambda}))$ un morphisme (pour chaque λ).

Décrivons une autre définition possible, qui soit un peu plus opérationnelle (on admettra, entre autres choses, que ces définitions sont bien équivalentes !). Si $X \subseteq \mathbb{P}^d$ est une variété quasiprojective, on considère des $(e+1)$-uplets de polynômes homogènes $f_0, \ldots, f_e$ *de même degré* en $d+1$ variables $t_0, \ldots, t_d$. Un tel $(e+1)$-uplet $f = (f_0 : \cdots : f_e)$ définit une application $V \to \mathbb{P}^e$ par $x \mapsto (f_0(x) : \cdots : f_e(x))$, où V est l'ensemble (ouvert de Zariski) des points x de X tels que $f_0(x), \ldots, f_e(x)$ ne s'annulent pas simultanément. Un morphisme $X \to \mathbb{P}^e$ est une application $h\colon X \to \mathbb{P}^e$ tel que des restrictions $h|_{V_\lambda}\colon V_\lambda \to \mathbb{P}^e$ puissent s'écrire sous la forme précédente, pour des ouverts V_λ recouvrant X. Si de plus l'image est contenue dans une variété quasiprojective $Y \subseteq \mathbb{P}^e$, on pourra dire qu'il s'agit d'un morphisme $X \to Y$.

Concrètement, donc, selon cette seconde définition, se donner un morphisme $X \to \mathbb{P}^e$, si $X = Z(I)$ est une variété projective avec I idéal radical homogène de $k[t_0, \ldots, t_d]$, revient à se donner un certain nombre d'écritures $(f_0^{(\lambda)} : \cdots : f_e^{(\lambda)})$ telles que (i) pour chaque λ, les polynômes $f_0^{(\lambda)}, \cdots, f_e^{(\lambda)}$ sont homogènes de même degré, (ii) les $f_i^{(\lambda)}$ et I (tous ensemble) engendrent un idéal irrelevant (ce qui par le Nullstellensatz revient à dire que pour tout point de $X = Z(I)$ il y a au moins un $f_i^{(\lambda)}$ qui ne s'annule pas), et (iii) $f_i^{(\lambda)} f_j^{(\mu)} - f_j^{(\lambda)} f_i^{(\mu)}$ appartient à I pour tous λ, μ, i, j (ce qui revient à dire que $(f_0^{(\lambda)} : \cdots : f_e^{(\lambda)})$ et $(f_0^{(\mu)} : \cdots : f_e^{(\mu)})$ définissent bien la même fonction). Pour définir un morphisme $X \to Y$ avec $Y = Z(J)$ une autre variété projective, on demande de plus (iv) que, pour chaque λ, les $f_0^{(\lambda)}, \ldots, f_e^{(\lambda)}$ vérifient, modulo I, les équations données par des générateurs de J.

Avant de donner des exemples, citons le fait suivant, qui aide à comprendre qu'on a énormément de rigidité dans la définition d'un morphisme (notamment,

une fois donnée la restriction de celui-ci à un ouvert dense V, le morphisme est complètement défini) :

Proposition 3.4.1. Si $h, h' \colon X \to Y$ sont deux morphismes entre variétés quasiprojectives et si h, h' coïncident sur une partie *dense* de X (pour la topologie de Zariski), alors $h = h'$. Plus généralement, l'ensemble des points où h et h' coïncident est un fermé de X.

On rappelle que si X est irréductible, alors tout ouvert de X non vide est dense (c'est même équivalent).

Exemples de morphismes :

¶ Soit C^+ le cercle, cette fois projectif, d'équation $x^2 + y^2 = z^2$ (équation homogénéisée de $x^2 + y^2 = 1$) dans $\mathbb{P}^2$ de coordonnées homogènes $(z : x : y)$ (sur un corps k de caractéristique $\neq 2$), et soit le $\mathbb{P}^1$ de coordonnées $(t_0 : t_1)$. On définit un morphisme $\mathbb{P}^1 \to C^+$ par $(t_0 : t_1) \mapsto (t_0^2 + t_1^2 : t_0^2 - t_1^2 : 2t_0t_1)$. Il est clair que ces équations définissent un morphisme $\mathbb{P}^1 \to \mathbb{P}^2$ car $t_0^2+t_1^2, t_0^2-t_1^2, 2t_0t_1$ engendrent tous les monômes de degré 2 donc un idéal irrelevant ; ensuite, comme $(t_0^2 - t_1^2)^2 + (2t_0t_1)^2 = (t_0^2 + t_1^2)^2$, ce morphisme arrive bien dans C^+.

Dans l'autre sens : on définit un morphisme $C^+ \to \mathbb{P}^1$ de la façon suivante : on commence par l'équation $(z : x : y) \mapsto (x + z : y)$, mais ceci ne définit un morphisme que sur l'ouvert complémentaire de $Z(x + z, y)$ (c'est-à-dire du point $(z : x : y) = (1 : -1 : 0)$). Il faut donc trouver une autre équation, ou plutôt une autre forme, sur un ouvert qui contienne ce point. Ce n'est pas difficile : en se disant que de façon assez générale on a $(x+z : y) = ((x+z)(x-z) : y(x-z)) = (x^2 - z^2 : y(x - z)) = (-y^2 : y(x - z)) = (y : z - x)$, on va considérer $(z : x : y) \mapsto (y : z - x)$, qui est, cette fois, défini sur le complémentaire de $Z(y, z - x)$, c'est-à-dire de du point $(z : x : y) = (1 : 1 : 0)$. Le calcul qu'on vient de faire montre que $(x + z : y) = (y : z - x)$ sur l'intersection des deux ouverts, donc ces deux équations se recollent bien en un unique morphisme $C^+ \to \mathbb{P}^1$.

La composée des morphismes qu'on vient de définir est l'identité : dans le sens $\mathbb{P}^1 \to C^+ \to \mathbb{P}^1$, c'est clair car l'identité s'obtient bien en recollant $(t_0 : t_1) \mapsto (2t_0^2 : 2t_0t_1)$ et $(t_0 : t_1) \mapsto (2t_0t_1 : 2t_1^2)$. Dans le sens $C^+ \to \mathbb{P}^1 \to C^+$, on constate que la composée de $(z : x : y) \mapsto (x + z : y)$ avec $(t_0 : t_1) \mapsto (t_0^2 + t_1^2 : t_0^2 - t_1^2 : 2t_0t_1)$ donne $(z : x : y) \mapsto (x^2 + 2xz + z^2 + y^2 : x^2 + 2xz + z^2 - y^2 : 2xy + 2yz)$ ce qui, modulo $x^2 + y^2 - z^2$, vaut $(2z(x + z) : 2x(x + z) : 2y(z + x))$, soit $(z : x : y)$ dès que $x + z \neq 0$. Comme l'ouvert $\{x + z \neq 0\}$ est dense, ceci suffit à montrer qu'on a affaire à l'identité.

On a donc prouvé que le cercle (projectif !) C^+ d'équation $x^2 + y^2 = z^2$ est isomorphe à $\mathbb{P}^1$.

¶ Un exemple avec des variétés ouvertes : $\mathbb{A}^{d+1} \setminus \{(0, 0)\} \to \mathbb{P}^d$ donné par $(x_0, \ldots, x_d) \mapsto (x_0 : \cdots : x_d)$.

4 Géométrie algébrique sur un corps non algébriquement clos

4.1 Crash-course de théorie de Galois

Rappel : corps parfait = corps de caractéristique 0 *ou* de caractéristique p tel que tout élément ait une racine p-ième = corps tel que tout polynôme irréductible soit à racines simples sur la clôture algébrique. Exemples : $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{F}_q$ sont parfaits comme l'est tout corps algébriquement clos. Contre-exemple : $\mathbb{F}_p(t)$ n'est pas parfait (t n'a pas de racine p-ième).

Si k est un corps parfait (et qu'on en fixe une fois pour toutes une clôture algébrique), on note $\mathrm{Gal}(k)$ ou Γ_k et on appelle **groupe de Galois absolu** de k le groupe des automorphismes de corps de sa clôture algébrique qui laissent k fixe (i.e. $\sigma(x) = x$ pour tout $x \in k$).

Exemples : $\Gamma_{\mathbb{R}} = \{\mathrm{id}_{\mathbb{C}}, (z \mapsto \bar{z})\}$ est le groupe cyclique d'ordre 2. Si k est algébriquement clos, Γ_k est trivial. Si $k = \mathbb{F}_q$ est fini, $\Gamma_{\mathbb{F}_q}$ contient au moins toutes les puissances $\mathrm{Frob}_q^i \colon x \mapsto x^{q^i}$ du Frobenius $\mathrm{Frob}_q \colon x \mapsto x^q$; il contient en fait d'autres éléments, mais « en gros » il n'y a que les puissances du Frobenius (au sens : la restriction de tout $\sigma \in \Gamma_{\mathbb{F}_q}$ à un $\mathbb{F}_{q^n}$ est de la forme Frob_q^i pour un certain $i \in \mathbb{Z}$ (qu'on peut voir dans $\mathbb{Z}/n\mathbb{Z}$ si on préfère) ; en tout cas, pour voir qu'un élément de k^{alg} (ou de n'importe quoi qui sera considéré plus bas) est fixé/stable par $\Gamma_{\mathbb{F}_q}$, il suffit de vérifier qu'il est fixé/stable par Frob_q.

Théorème 4.1.1. Si k est un corps parfait de clôture algébrique k^{alg}, un élément x de k^{alg} appartient à k si [et seulement si, mais ça c'est juste la définition de Γ_k] on a $\sigma(x) = x$ pour tout $\sigma \in \Gamma_k$.

Slogan : « rationnel = fixé par Galois ».

Si $k \subseteq K$ est une extension algébrique (on note parfois ça K/k, mauvaise notation car elle fait penser à un quotient), si k est parfait alors K l'est aussi, et Γ_K est un sous-groupe de Γ_k. Ce sous-groupe est *distingué* exactement lorsque $\sigma(K) = K$ (c'est-à-dire K est *globalement* stable par σ, pas nécessairement fixé point à point) pour tout $\sigma \in \Gamma_k$: dans ce cas on dit que K est une **extension galoisienne** de k, et on pose $\mathrm{Gal}(k \subseteq K) = \Gamma_k/\Gamma_K$, qui s'appelle groupe de Galois de l'extension $k \subseteq K$. Il peut se voir comme l'ensemble des automorphismes de K laissant k fixe. Remarque : si Γ_k est abélien (c'est le cas de $\mathbb{F}_q$), *toute* extension algébrique de k est galoisienne.

Théorème 4.1.2. — Si $k \subseteq K$ est une extension finie (donc algébrique) galoisienne, alors un élément x de K appartient à k si [et seulement si] on a $\sigma(x) = x$ pour tout $\sigma \in \mathrm{Gal}(k \subseteq K)$. De plus, il y a une bijection entre extensions intermédiaires $k \subseteq E \subseteq K$ et sous-groupes de $\mathrm{Gal}(k \subseteq K)$ don-

née par $E \mapsto \Gamma_E/\Gamma_K = \mathrm{Gal}(E \subseteq K)$ et réciproquement $H \mapsto \{x \in K : (\forall \sigma \in H)\, \sigma(x) = x\}$. (Note : l'extension $E \subseteq K$ est toujours galoisienne (on rappelle que $k \subseteq K$ était supposée l'être !), et $k \subseteq E$ l'est lorsque $\mathrm{Gal}(E \subseteq K)$ est distingué dans $\mathrm{Gal}(k \subseteq K)$.)

— Version absolue : pour k parfait, il y a une bijection entre les extensions finies (et en particulier, algébriques) $k \subseteq K$ de k dans une clôture algébrique k^{alg} fixée, et les sous-groupes de Γ_k qui sont « ouverts » au sens où ils contiennent un $\Gamma_{k'}$ pour k' extension finie de k.

La première partie du résultat suivant est une conséquence triviale de 4.1.1, la seconde est beaucoup plus subtile.

Théorème 4.1.3. Pour k parfait :

— Si $x \in \mathbb{A}^d(k^{\mathrm{alg}})$ est fixé par Γ_k, alors $x \in \mathbb{A}^d(k)$ (au sens où ses coordonnées affines sont dans k).

— Si $x \in \mathbb{P}^d(k^{\mathrm{alg}})$ est fixé par Γ_k, alors $x \in \mathbb{P}^d(k)$ (au sens où *il admet* des coordonnées homogènes dans k).

4.2 Variétés sur un corps non algébriquement clos

Soit k un corps parfait. Si I est un idéal de $k[t_1, \ldots, t_d]$, on définit l'idéal $I_{k^{\mathrm{alg}}} := I \cdot k^{\mathrm{alg}}[t_1, \ldots, t_d]$ engendré par I dans $k^{\mathrm{alg}}[t_1, \ldots, t_d]$.

Proposition 4.2.1. — L'idéal $I_{k^{\mathrm{alg}}}$ est radical si et seulement si I l'est.

— Un idéal J de $k^{\mathrm{alg}}[t_1, \ldots, t_d]$ est de la forme $I_{k^{\mathrm{alg}}}$ pour I idéal de $k[t_1, \ldots, t_d]$ si et seulement si $\sigma(J) = J$ pour tout $\sigma \in \Gamma_k$. Lorsque c'est le cas, $I = J \cap k[t_1, \ldots, t_d]$.

— Lorsque J est radical, c'est le cas (=J est de la forme $I_{k^{\mathrm{alg}}}$) si et seulement si $\sigma(Z(J)) = Z(J)$ dans $\mathbb{A}^d(k^{\mathrm{alg}})$. Remarque : $Z(J) = Z(I)$ dans $\mathbb{A}^d(k^{\mathrm{alg}})$.

— On a des bijections réciproques, décroissantes pour l'inclusion, entre idéaux radicaux de $k[t_1, \ldots, t_d]$ et fermés de Zariski de $\mathbb{A}^d(k^{\mathrm{alg}})$ stables par Galois, donnée par $I \mapsto Z(I_{k^{\mathrm{alg}}})$ et $E \mapsto \mathfrak{I}(E) \cap k[t_1, \ldots, t_d]$.

On qualifiera un fermé de Zariski X de $\mathbb{A}^d(k^{\mathrm{alg}})$ stable par Galois de k-variété algébrique affine ou variété algébrique affine *sur* k (moralité : c'est une variété dont les équations peuvent être définies sur k). On qualifie alors les éléments de $X \cap k^d$ (c'est-à-dire les points de X dont les coordonnées sont dans k, ou les solutions *dans* k des équations de X) de k-points de X, et on note généralement $X(k)$ cet ensemble. (Ainsi, $X(k^{\mathrm{alg}})$ est la même chose que X.)

Attention, $X(k)$ ne détermine pas X ; notamment, cet ensemble peut très bien être vide sans que X le soit (car le Nullstellensatz ne fonctionne que sur un corps

algébriquement clos). Par exemple, $Z(x^2 + y^2 + 1) \subseteq \mathbb{A}^2$ définit une variété algébrique affine sur $\mathbb{R}$ qui n'a aucun $\mathbb{R}$-point.

La même chose fonctionne en projectif : on a des bijections réciproques, décroissantes pour l'inclusion, entre idéaux homogènes radicaux de $k[t_0, \ldots, t_d]$ autres que $(t_0, \ldots, t_d)$ et fermés de Zariski de $\mathbb{P}^d(k^{\mathrm{alg}})$ stables par Galois, donnée par $I \mapsto Z(I_{k^{\mathrm{alg}}})$ et $E \mapsto \mathfrak{I}(E) \cap k[t_0, \ldots, t_d]$.

On appelle variété quasiprojective sur k une variété quasiprojective X (dans $\mathbb{P}^d$) sur k^{alg} qui soit stable par Galois (moralité : c'est une variété dont les équations peuvent être définies sur k). On peut donc définir une action de Galois sur $X(k^{\mathrm{alg}})$, et $X(k)$ est l'ensemble des points fixés par Galois (et pour toute extension k' de k, l'ensemble $X(k')$ est le sous-ensemble de $X(k^{\mathrm{alg}})$ fixé par $\Gamma_{k'}$).

Pour éviter les confusions, on note souvent $X_{k^{\mathrm{alg}}}$ la variété sur k^{alg} définie par X (c'est-à-dire celle où on oublie la structure sur k / l'action de Galois).

Attention : si un idéal $I \subseteq k[t_1, \ldots, t_d]$ est premier (cela signifie qu'il est radical et que la variété $X = Z(I) \subseteq \mathbb{A}^d$ définie sur k est irréductible au sens où elle n'est pas réunion de deux fermés plus petits définis sur k), cela n'implique pas que $I_{k^{\mathrm{alg}}}$ soit premier, c'est-à-dire que $X_{k^{\mathrm{alg}}}$ soit irréductible ; par contre, la réciproque est vraie. On dit parfois que X est *absolument irréductible* ou *géométriquement irréductible* lorsque $X_{k^{\mathrm{alg}}}$ est irréductible. Contre-exemple : $Z(x^2 + y^2)$ dans $\mathbb{A}^2$ sur $\mathbb{R}$ n'est pas absolument irréductible puisque sur $\mathbb{C}$ il est réunion des deux droites $Z(x + iy)$ et $Z(x - iy)$, mais sur $\mathbb{R}$ il est irréductible car tout fermé défini sur $\mathbb{R}$ qui contient une de ces droites doit contenir l'autre.

Quant aux idéaux *maximaux* de $k[t_1, \ldots, t_d]$, ils correspondent aux *orbites* sous Γ_k, c'est-à-dire aux ensembles (nécessairement finis) de k^{alg}-points tels que n'importe lequel puisse être envoyé sur n'importe lequel par un élément de Γ_k (c'est-à-dire, si on préfère, qu'aucun sous-ensemble non-vide n'est stable par Γ_k). (On peut, si on le souhaite, considérer que ce sont là les « points » de l'espace affine $\mathbb{A}^d$, auquel cas on les appelle « points fermés » pour bien les distinguer des « k-points », c'est-à-dire les éléments de k^d, ou orbites réduites à un seul élément.) Une remarque analogue vaut pour des variétés algébriques sur k plus générales : les idéaux maximaux de $k[t_1, \ldots, t_d]/I$, pour I idéal radical de $k[t_1, \ldots, t_d]$, correspondent aux orbites sous Γ_k de $Z(I)(k^{\mathrm{alg}})$.

4.3 Morphismes entre icelles

Si X et Y sont deux variétés quasiprojectives sur un corps parfait k, un morphisme $X_{k^{\mathrm{alg}}} \xrightarrow{f} Y_{k^{\mathrm{alg}}}$ sera considéré comme un morphisme $X \to Y$ de k-variétés lorsqu'il vérifie les conditions équivalentes suivantes :

— Il existe des équations à coefficients dans k définissant f.

— Le morphisme f commute à l'action de Galois, au sens où $\sigma(f(x)) = f(\sigma(x))$ pour tout $x \in X(k^{\mathrm{alg}})$.

(Cas particulier éclairant : si $f \in \mathbb{F}_{q^n}[t]$, alors $f(t)^q = f(t^q)$ si et seulement si $f \in \mathbb{F}_q[t]$.)

En particulier, f définit une application $X(k) \to Y(k)$, mais la donnée de celle-ci *ne suffit pas* à caractériser f (penser au fait que $X(k)$ peut très bien être vide !).

Pour les fonctions régulières, on a ce qu'on imagine : un morphisme $X \to \mathbb{A}^1$ est la même chose qu'une fonction régulière sur $X_{k^{\mathrm{alg}}}$ stable par Galois, et c'est ce qu'on appelle une fonction régulière sur X. Lorsque $X = Z(I) \subseteq \mathbb{A}^d$ est affine (avec $I = \mathfrak{I}(X)$ idéal de $k[t_1, \ldots, t_d]$), les fonctions régulières sur X sont les éléments de $\mathcal{O}(X) := k[t_1, \ldots, t_d]/I$, qui est donc plus petit que $\mathcal{O}(X_{k^{\mathrm{alg}}}) = k^{\mathrm{alg}}[t_1, \ldots, t_d]/I_{k^{\mathrm{alg}}}$. En général, on peut toujours définir une fonction régulière sur X par recollement de fonctions régulières sur des ouverts affines (c'est-à-dire : on peut le faire *sur* k, il n'y a pas besoin de passer à la clôture algébrique).

5 Quelques résultats fondamentaux de la géométrie algébrique

5.1 L'opposition affine-projectif

Théorème 5.1.1. Tout morphisme d'une variété projective connexe vers une variété affine est constant. (En particulier, toute fonction régulière sur une variété projective, c'est-à-dire morphisme vers $\mathbb{A}^1$, est constante sur chaque composante connexe.)

5.2 La dimension

Rappel : Si K est un corps contenant un corps k, on dit que des éléments x_i de K sont **algébriquement indépendants** (comprendre : « collectivement transcendants ») sur k lorsque les seuls polynômes $f \in k[t_1, \ldots, t_d]$ tel que $f(x_{i_1}, \ldots, x_{i_d}) = 0$ pour certains $i_1, \ldots, i_d$ deux à deux distincts sont les polynômes nuls. Ceci est équivalent au fait que le sous-corps $k(x_i)$ de K engendré par les x_i avec k est isomorphe au corps des fractions rationnelles sur autant d'indéterminées que de x_i (il est plus simple de penser au cas où les x_i sont en nombre fini, qui nous suffira). On appelle **base de transcendance** de K sur k un ensemble maximal d'éléments algébriquement indépendants, c'est-à-dire, un ensemble de x_i algébriquement indépendants sur k et tels que K soit algébrique sur le sous-corps $k(x_i)$ qu'ils engendrent au-dessus de k. Une base de transcendance de K sur k existe toujours,

et toutes ont le même cardinal : on appelle celui-ci **degré de transcendance** de K sur k et on le note $\deg.\,\mathrm{tr}_k(K)$.

Par exemple, $\deg.\,\mathrm{tr}_k\, k(t_1,\dots,t_d) = d$ (où $k(t_1,\dots,t_d)$ désigne le corps des fractions rationnelles en d indéterminées sur k). Lorsque K est algébrique sur k, on a $\deg.\,\mathrm{tr}_k\, K = 0$ et réciproquement. Par ailleurs, lorsque $k \subseteq K \subseteq L$ sont trois corps, on a toujours $\deg.\,\mathrm{tr}_k\, L = \deg.\,\mathrm{tr}_k\, K + \deg.\,\mathrm{tr}_K\, L$.

Définition 5.2.1. Si X est une variété *irréductible* sur un corps k, on appelle **fonction rationnelle** sur X une fonction régulière sur un ouvert non-vide=dense quelconque de X, en identifiant deux fonctions si elles coïncident sur l'intersection de leur domaine de définition ; on note $k(X)$ l'ensemble des fonctions régulières sur X. Lorsque X est une variété affine irréductible, $k(X)$ est le corps des fractions (noté $k(X)$) de $\mathcal{O}(X)$ (=l'anneau des fonctions régulières sur X, qui est intègre). De façon générale, $k(X)$ coïncide avec $k(U)$ pour n'importe quel ouvert non-vide=dense U de X (on peut donc définir $k(X) = \mathrm{Frac}\,\mathcal{O}(U)$ pour U un ouvert affine dense de X).

On appelle **dimension de** X le degré de transcendance sur k de $k(X)$.

Pour $\mathbb{A}^d$ ou $\mathbb{P}^d$, le corps des fractions rationnelles est $k(t_1,\dots,t_d)$ et $k(\frac{t_1}{t_0},\dots,\frac{t_d}{t_0})$. La dimension de $\mathbb{A}^d$ ou $\mathbb{P}^d$ est donc d. De façon générale, d'après ce qu'on vient de dire, la dimension d'une variété irréductible est égale à celle de n'importe lequel de ses ouverts non-vides.

(Lorsque X n'est pas irréductible, on appelle dimension de X la plus grande dimension d'une composante irréductible de X. Parfois on convient que la dimension du vide est -1.)

La dimension de X est une notion « géométrique » : on a $\dim X = \dim X_{k^{\mathrm{alg}}}$.

Théorème 5.2.2 (Hauptidealsatz de Krull)**.** Soit X une variété irréductible de dimension d et $f \in \mathcal{O}(X)$ un élément qui n'est pas inversible (c'est-à-dire $Z(f) \neq \varnothing$) et pas nul. Alors chaque composante irréductible de $Z(f)$ est de dimension $d-1$.

Variante projective : si X est une variété irréductible de dimension d dans $\mathbb{P}^e$ et f homogène (en $e+1$ variables) non constant sur X. Alors chaque composante irréductible de $X \cap Z(f)$ est de dimension $d-1$, *et de plus* $X \cap Z(f)$ *n'est pas vide*[5] lorsque $d \geq 1$.

Corollaire 5.2.3. Si $f_1,\dots,f_r$ sont des polynômes homogènes en $e+1$ variables, avec $r \leq e$, alors $Z(f_1,\dots,f_r) \neq \varnothing$, c'est-à-dire que sur k corps algébriquement clos, les r équations $f_i = 0$ ont une solution (non-nulle) commune.

5. On rappelle que « non vide » signifie ici que la variété a des points sur k^{alg} algébriquement clos, pas nécessairement qu'elle a des k-points.

De plus, $Z(f_1, \ldots, f_r)$ est de dimension *au moins* $e - r$. Il peut évidemment être de dimension plus grande (les f_i pourraient être tous égaux, par exemple). Lorsqu'il est exactement de dimension $e - r$, on dit que les f_i sont *en intersection complète* (projective, globale).

Corollaire 5.2.4. Si X est une variété algébrique (quasiprojective) irréductible de dimension d, alors le seul fermé Y de X tel que $\dim Y = d$ est X lui-même. Par ailleurs, il existe toujours des fermés irréductibles Y de dimension $d - 1$ dans X.

Par conséquent, on peut définir la dimension de X comme $1 + \max \dim Y$ où le $\max$ est pris sur tous les fermés irréductibles de X différents de X (et cette définition récursive a bien un sens !).

Théorème 5.2.5. Soit $f\colon Z \to X$ un morphisme de variétés algébriques (quasi-projectives) irréductibles, surjectif (au sens où pour tout $x \in X$ il existe $z \in Z$ tel que $x = f(z)$, x, z étant des points sur un corps k^{alg} algébriquement clos, cf. la section suivante), et soit $d = \dim X$ et $e = \dim Z$. Alors $e \geq d$, et de plus :

— Si $x \in X$, alors toute composante de $f^{-1}(x)$ (cf. section suivante) est de dimension *au moins* $e - d$.

— Il existe un ouvert non vide (donc dense) $U \subseteq X$ tel que $\dim f^{-1}(x) = e - d$ (au sens où toute composante irréductible de $f^{-1}(x)$ a cette dimension) si $x \in U$.

Voici enfin un résultat qui permet, notamment avec les outils de la section 6 (bases de Gröbner), de rendre algorithmique le calcul des dimensions :

Théorème 5.2.6.

— **Variante projective :** Soit I un idéal homogène de $k[t_0, \ldots, t_d]$. La fonction « de Hilbert-Samuel » qui à $\ell \in \mathbb{N}$ associe la dimension (en tant que k-espace vectoriel) $\dim_k k[t_0, \ldots, t_d]^{[\ell]}/I^{[\ell]} = \frac{(d+\ell)!}{d!\,\ell!} - \dim_k I^{[\ell]}$ de l'ensemble des polynômes homogènes de degré ℓ modulo ceux de I, coïncide avec un polynôme (« de Hilbert-Samuel ») pour ℓ suffisamment grand : le degré de ce polynôme est exactement la dimension de la variété $Z(I) \subseteq \mathbb{P}^d$ définie par l'idéal I (et en particulier, les polynômes de Hilbert-Samuel de I et $\sqrt{I}$ ont même degré).
De plus, en anticipant sur les définitions de la section 6 : pour tout tout ordre admissible $\preceq$, la fonction de Hilbert-Samuel de I coïncide avec celle de $\mathrm{in}_{\preceq}(I)$ et est égale au nombre de monômes de degré ℓ qui n'appartiennent pas à $\mathrm{in}_{\preceq}(I)$. (Ceci permet de la calculer à partir d'une base de Gröbner de I.)

— **Variante affine :** Soit I un idéal de $k[t_1, \ldots, t_d]$. La fonction « de Hilbert-Samuel affine » qui à $\ell \in \mathbb{N}$ associe la dimension (en tant que k-espace vectoriel) $\dim_k k[t_1, \ldots, t_d]^{[\leq \ell]}/I^{[\leq \ell]} = \frac{(d+\ell)!}{d!\,\ell!} - \dim_k I^{[\ell]}$ de l'ensemble des polynômes de degré total $\leq \ell$ modulo ceux de I, coïncide avec un

polynôme (« de Hilbert-Samuel affine ») pour ℓ suffisamment grand : le degré de ce polynôme est exactement la dimension de la variété $Z(I) \subseteq \mathbb{A}^d$ définie par l'idéal I (et en particulier, les polynômes de Hilbert-Samuel affine de I et $\sqrt{I}$ ont même degré).
De plus, en anticipant sur les définitions de la section 6 : pour tout tout ordre admissible *gradué* $\preceq$, la fonction de Hilbert-Samuel affine de I coïncide avec celle de $\mathrm{in}_\preceq(I)$ et est égale au nombre de monômes de degré $\leq \ell$ qui n'appartiennent pas à $\mathrm{in}_\preceq(I)$. (Ceci permet de la calculer à partir d'une base de Gröbner de I.)

Exemple : Pour $\mathbb{P}^d$ (i.e., pour I l'idéal nul), le k-espace vectoriel $k[t_0, \ldots, t_d]^{[\ell]}$ des polynômes homogènes de degré ℓ en $d+1$ indéterminées a pour base les monômes de degré (total) ℓ, qui sont au nombre de $\frac{(d+\ell)!}{d!\,\ell!}$. C'est là la fonction de Hilbert-Samuel de $\mathbb{P}^d$ (c'est aussi la fonction de Hilbert-Samuel affine de $\mathbb{A}^d$), et son terme dominant vaut $\frac{1}{d!}\,\ell^d$, ce qui est cohérent avec le fait que $\mathbb{P}^d$ (ou $\mathbb{A}^d$) est de dimension d.

Si on considère maintenant le cercle $C^+ = Z(x^2 + y^2 - z^2)$ dans $\mathbb{P}^2$, les polynômes de degré ℓ en x, y, z modulo z^2 peuvent se réduire en un polynôme de degré ℓ en x, y, plus z fois un polynôme de degré $\ell - 1$ en x, y : leur dimension est donc $2\ell + 1$ (une base est donnée par $x^\ell, x^{\ell-1}y, \ldots, y^\ell, x^{\ell-1}z, x^{\ell-2}yz, \ldots, y^{\ell-1}z$), donc le polynôme de Hilbert-Samuel vaut $2\ell + 1$. On voit ici que le cercle est de dimension 1.

5.3 L'image d'un morphisme

Si $X \xrightarrow{f} Y$ est un morphisme entre variétés quasiprojectives et $Y' \subseteq Y$ un fermé ou un ouvert (ou l'intersection d'un fermé et d'un ouvert) dans Y, il est facile de définir l'*image réciproque* de Y' par f : il suffit de « tirer » les équations de Y' de Y à X, c'est-à-dire écrire les équations $h \circ f = 0$ pour chaque équation $h = 0$ de Y' (et pareil avec $\neq 0$ si on a affaire à un ouvert).

Définir l'*image (directe)* d'un $X' \subseteq X$ est plus délicat. Quitte à restreindre f à X', on peut supposer $X' = X$, et la question devient celle de définir l'image de f : notamment, quel est l'ensemble des $y \in Y$ tels qu'il existe $x \in X$ (x, y des points sur k^{alg}) pour lequel $f(x) = y$?

Théorème 5.3.1 (Chevalley)**.** — L'image d'un morphisme $X \xrightarrow{f} Y$ entre variété quasiprojectives est « constructible » dans Y, au sens suivant : il existe $Y'_1, \ldots, Y'_s \subseteq Y$, chacun intersections d'un ouvert et d'un fermé dans Y (c'est-à-dire que chaque Y'_i est une sous-variété quasiprojective de Y), tels que, pour $y \in Y$, on ait $\exists i (y \in Y'_i)$ si et seulement si il existe $x \in X$ pour lequel $f(x) = y$.

— Si X est projective, alors l'image d'un morphisme $X \xrightarrow{f} Y$ est un *fermé* dans Y.

5.4 Vecteurs tangents, points lisses, et différentielles

Si $X = Z(I) \subseteq \mathbb{A}^d$ est une variété affine où I est un idéal radical engendré par $f_1, \ldots, f_r \in k[t_1, \ldots, t_d]$, et si $x \in X(k)$ (on prendra généralement k algébriquement clos ici), on appelle **vecteur tangent à X en x** un élément du noyau de la matrice $\left.\frac{\partial f_i}{\partial t_j}\right|_{x_1,\ldots,x_d}$, c'est-à-dire un d-uplet $v_1, \ldots, v_d$ tel que $\sum_{j=1}^{d} \left.\frac{\partial f_i}{\partial t_j}\right|_{x_1,\ldots,x_d} v_j = 0$. Intuitivement, il faut comprendre un tel élément comme un vecteur basé en $(x_1, \ldots, x_d)$ et le reliant à $(x_1 + v_1\varepsilon, \ldots, x_d + v_d\varepsilon)$ avec ε infinitésimal ($\varepsilon^2 = 0$). L'espace vectoriel des vecteurs tangents à X en x (ou simplement **espace tangent à X en x**) se note T_xX.

Si X est une variété algébrique quasiprojective quelconque, on rappelle que tout point $x \in X$ a un voisinage affine V, et on définit alors $T_xX = T_xV$. (Cette définition passe sous silence un certain nombre de choses, par exemple la manière dont on identifie T_xV et T_xV' si V, V' sont deux voisinages affines différents du même point x, à commencer par le fait qu'ils ont la même dimension : cela est en fait justifié par la notion de différentielle d'un morphisme, expliquée plus bas.)

Proposition 5.4.1. Si X est une variété algébrique quasiprojective irréductible sur un corps k, pour tout $x \in X$ on a $\dim_k T_xX \geq \dim X$.

Un point x tel que l'espace tangent T_xX à X en ce point soit d'une dimension (comme espace vectoriel) égale à la dimension de X (comme variété algébrique), c'est-à-dire la dimension minimale que peut avoir cet espace tangent, est appelé un point **lisse** (ou **régulier**, ou **nonsingulier**) de X. Lorsque tout point de X (sur un corps algébriquement clos !) est lisse, on dit que X lui-même est lisse (ou régulier) (sur son corps de base).

(Pour une variété réductible, un point situé sur une seule composante irréductible est dit lisse lorsqu'il est lisse sur la composante en question ; et un point situé sur plusieurs composantes irréductibles à la fois n'est jamais lisse — on peut prendre ça comme définition ou le montrer en prenant comme définition de la lissité le fait que la dimension de l'espace tangent au point considéré soit égale à la plus grande dimension d'une composante irréductible passant par ce point.)

Proposition 5.4.2. Soit X une variété quasiprojective sur un corps algébriquement clos k : alors les points lisses de X forment un ouvert de Zariski.

Démonstration. L'affirmation est locale, donc on peut supposer X affine. Si X est de codimension r (c'est-à-dire de dimension $d - r$ dans $\mathbb{A}^d$), le fait que x soit

lisse se traduit par le fait que la matrice des dérivées partielles en x des équations définissant X est de rang *au moins* r (sachant qu'elle ne peut pas être strictement supérieure). Or ceci se traduit par le fait qu'il existe un mineur $r \times r$ de cette matrice qui ne s'annule pas : la réunion des ouverts définis par tous les mineurs $r \times r$ (qui sont bien polynomiaux dans les variables) donne bien une condition ouverte de Zariski. ☺

Remarque 5.4.3. — D'après 5.2.2, une hypersurface $Z(f)$ dans $\mathbb{A}^d$, pour f non constant, est de dimension $d-1$, donc elle est lisse ssi aucun point de $Z(f)$ n'annule simultanément les d dérivées partielles de f. Grâce au Nullstellensatz, ceci peut encore se reformuler en : $Z(f)$ est lisse ssi les polynômes f et $\frac{\partial f}{\partial t_i}$ (soit $d+1$ polynômes au total) engendrent l'idéal unité de $k[t_1, \ldots, t_d]$.

— Variante projective : pour f homogène de degré non nul dans $k[t_0, \ldots, t_d]$, on peut montrer que $Z(f) \subseteq \mathbb{P}^d$ est lisse ssi les polynômes $\frac{\partial f}{\partial t_i}$ n'ont aucun zéro commun sur k (algébriquement clos !), car un zéro commun des $\frac{\partial f}{\partial t_i}$ est forcément zéro de $\deg(f) \cdot f = \sum_{i=0}^{d} t_i \frac{\partial f}{\partial t_i}$. Grâce au Nullstellensatz projectif, on peut encore reformuler cela en : les $\frac{\partial f}{\partial t_i}$ engendrent un idéal irrelevant.

— Quand $X = Z(f_1, \ldots, f_r)$ (affine, disons dans $\mathbb{A}^d$) est définie par plusieurs polynômes $f_1, \ldots, f_r$, *si* la matrice $\frac{\partial f_i}{\partial t_j}$ est de rang r en un point de $X = Z(f_1, \ldots, f_r)$, on peut conclure que ce point est lisse et que X est de dimension $d-r$. En revanche, lorsque le rang est plus petit que r, on ne peut pas conclure sauf en connaissant la dimension de X.

Proposition 5.4.4. Soit X une variété quasiprojective : alors il existe un point lisse de X sur un corps algébriquement clos k — par conséquent, il existe un ouvert dense de points lisses sur une variété quasiprojective irréductible.

Ceci permet parfois de calculer la dimension d'une variété, en reformulant en : la dimension d'une variété irréductible X est le *minimum* des dimensions des espaces vectoriels $T_x X$ (donc, dans $\mathbb{A}^d$, la codimension est le plus grand rang possible que prend la matrice des dérivés partielles).

Différentielle d'un morphisme. Si $h\colon X \to Y$ est un morphisme entre variétés quasiprojectives sur un corps algébriquement clos k et $x \in X$, on a une application $dh_x\colon T_x X \to T_{h(x)} Y$ qui est définie de la façon suivante. Quitte à remplacer X par un voisinage affine de x et Y par un voisinage affine de $h(x)$, on peut supposer que X et Y sont affines. Dans ce cadre, si X est défini par des équations [6]

6. Ce genre de formulation sous-entend non seulement que $X = Z(f_1, \ldots, f_r)$ mais, plus fortement, que l'idéal $(f_1, \ldots, f_r)$ est *radical*, c'est-à-dire que c'est $\mathfrak{I}(X)$.

$f_1 = \cdots = f_r = 0$ dans $\mathbb{A}^d$ (de sorte que T_xX se voit comme l'ensemble des (v_i) tels que $\sum_{j=1}^d \frac{\partial f_i}{\partial t_j}\Big|_{x_1,\ldots,x_d} v_j = 0$) et Y par $g_1 = \cdots = g_s = 0$ dans $\mathbb{A}^e$ (de sorte que T_yY se voit comme l'ensemble des (w_i) tels que $\sum_{j=1}^e \frac{\partial g_i}{\partial u_j}\Big|_{y_1,\ldots,y_d} w_j = 0$), et le morphisme h par des polynômes $(h_1, \ldots, h_e)$ (vérifiant $g_i(h_1, \ldots, h_e) \equiv 0$ modulo $f_1, \ldots, f_r$) envoyant $(x_1, \ldots, x_d)$ sur $(h_1(x_1, \ldots, x_d), \ldots, h_e(x_1, \ldots, x_d))$, alors dh_x envoie $(v_1, \ldots, v_d)$ sur $(w_1, \ldots, w_e)$ où $w_i = \sum_{j=1}^d \frac{\partial h_i}{\partial t_j}\Big|_{x_1,\ldots,x_d} v_j$ (et la condition souhaitée, $\sum_{i=1}^e w_j \frac{\partial g_i}{\partial u_j}\Big|_{y_1,\ldots,y_d} = 0$ est une conséquence de la formule des dérivées composées appliquée à $g_i(h_1, \ldots, h_e) \equiv 0$: on a $\sum_{j=1}^e \frac{\partial g_i}{\partial u_j}\frac{\partial h_j}{\partial t_l}$ combinaison des $\frac{\partial f_i}{\partial t_j}$). Cette application dh_x est linéaire (pour chaque x donné) : on l'appelle **différentielle** du morphisme h au point x.

Si $h = h'' \circ h'$, alors on a $dh_x = dh''_{h'(x)} \circ dh'_x$ comme on s'y attend.

Lissité des morphismes. On ne définira le concept de morphisme lisse entre variétés quasiprojectives $X \to Y$ que lorsque Y elle-même est lisse. Plus exactement, on dit qu'un morphisme $X \xrightarrow{h} Y$ est *lisse* en un point $x \in X$ tel que Y soit lisse en $h(x)$, lorsque $dh_x \colon T_xX \to T_{h(x)}Y$ est *surjective*. On dit qu'un morphisme $X \to Y$, avec Y lisse, est lisse (partout) lorsque la différentielle est surjective en tout point. Une conséquence importante de la lissité de h est que la fibre $h^{-1}(y)$ est elle-même lisse (en tant que variété, un fermé à l'intérieur de X) pour chaque $y \in Y$.

6 Introduction aux bases de Gröbner

(À part pour la proposition 6.5.2, toute cette partie ne dépend que de la partie 1 et d'aucune des suivantes.)

6.1 Monômes et idéaux monomiaux

On appelle **monôme** de $k[t_1, \ldots, t_d]$ un $t_1^{\ell_1} \cdots t_d^{\ell_d}$. On dit qu'un monôme $t_1^{\ell_1} \cdots t_d^{\ell_d}$ **divise** un monôme $t_1^{\ell'_1} \cdots t_d^{\ell'_d}$ lorsque $\ell_i \leq \ell'_i$ pour tout i (c'est bien la relation de divisibilité dans l'anneau factoriel $k[t_1, \ldots, t_d]$, restreinte aux monômes, et le rapport est alors lui-même un monôme). Un **terme** est un monôme multiplié par une constante (=élément de k) non nulle : on parle alors du monôme *de* ce terme. Tout polynôme s'écrit de façon unique comme somme de termes dont les monômes sont distincts : ce sont les termes de (=intervenant dans) ce polynôme.

Commençons par la remarque suivante, qui est évidente, mais essentielle :

Proposition 6.1.1. Si $s_1, \ldots, s_r$ sont des monômes de $k[t_1, \ldots, t_d]$, alors pour chaque terme cs de $g_1 s_1 + \cdots + g_r s_r$ (où $g_1, \ldots, g_r \in k[t_1, \ldots, t_d]$) le monôme s de ce terme est divisible par l'un des s_i.

Démonstration. En développant l'écriture $g_1 s_1 + \cdots + g_r s_r$, puisque la somme comporte le terme cs, au moins un des facteurs comporte un terme dont le monôme est s, ce qui montre bien que s est divisible par un des s_i. ☺

Corollaire 6.1.2. Si $s_1, \ldots, s_r$ sont des monômes de $k[t_1, \ldots, t_d]$, l'idéal qu'ils engendrent est exactement l'idéal des polynômes dont le monôme de chaque terme est divisible par un des s_i.

Démonstration. On vient de montrer que si f est dans $(s_1, \ldots, s_r)$ alors le monôme de chaque terme de f est divisible par un des s_i. Réciproquement, si c'est le cas, f est somme de termes multiples des s_i, qui appartiennent donc à l'idéal engendré par les s_i. ☺

On appelle **idéal monomial** un idéal de $k[t_1, \ldots, t_d]$ qui peut être engendré par des monômes : le corollaire ci-dessus montre que si I est un idéal monomial, alors tout terme d'un élément de I est encore un élément de I. Réciproquement, si I est un idéal tel que tout terme d'un élément de I soit un élément de I, alors I est monomial (en effet, on peut choisir un ensemble de générateurs de I, et les monômes des termes de ces générateurs donnent des éléments de I qui engendrent les générateurs choisis, donc engendrent I).

6.2 Ordres admissibles sur les monômes

On appelle **ordre admissible** (ou **ordre monomial**) sur les monômes de $k[t_1, \ldots, t_d]$ une relation d'ordre total $\preceq$ sur les monômes de ce dernier telle que :

— $1 \preceq s$ pour tout monôme s, et

— si $s_1 \preceq s_2$ et s est un monôme quelconque, alors $ss_1 \preceq ss_2$.

(On notera souvent abusivement $cs \preceq c's'$, lorsque $cs, c's'$ sont deux termes, pour signifier que leurs monômes vérifient $s \preceq s'$.)

Si de plus l'ordre vérifie la propriété que $\deg s < \deg s'$ implique $s \preceq s'$, on dit qu'il est **gradué**.

Proposition 6.2.1. Si $\preceq$ est un ordre admissible sur les monômes de $k[t_1, \ldots, t_d]$, alors

— si $s_1 | s_2$ alors $s_1 \preceq s_2$,

— $\preceq$ est un bon ordre (c'est-à-dire : tout ensemble non vide de monômes a un plus petit élément pour $\preceq$, ou de façon équivalente, il n'y a pas de suite infinie strictement décroissante de monômes pour $\preceq$).

Démonstration. Le premier point est évident : si $s_2 = ss_1$ alors $1 \preceq s$ entraîne $s_1 \preceq ss_1 = s_2$. Montrons le second : si S est un ensemble de monômes, soit I l'idéal qu'ils engendrent ; comme $k[t_1, \ldots, t_d]$ est noethérien, il existe un sous-ensemble fini $S_0 \subseteq S$ qui engendre le même idéal I. Soit s le plus petit élément de S_0 : on prétend que s est aussi le plus petit élément de S. En effet, si $s' \in S$ alors $s' \in I$ donc s' s'écrit comme combinaison d'éléments de S_0, mais alors d'après 6.1.1, s' est simplement multiple d'un élément de S_0, et d'après le premier point, $s \preceq s'$, ce qui conclut. ☺

Lorsque $d = 1$, le seul ordre admissible sur les monômes est évidemment celui donné par $t^\ell \preceq t^{\ell'}$ ssi $\ell \leq \ell'$.

Une fois fixé un ordre admissible $\preceq$ sur les monômes, si $f \in k[t_1, \ldots, t_d]$ est non nul, on note $\mathrm{in}_\preceq(f)$ (ou simplement $\mathrm{in}(f)$ si l'ordre est sous-entendu) et on appelle **terme initial** (ou **terme de tête**) de f le terme au *plus grand* monôme pour l'ordre en question. (Lorsque $d = 1$, pour le seul ordre admissible sur les monômes, ceci est simplement le terme dominant de f.) Si $f = 0$ on pose (un peu abusivement) $\mathrm{in}(f) = 0$.

Exemples importants d'ordres admissibles sur les monômes : (on supposera toujours, quitte à renuméroter les variables, que $t_1 \preceq t_2 \preceq \cdots \preceq t_d$) :

* L'**ordre lexicographique (pur)** est défini par $t_1^{\ell_1} \cdots t_d^{\ell_d} \preceq_{\mathtt{lex}} t_1^{\ell'_1} \cdots t_d^{\ell'_d}$ ssi $\ell_i < \ell'_i$ pour le *plus grand* i tel que $\ell_i \neq \ell'_i$. Pour cet ordre on a donc $1 \preceq t_1 \preceq t_1^2 \preceq t_1^3 \preceq \cdots \preceq t_2 \preceq t_1t_2 \preceq t_1^2t_2 \preceq \cdots \preceq t_2^2 \preceq t_1t_2^2 \preceq \cdots \preceq t_2^3 \preceq \cdots \preceq t_3 \preceq t_1t_3 \preceq t_1^2t_3 \preceq \cdots \preceq t_2t_3 \preceq t_1t_2t_3 \preceq \cdots \preceq t_3^2 \preceq \cdots \preceq t_4 \preceq \cdots$. (Attention, l'ordre donne le poids fort à l'exposant de la dernière variable, ce qui correspond à la convention faite $t_1 \preceq t_2 \preceq \cdots \preceq t_d$; plus généralement, tout ordre total sur l'ensemble des variables définit un unique ordre lexicographique pur associé.)

Caractérisation : Si $\mathrm{in}_{\mathtt{lex}}(f) \in k[t_1, \ldots, t_s]$ (pour un $s \leq d$) alors $f \in k[t_1, \ldots, t_s]$.

* L'**ordre lexicographique par degré** ou **ordre lexicographique gradué** est défini par $t_1^{\ell_1} \cdots t_d^{\ell_d} \preceq_{\mathtt{glex}} t_1^{\ell'_1} \cdots t_d^{\ell'_d}$ ssi $\sum \ell_i < \sum \ell'_i$ ou $\sum \ell_i = \sum \ell'_i$ et $\ell_i < \ell'_i$ pour le *plus grand* i tel que $\ell_i \neq \ell'_i$. Autrement dit, les monômes sont classés par degré total en priorité puis, faute de cela, par l'ordre lexicographique pur défini ci-dessus. Pour cet ordre, on a donc $1 \preceq t_1 \preceq t_2 \preceq t_3 \preceq t_4 \preceq \cdots \preceq t_1^2 \preceq t_1t_2 \preceq t_2^2 \preceq t_1t_3 \preceq t_2t_3 \preceq t_3^2 \preceq \cdots \preceq t_1^3 \preceq t_1^2t_2 \preceq t_1t_2^2 \preceq t_2^3 \preceq t_1^2t_3 \preceq t_1t_2t_3 \preceq \cdots$. (Même remarque que ci-dessus : il y a un tel ordre pour chaque ordre total sur les variables.)

Caractérisation : L'ordre $\preceq_{\mathtt{glex}}$ raffine l'ordre partiel donné par le degré total ; et si f homogène vérifie $\mathrm{in}_{\mathtt{glex}}(f) \in k[t_1, \ldots, t_s]$ (pour un $s \leq d$) alors $f \in k[t_1, \ldots, t_s]$.

* L'**ordre lexicographique inversé par degré** (ou **...gradué**) est défini par $t_1^{\ell_1}\cdots t_d^{\ell_d} \preceq_{\texttt{grevlex}} t_1^{\ell'_1}\cdots t_d^{\ell'_d}$ ssi $\sum \ell_i < \sum \ell'_i$ ou $\sum \ell_i = \sum \ell'_i$ et $\ell_i > \ell'_i$ (attention au sens !) pour le *plus petit* i tel que $\ell_i \neq \ell'_i$. Pour cet ordre, on a donc $1 \preceq t_1 \preceq t_2 \preceq t_3 \preceq t_4 \preceq \cdots \preceq t_1^2 \preceq t_1t_2 \preceq t_1t_3 \preceq t_1t_4 \preceq \cdots \preceq t_2^2 \preceq t_2t_3 \preceq \cdots \preceq t_3^2 \preceq \cdots \preceq t_1^3 \preceq t_1^2t_2 \preceq t_1^2t_3 \preceq \cdots \preceq t_1t_2^2 \preceq t_1t_2t_3 \preceq \cdots \preceq t_2^3 \preceq \cdots$. (Même remarque que ci-dessus : il y a un tel ordre pour chaque ordre total sur les variables. De plus, $\preceq_{\texttt{grevlex}}$ et $\preceq_{\texttt{glex}}$ coïncident lorsqu'il n'y a que deux variables, une fois fixé l'ordre entre celles-ci.)

Caractérisation : L'ordre $\preceq_{\texttt{grevlex}}$ raffine l'ordre partiel donné par le degré total ; et si f homogène vérifie $\mathrm{in}_{\texttt{grevlex}}(f) \in (t_1, \ldots, t_s)$ (pour un $s \leq d$) alors $f \in (t_1, \ldots, t_s)$.

6.3 Bases de Gröbner

Si I est un idéal de $k[t_1, \ldots, t_d]$ (et $\preceq$ un ordre admissible), on appelle $\mathrm{in}_\preceq(I)$ l'idéal engendré par les $\mathrm{in}_\preceq(f)$ pour tous les $f \in I$ (c'est donc un idéal monomial). Attention ! il n'y a aucune raison que prendre les $\mathrm{in}_\preceq(f)$ pour f parcourant des générateurs de I suffise à engendrer $\mathrm{in}_\preceq(I)$.

Définition 6.3.1. Si I est un idéal de $k[t_1, \ldots, t_d]$ et $\preceq$ un ordre admissible sur les monômes de ce dernier, on appelle **base de Gröbner** de I un ensemble $f_1, \ldots, f_r$ d'éléments de I tels que $\mathrm{in}_\preceq(f_1), \ldots, \mathrm{in}_\preceq(f_r)$ engendrent $\mathrm{in}_\preceq(I)$.

A priori, rien ne dit que $f_1, \ldots, f_r$ engendrent I. C'est pourtant le cas :

Proposition 6.3.2. Dans les conditions ci-dessus, on a $I = (f_1, \ldots, f_r)$.

Démonstration. On a $I \supseteq (f_1, \ldots, f_r)$ puisque les f_i sont supposés dans I. Supposons maintenant qu'il n'y ait pas égalité. Soit $h \in I$ un polynôme avec le monôme dans $\mathrm{in}(h)$ le plus petit possible (pour $\preceq$) tel que $h \notin (f_1, \ldots, f_r)$. Puisque $\mathrm{in}(h) \in \mathrm{in}(I)$, on peut écrire $\mathrm{in}(h) = g_1 \mathrm{in}(f_1) + \cdots + g_r \mathrm{in}(f_r)$ par l'hypothèse faite sur les f_i (pour certains $g_1, \ldots, g_r$). D'après 6.1.1, ceci montre que $\mathrm{in}(h) = cs\,\mathrm{in}(f_i)$ pour un certain monôme s et c une constante. On a alors $sf_i \in I$, et $\mathrm{in}(csf_i) = cs\,\mathrm{in}(f_i) = \mathrm{in}(h)$, donc $h - csf_i$, qui appartient à I, a un terme initial de monôme strictement plus petit que h, donc par minimalité de ce dernier, $h - csf_i \in (f_1, \ldots, f_r)$. Mais alors $h \in (f_1, \ldots, f_r)$, une contradiction. ☺

Une évidence : tout idéal admet une base de Gröbner. En effet, parmi les $\mathrm{in}(f)$ pour $f \in I$ qui engendrent $\mathrm{in}(I)$ on peut extraire un ensemble fini engendrant $\mathrm{in}(I)$ — il s'agit d'une base de Gröbner de I.

Algorithme 6.3.3 (algorithme de division)**.** Soient $f, f_1, \ldots, f_r \in k[t_1, \ldots, t_d]$ et $\preceq$ un ordre admissible sur les monômes. Alors il existe une écriture

$$f = g_1 f_1 + \cdots + g_r f_r + \rho \qquad (*)$$

où $g_1, \ldots, g_r, \rho \in k[t_1, \ldots, t_d]$, où aucun des monômes de ρ n'est divisible par un des $\mathrm{in}(f_i)$, et où $\mathrm{in}(g_i f_i) \preceq \mathrm{in}(f)$ pour chaque i ; et on va donner un algorithme pour calculer cette écriture ; un tel ρ s'appelle un **reste** de f par rapport au $f_1, \ldots, f_r$ et pour l'ordre monomial $\preceq$ (on dit aussi que l'écriture $(*)$ s'appelle une **écriture standard** de f par rapport aux $f_1, \ldots, f_r$ et pour cet ordre monomial).

Lorsque les $f_1, \ldots, f_r$ forment une base de Gröbner (d'un idéal $I = (f_1, \ldots, f_r)$), on a $f \in (f_1, \ldots, f_r)$ si et seulement si $\rho = 0$, et ρ est défini de façon unique par f.

Description de l'algorithme. Si aucun terme de f n'est divisible par aucun des $\mathrm{in}(f_i)$, retourner $\rho = f$ (et tous les $g_i = 0$). Sinon, soit $cs\,\mathrm{in}(f_i)$ (où $c \neq 0$ est une constante et s un monôme) le $\preceq$-plus grand terme de f qui soit divisible par un des $\mathrm{in}(f_i)$: on applique récursivement l'algorithme à $f' = f - csf_i$ (qui vérifie $\mathrm{in}(f') \preceq \mathrm{in}(f)$), si $f' = g'_1 f_1 + \cdots + g'_r f_r + \rho'$ est le résultat, renvoyer $g_j = g'_j$ sauf $g_i = g'_i + cs$, et $\rho = \rho'$. ☺

Démonstration. L'algorithme termine car le $\preceq$-plus grand monôme de f divisible par un des $\mathrm{in}(f_i)$ décroît strictement à chaque itération, or $\preceq$ est un bon ordre (cf. 6.2.1). La propriété sur ρ est évidente. La propriété $\mathrm{in}(g_j f_j) \preceq \mathrm{in}(f)$ découle par induction de $\mathrm{in}(g'_j f_j) \preceq \mathrm{in}(f') \preceq \mathrm{in}(f)$ et $\mathrm{in}(csf_i) = cs\,\mathrm{in}(f_i) = c\,\mathrm{in}(f)$.

Si $\rho = 0$, le fait que $f \in (f_1, \ldots, f_r)$ est trivial. Si $f_1, \ldots, f_r$ forment une base de Gröbner et $f \in (f_1, \ldots, f_r)$, comme on a aussi $\rho \in (f_1, \ldots, f_r)$, alors $\mathrm{in}(\rho) \in (\mathrm{in}(f_1), \ldots, \mathrm{in}(f_r))$, ce qui vu le fait qu'aucun monôme de ρ n'est divisible par un des $\mathrm{in}(f_i)$, n'est possible que si $\rho = 0$ (cf. 6.1.1) ; de même, si ρ et ρ' sont deux restes différents du même f, disons $f = g_1 f_1 + \cdots + g_r f_r + \rho$ et $f = g'_1 f_1 + \cdots + g'_r f_r + \rho'$, alors $(g'_1 - g_1) f_1 + \cdots + (g'_r - g_r) f_r + (\rho' - \rho)$ est une écriture standard de 0, donc $\rho' = \rho$. ☺

Moralité : Connaître une base de Gröbner d'un idéal I permet de répondre à la question de savoir si $f \in I$ pour un idéal donné. Mieux, si $(f_1, \ldots, f_r)$ est cette base de Gröbner, l'ensemble des classes des monômes qui ne sont divisibles par aucun des $\mathrm{in}(f_i)$ constitue une base de $k[t_1, \ldots, t_d]/I$, ce qui, avec l'algorithme de division, permet de calculer dans l'anneau en question.

Lorsque $f_1, \ldots, f_r$ ne forment pas une base de Gröbner, on peut très bien avoir $\rho \neq 0$ et pourtant que ρ (c'est-à-dire, f) appartienne à l'idéal $(f_1, \ldots, f_r)$. Par exemple, pour deux polynômes, $g_1 f_1 + g_2 f_2$ pourrait avoir un terme initial beaucoup plus petit que ceux de f_1, f_2 à cause d'une annulation entre ceux-ci (dans ce cas, l'algorithme de division appliqué à $g_1 f_1 + g_2 f_2$ par rapport à f_1, f_2

donnerait $g_1 f_1 + g_2 f_2$ lui-même comme reste, bien que ce polynôme appartienne à (f_1, f_2)). L'algorithme de Buchberger pour calculer les bases de Gröbner se fonde sur l'idée qu'il suffit d'éviter ce phénomène.

6.4 L'algorithme de Buchberger

Soient $f_1, \ldots, f_r \in k[t_1, \ldots, t_d]$: pour chaque couple (i, j) (où $i \neq j$), on définit le **polynôme de syzygie** entre f_i et f_j :

$$f_{i,j} = c_{j,i} s_{j,i} f_i - c_{i,j} s_{i,j} f_j$$
$$\text{où } c_{i,j} s_{i,j} = \text{in}(f_i) / \operatorname{pgcd}(\text{in}(f_i), \text{in}(f_j))$$

Le pgcd (unitaire) de deux termes cs et $c's'$ étant défini comme le plus grand monôme (pour n'importe quel ordre admissible, ou pour l'ordre partiel de divisibilité) parmi les monômes qui divisent à la fois s et s' (c'est-à-dire $t_1^{\min(\ell_1, \ell'_1)} \cdots t_d^{\min(\ell_d, \ell'_d)}$ si $s = t_1^{\ell_1} \cdots t_d^{\ell_d}$ et $s' = t_1^{\ell'_1} \cdots t_d^{\ell'_d}$). Remarquons que $c_{i,j} s_{i,j} f_i$ et $c_{j,i} s_{j,i} f_j$ ont le même terme initial, de sorte que celui de $f_{i,j}$ a un monôme strictement plus petit. (Bien sûr, $f_{i,i} = 0$ pour tout i, donc on ne s'intéresse qu'aux $f_{i,j}$ pour $i \neq j$.)

On appelle **module des relations** entre $f_1, \ldots, f_r$ l'ensemble (qui est un sous-module de $(k[t_1, \ldots, t_d])^r$, d'où le terme) des $(g_1, \ldots, g_r)$ tels que $g_1 f_1 + \cdots + g_r f_r = 0$, ces $(g_1, \ldots, g_r)$ étant appelés des **relations** entre les f_i (relation non-triviale si les g_i ne sont pas tous nuls).

Soit $\rho_{i,j}$ le reste (au sens de 6.3.3) de $f_{i,j}$ par rapport aux $f_1, \ldots, f_r$ (pour un ordre monomial $\preceq$) : si les $f_1, \ldots, f_r$ forment une base de Gröbner alors $\rho_{i,j} = 0$ puisque $f_{i,j} \in (f_1, \ldots, f_r)$. Ce qui est plus surprenant est que la réciproque est également vraie :

Théorème 6.4.1 (critère de Buchberger)**.** Avec les notations ci-dessus, on a $\rho_{i,j} = 0$ pour tous i, j si et seulement $f_1, \ldots, f_r$ forment une base de Gröbner (de l'idéal qu'ils engendrent).

(Spears-Schreyer) De plus, lorsque c'est le cas, les relations $c_{j,i} s_{j,i} f_i - c_{i,j} s_{i,j} f_j - \sum_u g_u^{(i,j)} f_u$, où $f_{i,j} = g_1^{(i,j)} f_1 + \cdots + g_r^{(i,j)} f_r$ est une écriture standard de $f_{i,j}$, engendrent [7] le module des relations entre $f_1, \ldots, f_r$.

Algorithme 6.4.2 (algorithme de Buchberger)**.** Donné $f_1, \ldots, f_r \in k[t_1, \ldots, t_d]$, on peut calculer effectivement une base de Gröbner de l'idéal qu'ils engendrent.

7. En fait, les relations en question forment elles-même une base de Gröbner du module des relations, si on prend la peine de définir la notion de « base de Gröbner » d'un module et non seulement d'un idéal, pour un ordre admissible sur les monômes de $k[t_1, \ldots, t_d]^r$ qui se déduit facilement de $\preceq$.

Description de l'algorithme. Calculer les $\rho_{i,j}$ définis plus hauts : si les $\rho_{i,j}$ sont tous nuls, terminer (les $f_1, \ldots, f_r$ forment une base de Gröbner). Si un des $\rho_{i,j}$ est non nul, dès qu'on le trouve, ajouter ce $\rho_{i,j}$ parmi les $f_1, \ldots, f_r$ (c'est-à-dire, recommencer l'algorithme avec $f_1, \ldots, f_r, \rho_{i,j}$). ☺

Démonstration. L'algorithme termine car l'idéal engendré par $\mathrm{in}(f_1), \ldots, \mathrm{in}(f_r)$ ne cesse de croître strictement : le processus doit donc terminer, ce qui ne peut se produire que parce que tous les $\rho_{i,j}$ sont tous nuls, et le critère précédent permet de dire qu'on a bien une base de Gröbner. ☺

Bases de Gröbner réduites.

Définition 6.4.3. Une base de Gröbner $f_1, \ldots, f_r$ est dite **réduite** lorsque, pour $i \neq j$, le monôme du terme $\mathrm{in}(f_i)$ ne divise aucun des monômes apparaissant dans f_j, et si, de plus, chacun des termes $\mathrm{in}(f_i)$ est unitaire (=la constante devant le monôme est 1).

On peut facilement calculer une base de Gröbner réduite à partir d'une base de Gröbner, en soustrayant, pour chaque f_j, chaque terme divisible par un des $\mathrm{in}(f_i)$ (et en commençant par le plus grand pour l'ordre monomial), le multiple de f_i qui permet de l'annuler, et en répétant cette opération aussi souvent que nécessaire (il est clair que cela termine). Il faut, bien sûr, retirer tous les éléments nuls, puis normaliser à 1 la constante devant le monôme initial de chaque f_i.

Proposition 6.4.4. Pour un idéal I de $k[t_1, \ldots, t_d]$ et un ordre admissible $\preceq$, il existe une unique base de Gröbner réduite (on l'appelle donc *la* base de Gröbner réduite de I pour cet ordre).

6.5 Bases de Gröbner et élimination

Proposition 6.5.1. Soit I un idéal de $k[t_1, \ldots, t_d]$ et $s \leq d$: si $f_1, \ldots, f_r$ est une base de Gröbner de I pour l'ordre $\preceq_{\texttt{lex}}$ (où on est convenu que $t_1 \preceq t_2 \preceq \cdots \preceq t_d$), alors ceux des f_i qui appartiennent à $k[t_1, \ldots, t_s]$ forment une base de Gröbner de $I \cap k[t_1, \ldots, t_s]$.

(En fait, il suffit que l'ordre $\preceq$ utilisé vérifie la propriété : si $\mathrm{in}_{\preceq}(f) \in k[t_1, \ldots, t_s]$ alors $f \in k[t_1, \ldots, t_s]$. Une façon parfois plus efficace que l'ordre lexicographique pur, *si on connaît s à l'avance*, consiste à prendre l'ordre sur le degré total en les seules variables $t_1, \ldots, t_s$ comme premier critère de comparaison, et en cas d'égalité comparer avec $\preceq_{\texttt{grevlex}}$.)

Proposition 6.5.2. Soit I un idéal de $k[t_1, \ldots, t_d]$ et $s \leq d$. Alors $Z(I \cap k[t_1, \ldots, t_s])$ est l'adhérence de Zariski dans $\mathbb{A}^s$ de la projection (c'est-à-dire l'image au sens de 5.3 par le morphisme $\mathbb{A}^d \to \mathbb{A}^s$ qui projette sur les s premières coordonnées c'est-à-dire $(x_1, \ldots, x_d) \mapsto (x_1, \ldots, x_d)$) de $Z(I)$.

7 Les courbes

7.1 Corps des fonctions et morphismes vers $\mathbb{P}^1$

Définition 7.1.1. On appelle **courbe (projective lisse)** sur un corps k une variété algébrique projective lisse géométriquement irréductible [8] de dimension 1 sur k. Lorsque la variété n'est pas supposée lisse, on parle de courbe « non nécessairement lisse ».

Les fermés de Zariski d'une courbe qui ne sont pas la courbe tout entière sont de dimension zéro (cf. 5.2.2) donc sont (sur k^{alg}) des réunions finies de points.

Si C est une courbe non nécessairement lisse, on note $k(C)$ le corps des fonctions rationnelles sur C (cf. 5.2.1). Rappelons qu'il s'agit des fonctions régulières sur un ouvert non-vide (=dense) de C, définies sur k (où on identifie deux fonctions quand elles coïncident sur l'intersection des ouverts sur lesquels elles sont données) ; on l'appelle simplement **corps des fonctions** de C. On a $k(C) = \mathrm{Frac}(\mathcal{O}(U))$ pour n'importe quel ouvert affine [9] non-vide (=dense) de C. On appelle évidemment **constantes** les éléments de k vus dans $k(C)$.

On note aussi $k^{\mathrm{alg}}(C)$ le corps des fonctions rationnelles sur $C_{k^{\mathrm{alg}}}$, c'est-à-dire après passage à la clôture algébrique k^{alg} de k. On voit $k(C)$ à l'intérieur de $k^{\mathrm{alg}}(C)$; pour k parfait, le corps $k(C)$ est simplement le corps des éléments de $k^{\mathrm{alg}}(C)$ fixés par le groupe de Galois absolu de k.

Le degré de transcendance de $k(C)$ (ou $k^{\mathrm{alg}}(C)$) sur k (ou k^{alg}, s'agissant de $k^{\mathrm{alg}}(C)$) est 1 : c'est-à-dire qu'il existe des éléments de $k(C)$ n'appartenant pas à k^{alg}, et que deux tels éléments sont toujours algébriques l'un par rapport à l'autre.

Exemple : $\mathbb{P}^1$ sur k est une courbe sur k, son corps des fonctions est $k(\mathbb{P}^1) = k(t)$ où t est un paramètre affine quelconque sur $\mathbb{P}^1$; et on a bien sûr $k^{\mathrm{alg}}(\mathbb{P}^1) = k^{\mathrm{alg}}(t)$.

Définition 7.1.2. Soit X une variété quasiprojective irréductible (non nécessairement lisse), et P un k^{alg}-point de X, on note $\mathcal{O}_{X,P}$ et on appelle **anneau local de X en P** le sous-anneau de $k(X)$ formé des fonctions rationnelles qui sont données sur un ouvert contenant P. Ces fonctions sont dites **régulières en P**.

Grâce au recollement on peut affirmer que, si U est la réunion de tous les ouverts sur lesquels f peut être donnée comme une fonction régulière, on peut effectivement représenter f comme une fonction régulière sur tout U : on appelle U **l'ouvert de régularité** de f (ou parfois l'ouvert de définition).

8. C'est-à-dire qu'elle est irréductible quand on la voit sur la clôture algébrique k^{alg} de k.
9. En fait, on verra que tout ouvert de C différent de C est automatiquement affine.

On peut décrire $\mathcal{O}_{X,P}$ autrement : si U est un ouvert affine contenant P, et $\mathfrak{m}_P$ l'idéal maximal de $\mathcal{O}(U)$ des fonctions s'annulant en P, alors $\mathcal{O}_{X,P}$ est le *localisé* de $\mathcal{O}(U)$ en l'idéal $\mathfrak{m}_P$ (c'est-à-dire inversant toutes les fonctions qui ne sont pas dans $\mathfrak{m}_P$, cf. les remarques suivant 1.3.1). Il s'agit bien d'un anneau local au sens définit en 1.1.

Le fait suivant peut sembler clair, mais il joue un rôle crucial [10] pour expliquer pourquoi la dimension 1 est particulièrement simple :

Proposition 7.1.3. Si C est une courbe non nécessairement lisse, et P un k^{alg}-point *lisse* de C, alors pour tout $f \in k(C)$ non nul on a $f \in \mathcal{O}_{C,P}$ ou bien $f^{-1} \in \mathcal{O}_{C,P}$.

Autrement dit : pour f une fonction rationnelle sur une courbe C et P un point lisse sur C, si f n'est pas régulière en P alors f^{-1} l'est.

Pour C une courbe (lisse), on peut considérer une fonction rationnelle $f \in k(C)$ comme une fonction régulière $U \to \mathbb{A}^1$ sur son ouvert U de régularité (l'ensemble des points où f est régulière). La proposition affirme donc que les ouverts de régularité U de f et U' de f^{-1} recouvrent C. Les morphismes $U \to \mathbb{P}^1$ et $U' \to \mathbb{P}^1$ définis par $P \mapsto (1 : f(P))$ et $P \mapsto (f^{-1}(P) : 1)$ se recollent et définissent donc un morphisme $C \to \mathbb{P}^1$ qu'on veut identifier à f. Réciproquement, tout morphisme $C \to \mathbb{P}^1$ qui n'est pas constamment égal à ∞ (=le point complémentaire de $\mathbb{A}^1$) définit une fonction régulière sur l'ouvert $U = f^{-1}(\mathbb{A}^1)$ de C. On a donc expliqué pourquoi :

Proposition 7.1.4. Si C est une courbe (lisse), les fonctions rationnelles sur C s'identifient (comme expliqué ci-dessus) aux morphismes $C \to \mathbb{P}^1$ non constamment égaux à ∞.

Plus généralement, tout morphisme d'un ouvert non-vide de C vers une variété *projective* Y s'étend à C tout entier.

7.1.5. Une remarque sur Galois. Quand on considère les points d'une variété sur un corps k parfait non algébriquement clos, il est parfois préférable de considérer les k^{alg}-points séparément (qu'on peut appeler *points géométriques* pour insister), parfois il est préférable de considérer ensemble tous les k^{alg}-points qui s'envoie les uns sur les autres par l'action du groupe de Galois absolu $\mathrm{Gal}(k)$ de k, c'est-à-dire les « orbites galoisiennes » de points géométriques, qu'on appelle aussi *points fermés*. Par exemple, pour droite affine $\mathbb{A}^1$ réelle, les $\mathbb{C}$-points i et $-i$ constituent collectivement un point fermé, défini par l'équation $t^2 + 1$. L'intérêt des points fermés est qu'ils correspondent aux idéaux maximaux (sur k) pour

10. Pour voir qu'il n'est pas vrai de façon plus générale, penser à la fonction rationnelle x/y sur $\mathbb{P}^2$, où x, y sont deux des trois coordonnées homogènes : ni elle ni son inverse ne sont régulières au point $x = y = 0$.

une variété affine sur k (exemple : l'idéal des polynômes réels s'annulant en i est le même que celui des polynômes réels s'annulant en $-i$, c'est l'idéal engendré par t^2+1). On appelle *degré* d'un point fermé le nombre de points géométriques qui le constitue : c'est aussi le degré (=la dimension comme k-espace vectoriel) du corps résiduel $\kappa(P) = \mathcal{O}(X)/\mathfrak{m}_P$ si X est affine et $\mathfrak{m}_P$ l'idéal correspondant au point fermé P. Certains résultats s'énoncent mieux en parlant d'un point fermé de degré n, d'autres en parlant de n points géométriques (constituant une orbite galoisienne).

7.2 Valuation d'une fonction en un point

Soit C une courbe (non nécessairement lisse) et P un k^{alg}-point lisse sur C. On appelle $\mathfrak{m}_P$ l'idéal dans $\mathcal{O}_{C,P}$ formé des fonctions s'annulant en P.

Proposition 7.2.1. Avec les notations ci-dessus, il existe une unique fonction $\mathrm{ord}_P \colon k(C) \to \mathbb{Z} \cup \{+\infty\}$ vérifiant :

- si $\mathrm{ord}_P(f) = +\infty$ ssi $f = 0$, et $\mathrm{ord}_P(c) = 0$ pour tout $c \in k^\times$,
- si $f, g \in k(C)$, on a $\mathrm{ord}_P(f+g) \geq \min(\mathrm{ord}_P(f), \mathrm{ord}_P(g))$ (note : ceci implique qu'il y a égalité si $\mathrm{ord}_P(f) \neq \mathrm{ord}_P(g)$),
- si $f, g \in k(C)$, on a $\mathrm{ord}_P(fg) = \mathrm{ord}_P(f) + \mathrm{ord}_P(g)$,
- on a $\mathrm{ord}_P(f) \geq 0$ ssi $f \in \mathcal{O}_{C,P}$ (i.e., f est régulière en P), et $\mathrm{ord}_P(f) > 0$ ssi $f \in \mathfrak{m}_P$ (i.e., f s'annule en P),
- il existe des f tels que $\mathrm{ord}_P(f) = 1$.

Cette fonction s'appelle la **valuation en** P ou l'**ordre (du zéro) en** P. Lorsque $\mathrm{ord}_P(f) = v > 0$, on dit que f a un zéro d'ordre v en P ; lorsque $\mathrm{ord}_P(f) = (-v) < 0$, on dit que f a un pôle d'ordre v en P ; lorsque $\mathrm{ord}_P(f) = 0$, on dit que f est inversible en P (cela signifie bien que f est inversible dans $\mathcal{O}_{C,P}$) ; lorsque $\mathrm{ord}_P(f) = 1$, on dit que f est une **uniformisante** en P (il n'est pas difficile de voir que cela signifie que f engendre l'idéal $\mathfrak{m}_P$).

Exemple : Si on voit $k(t)$ comme $k(\mathbb{P}^1)$, alors

- pour $P \in \mathbb{A}^1(k) = k$, la valuation en P est bien l'ordre d'annulation en P de la fraction rationnelle f (en particulier, si f est un polynôme, $\mathrm{ord}_P(f)$ est la multiplicité de $(t-P)$ dans la décomposition en facteurs irréductibles de f ; et si $P = 0$, c'est ce qu'on appelle souvent, sans autre précision, la valuation d'un polynôme) ;
- pour $P = \infty$, la valuation en ∞ d'un polynôme est l'opposé de son degré, et la valuatin en ∞ d'une fraction rationnelle f est le degré de son dénominateur moins le degré de son numérateur ;
- pour $P \in \mathbb{A}^1(k^{alg}) = k^{\mathrm{alg}}$, la valuation en P d'un polynôme f est la multiplicité de μ_P dans la décomposition en facteurs irréductibles de celui-ci, où

μ_P est le polynôme minimal de P (par exemple, sur les réels, $\mathrm{ord}_i(t^2+1) = 1$), et pour une fraction rationnelle on peut bien sûr le calculer comme l'ordre du numérateur moins celui du dénominateur.

Remarquons que $\mathrm{ord}_P(f)$ est le même que f soit considéré comme vivant dans $k(C)$ ou dans $k^{\mathrm{alg}}(C)$ (à cause de l'unicité affirmée pour la fonction ord_P). Par ailleurs, pour $f \in k(C)$, on a $\mathrm{ord}_P(f) = \mathrm{ord}_{\sigma(P)}(f)$ pour tout $\sigma \in \mathrm{Gal}(k)$ (le groupe de Galois absolu de k), autrement dit, $\mathrm{ord}_P(f)$ ne dépend que de l'orbite de P par $\mathrm{Gal}(k)$ (c'est-à-dire, du point fermé défini par P).

Proposition 7.2.2. Soit C une courbe (lisse) sur un corps k. Alors toute fonction $k(C) \to \mathbb{Z} \cup \{+\infty\}$ vérifiant les trois premières et la dernière des propriétés énumérées pour ord_P en 7.2.1 est de la forme ord_P pour un certain $P \in C(k^{\mathrm{alg}})$.

Les ord_P sont distinctes lorsque les points P ne sont pas conjugués par Galois (cf. ci-dessus) : on va voir un résultat plus précis affirmant qu'elles sont, en fait, aussi indépendantes que possible (7.2.4 ci-dessous).

Proposition 7.2.3. Soit C une courbe (lisse) sur un corps k :

— Pour tout $f \in k(C)$, il n'y a qu'un nombre fini de $P \in C(k^{\mathrm{alg}})$ tels que $\mathrm{ord}_P(f) \neq 0$.

— Si $\mathrm{ord}_P(f) \geq 0$ pour tout $P \in C(k^{\mathrm{alg}})$, alors $f \in k$ (la fonction est constante).

Démonstration. La première affirmation vient de ce que tout fermé de Zariski d'une courbe est fini. La seconde découle de ce que toute fonction régulière (ce qu'est un f comme annoncé) sur une variété projective connexe est constante (cf. 5.1.1). ☺

Proposition 7.2.4 (lemme d'approximation)**.** Soit C une courbe sur un corps k et U un ouvert affine [11] de C. Soient $Q_1, \ldots, Q_s$ des points dans U dont aucun n'est image d'un autre sous l'action de Galois (=dont les orbites sous $\mathrm{Gal}(k)$ sont deux à deux disjointes, =dont les idéaux maximaux $\mathfrak{m}_{Q_i}$ sont deux à deux distincts, =définissant des points fermés deux à deux distincts), et $f_1, \ldots, f_s \in k(C)$ et $v_1, \ldots, v_s \in \mathbb{Z}$. Alors il existe $f \in k(C)$ telle que

$$\begin{aligned} \mathrm{ord}_{Q_i}(f - f_i) &\geq v_i \quad \text{pour tout } i \\ \mathrm{ord}_P(f) &\geq 0 \quad \text{pour tout } P \in U \setminus \{\sigma(Q_i)\} \end{aligned}$$

Moralité : On peut toujours trouver une fonction f qui approche les fonctions f_i spécifiées à l'ordre v_i spécifié aux points Q_i spécifiés, et qui soit régulière à tout point de U sauf évidemment ceux pour lesquels la condition imposée demande qu'ils ne le soient pas.

11. Cf. note 9.

Remarque : Ce résultat recouvre l'existence des polynômes interpolateurs de Lagrange (pour $C = \mathbb{P}^1$ et $U = \mathbb{A}^1$, les f_i des polynômes ayant les développements de Taylor souhaités aux ordres v_i, le résultat montre qu'il existe un polynôme f ayant les développements spécifiés aux ordres spécifiés).

Idée de démonstration. Pour $Q \in U$, si $\mathfrak{m}_Q$ désigne l'idéal des fonctions de $\mathcal{O}(U)$ s'annulant en Q, i.e., telles que $\mathrm{ord}_Q(h) \geq 1$, le point clé est que $\mathfrak{m}_Q \neq \mathfrak{m}_{Q'}$ si Q et Q' ne sont pas conjugués par Galois, donc il existe une fonction $h \in \mathcal{O}(U)$ telle que $\mathrm{ord}_Q(h) \geq 1$ et $\mathrm{ord}_{Q'}(h) = 0$, et, quitte à diviser par une constante, autant supposer $h(Q') = 1$, et une autre h' telle que $h'(Q) = 1$ et $\mathrm{ord}_{Q'}(h') \geq 1$. Quitte à multiplier de telles fonctions entre elles et à les elever à des puissances assez grandes, on peut obtenir des h_i telles que $h_i(Q_i) = 1$ et $\mathrm{ord}_{Q_j}(h_i) \geq \min(1, v_i)$ si $j \neq i$. Lorsque les f_i sont dans $\mathcal{O}(U)$, poser $f = \sum_i f_i h_i$ convient. Sinon, on met les f_i sur un même dénominateur et en cherchant h comme une fraction sur le dénominateur en question on se ramène à un problème d'approximation sur le numérateur. ☺

Proposition 7.2.5. Soit P un k^{alg}-point lisse d'une courbe C non nécessairement lisse sur un corps k, et pour $v \geq 0$ soit $\mathfrak{m}_P^v = \{f \in k(C) : \mathrm{ord}_P(f) \geq v\}$ (idéal de $\mathcal{O}_{C,P}$). Alors $\mathcal{O}_{C,P}/\mathfrak{m}_P^v$ est un espace vectoriel de dimension v sur le corps $\kappa(P) := \mathcal{O}_{C,P}/\mathfrak{m}_P$, donc dv sur k, où d est le degré de P, c'est-à-dire (pour k parfait) le nombre de conjugués de P sous l'action de Galois.

Démonstration. Il existe une uniformisante t de C en P : il n'est pas difficile de voir que $1, t, t^2, \ldots, t^{v-1}$ forment une base de $\mathcal{O}_{C,P}/\mathfrak{m}_P^v$ sur $\kappa(P)$ (cf. 7.1.5 pour la dimension de $\kappa(P)$ sur k). ☺

7.3 Morphismes entre courbes

Proposition 7.3.1. Tout morphisme entre courbes non nécessairement lisses est soit constant ou surjectif.

Démonstration. Soit $h\colon C' \to C$ un tel morphisme. Puisque C' est projective, l'image de h est un fermé dans C (cf. 5.3.1). Si c'est C, le morphisme est surjectif. Sinon, c'est un ensemble fini, et comme C' est connexe, il est réduit à un point, donc h est constant. ☺

Si $h\colon C' \to C$ est un morphisme non constant de courbes sur k, à tout $f \in k(C)$, vu comme un morphisme $C \to \mathbb{P}^1$ (non constamment égal à ∞), on peut associer $h^*(f) := h \circ f\colon C' \to \mathbb{P}^1$ vu comme un élément de $k(C')$ (car il est n'est pas constant égal à ∞). (Si on préfère, pour U ouvert affine de C, le morphisme d'algèbres $h^*\colon \mathcal{O}(U) \to \mathcal{O}(h^{-1}(U))$ donne un $h^*\colon k(C) \to k(C')$ entre les corps des fractions ; ceci fonctionne même si C, C' ne sont pas supposées lisses.) Il

s'agit d'un morphisme de k-algèbres qui sont des corps, donc automatiquement injectif : c'est-à-dire que h^* plonge $k(C)$ comme un sous-corps de $k(C')$ (en commutant à l'action du groupe de Galois, et en particulier en préservant k). Avec ce plongement, $k(C')$ est une extension *algébrique* de $k(C)$ (car tous deux ont le même degré de transcendance, 1, sur k), et $k(C')$ est engendré en tant que corps, sur k donc sur $k(C)$, par un nombre fini d'éléments : ceci montre que $k(C')$ est une *extension finie* de $k(C)$ (c'est-à-dire, de dimension finie comme $k(C)$-espace vectoriel), et son degré (=sa dimension comme $k(C)$-espace vectoriel) s'appelle le **degré** de h, noté $\deg h$. Lorsque h est un morphisme constant, on pose $\deg h = 0$.

Exemple : Si $h \in k[t]$, on peut voir h comme un morphisme $\mathbb{P}^1 \to \mathbb{P}^1$ (par $(t_0 : t_1) \mapsto (t_0^{\deg h} : t_0^{\deg h}\, h(t_1/t_0))$, cf. 3.3 ; ou, de façon équivalente, en considérant h comme un élément de $k(t) = k(\mathbb{P}^1)$ qui définit donc un morphisme $\mathbb{P}^1 \to \mathbb{P}^1$). L'inclusion h^* est celle qui considère $k(u)$ pour $u = h(t)$ comme un sous-corps de $k(t)$. Manifestement, le polynôme minimal de t sur $k(u)$ est justement $h(x) - u$ (écrit en l'indéterminée x), qui est de degré $\deg h$, donc le degré de h en tant que polynôme ou en tant que morphisme est le même !

Fonctorialité : Si $C'' \xrightarrow{h'} C' \xrightarrow{h} C$ sont deux morphismes entre courbes, on a $(h' \circ h)^* = h^* \circ h'^*$, c'est-à-dire que $k(C)$ se voit à l'intérieur de $k(C')$ quand celui-ci se voit à l'intérieur de $k(C'')$. Grâce à la composition des degrés dans les extensions de corps, on a $\deg(h' \circ h) = \deg(h') \cdot \deg(h)$.

Proposition 7.3.2. Si C, C' sont deux courbes sur k, où C peut ne pas être lisse (mais C' est tenue de l'être), et si $\iota \colon k(C) \to k(C')$ est une inclusion fixant k du corps $k(C)$ dans $k(C')$, alors il existe un unique morphisme $h \colon C' \to C$ de courbes sur k tel que $\iota = h^*$.

Esquisse de démonstration. Si $C \subseteq \mathbb{P}^d$, on peut considérer les rapports $t_1/t_0, \ldots, t_d/t_0$ de coordonnées homogènes sur $\mathbb{P}^d$ comme des éléments de $k(C)$. Leurs images par ι dans $k(C')$ définissent un morphisme d'un ouvert non vide de C' vers $\mathbb{P}^d$, donc de tout C' vers $\mathbb{P}^d$ (cf. 7.1.4), et comme ces fonctions vérifient les équations de C dans $\mathbb{P}^d$, on a un morphisme $C' \xrightarrow{h} C$, qui vérifie $h^* = \iota$. De plus, une fois C plongé dans $\mathbb{P}^d$ comme on l'a fait, c'était le seul morphisme possible, donc on a bien l'unicité. ☺

Corollaire 7.3.3. Si C, C' sont deux courbes (lisses) sur k et $h \colon C' \to C$ un morphisme de degré 1, alors h est un isomorphisme.

Démonstration. Dire que h est un morphisme de degré 1 signifie que h^* est un isomorphisme de $k(C)$ avec $k(C')$. Son isomorphisme réciproque peut lui-même s'écrire sous la forme g^* d'après la proposition qui précède, et les relations de fonctorialité $(h \circ g)^* = g^* \circ h^*$ et $(g \circ h)^* = h^* \circ g^*$ ainsi que l'unicité du morphisme dans la proposition montrent que $h \circ g = \mathrm{id}_{C'}$ et $g \circ h = \mathrm{id}_C$. ☺

Revenons brièvement sur le corps des fonctions d'une courbe.

On sait que $k(C)$ est engendré (en tant que corps) [12] par un nombre fini d'éléments au-dessus de k (en effet, si U est un ouvert affine non-vide de C, alors $\mathcal{O}(U)$ est une k-algèbre de type fini, et si $x_1, \ldots, x_r$ en sont des générateurs, ils engendrent aussi $k(C) = \mathrm{Frac}(\mathcal{O}(U))$ en tant que corps sur k). D'autre part, remarquons que $k^{\mathrm{alg}} \cap k(C) = k$ (ce qui est clair si on a décrit $k(C)$ comme les éléments de $k^{\mathrm{alg}}(C)$ fixes par Galois), c'est-à-dire que tout élément de $k(C)$ algébrique sur k est en fait dans $k(C)$. Ces remarques sont pertinentes car :

Proposition 7.3.4. Soit K un corps contenant k, de degré de transcendance 1 dessus, engendré en tant que corps par un nombre fini d'éléments au-dessus de k (ou, de façon équivalente, K est de degré *fini* sur $k(t)$ où $t \in K$ est transcendant sur k), et tel que k soit algébriquement fermé dans K. Alors K est le corps des fonctions $k(C)$ d'une certaine courbe (lisse) C sur k.

Le corollaire suivant permet d'oublier les courbes non lisses :

Corollaire 7.3.5. Soit C une courbe non nécessairement lisse. Alors il existe un morphisme $\tilde{C} \to C$ depuis une courbe lisse $\tilde{C}$ vers C, unique à isomorphisme unique près de $\tilde{C}$ au-dessus [13] de C, qui soit de degré 1, c'est-à-dire que ν^* identifie $k(C)$ à $k(\tilde{C})$. La courbe $\tilde{C}$ s'appelle la **normalisation** de C.

Démonstration. La proposition garantit qu'il existe une courbe lisse $\tilde{C}$ de corps des fonctions $k(C)$. Le morphisme identité $k(C) \to k(\tilde{C})$ donne alors d'après 7.3.2 le morphisme $\nu\colon \tilde{C} \to C$ désiré. L'unicité est analogue à 7.3.3. ☺

Corollaire 7.3.6. Soit C une courbe (lisse) sur un corps k. Si K est un sous-corps de $k(C)$ contenant k et tel que $k(C)$ soit fini sur K (c'est-à-dire, de dimension finie comme K-espace vectoriel), alors il existe une courbe C_0 et un morphisme $h\colon C \to C_0$, unique à isomorphisme près de C_0 au-dessous de C, tel que h^* plonge $k(C_0)$ comme le sous-corps K de $k(C)$.

Démonstration. Le corps K est de degré de transcendance 1 sur k car $k(C)$ est algébrique sur K ; et k est algébriquement fermé dans K. Le point non-évident est que K est engendré par un nombre fini d'éléments sur k : mais K contient un élément t transcendant sur k, et $k(C)$, donc K, est de degré fini sur $k(t)$. Ainsi K peut bien s'écrire comme $k(C_0)$ pour une certaine courbe C_0, et l'inclusion $K = k(C_0) \to k(C)$ fournit un morphisme $C \to C_0$ d'après 7.3.2. De nouveau, l'unicité découle aussi de 7.3.2 de manière analogue à 7.3.3. ☺

12. Ceci signifie qu'il existe $x_1, \ldots, x_r \in k(C)$ tels que tout sous-corps de $k(C)$ contenant k et $x_1, \ldots, x_r$ soit $k(C)$ tout entier.

13. Ceci signifie que si $\tilde{C} \xrightarrow{\nu} C$ et $\tilde{C}' \xrightarrow{\nu'} C$ sont deux morphismes comme expliqué, alors il existe un unique isomorphisme $\tilde{C}' \xrightarrow{h} \tilde{C}$ tel que $\nu' = h \circ \nu$.

7.4 Ramification d'un morphisme

Proposition 7.4.1. Si $h\colon C' \to C$ est un morphisme non constant entre courbes sur k, pour tout point P de C' (sur k^{alg}), il existe un (unique) entier $e_P \geq 1$ tel que $\operatorname{ord}_P h^*(f) = e_P \operatorname{ord}_{h(P)} f$ pour tout $f \in k(C)$. On appelle e_P l'**indice de ramification** de h en P.

Remarque 7.4.2. Si $h \in k(C)$ n'est pas constant, on peut considérer h comme un morphisme $C \to \mathbb{P}^1$ correspondant à l'inclusion $k(t) \cong k(h) \subseteq k(C)$. En voyant h comme $h^*(t)$, on voit que $e_P = \operatorname{ord}_P h$ pour tout P tel que $h(P) = 0$. Si P est tel que $h(P) = \infty$ alors $e_P = -\operatorname{ord}_P h$. Enfin, si $h(P)$ n'est ni 0 ni ∞ alors $e_P = \operatorname{ord}_P(h - h(P))$.

Proposition 7.4.3. Pour $h\colon C' \to C$ un morphisme non constant entre courbes sur k et P un point de C' (sur k^{alg}), l'indice de ramification e_P de h en P vaut 1 ssi h est lisse en P (c'est-à-dire que $dh_P\colon T_P C' \to T_{h(P)} C$ est un isomorphisme [14] de k^{alg}-espaces vectoriels de dimension 1, cf. 5.4 *in fine*).

Proposition 7.4.4. Soit $h\colon C' \to C$ un morphisme non constant entre courbes sur k. Pour tout point Q de C, on a

$$\sum_{h(P)=Q} e_P = \deg h$$

où la somme est prise sur tous les points P de C' (sur k^{alg}) tels que $h(P) = Q$.

Idée-clé de démonstration. Soit U un ouvert affine de C contenant Q, et $U' = h^{-1}(U)$ son image réciproque dans C' (qui est également affine) ; on considère la k-algèbre $\mathcal{O}(U')/h^*\mathfrak{m}_Q\mathcal{O}(U')$ des fonctions sur U' modulo l'idéal $h^*\mathfrak{m}_Q$ engendré par les $h \circ f$ avec $f \in \mathcal{O}(U)$: on peut montrer que cette k-algèbre $\mathcal{O}(U')/h^*\mathfrak{m}_Q\mathcal{O}(U')$ est un k-espace vectoriel de dimension $\deg h$. Mais le lemme d'approximation 7.2.4 permet de montrer que cette algèbre est le produit d'algèbres $\mathcal{O}(U)/\mathfrak{m}_P\mathcal{O}(U)$ où $\mathfrak{m}_P$ parcourt les idéaux maximaux tels que $h(P) = Q$ (un seul par orbite sous Galois), et la dimension de ce produit est $\sum_{h(P)=Q} e_P$ d'après 7.2.5. ☺

Corollaire 7.4.5. Soit C une courbe sur un corps k, et soit $f \in k(C)$ non constant. Alors

$$\sum_P \operatorname{ord}_P(f) = 0$$

14. La définition de la lissité demande seulement que dh_P soit surjective, mais comme les espaces au départ et à l'arrivée ont même dimension, c'est alors un isomorphisme.

où la somme est prise sur tous les points P de C. Plus précisément,

$$\begin{array}{c}\sum_{P\,:\,\mathrm{ord}_P(f)>0}\mathrm{ord}_P(f)=\deg f\\ \sum_{P\,:\,\mathrm{ord}_P(f)<0}\mathrm{ord}_P(f)=-\deg f\end{array}$$

Démonstration. On a vu en 7.4.2 que si f est vu comme un morphisme $C\to\mathbb{P}^1$, alors son indice de ramification en un point P de C tel que $f(P)=0$ est $e_P=\mathrm{ord}_P(f)$, et en un point P tel que $f(P)=\infty$ est $e_P=-\mathrm{ord}_P(f)$. La proposition précédente permet de conclure. ☺

7.5 Diviseurs sur une courbe

Définition 7.5.1. Soit C une courbe (lisse) sur un corps parfait k. On appelle **diviseur** sur C une combinaison linéaire formelle (finie) $\sum n_P(P)$, à coefficients dans $\mathbb{Z}$, de k^{alg}-points de C, qui soit stable par l'action du groupe de Galois absolu $\mathrm{Gal}(k)$ (ou, si on préfère, une combinaison linéaire formelle de « points fermés » de C, chacun étant vu comme la somme d'une orbite galoisienne).

On appelle **degré** du diviseur $\sum_{P\in C}n_P\cdot(P)$ l'entier $\sum_{P\in C}n_P$.

Si $f\in k(C)$ n'est pas constant, on peut notamment considérer les diviseurs

$$\begin{array}{c}f^*((0)):=\sum_{P\,:\,\mathrm{ord}_P(f)>0}\mathrm{ord}_P(f)\,(P)\\ f^*((\infty)):=\sum_{P\,:\,\mathrm{ord}_P(f)<0}-\mathrm{ord}_P(f)\,(P)\\ f^*((0)-(\infty))=\mathrm{div}(f):=\sum_{P\in C}\mathrm{ord}_P(f)\,(P)\end{array}$$

appelés respectivement **diviseur des zéros**, **diviseur des pôles** et **diviseur principal** définis par f (différence des deux premiers). Le contenu du corollaire 7.4.5 est que ces diviseurs ont degré respectivement $\deg f$, $\deg f$ et 0.

Plus généralement, si $h\colon C'\to C$ est un morphisme non constant entre courbes, et $D=\sum_{P\in C}n_P\cdot(P)$ un diviseur sur C, on définit $h^*(D)=\sum_{Q\in C'}n_{h(Q)}e_Q\cdot(Q)$ qu'on appelle **image réciproque** (ou **tiré en arrière**) de D par h : il est clair que le diviseur des zéros $f^*((0))$ défini ci-dessus est bien le tiré en arrière du diviseur (0) sur $\mathbb{P}^1$ par f vu comme morphisme $C\to\mathbb{P}^1$. Il est évident que le tiré en arrière d'un diviseur principal est encore principal (en fait, $h^*(\mathrm{div}(f))=\mathrm{div}(f\circ h)$). On peut aussi définir l'**image directe** (ou **poussé en avant**) par h d'un diviseur $D'=\sum_{Q\in C'}n_Q\cdot(Q)$ sur C' comme $h_*(D')=\sum_{Q\in C'}n_Q\cdot(h(Q))$: il est aussi vrai, mais un chouïa moins évident, que l'image directe d'un diviseur principal est un diviseur principal.

Proposition 7.5.2. Si $h\colon C'\to C$ est un morphisme non constant entre courbes, pour tout diviseur D sur C on a

$$h_*h^*D=(\deg h)\,D$$

Démonstration. C'est une conséquence immédiate de 7.4.4 (et du fait qu'un morphisme non-constants entre courbes est surjectif !, cf. 7.3.1). ☺

Définition 7.5.3. On appelle **principal** un diviseur (de degré zéro) de la forme $\mathrm{div}(f) := \sum_{P \in C} \mathrm{ord}_P(f) \cdot (P)$ pour une certaine fonction $f \in k(C)$ non constante. Les diviseurs principaux forment un sous-groupe du groupe des diviseurs (car $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$, cf. 7.2.1) : on dit que deux divieurs sont **linéairement équivalents** (notation : $D \sim D'$) lorsque leur différence est un diviseur principal. Le groupe des diviseurs (resp. diviseurs de degré 0) modulo les diviseurs principaux (=modulo équivalence linéaire) s'appelle **groupe de Picard** (resp. groupe de Picard de degré zéro) de la courbe C, noté $\mathrm{Pic}(C)$ (resp. $\mathrm{Pic}^0(C)$).

Exemple : Sur $\mathbb{P}^1$, pour tout diviseur $\sum n_P \cdot (P)$ de degré zéro, on peut trouver une fraction rationnelle $\prod (t - P)^{n_P}$ qui a les ordres n_P à ceux des points P qui sont dans $\mathbb{A}^1$, et le degré à l'infini sera automatiquement le bon puisque $\sum n_P = 0$. Ceci montre que *tout diviseur de degré zéro sur* $\mathbb{P}^1$ *est principal*, donc que $\mathrm{Pic}^0(\mathbb{P}^1) = 0$, et $\mathrm{Pic}(\mathbb{P}^1) = \mathbb{Z}$.

On a un morphisme de degré $\deg\colon \mathrm{Pic}(C) \to \mathbb{Z}$, dont le noyau est $\mathrm{Pic}^0(C)$. Si la courbe C vérifie $C(k) \neq \varnothing$, c'est-à-dire qu'il existe P un k-point sur C, alors tout diviseur peut s'écrire comme somme de $n(P)$ et d'un diviseur de degré zéro, et il est facile de voir que $\mathrm{Pic}(C) = \mathrm{Pic}^0(C) \oplus \mathbb{Z}$ (où $\mathbb{Z}$ désigne $\mathbb{Z} \cdot (P)$, le groupe des diviseurs de la forme $n \cdot (P)$).

Attention : Pour une fois, le slogan « rationnel = fixe par Galois » n'est pas vérifié : quand C est une courbe sur un corps k parfait non algébriquement clos, il faut bien distinguer le groupe de Picard rationnel $\mathrm{Pic}\, C$ de C, c'est-à-dire les diviseurs stables par Galois modulos ceux de la forme $\mathrm{div}(f)$ avec $f \in k(C)$, et le groupe de Picard fixé par Galois noté $(\mathrm{Pic}\, C_{k^{\mathrm{alg}}})^{\mathrm{Gal}(k)}$, c'est-à-dire les classes des diviseurs D tels que $\sigma(D)$ soit linéairement équivalent à D (sur k^{alg}) pour tout $\sigma \in \mathrm{Gal}(k)$. (Un exemple de situation où il y a une différence est celui de la conique sans points $\{t_0^2 + t_1^2 + t_2^2 = 0\} \subset \mathbb{P}^2_{\mathbb{R}}$: les diviseurs rationnels sont tous de degré pair, donc $\mathrm{Pic}\, C$ est le sous-groupe $2\mathbb{Z}$ si on identifie $\mathrm{Pic}\, C_{\mathbb{C}}$ à $\mathbb{Z}$ via le degré, sur lequel $\Gamma_{\mathbb{R}}$ opère trivialement.) Certains auteurs appellent (à tort) $\mathrm{Pic}\, C$ ce deuxième groupe (d'autres encore appellent $\mathrm{Pic}\, C$ tout le groupe de Picard géométrique $\mathrm{Pic}\, C_{k^{\mathrm{alg}}}$) : il faut donc faire attention à qui utilise quoi. Cependant, cette distinction ne doit pas nous inquiéter, parce qu'on peut montrer que $\mathrm{Pic}\, C$ coïncide bien avec le groupe $(\mathrm{Pic}\, C_{k^{\mathrm{alg}}})^{\mathrm{Gal}(k)}$ des invariants sous Galois lorsque k est un corps fini *ou bien* que $C(k) \neq \varnothing$ (=la courbe a un point rationnel).

7.6 Différentielles

Proposition 7.6.1. Soit C une courbe (lisse) sur un corps k. Il existe un $k(C)$-espace vectoriel de dimension 1, noté [15] Ω^1_C et appelé **espace des (formes) différentielles méromorphes** sur C, et une application k-linéaire $d\colon k(C) \to \Omega^1_C$, vérifiant les conditions suivantes :

— on a $dc = 0$ pour $c \in k$,

— on a $d(fg) = f\,dg + g\,df$ pour $f, g \in k(C)$,

— si $t \in k(C)$ vérifie $\mathrm{ord}_P(t) = 1$ en au moins un point alors $dt \neq 0$,

et ces conditions caractérisent à isomorphisme près Ω^1_C muni de l'application $d\colon k(C) \to \Omega^1_C$.

La moralité est que $\frac{df}{dt}$ a un sens, comme élément de $k(C)$, dès que f et t sont deux éléments de $k(C)$ et que t est une uniformisante en au moins un point ou simplement [16] que $dt \neq 0$.

Remarque : On peut relier $\frac{df}{dt} \in k(C)$ à ce qui a été fait en 5.4 de la façon suivante : si Q est un point de C tel que t et f soient régulières en Q, on peut voir t et f comme deux morphismes $U \to \mathbb{A}^1$ pour un certain voisinage (affine, disons) U de Q, on a des applications linéaires $dt_Q\colon T_QC \to k^{\mathrm{alg}}$ et $df_Q\colon T_QC \to k^{\mathrm{alg}}$, et la valeur de $\frac{df}{dt}$ en Q est le rapport entre ces deux applications linéaires (ceci a bien un sens car ce sont des applications entre espaces de dimension 1).

Proposition 7.6.2. Soit C une courbe (lisse) sur un corps k, P un point de C et t une uniformisante en P (i.e., $\mathrm{ord}_P(t) = 1$). Pour $f \in k(C)$, on a

— $\mathrm{ord}_P(df/dt) = \mathrm{ord}_P(f) - 1$ si $\mathrm{ord}_P(f) \neq 0$ dans k (i.e., $\mathrm{ord}_P(f)$ n'est pas multiple de la caractéristique), et

— $\mathrm{ord}_P(df/dt) \geq 0$ si $\mathrm{ord}_P(f) \geq 0$.

(Ces propriétés découlent des propriétés correspondantes des polynômes.)

Définition 7.6.3. Si C est une courbe (lisse) sur un corps k, P un point de C (sur k^{alg}) et $\omega \in \Omega^1_C$, on définit

$$\mathrm{ord}_P(\omega) = \mathrm{ord}_P(\omega/dt)$$

où $t \in k(C)$ est tel que $\mathrm{ord}_P(t) = 1$ (=est une uniformisante en P). Cette définition ne dépend pas du choix de t.

Si $\omega \neq 0$, le diviseur $\mathrm{div}(\omega) := \sum_P \mathrm{ord}_P(\omega) \cdot (P)$ s'appelle **diviseur canonique** de la forme différentielle ω.

15. Notation abusive, en fait. Une bonne notation serait $\Omega^1_{C/k} \otimes_{\mathcal{O}_C} k(C)$, mais c'est un peu encombrant.

16. Si k est de caractéristique zéro, cette condition est réalisée dès que t n'est pas constant.

La définition de $\mathrm{ord}_P(\omega)$ ne dépend pas du choix de t, car si $t' = ut$ où $\mathrm{ord}_P(u) = 0$, alors $dt'/dt = u + t\,(du/dt)$, et $\mathrm{ord}_P(du/dt) \geq 0$ d'après 7.6.2 donc $\mathrm{ord}_P(t\,(du/dt)) \geq 1$, ce qui assure $\mathrm{ord}_P(dt'/dt) = 0$, et donc $\mathrm{ord}_P(\omega/dt') = \mathrm{ord}_P(\omega/dt)$.

La définition qu'on vient de faire permet de reformuler la proposition 7.6.2 en :

Proposition 7.6.4. Soit C une courbe (lisse) sur un corps k, et P un point de C. Pour $f \in k(C)$, on a

— $\mathrm{ord}_P(df) = \mathrm{ord}_P(f) - 1$ si $\mathrm{ord}_P(f) \neq 0$ dans k (i.e., $\mathrm{ord}_P(f)$ n'est pas multiple de la caractéristique), et

— $\mathrm{ord}_P(df) \geq 0$ si $\mathrm{ord}_P(f) \geq 0$.

Exemple : Soit t la coordonnée affine sur $\mathbb{A}^1$, vue comme élément de $k(\mathbb{P}^1) = k(t)$. Alors dt a pour ordre 0 en tout $P \neq \infty$ (en $P = 0$ c'est clair d'après la proposition qui précède, et en tout autre $P \in \mathbb{A}^1$ on peut remarquer que $dt = d(t - P)$ d'après les règles de calcul, donc de même dt est d'ordre 0) ; en ∞, en revanche, son ordre est -2 puisque l'ordre de t est -1. On a donc $\mathrm{div}(dt) = -2(\infty)$.

La classe de $\mathrm{div}(\omega)$ dans $\mathrm{Pic}(C)$ ne dépend pas du choix de $\omega \neq 0$, puisque visiblement $\mathrm{div}(f\omega) = \mathrm{div}(f) + \mathrm{div}(\omega)$. Cette classe s'appelle la **classe canonique** dans $\mathrm{Pic}(C)$ (très souvent notée K). On vient par exemple de voir que la classe canonique de $\mathbb{P}^1$ est de degré -2.

Exemple : Soit C la courbe d'équation $y^2 = h(x)$ où $h(t) \in k[t]$ est de degré 3 (c'est-à-dire, C la complétée projective de cette courbe affine, complétée d'équation $ZY^2 = Z^3 h(X/Z)$ si X, Y, Z sont les coordonnées homogènes avec $y = Y/Z$ et $x = X/Z$). Soit $h(t) = (t - \lambda_1)(t - \lambda_2)(t - \lambda_3)$ la factorisation de h sur k^{alg}. Outre les points affines, la courbe C a un unique point à l'infini noté O (en coordonnées homogènes, $X = Z = 0$). Le diviseur de la fonction y sur C est $(P_1) + (P_2) + (P_3) - 3(O)$ où P_i est le point de coordonnées affines $(\lambda_i, 0)$ (ce sont les trois points où y s'annule, alors que O est le point où y a un pôle triple). Le diviseur de $x - \lambda_i$ est $2(P_i) - 2(O)$, d'où il résulte que dx a un ordre 1 en chaque P_i et -3 en O, et 0 partout ailleurs. Autrement dit, le diviseur de dx est le même que celui de y, ou, si on veut, la différentielle $\omega := dx/y$ a un ordre 0 partout. Ceci signifie que la classe canonique K sur C est *nulle*.

7.7 Le théorème de Riemann-Roch

Définition 7.7.1. Un diviseur D sur une courbe C est dit **effectif**, noté $D \geq 0$, lorsque D est combinaison de points à coefficients positifs : $D = \sum n_P \cdot (P)$ avec $n_P \geq 0$ pour tout P.

Si $D = \sum n_P \cdot (P)$ est un diviseur (non nécessairement effectif) sur une courbe C, on note $\mathscr{L}(D)$ ou parfois $\mathcal{O}(D)$ le k-espace vectoriel $\{f \in k(C) : \mathrm{div}(f) + D \geq 0\}$ des fonctions rationnelles sur C vérifiant $\mathrm{ord}_P(f) \geq -n_P$ pour tout point P de C. (S'il faut lui donner un nom, c'est « l'(ensemble des sections globales du) faisceau associé à D ».)

Remarque 7.7.2. Si D et D' sont linéairement équivalents, alors $\mathscr{L}(D) \cong \mathscr{L}(D')$ comme k-espaces vectoriels. En effet, si $D = D' + \mathrm{div}(g)$ et $f \in \mathscr{L}(D)$ alors $\mathrm{div}(fg) + D' = \mathrm{div}(f) + D \geq 0$ donc $fg \in \mathscr{L}(D')$ et réciproquement. On peut donc considérer que $\mathscr{L}(D)$ ne dépend que de la classe de D dans $\mathrm{Pic}(C)$.

D'autre part, l'ensemble $\{\omega \in \Omega^1_C : \mathrm{div}(\omega) \geq 0\}$ (des différentielles « holomorphes ») peut être identifié à $\mathscr{L}(K)$ pour les mêmes raisons. (Et plus généralement, $\mathscr{L}(K - D)$ peut être identifié à $\{\omega \in \Omega^1_C : \mathrm{div}(\omega) - D \geq 0\}$.)

Proposition 7.7.3. Le k-espace vectoriel $\mathscr{L}(D)$ est de dimension finie.

On note $l(D)$ cette dimension. Notons par exemple que $l(0) = 1$ (le diviseur nul, à ne pas confondre avec le diviseur (0) sur $\mathbb{P}^1$!), puisque $\mathscr{L}(0) = \mathcal{O}(C) = k$ (les seules fonctions régulières partout sont les constantes, d'après 7.2.3).

Proposition 7.7.4. — Si $\deg D < 0$ alors $l(D) = 0$.
— Si $\deg D = 0$ et $l(D) \neq 0$ alors $l(D) = 1$ et $D \sim 0$.

Démonstration. Dire que $l(D) \neq 0$ signifie que pour un certain f on a $D' := \mathrm{div}(f) + D \geq 0$. Or le degré de $\mathrm{div}(f)$ est nul (et le degré d'un diviseur effectif D' est évidemment positif), donc le degré de D est ≥ 0. De plus, si le degré de D (donc de D') est nul, cela signifie que $\mathrm{div}(f) + D = 0$, c'est-à-dire $D \sim 0$, qui entraîne $l(D) = 1$. ☺

Théorème 7.7.5 (Riemann-Roch)**.** Il existe un entier $g \geq 0$, appelé **genre** de C tel que pour tout diviseur D on ait, en notant K un diviseur canonique :

$$l(D) - l(K - D) = \deg D + 1 - g$$

Corollaire 7.7.6. — Pour K un diviseur canonique sur une courbe C, on a :

$$l(K) = g$$
$$\deg(K) = 2g - 2$$

— Si D est un diviseur avec $\deg D > 2g - 2$, alors $l(D) = \deg D + 1 - g$.

Démonstration. Pour la première affirmation, appliquer Riemann-Roch à $D = 0$ donne $1 - l(K) = 0 + 1 - g$, d'où $l(K) = g$; puis à $D = K$ donne $g - 1 = \deg K + 1 - g$ d'où $\deg K = 2g - 2$. Pour la seconde affirmation, on utilise 7.7.4 pour conclure que $l(K - D) = 0$. ☺

Remarque : Si C est une courbe sur un corps k, alors le genre de C est égal au genre de $C_{k^{\mathrm{alg}}}$. En effet, un diviseur canonique K sur C est encore un diviseur canonique quand on le voit sur $C_{k^{\mathrm{alg}}}$, et son degré, censé valoir $2g-2$ est le même qu'on le voie d'une façon ou d'une autre. On dit que le genre est un *invariant géométrique*.

S'agissant de $\mathbb{P}^1$, on a vu que $\deg(K) = -2$ donc $g = 0$. La réciproque est vraie :

Corollaire 7.7.7. Soit C une courbe (lisse !) de genre 0 sur un corps algébriquement clos : alors C est isomorphe à $\mathbb{P}^1$.

Démonstration. Soient P, Q deux points distincts de C : on applique Riemann-Roch au diviseur $D := (P) - (Q)$. Comme $\deg D = 0 > -2 = 2g - 2$, le corollaire précédent montre que $l(D) = 1$. Mais 7.7.4 montre que $D \sim 0$, c'est-à-dire qu'il existe $f \in k(C)$ tel que $\mathrm{div}(f) = (P) - (Q)$. En considérant f comme un morphisme $C \to \mathbb{P}^1$, on voit que $\deg f = 1$ (cf. 7.4.5), donc f est un isomorphisme (cf. 7.3.3). ☺

Remarque : Cette démonstration utilise le fait que k est algébriquement clos pour pouvoir fabriquer le diviseur $(P) - (Q)$ comme différence de deux diviseurs de degré 1. En fait, on peut faire mieux : il suffit que $C(k)$ soit non-vide (démonstration : si $P \in C(k)$, Riemann-Roch appliqué au diviseur (P) montre que $l((P)) = 2$, donc il existe une fonction f non-constante, admettant au plus un pôle simple en P, donc admettant effectivement un pôle simple en P d'après 7.2.3, et du coup $\mathrm{div}(f)$, qui doit être de degré 0, est de la forme $(P) - (Q)$, et le reste est comme ci-dessus). On ne peut pas se dispenser de cette hypothèse $C(k) \neq \varnothing$: si C est la conique [17] d'équation projective $t_0^2 + t_1^2 + t_2^2 = 0$ dans $\mathbb{P}^2$ sur les réels, qui a $C(\mathbb{R}) = \varnothing$, alors C a pour genre 0 car le genre est un invariant géométrique (cf. ci-dessus) et que, sur les complexes, cette conique est isomorphe au cercle (quitte à changer t_0 en it_0) donc à $\mathbb{P}^1$ (cf. exemples de 3.4). Pourtant, C ***n'est pas*** isomorphe à $\mathbb{P}^1$ sur les réels, précisément parce que $C(\mathbb{R}) = \varnothing$ alors que $\mathbb{P}^1(\mathbb{R}) \neq \varnothing$!

Corollaire 7.7.8. Si C est une courbe, tout ouvert U de C autre que C tout entier est affine. (Cf. 7.2.4 pour un contexte utile de ce résultat.)

Démonstration (partielle). Le cas $U = \varnothing$ est vrai (on a $U = \mathrm{Spec}\, 0$ où 0 désigne l'anneau nul) mais inintéressant : supposons donc U non vide.

On admet [18] le résultat suivant : si $f : C \to C_0$ est un morphisme non-constant de courbes, alors l'image réciproque par f de tout ouvert affine de C_0 est affine.

17. En fait, on peut montrer que toute courbe de genre 0 peut s'écrire comme une conique plane.

18. Il n'y a pas d'arnaque : c'est là un résultat beaucoup plus facile et moins profond que Riemann-Roch ; il s'agit de dire que f est un morphisme « fini », donc en particulier « affine » c'est-à-dire que l'image réciproque d'un ouvert affine est affine.

Soit P un point du complémentaire de U : le théorème de Riemann-Roch, et notamment le corollaire 7.7.6, montre que si n est assez grand, alors $l(n\cdot(P)) > 1$, autrement dit, il existe une fonction $f \in k(C)$ non constante et régulière partout sauf en P (où elle ne peut pas être régulière). En considérant f comme un morphisme $C \to \mathbb{P}^1$, on voit alors que $U' := C\setminus\{P\} = f^{-1}(\mathbb{A}^1)$, et d'après le résultat admis, U' est affine. Le lemme d'approximation 7.2.4 montre que si $Q_1, \ldots, Q_s$ sont les points de $U'\setminus U$, il existe une fonction h ayant un pôle d'ordre 1 en chacun des Q_i et régulière sur tout $U \setminus \{Q_i\}$; si de plus on exige que h ait un zéro d'ordre très élevé (c'est-à-dire supérieur à s) en un quelconque autre point R (ce que le lemme d'approximation permet toujours de faire), on assure que h aura aussi un pôle en P d'après 7.4.5. Autrement dit, ceci assure que $U = h^{-1}(\mathbb{A}^1)$ (en voyant de nouveau h comme un morphisme $C \to \mathbb{P}^1$), ce qui conclut. ☺