Courbes algébriques
(notes de cours v2)

David A. Madore

12 février 2018

ACCQ205

Git : `58b727e Sat Feb 10 21:58:27 2018 +0100`

Table des matières

1 Prolégomènes d'algèbre commutative

1.1 Anneaux réduits, intègres

1.1.1. 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**. (Pour tout anneau A, il existe un unique morphisme de A vers l'anneau nul ; en revanche,

il n'existe un morphisme de l'anneau nul vers A que si A est lui-même l'anneau nul.)

1.1.2. On rappelle qu'un **idéal** d'un anneau A est un sous-groupe additif I de A tel que $AI \subseteq I$; on dispose alors d'une structure d'anneau sur le groupe abélien quotient A/I (la multiplication étant définie par $(x+I)\,(y+I) = xy+I$ où $z+I$ désigne la classe de z modulo I). On peut aussi définir un idéal comme le noyau d'un morphisme d'anneaux (le noyau de la surjection canonique $A \mapsto A/I$ étant justement I).

Il est souvent utile de se rappeler que les idéaux d'un quotient A/I correspondent exactement aux idéaux de A contenant I ; plus précisément, si J est un idéal de A contenant I, l'image J/I de J par la surjection canonique $A \to A/I$ est un idéal de A/I, et l'application $J \mapsto J/I$ définit une bijection entre idéaux J de A contenant I et idéaux de A/I. De surcroît, le quotient de A/I par J/I s'identifie à A/J.

1.1.3. On aura fréquemmment besoin du fait suivant : quel que soit le morphisme d'anneaux $\psi\colon A \to B$, l'*image* $\operatorname{im}\psi := \{\psi(x) : x \in A\}$ de ψ (qui est un sous-anneau de B) s'identifie au quotient $A/\ker\psi$ de A par le noyau de ψ : l'identification se fait par l'isomorphisme $\tilde{\psi}$ qui envoie la classe de $z \in A$ modulo $\ker\psi$ sur l'image $\psi(z) \in B$. (Si on veut, on a factorisé le morphisme $\psi\colon A \to B$ comme composée de la surjection canonique $A \to A/\ker\psi$, suivie d'un isomorphisme $\tilde{\psi}$, suivie de l'injection canonique $\operatorname{im}\psi \to B$.) De façon plus concise, « un morphisme d'anneaux identifie son image au quotient de sa source par son noyau ».

Dans le cas particulier où ψ est surjectif, ceci signifie qu'un morphisme surjectif $\psi\colon A \to B$ permet d'identifier B au quotient $A/\ker\psi$ de A par son noyau.

1.1.4. 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 $a_1x_{i_1} + \cdots + a_nx_{i_n}$ 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 $a_1x_1 + \cdots + a_nx_n$ 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**.

Dans tout anneau, on peut définir l'**idéal nul** $(0) = \{0\}$, également noté 0, et l'**idéal unité** $(1) = A$. Remarquons que le quotient de A par l'idéal nul est simplement A, tandis que le quotient de A par l'idéall unité est l'anneau nul. On appelle parfois **strict** un idéal qui n'est pas l'idéal unité.

1.1.5. Si k est un anneau, une **k-algèbre** (là aussi : implicitement commutative)

est la donnée d'un morphisme d'anneaux $k \xrightarrow{\varphi_A} A$ appelé **morphisme structural** de l'algèbre. On peut multiplier un élément de A par un élément de k avec : $c \cdot x = \varphi_A(c)\, x \in A$ (pour $c \in k$ et $x \in A$). Un morphisme de k-algèbres est un morphisme d'anneaux $A \xrightarrow{\psi} B$ tel que le morphisme structural $k \xrightarrow{\varphi_B} B$ de B soit la composée $k \xrightarrow{\varphi_A} A \xrightarrow{\psi} B$ de celui de A avec le morphisme considéré.

De façon équivalente, une k-algèbre est un k-module qui est muni d'une multiplication k-bilinéaire qui en fait un anneau, et les morphismes de k-algèbres sont les applications k-linéaires qui préservent la multiplication ; le morphisme structural peut alors se retrouver par $c \mapsto c \cdot 1$. Notons qu'une $\mathbb{Z}$-algèbre est exactement la même chose qu'un anneau (raison pour laquelle il est souvent préférable d'énoncer les résultats en parlant de k-algèbres pour plus de généralité).

Dans la pratique, cependant k sera généralement un corps : une k-algèbre est donc un k-espace vectoriel muni d'une multiplication k-bilinéaire qui en fait un anneau, et le morphisme structural est automatiquement injectif si l'algèbre n'est pas l'algèbre nulle.

1.1.6. Un élément a d'un anneau A est dit **régulier**, resp. **inversible**, lorsque $x \mapsto ax$ est injectif, resp. bijectif, autrement dit lorsque $ax = 0$ implique $x = 0$ (la réciproque est toujours vraie), resp. lorsqu'il existe x (appelé inverse de a) tel que $ax = 1$.

Un élément a qui n'est pas régulier est également appelé **diviseur de zéro** : cela signifie qu'il existe $x \neq 0$ tel que $ax = 0$.

Un élément a de A est inversible si et seulement si l'idéal (a) qu'il engendre est l'idéal unité $(1) = A$. De façon équivalente, un élément *n'est pas* inversible si et seulement il appartient à un idéal strict (c'est-à-dire, autre que l'idéal unité).

Dans un anneau, l'ensemble noté $A^\times$ des éléments inversibles est un groupe, aussi appelé groupe des **unités** de A. Une « unité » est simplement un élément inversible.

1.1.7. Un **corps** est un anneau k dans lequel l'ensemble $k^\times$ des éléments inversibles est égal à l'ensemble $k \setminus \{0\}$ des éléments non-nuls : autrement dit, un corps est un anneau dans lequel ($0 \neq 1$ et) tout élément non-nul est inversible. De façon équivalente, un corps est un anneau ayant exactement deux idéaux (qui sont alors 0 et lui-même). Par convention, l'anneau nul n'est pas un corps.

Un idéal $\mathfrak{m}$ d'un anneau A est dit **maximal** lorsque l'anneau quotient $A/\mathfrak{m}$ est un corps : de façon équivalente, lorsque $\mathfrak{m} \neq A$ et que $\mathfrak{m}$ est maximal pour l'inclusion parmi les idéaux $\neq A$.

1.1.8. Un anneau dans A dans lequel l'ensemble des éléments réguliers est égal à l'ensemble $A \setminus \{0\}$ des éléments non-nuls est dit **intègre** : autrement dit, un anneau intègre est un anneau dans lequel ($0 \neq 1$ et) $ab = 0$ implique $a = 0$ ou

$b = 0$ (la réciproque est toujours vraie). Par convention, l'anneau nul n'est pas intègre.

Un corps est, en particulier, un anneau intègre.

Un idéal $\mathfrak{p}$ d'un anneau A est dit **premier** lorsque l'anneau quotient $A/\mathfrak{p}$ est un anneau intègre, autrement dit lorsque $\mathfrak{p} \neq A$ et que $ab \in \mathfrak{p}$ implique $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$ (la réciproque est toujours vraie).

Un idéal maximal est, en particulier, premier.

1.1.9. Un élément x d'un anneau A est dit **nilpotent** lorsqu'il existe $n \geq 0$ tel que $x^n = 0$. Un anneau dans lequel le seul élément nilpotent est 0 est dit **réduit**.

Un anneau intègre (et *a fortiori* un corps) est, en particulier, un anneau réduit (on démontre par récurrence sur n que $x^n = 0$ implique $x = 0$).

Un idéal $\mathfrak{r}$ d'un anneau A est dit **radical** lorsque l'anneau quotient $A/\mathfrak{r}$ est un anneau réduit, autrement dit lorsque $x^n \in \mathfrak{r}$ implique $x \in \mathfrak{r}$ (la réciproque est toujours vraie).

Un idéal premier (et *a fortiori* un idéal maximal) est, en particulier, un idéal radical.

1.1.10. À titre d'exemple, parmi les idéaux de $\mathbb{Z}$ (dont on rappelle qu'ils sont de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$) :

— l'idéal $2\mathbb{Z}$ est maximal puisque le quotient $\mathbb{Z}/2\mathbb{Z}$ est un corps ;

— l'idéal 0 est premier mais pas maximal puisque le quotient $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$ est un anneau intègre mais pas un corps ;

— l'idéal $6\mathbb{Z}$ est radical mais pas premier puisque le quotient $\mathbb{Z}/6\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ est un anneau réduit (car $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$ le sont) mais pas intègre (car 2×3 est nul modulo 6) ;

— l'idéal $4\mathbb{Z}$ n'est pas radical puisque le quotient $\mathbb{Z}/4\mathbb{Z}$ n'est pas réduit.

Pour donner un exemple moins évident, dans l'anneau $k[x, y]$ des polynômes à deux indéterminées x, y sur un corps k, l'idéal (y) (des polynômes s'annulant identiquement sur l'axe des abscisses) est premier mais non maximal puisque $k[x, y]/(y) \cong k[x]$, tandis que l'idéal (x, y) (des polynômes s'annulant à l'origine) est maximal puisque $k[x, y]/(x, y) \cong k$.

Le résultat ensembliste suivant sera admis :

Lemme 1.1.11 (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 M maximal pour l'inclusion (c'est-à-dire que si $I \supseteq M$ avec $I \in \mathscr{F}$ alors $I = M$).

Proposition 1.1.12. 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 [1] (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. ☺

Corollaire 1.1.13. Dans un anneau A, l'ensemble $A^\times$ des éléments inversibles est le complémentaire de la réunion de tous les idéaux maximaux de A.

Démonstration. On a remarqué en 1.1.6 qu'un élément est non-inversible si et seulement si il appartient à un idéal strict (c'est-à-dire, autre que l'idéal unité) ; la proposition 1.1.12 assure que tout idéal strict est inclus dans un idéal maximal, donc tout élément non-inversible appartient à un idéal maximal, et réciproquement, comme un idéal maximal est (par définition) strict, il ne contient que des éléments non-inversibles. ☺

1.1.14. On peut introduire la terminologie suivante : un anneau **local** est un anneau A ayant *exactement un* idéal maximal $\mathfrak{m}$ (on vient de voir que tout anneau non nul a au moins un idéal maximal). Le (corps) quotient $A/\mathfrak{m}$ s'appelle alors **corps résiduel** de l'anneau local.

Proposition 1.1.15. Dans un anneau, l'ensemble des éléments nilpotents est un idéal : c'est le plus petit idéal radical (ou l'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 $\mathfrak{N}$ des nilpotents est un idéal car si $x^m = 0$ et $y^n = 0$ alors on a $(x+y)^{m+n} = 0$ en développant (ceci montre la stabilité par addition, les autres prioriétés d'un idéal sont évidentes). Cet idéal $\mathfrak{N}$ est inclus dans tout idéal radical $\mathfrak{r}$, car $x^n = 0$ donne $x^n \in \mathfrak{r}$ donc $x \in \mathfrak{r}$ vu que $\mathfrak{r}$ est radical ; et $\mathfrak{N}$ est lui-même radical car si x^n est nilpotent alors x est aussi nilpotent. Ainsi, $\mathfrak{N}$ est bien le plus petit idéal radical, ou l'intersection des idéaux radicaux.

Comme $\mathfrak{N}$ est inclus dans tout idéal radical, il est en particulier inclus dans tout idéal *premier*. Il reste à montrer, réciproquement, que si z est inclus dans tout idéal premier, alors z est nilpotent.

Supposons que z ne soit 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

1. La réunion de deux idéaux n'est généralement pas un idéal, car si $x \in I$ et $x' \in I'$, la 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 $x + x' \in \bigcup_{I\in\mathscr{T}} I$.

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 [2] $\mathfrak{p} + (x)$ 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 $xy \notin \mathfrak{p}$.

Enfin, dire que le quotient de A par son nilradical est réduit signifie exactement que si une puissance d'un élément est nilpotente alors cet élément lui-même est nilpotent, ce qui est évident. ☺

Corollaire 1.1.16. 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 l'intersection des idéaux radicaux de A contenant I, et c'est aussi l'intersection des idéaux premiers de A contenant I. On l'appelle le **radical** de l'idéal I et on le note $\sqrt{I}$.

Démonstration. Appliquons la proposition 1.1.15 à l'anneau quotient A/I, en se rappelant que les idéaux de A/I correspondent aux idéaux de A contenant I et ont les mêmes quotients (cf. 1.1.2) : comme un nilpotent de A/I est précisément la classe modulo I d'un $z \in A$ tel que $z^n \in I$ pour un certain n, la proposition nous permet d'affirmer que l'ensemble de ces z est un idéal de A, que c'est le plus petit idéal radical contenant I ou l'intersection des idéaux radicaux contenant I, et aussi l'intersection des idéaux premiers contenant I. ☺

1.1.17. On a défini la notion d'« idéal radical » (en 1.1.9) et de « radical d'un idéal » (en 1.1.16), mais ceci ne cause pas de confusion parce que les idéaux radicaux sont justement ceux qui sont égaux à leur radical, et que le radical d'un idéal est un idéal radical. (Autrement dit, I est radical si et seulement si $I = \sqrt{I}$, et $\sqrt{I}$ est toujours radical.) On peut donc traiter le deux concepts comme essentiellement synonymes.

1.1.18. On a vu en 1.1.15 que l'intersection des idéaux premiers d'un anneau coïncide avec l'intersection des idéaux radicaux, et que c'est l'ensemble des éléments nilpotents, appelé « nilradical ».

Par souci de parallélisme, on peut se demander ce qu'on peut dire de l'intersection des idéaux *maximaux* d'un anneau : celle-ci porte aussi un nom, à savoir **radical de Jacobson** de l'anneau en question : on peut montrer que c'est l'ensemble des z tels que $1 - cz$ soit inversible pour tout c dans l'anneau.

2. 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 $I \cup \{x\}$.

1.2 Anneaux noethériens

1.2.1. On a dit en 1.1.4 qu'un idéal I d'un anneau A est dit **de type fini** (en tant qu'*idéal*) lorsqu'il est engendré (en tant qu'idéal !) par un nombre fini d'éléments $x_1, \dots, x_n$, autrement dit, $I = (x_1, \dots, x_n) := \{\sum_{i=1}^{n} a_i x_i : (a_1, \dots, a_n) \in A\}$.

Si c'est le cas, en fait, de toute famille $(y_i)_{i\in\Lambda}$ d'éléments qui engendrent I on peut extraire une sous-famille finie qui l'engendre. En effet, si I est engendré par $x_1, \dots, x_n$ et est aussi engendré par $(y_i)_{i\in\Lambda}$, alors l'écriture de chaque x_j comme combinaison A-linéaire des y_i ne fait intervenir qu'un nombre fini de ceux-ci, donc un nombre fini des y_i suffit à exprimer tous les x_j donc tous les éléments de I.

1.2.2. Un anneau A est dit **noethérien** lorsque tout idéal I de A est de type fini.

Un corps (ou un anneau principal, c'est-à-dire un anneau intègre dans lequel tout idéal est principal) sont en particulier des anneaux noethériens. L'anneau $\mathbb{Z}$ est noethérien.

Remarquons aussi qu'un *quotient* d'un anneau noethérien est noethérien. En effet, les idéaux de A/J sont de la forme I/J avec I un idéal de A contenant J, et si I est de type fini alors I/J l'est aussi (il est engendré par les classes modulo J des éléments qui engendrent I). On peut aussi utiliser la proposition suivante :

Proposition 1.2.3. Un anneau A est noethérien si et seulement si 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).

Démonstration. Supposons que A soit noethérien. Soit $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ une suite croissante d'idéaux de A, et soit $I_\infty := \bigcup_{n=0}^{+\infty} I_n$ la réunion de tous ces idéaux : comme on le vérifie facilement (ou cf. la note dans la démonstration de 1.1.12), ce I_∞ est encore un idéal de A. Comme A est noethérien, il est de type fini : il existe donc un nombre fini d'éléments qui l'engendrent, et tous ces éléments appartiennent à un certain I_N de la suite ; on a alors $I_N = I_\infty$.

Réciproquement, supposons que toute suite croissante d'idéaux de A stationne, et soit I un idéal quelconque de A : on veut montrer que I est de type fini. Supposons par l'absurde que ce ne soit pas le cas. Définissons par récurrence une suite d'éléments (a_n). Comme I n'est pas de type fini donc pas égal à l'idéal $I_n := (a_1, \dots, a_n)$ engendré par les n premiers termes de la suite (on pose $I_0 = (0)$), on peut choisir un élément $a_{n+1} \in I$ tel que $a_{n+1} \notin I_n$. On a alors une suite strictement croissante $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots$ (tous contenus dans I), ce qui contredit l'hypothèse sur A. ☺

Proposition 1.2.4 (théorème de la base de Hilbert)**.** Si k est un anneau noethérien, alors l'anneau $k[t]$ des polynômes à une indéterminée sur k est noethérien.

Démonstration. Soit $I \subseteq k[t]$ 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 k 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. ☺

Corollaire 1.2.5. Soit k un corps ou $\mathbb{Z}$, ou plus généralement un anneau noethérien. Alors l'anneau $k[t_1, \ldots, t_n]$ des polynômes en n indéterminées sur k est un anneau noethérien.

Démonstration. La proposition précédente montre que si k est noethérien alors $k[t]$ est noethérien, et une récurrence immédiate montre que $k[t_1, \ldots, t_n]$ est noethérien. ☺

1.2.6. Si $(x_i)_{i \in \Lambda}$ sont des éléments d'une k-algèbre A, l'intersection de toutes les sous-k-algèbres de A contenant les x_i est une sous-k-algèbre et s'appelle la (sous-)k-algèbre **engendrée** par les x_i : c'est l'ensemble de tous les éléments de A qui peuvent être obtenus à partir de 1 et des x_i par sommes, produits par éléments de k et produits binaires ; de façon plus simple, c'est l'ensemble des toutes les expressions polynomiales sur k en les x_i, c'est-à-dire des valeurs $f(x_{i_1}, \ldots, x_{i_n})$ avec $f \in k[t_1, \ldots, t_n]$ (un polynôme en n indéterminées sur k) et $i_1, \ldots, i_n \in \Lambda$.

Lorsque Λ est fini : la sous-k-algèbre engendrée par $x_1, \ldots, x_n$ est l'ensemble des toutes les valeurs $f(x_1, \ldots, x_n)$ où $f \in k[t_1, \ldots, t_n]$ est un polynôme à coefficients dans k ; on pourra noter $k[x_1, \ldots, x_n]$ (cf. l'avertissement ci-dessous) cette sous-algèbre ; une telle sous-algèbre (engendrée par un nombre fini d'éléments) est dite de **de type fini** (en tant que k-algèbre). Autrement dit, une k-algèbre A est dite de type fini lorsqu'il existe $x_1, \ldots, x_n \in A$ (en nombre fini) tels que tout élément de A s'écrive de la forme $f(x_1, \ldots, x_n)$ pour un certain polynôme $f \in k[t_1, \ldots, t_n]$.


On prendra garde au fait que la même notation $k[x_1, \ldots, x_n]$ peut désigner soit la k-algèbre engendrée par $x_1, \ldots, x_n$ dans une k-algèbre A plus grande, soit

l'anneau des polynômes à n indéterminées $x_1, \dots, x_n$ sur k. Ces conventions sont cependant cohérentes en ce sens que l'anneau des polynômes à n indéterminées sur k est bien la k-algèbre engendrée par les indéterminées (cf. le point suivant). Il faut donc prendre garde à ce que sont $x_1, \dots, x_n$ quand cette notation apparaît : si aucune remarque n'est faite et que les x_i n'ont pas été introduits auparavant, il est généralement sous-entendu que ce sont des indéterminées.

1.2.7. Une k-algèbre A est de type fini lorsqu'il existe $x_1, \dots, x_n \in A$ tels que le morphisme $k[t_1, \dots, t_n] \to A$ (de la k-algèbre $k[t_1, \dots, t_n]$ des polynômes en n indéterminées vers A), dit morphisme d'évaluation, qui à f associe $f(x_1, \dots, x_n)$ est *surjectif*. Or on rappelle (cf. 1.1.3) qu'un morphisme d'anneaux surjectif $\psi\colon A' \to A$ permet d'identifier l'image A au quotient $A'/\ker\psi$ de A' par le noyau de ψ. Donc toute k-algèbre de type fini peut s'écrire sous la forme du quotient $k[t_1, \dots, t_n]/I$ d'un anneau de polynômes $k[t_1, \dots, t_n]$ par un idéal de ce dernier ; réciproquement, un tel quotient est visiblement de type fini (il est engendré par les classes modulo I des indéterminées).

En résumé, on peut donc dire qu'une k-algèbre de type fini est la même chose qu'un quotient d'un anneau de polynômes (en un nombre fini d'indéterminées).

En rassemblant ce fait avec 1.2.5 et avec le fait qu'un quotient d'un anneau noethérien est noethérien, on obtient :

Corollaire 1.2.8. Soit k un corps ou $\mathbb{Z}$, ou plus généralement un anneau noethérien. Alors toute k-algèbre de type fini est un anneau noethérien.

1.3 Localisation

1.3.1. On dit qu'une partie S d'un anneau A est **multiplicative** lorsque $1 \in S$ et qu'on a $ss' \in S$ dès que $s, s' \in S$.

On notera les deux exemples suivants de parties multiplicatives :

— Si $f_1, \dots, f_n \in A$, alors l'ensemble $\{f_1^{i_1} \cdots f_n^{i_n} : i_1, \dots, i_n \in \mathbb{N}\}$ des monômes en $f_1, \dots, f_n$ (où on convient que tout élément élevé à la puissance 0 vaut 1) est une partie multiplicative : c'est la plus petite partie multiplicative contenant $f_1, \dots, f_n$, dite aussi partie multiplicative *engendrée* par $f_1, \dots, f_n$.

— Si $\mathfrak{p}$ est un idéal premier de A (cf. 1.1.8), alors son complémentaire $A \setminus \mathfrak{p}$ est une partie multiplicative. En particulier, si A est un anneau intègre, l'ensemble $A\setminus\{0\}$ des éléments non nuls de A est une partie multiplicative.

1.3.2. Donnée une partie multiplicative S dans un anneau A, on souhaite maintenant fabriquer un anneau qu'on notera $A[S^{-1}]$ où les éléments de S sont rendus inversibles (la logique d'exiger que S soit multiplicative est que, si s et s' sont inversibles, forcément ss' le sera). On va voir les éléments de $A[S^{-1}]$ comme

des fractions a/s avec $a \in A$ et $s \in S$, mais il faut se demander à quelle condition on veut poser $a_1/s_1 = a_2/s_2$: c'est certainement le cas si $a_2 s_1 - a_1 s_2 = 0$, mais il s'avère que cette condition ne suffit pas (elle ne définit pas une relation d'équivalence en général), et certainement s'il existe $t \in S$ et $c \in A$ tels que $tc = 0$, on va vouloir que c devienne nul dans $A[S^{-1}]$: c'est ce qui motive l'apparition de t dans la définition suivante.

1.3.3. Lorsque S est une partie multiplicative, on définit un anneau noté $A[S^{-1}]$ (ou $S^{-1}A$) de la façon suivante :

— Les éléments de $A[S^{-1}]$ sont notés a/s avec $a \in A$ et $s \in S$, où on identifie $a_1/s_1 = a_2/s_2$ lorsqu'il existe $t \in S$ tel que $t(a_2 s_1 - a_1 s_2) = 0$. Plus exactement, cela signifie qu'on considère la relation d'équivalence $\sim$ sur $A \times S$ définie par $(a_1, s_1) \sim (a_2, s_2)$ lorsqu'il existe $t \in S$ tel que $t(a_2 s_1 - a_1 s_2) = 0$, on appelle $A[S^{-1}]$ l'ensemble $(A \times S)/\sim$ des classes d'équivalences, et on note a/s la classe de (a, s) pour cette relation.

— 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 $1/1$).

Il faut vérifier que la relation $\sim$ est bien une relation d'équivalence, que les opérations sont bien définies (c'est-à-dire ne dépendent pas des représentants choisis des classes pour $\sim$), et qu'on obtient bien ainsi un anneau. Nous omettons les calculs un peu fastidieux, mais à titre d'exemple, vérifions que l'addition est bien définie : pour que l'écriture $(a/s)+(a'/s') = (a's+as')/(ss')$ ait un sens, elle ne doit pas dépendre des représentants a/s et a'/s' choisis des éléments à ajouter, c'est-à-dire qu'on doit vérifier que si $(a_1, s_1) \sim (a_2, s_2)$, et si $(a'_1, s'_1) \sim (a'_2, s'_2)$, alors on a $(a'_1 s_1 + a_1 s'_1, s_1 s'_1) \sim (a'_2 s_2 + a_2 s'_2, s_2 s'_2)$; mais par hypothèse, il existe donc t tel que $t(a_2 s_1 - a_1 s_2) = 0$ et t' tel que $t'(a'_2 s'_1 - a'_1 s'_2) = 0$, et en multipliant la première égalité par $t' s'_1 s'_2$, la seconde par $t s_1 s_2$ et en les ajoutant, on obtient $tt'(s_1 s'_1(a'_2 s_2 + a_2 s'_2) - s_2 s'_2(a'_1 s_1 + a_1 s'_1)) = 0$, ce qui donne bien $(a'_1 s_1 + a_1 s'_1, s_1 s'_1) \sim (a'_2 s_2 + a_2 s'_2, s_2 s'_2)$ comme annoncé.

On a de plus un morphisme d'anneaux $A \to A[S^{-1}]$ envoyant $a \in A$ sur $a/1$ qu'on peut appeler morphisme « naturel » ou « canonique » dans ce contexte.

L'anneau $A[S^{-1}]$ ainsi défini (muni du morphisme $A \to A[S^{-1}]$, donc vu comme A-algèbre si on le souhaite) s'appelle la **localisation** (ou le localisé) de A inversant la partie multiplicative S.

1.3.4. On prendra garde au fait que le morphisme naturel $A \to A[S^{-1}]$ n'est pas forcément injectif (c'est-à-dire qu'on peut avoir $a/1 = 0$ dans $A[S^{-1}]$ sans que a soit nul dans A). En fait, il est injectif si et seulement si tout élément de S est régulier (cf. 1.1.6) : en effet, le fait que $t \in S$ soit un diviseur de zéro signifie que $ta = 0$ pour un certain $a \neq 0$, ce qui s'écrit aussi $t(a - 0) = 0$, témoignant que $(a, 1) \sim (0, 1)$. Le cas le plus extrême est celui où S contient 0, et alors $A[S^{-1}]$

est l'anneau nul.

Lorsque S ne contient que des éléments réguliers, la définition de $A[S^{-1}]$ est légèrement simplifiée puisqu'on a $a_1/s_1 = a_2/s_2$ si et seulement si $a_2 s_1 - a_1 s_2 = 0$.

1.3.5. Conformément aux exemples donnés en 1.3.1, les cas particuliers suivants sont importants :

Si $\mathfrak{p}$ est un idéal 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** $\mathfrak{p}$.

De façon encore plus particulière, 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.

Si $f_1, \dots, f_n \in A$ et si $S = \{f_1^{i_1} \cdots f_n^{i_n} : i_1, \dots, i_n \in \mathbb{N}\}$ est la partie multiplicative qu'ils engendrent, la localisé $A[S^{-1}]$ se note aussi $A[f_1^{-1}, \dots, f_n^{-1}]$. En fait, seul le cas $n = 1$ est vraiment intéressant car on a $A[f_1^{-1}, \dots, f_n^{-1}] \cong A[h^{-1}]$ où $h = f_1 \cdots f_n$ (l'isomorphisme envoie $a/(f_1^{i_1} \cdots f_n^{i_n})$ sur $(a f_1^{i-i_1} \cdots f_n^{i-i_n})/h^i$ où $i = \max(i_1, \dots, i_n)$). Ce cas peut se décrire explicitement d'une autre manière :

Proposition 1.3.6. Si A est un anneau et $f \in A$, alors l'anneau quotient $A[t]/(tf - 1)$ (de l'anneau $A[t]$ des polynômes en une indéterminée par son idéal engendré par $tf - 1$) est isomorphe à $A[f^{-1}]$.

Plus précisément, un isomorphisme $\varphi\colon A[t]/(tf-1) \to A[f^{-1}]$ s'obtient en envoyant la classe (modulo $tf - 1$) d'un $g \in A[t]$ sur $g(1/f)$ (évaluation de g en l'élément $1/f$ de $A[f^{-1}]$), et sa réciproque $\psi\colon A[f^{-1}] \to A[t]/(tf-1)$ envoye a/f^i sur la classe de at^i (modulo $tf - 1$).

Démonstration. Le morphisme d'évaluation $A[t] \to A[f^{-1}]$ qui envoie un polynôme $g \in A[t]$ sur son évaluation $g(1/f)$ en $1/f$ envoie $tf - 1$ sur 0 (puisque $1/f$ est l'inverse de f dans $A[f^{-1}]$) : autrement dit, $tf - 1$ est dans le noyau de ce morphisme d'évaluation, et on en déduit un morphisme d'anneaux $\varphi\colon A[t]/(tf-1) \to A[f^{-1}]$ comme décrit. Il reste à vérifier que c'est un isomorphisme, et que sa réciproque est celle qui a été décrite.

Tout élément de $A[f^{-1}]$ est (par définition) de la forme a/f^i pour un certain $i \in \mathbb{N}$: c'est-à-dire qu'il s'écrit $\varphi(a\bar{t}^i)$ (en notant $\bar{t}$ la classe de t modulo $tf - 1$). Ceci montre déjà la surjectivité de φ.

Montrons l'injectivité : pour cela, observons que $\bar{t}f = 1$ dans $A[t]/(tf-1)$, donc f y est inversible d'inverse $\bar{t}$. Si $g = c_0 + c_1 t + \cdots + c_n t^n \in A[t]$ vérifie $g(1/f) = 0$, c'est-à-dire $c_0 + c_1(1/f) + \cdots + c_n(1/f)^n = 0$ dans $A[f^{-1}]$, ceci se réécrit $(c_0 f^n + c_1 f^{n-1} + \cdots + c_n)/f^n = 0$ dans $A[f^{-1}]$, soit, par définition

de $A[f^{-1}]$, qu'il existe un $j \in \mathbb{N}$ tel que $c_0 f^{n+j} + c_1 f^{n+j-1} + \cdots + c_n f^j = 0$ dans A, et en particulier cette égalité vaut dans $A[t]/(tf-1)$, mais en multipliant par $(\bar{t})^{n+j}$ et en se rappelant que $\bar{t}$ est l'inverse de f, on a $c_0 + c_1\bar{t} + \cdots + c_n\bar{t}^n = 0$, si bien que la classe $\bar{g} = g(\bar{t})$ de g (modulo $tf-1$) est nulle : on a bien montré l'injectivité de φ.

On sait maintenant que φ est un isomorphisme d'anneaux. Comme $\varphi(a\bar{t}^i) = a/f^i$, la réciproque de φ envoie a/f^i sur la classe $a\bar{t}^i$ de at^i modulo $tf-1$, c'est donc bien l'application ψ décrite (et en particulier, celle-ci est un morphisme d'anneaux). ☺

1.3.7. Lorsque A est un anneau *intègre* (cf. 1.1.8), tout localisé $A[S^{-1}]$ avec $0 \notin S$ peut se décrire comme un sous-anneau du corps des fractions $\mathrm{Frac}(A)$, à savoir celui engendré par A et les inverses (dans $\mathrm{Frac}(A)$) des éléments de S, donc concrètement l'ensemble des quotients a/f où $a \in A$ et $f \in S$ (interprétés comme des vrais quotients dans le corps $\mathrm{Frac}(A)$).

1.4 Anneaux factoriels et lemme de Gauß

1.4.1. Un élément p d'un anneau intègre A est dit **irréductible** lorsque pour toute écriture de p comme un produit $p = fg$ de deux éléments de A, exactement un des deux facteurs f, g est une unité (c'est-à-dire, est inversible). Par convention, ni 0 ni les unités ne sont considérés comme irréductibles ; en revanche, le produit d'un irréductible par une unité est encore un irréductible.

Dans le cas de $\mathbb{Z}$, les éléments irréductibles sont les nombres premiers et leurs inverses ; dans le cas de $k[t_1, \ldots, t_d]$, on obtient la notion usuelle de polynôme irréductible.

1.4.2. On dit qu'un anneau intègre A est **factoriel** lorsque tout élément non-nul s'écrit comme produit d'une unité et d'éléments irréductibles, et que de plus cette décomposition en facteurs irréductibles est unique au sens où on peut toujours passer entre deux telles écritures quitte à permuter l'ordre des facteurs et à les multiplier par des unités de A. Autrement dit : (1) pour tout $a \in A$ non nul, il existe u une unité et $p_1, \ldots, p_r$ irréductibles tels que $a = up_1 \cdots p_r$, et (2) si $p_1, \ldots, p_r$ et $q_1, \ldots, q_s$ sont irréductibles et $q_1 \cdots q_s = up_1 \cdots p_r$ avec u une unité, alors $s = r$ et il existe une permutation $\sigma \colon \{1, \ldots, r\} \to \{1, \ldots, r\}$ telle que $q_{\sigma(i)} = u_i p_i$ avec u_i une unité.

L'anneau $\mathbb{Z}$ est factoriel : c'est l'affirmation standard sur l'existence et l'unicité de la décomposition en facteurs premiers. Comme on va le signaler en 1.4.4 ci-dessous, l'anneau $k[t_1, \ldots, t_d]$ des polynômes en d indéterminées sur un corps k est lui aussi factoriel. On peut par ailleurs montrer que la localisation $A[S^{-1}]$ d'un anneau factoriel est encore factorielle (lorsque $0 \neq S$).

1.4.3. Si p est un élément irréductible d'un anneau factoriel A, alors, lorsque p

divise un produit fg, il divise forcément l'un des facteurs f, g (en effet, p apparaît dans la décomposition en facteurs irréductibles de fg, qui par unicité s'obtient en regroupant celle de f et celle de g, donc p divise l'un de ces deux éléments). Autrement dit, on a montré que l'idéal (p) est un idéal premier.

Réciproquement, si (p) est un idéal premier non nul dans un anneau factoriel A, alors p est irréductible (en effet, si p était produit d'au moins deux irréductibles, aucun de ces irréductibles ne serait un multiple de p mais leur produit le serait).

(Un élément $p \neq 0$ d'un anneau intègre tel que l'idéal (p) soit premier est parfois dit « premier » : dans un anneau intègre quelconque, ceci implique toujours « irréductible », mais la réciproque ne vaut pas en général. On peut montrer qu'un anneau intègre est factoriel si et seulement si tout élément non nul admet une factorisation comme produit d'une unité et d'éléments premiers.)

1.4.4. Concernant les anneaux de polynômes, on a le **lemme de Gauß** suivant : si A est un anneau factoriel et K son corps des fractions, alors l'anneau $A[t]$ des polynômes en une indéterminée sur A est factoriel ; et par ailleurs $f \in A[t]$ est irréductible (dans $A[t]$) si et seulement si f est constant et irréductible dans A, *ou bien* f est irréductible dans $K[t]$ et le pgcd (dans A) des coefficients de f vaut 1 (on dit que f est **primitif** lorsque cette dernière condition est vérifiée).

Le point-clé dans la démonstration est de montrer que le pgcd $c(f)$ des coefficients d'un polynôme dans $A[t]$, aussi appelé **contenu** de f, est multiplicatif (i.e., $c(fg) = c(f)\,c(g)$) ; la décomposition en facteurs irréductibles dans $A[t]$ d'un élément de $A[t]$ s'obtient alors à partir de celle de $K[t]$ et de celle dans A du contenu.

On en déduit que pour tout d, l'anneau $k[t_1, \ldots, t_d]$ des polynômes en d indéterminées sur un corps k est un anneau factoriel ; et de plus, qu'un polynôme $f \in k[t_1, \ldots, t_d, z]$ (en $d+1$ indéterminées) irréductible et faisant effectivement intervenir t est encore irréductible dans $k(t_1, \ldots, t_d)[t]$, et réciproquement, qu'un polynôme irréductible dans $k(t_1, \ldots, t_d)[t]$ donne un polynôme irréductible dans $k[t_1, \ldots, t_d, t]$ quitte à multiplier par le pgcd des dénominateurs.

On retient par ailleurs de 1.4.3 qu'un polynôme $f \in k[t_1, \ldots, t_d]$ non-nul est irréductible si et seulement si l'idéal (f) qu'il engendre est premier.

2 Variétés algébriques affines sur un corps algébriquement clos

2.0.1. Dans cette section, sauf précision expresse du contraire, k sera un corps algébriquement clos.

On notera $\mathbb{A}^d(k) = k^d$ l'ensemble des d-uplets à coordonnées dans k. On

l'appelle **espace affine de dimension** d sur k (on parle de droite ou plan affine lorsque $d = 1, 2$). Si k est clair d'après le contexte, il sera aussi parfois noté $\mathbb{A}^d$.

Si $x = (x_1, \ldots, x_d) \in \mathbb{A}^d(k)$ et si $f \in k[t_1, \ldots, t_d]$ est un polynôme en autant de variables, on notera simplement $f(x)$ (l'évaluation de f en x) pour $f(x_1, \ldots, x_d)$. On dit que x est un zéro de f lorsque $f(x) = 0$.

2.1 Correspondance entre fermés de Zariski et idéaux

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

2.1.1. Si $\mathscr{F}$ est une partie de $k[t_1, \ldots, t_d]$, on définit un ensemble $Z(\mathscr{F}) = \{(x_1, \ldots, x_d) \in k^d : (\forall f \in \mathscr{F})\, f(x_1, \ldots, x_d) = 0\}$, autrement dit, l'ensemble des zéros communs à tous les éléments de $\mathscr{F}$.

Lorsque $\mathscr{F}$ est un ensemble fini $\{f_1, \ldots, f_r\}$, on note simplement $Z(f_1, \ldots, f_r)$ cet ensemble de zéros communs à $f_1, \ldots, f_r$.

2.1.2. Remarques évidentes : si $\mathscr{F} \subseteq \mathscr{F}'$ alors $Z(\mathscr{F}) \supseteq Z(\mathscr{F}')$ (la fonction Z est dite « décroissante pour l'inclusion »); on a $Z(\mathscr{F}) = \bigcap_{f \in \mathscr{F}} Z(f)$.

Si I est l'idéal engendré par $\mathscr{F}$ (cf. 1.1.4) alors $Z(I) = Z(\mathscr{F})$ (car si tous les éléments de $\mathscr{F}$ s'annulent en x, alors toute combinaison linéaire de tels éléments s'y annule aussi). S'il s'agit d'étudier les $Z(\mathscr{F})$, on peut donc se contenter de regarder les $Z(I)$ avec I idéal de $k[t_1, \ldots, t_d]$.

Mieux : si $\sqrt{I} = \{f : (\exists n)\, f^n \in I\}$ désigne le radical de l'idéal I (cf. 1.1.16), on a $Z(\sqrt{I}) = Z(I)$ (car si f^n s'annule en x alors f s'y annule aussi). On peut donc se contenter de considérer les $Z(I)$ avec I idéal radical.

2.1.3. On appellera **fermé de Zariski** dans k^d, ou **variété algébrique affine** sur k, 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.

2.1.4. 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 $(t_1 - x_1, \ldots, t_d - x_d)$; on remarquera au passage 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 $Z(\sum_{i \in \Lambda} I_i) = \bigcap_{i \in \Lambda} Z(I_i)$ (où $\sum_{i \in \Lambda} I_i$ désigne l'idéal engendré par $\bigcup_{i \in \Lambda} I_i$).

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 $x \in Z(I')$).

(Le fait que le vide et le plein soient des fermés de Zariski, que toute intersection de fermés de Zariski soit un fermé de Zariski, et que la réunion de deux fermés de Zariski soit un fermé de Zariski justifie le terme de « fermés », car ce sont là les axiomes demandés sur les fermés d'un espace topologique.)

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

2.1.5. Réciproquement, si E est une partie de k^d, on note $\mathfrak{I}(E) = \{f \in k[t_1, \dots, t_d] : (\forall (x_1, \dots, x_d) \in E)\, f(x_1, \dots, x_d) = 0\}$ l'ensemble des polynômes s'annulant en tous les points de E.

Il est clair c'est un idéal de $k[t_1, \dots, t_d]$, et même un idéal radical.

2.1.6. 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 $\mathfrak{I}(E) \neq k[t_1, \dots, t_d]$ dès que $E \neq \varnothing$.

On a de façon triviale $\mathfrak{I}(\varnothing) = k[t_1, \dots, t_d]$.

Le rapport entre ces deux fonctions

2.1.7. 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 ». Appelons $(*)$ cette équivalence.

En particulier, en appliquant $(*)$ à $\mathscr{F} = \mathfrak{I}(E)$, on voit que $E \subseteq Z(\mathfrak{I}(E))$ pour toute partie E de k^d : appelons (†) cette observation. En appliquant $(*)$ à $E = Z(\mathscr{F})$, on a $\mathscr{F} \subseteq \mathfrak{I}(Z(\mathscr{F}))$: appelons (‡) cette observation.

Comme $\mathfrak{I}$ est décroissante pour l'inclusion, de l'observation (†) que $E \subseteq Z(\mathfrak{I}(E))$, on déduit $\mathfrak{I}(E) \supseteq \mathfrak{I}(Z(\mathfrak{I}(E)))$. Mais par ailleurs, en appliquant l'observation (‡) que $\mathscr{F} \subseteq \mathfrak{I}(Z(\mathscr{F}))$ à $\mathscr{F} = \mathfrak{I}(E)$, on en déduit $\mathfrak{I}(E) \subseteq \mathfrak{I}(Z(\mathfrak{I}(E)))$. On a donc montré $\mathfrak{I}(E) = \mathfrak{I}(Z(\mathfrak{I}(E)))$ pour toute partie E de k^d. De même (le raisonnement étant complètement symétrique entre Z et $\mathfrak{I}$), on a $Z(\mathscr{F}) = Z(\mathfrak{I}(Z(\mathscr{F})))$ pour tout ensemble $\mathscr{F}$ de polynômes.

On a donc prouvé :

Proposition 2.1.8. Avec les notations ci-dessus :

- Les parties E de k^d vérifiant $E = Z(\mathfrak{I}(E))$ sont exactement celles de la forme $Z(\mathscr{F})$ pour un certain $\mathscr{F}$, c'est-à-dire les fermés de Zariski, et dans ce cas on peut prendre $\mathscr{F} = \mathfrak{I}(E)$, qui est un idéal radical.
- Les parties I de $k[t_1, \dots, t_d]$ vérifiant $I = \mathfrak{I}(Z(I))$ sont exactement celles 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 $k[t_1, \dots, t_d]$.
- Les fonctions $\mathfrak{I}$ et Z se restreignent en des bijections réciproques, décroissantes pour l'inclusion, entre l'ensemble des fermés de Zariski E de k^d et l'ensemble des idéaux (forcément radicaux) I de $k[t_1, \dots, t_d]$ tels que $I = \mathfrak{I}(Z(I))$.

2.1.9. Le résultat ci-dessus est complètement formel : on n'a fait aucun usage de l'hypothèse que k est algébriquement clos, on n'a essentiellement utilisé que le fait que Z et $\mathfrak{I}$ sont décroissantes et qu'on a $E \subseteq Z(\mathscr{F})$ ssi $\mathscr{F} \subseteq \mathfrak{I}(E)$.

La caractérisation ci-dessus a ceci d'insatisfaisant qu'on n'a pas caractérisé quels idéaux radicaux I vérifient $I = \mathfrak{I}(Z(I))$. On va voir ci-dessous que c'est le cas de tous les idéaux radicaux de $k[t_1, \ldots, t_d]$, mais à la différence de la proposition qu'on vient de voir, c'est un résultat qui a un vrai contenu mathématique.

2.2 Le Nullstellensatz

2.2.1. De l'allemand « der Satz » = la phrase, le théorème mathématique, « die Stelle » = l'endroit, et « die Nullstelle » = le lieu d'annulation, le zéro d'un polynôme : le « **Nullstellensatz** », littéralement, « théorème du lieu d'annulation », s'appelle aussi « théorème des zéros de Hilbert ».

On rappelle que k est supposé algébriquement clos (hypothèse qui n'a pas servi jusqu'à présent).

Il existe plusieurs formulations du Nullstellensatz, qu'on peut déduire les unes les autres. Formulons d'abord celle qui caractérise les idéaux *maximaux* de $k[t_1, \ldots, t_d]$: on rappelle qu'on a déjà introduit (cf. 2.1.4) la notation $\mathfrak{m}_x := \mathfrak{I}(x)$ si $x \in k^d$ (idéal associé à un *singleton*) pour l'ensemble des polynômes s'annulant en x, que c'est un idéal maximal, et qu'il est engendré par $t_1 - x_1, \ldots, t_d - x_d$ si $x = (x_1, \ldots, x_d)$; la proposition suivante affirme que, lorsque k est algébriquement clos, ce sont les seuls idéaux maximaux de $k[t_1, \ldots, t_d]$.

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

Ce fait est vrai en général, mais on ne donnera une démonstration que dans le cas particulier où k est indénombrable (il s'agit d'une astuce qui simplifie la démonstration).

Démonstration dans le cas particulier où k est indénombrable. Soit $\mathfrak{M}$ un idéal maximal de $k[t_1, \ldots, t_d]$. On va montrer que $\mathfrak{M}$ est de la forme $\mathfrak{m}_x$ pour un certain $x \in k^d$. Pour cela, on montre d'abord $Z(\mathfrak{M}) \neq \varnothing$.

Soit $K = k[t_1, \ldots, t_d]/\mathfrak{M}$. Il s'agit d'un corps (puisque $\mathfrak{M}$ est maximal). Il est de dimension au plus dénombrable en tant que k-espace vectoriel, c'est-à-dire qu'il a une famille génératrice dénombrable, à savoir les images des monômes en les t_i. Si K contenait un élément transcendant τ sur k, le corps $k(\tau)$ qu'il engendre s'identifierait au corps des fractions rationnelles en une indéterminée, et par décomposition des fractions rationnelles en éléments simples, la famille

des $\frac{1}{\tau - x}$ pour x parcourant k serait linéairement indépendante sur k ; mais cette famille est indénombrable puisque k a supposé l'être : on aurait donc une famille linéairement indépendate (sur k) dans $k(\tau)$, donc dans K, ce qui contredit le fait que la dimension de ce dernier est au plus dénombrable. Bref, il est impossible que K contienne un transcendant sur k : c'est donc que K est algébrique sur k. Comme k était supposé algébriquement clos, on a en fait $K = k$ (au sens où le morphisme $k \to K$ envoyant un élément sur de k la classe du polynôme constant modulo $\mathfrak{M}$ est un isomorphisme). Les classes des indéterminées $t_1, \ldots, t_d$ définissent donc 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, $x := (x_1, \ldots, x_d) \in Z(\mathfrak{M})$, ce qui montre $Z(\mathfrak{M}) \neq \varnothing$.

Mais dès lors qu'on a montré qu'il existe $x \in Z(\mathfrak{M})$, on a $\mathfrak{M} \subseteq \mathfrak{m}_x$ (cf. 2.1.7($*$)), et comme $\mathfrak{M}$ est maximal, c'est que $\mathfrak{M} = \mathfrak{m}_x$, comme annoncé. ☺

Proposition 2.2.3 (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. 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 la proposition 2.2.2 montre que $\mathfrak{M} = \mathfrak{m}_x$ pour un certain $x \in k^d$, ce qui implique $Z(I) \supseteq Z(\mathfrak{m}_x) = \{x\}$, et notamment $Z(I) \neq \varnothing$. ☺

On peut aussi reformuler ce résultat de la façon suivante : remarquons au préalable que si $f_1, \ldots, f_r$ et $g_1, \ldots, g_r$ sont des polynômes en d variables tels que $g_1 f_1 + \cdots + g_r f_r = 1$, alors $f_1, \ldots, f_r$ n'ont aucun zéro commun (car en un tel zéro le membre de gauche de l'égalité s'annulerait, mais le membre de droite y vaut 1).

Proposition 2.2.4 (Nullstellensatz faible)**.** Soit k un corps algébriquement clos. Si $f_1, \ldots, f_r \in k[t_1, \ldots, t_d]$ sont des polynômes en d variables sans zéro commun, c'est-à-dire si $Z(f_1, \ldots, f_r) = \varnothing$, alors il existe $g_1, \ldots, g_r \in k[t_1, \ldots, t_d]$ tels que $g_1 f_1 + \cdots + g_r f_r = 1$, c'est-à-dire que $f_1, \ldots, f_r$ engendrent l'idéal unité.

Démonstration. Soit I l'idéal engendré par $f_1, \ldots, f_r$: comme $Z(I) = Z(f_1, \ldots, f_r)$ (cf. 2.1.2), la proposition 2.2.3 montre que $Z(f_1, \ldots, f_r) = \varnothing$ implique que I contient 1, ce qui est bien la conclusion annoncée. ☺

Réciproquement, cette formulation permet de retrouver la formulation 2.2.3, il suffit de se rappeler que tout idéal de $k[t_1, \ldots, t_d]$ est engendré par un nombre fini d'éléments (théorème de la base de Hilbert, 1.2.5).

Théorème 2.2.5 (Nullstellensatz ou théorème des zéros de Hilbert)**.** Soit k un corps algébriquement clos. Soit I un idéal de $k[t_1, \ldots, t_d]$: alors $\mathfrak{I}(Z(I)) = \sqrt{I}$ (le radical de I).

Démonstration. On sait déjà 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 $f \in \sqrt{I}$, autrement dit $f^n \in I$ pour un certain n.

Soit z une nouvelle indéterminée, et soit J l'idéal engendré par I et $zf - 1$ dans $k[t_1, \ldots, t_d, z]$. On a $Z(J) = \varnothing$ (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 2.2.3 entraîne $J = k[t_1, \ldots, t_d, z]$. En réduisant modulo $zf - 1$, cela signifie que l'idéal engendré par I dans $k[t_1, \ldots, t_d, z]/(zf - 1)$ est l'idéal unité.

Maintenant considérons l'anneau localisé $k[t_1, \ldots, t_d, f^{-1}]$ (c'est-à-dire, $k[t_1, \ldots, t_d][f^{-1}]$, cf. 1.3.5), et soit $I[f^{-1}]$ l'idéal engendré par I dans cet anneau. On a $k[t_1, \ldots, t_d, f^{-1}] = k[t_1, \ldots, t_d, z]/(zf - 1)$ d'après 1.3.6, et le paragraphe précédent montre donc que $I[f^{-1}]$ est l'idéal unité. Concrètement, cela signifie que $1 \in k[t_1, \ldots, t_d, f^{-1}]$ s'écrit comme combinaison linéaire, à coefficients dans $k[t_1, \ldots, t_d, f^{-1}]$, d'éléments de I ; en mettant les coefficients en question sous la forme h/f^i où $h \in k[t_1, \ldots, t_d]$ et où $i \in \mathbb{N}$, et en ramenant tous ces coefficients sur un même dénominateur f^n (par la définition de $k[t_1, \ldots, t_d, f^{-1}]$), on voit que finalement on a écrit f^n comme combinaison linéaire, à coefficients dans $k[t_1, \ldots, t_d]$, d'éléments de I : c'est-à-dire que $f^n \in I$, ce qu'on voulait prouver. ☺

2.2.6. La moralité du Nullstellensatz est que (sur un corps algébriquement clos !) on peut « essentiellement » retrouver des équations polynomiales $f_1, \ldots, f_r$ à partir du lieu $Z(f_1, \ldots, f_r)$ de leurs solutions (le fermé de Zariski qu'elles définissent) : le « essentiellement » signifie que, à défaut de retrouver $f_1, \ldots, f_r$ eux-mêmes, on retrouve l'idéal radical qu'ils engendrent (si $f_1, \ldots, f_r$ engendrent un idéal radical, on retrouve l'idéal en question).

On peut maintenant utiliser le Nullstellensatz pour revoir l'énoncé 2.1.8 :

Scholie 2.2.7. 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).

2.3 Ouverts de Zariski et ouverts relatifs

2.3.1. Un **ouvert de Zariski** de k^d est par définition le complémentaire d'un fermé de Zariski. De façon équivalente, si on note $D(f) := \{x \in k^d : f(x) \neq 0\}$, un ouvert de Zariski est un ensemble de la forme $D(f_1) \cap \cdots \cap D(f_r)$ (en effet, tout

idéal I de $k[t_1, \ldots, t_d]$ est engendré par un nombre fini d'éléments $f_1, \ldots, f_r$, et le complémentaire de $Z(I) = Z(f_1, \ldots, f_r)$ est alors $D(f_1) \cup \cdots \cup D(f_r)$). Les $D(f)$ sont parfois appelés **ouverts principaux**.

Les propriétés vues sur les fermés de Zariski (cf. 2.1.4) montrent, par passage au complémentaire que : (i) $\varnothing$ et k^d sont des ouverts de Zariski, (ii) une réunion quelconque d'ouverts de Zariski est un ouvert de Zariski, et (iii) une intersection finie d'ouverts de Zariski est un ouvert de Zariski. Ces propriétés sont constitutives de la notion de « topologie », et on appellera **topologie de Zariski** l'ensemble de tous les ouverts de Zariski.

2.3.2. Si X est une variété algébrique affine sur k (= un fermé de Zariski dans k^d), on appelle **fermé** ou **ouvert de Zariski** *de* X l'intersection de X avec un fermé ou ouvert de Zariski de k^d. (Cette définition générale porte le nom de *topologie induite* sur X par la topologie de Zariski de k^d.)

Ainsi, un fermé de Zariski de X est simplement un fermé de Zariski inclus dans X, tandis qu'un ouvert de Zariski de X est un ensemble de la forme $X \cap (D(f_1) \cup \cdots \cup D(f_r))$. On parlera parfois d'ouvert *relatif* dans X.

2.4 Fermés irréductibles et idéaux premiers

2.4.1. On dit qu'un fermé de Zariski $X \subseteq k^d$ non vide est **irréductible** lorsqu'on ne peut pas l'écrire comme réunion de deux fermés de Zariski strictement plus petits : autrement dit, lorsque $X = X' \cup X''$, où X', X'' sont deux fermés de Zariski (forcément contenus dans X), implique $X' = X$ ou $X'' = X$.

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 $Z(xy)$. Le problème vient manifestement du fait que le polynôme xy n'est pas irréductible. Essayons de préciser les conditions qui font qu'un fermé de Zariski soit irréductible :

Proposition 2.4.2. Un fermé de Zariski $X \subseteq k^d$ est irréductible si, et seulement si, l'idéal $\mathfrak{I}(X)$ est premier.

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

Réciproquement, supposons X irréductible : on veut montrer que $\mathfrak{I}(X)$ est premier. Soient f', f'' tels que $f'f'' \in \mathfrak{I}(X)$: posons $X' = Z(\mathfrak{I}(X) + (f'))$ et $X'' = Z(\mathfrak{I}(X) + (f''))$. On a $X' \subseteq X$ et $X'' \subseteq X$ puisque $X = Z(\mathfrak{I}(X))$, et en fait $X' = X \cap Z(f')$ et $X'' = X \cap Z(f'')$; on a par ailleurs $X = X' \cup X''$ (car si $x \in X$ alors $f'(x)\, f''(x) = 0$ donc soit $f'(x) = 0$ soit $f''(x) = 0$, et dans le premier cas $x \in X'$ et dans le second $x \in X''$). Puisqu'on a supposé X irréductible, on a, disons, $X' = X$, c'est-à-dire $X \subseteq Z(f')$, ce qui signifie $f' \in \mathfrak{I}(X)$ (cf. 2.1.7($*$)). Ceci montre bien que $\mathfrak{I}(X)$ est premier. ☺

2.4.3. En combinant le résultat ci-dessus avec le Nullstellensatz, on voit que (en se rappelant que le corps k est supposé algébriquement clos !) le fermé $Z(\mathfrak{p})$ est irréductible lorsque $\mathfrak{p}$ est un idéal premier de $k[t_1, \ldots, t_d]$.

Notamment, on retient de 1.4.4 que si $f \in k[t_1, \ldots, t_d]$ est un polynôme irréductible, alors $Z(f) = \{x \in k^d : f(x) = 0\}$ est un fermé irréductible. Ceci justifie au moins partiellement la terminologie.

2.4.4. La notion de fermé irréductible peut encore se reformuler de la manière suivante : X est irréductible si et seulement si lorsqu'un ouvert relatif U de X (cf. 2.3.2) est contenu dans un fermé F de X, on a soit $U = \varnothing$ soit $F = X$. (Pour vérifier l'équivalence, on pose $U = X \setminus X'$ et $X'' = F$, et alors $U \subseteq F$ signifie $X' \cup X'' = X$.)

Encore une autre reformulation est la suivante : X est irréductible si et seulement si deux ouverts relatifs non vides U, V de X se rencontrent toujours. (Pour vérifier l'équivalence, on pose $U = X \setminus X'$ et $V = X \setminus X''$, et alors $U \cap V = \varnothing$ signifie $X' \cup X'' = X$.)

Autrement dit, *X est irréductible si et seulement si tout ouvert non vide est dense* (une partie d'un espace topologique étant dite « dense » lorsque le seul fermé qui la contient est l'espace tout entier, ou, de façon équivalente, lorsqu'elle rencontre tout ouvert non vide).

2.5 L'anneau d'un fermé de Zariski : fonctions régulières

2.5.1. On suppose toujours que k est algébriquement clos. Considérons $I \subseteq k[t_1, \ldots, t_d]$ un idéal radical et $X = Z(I)$ le fermé de Zariski qu'il définit. On rappelle que $I = \mathfrak{I}(X)$ par le Nullstellensatz, c'est-à-dire qu'un polynôme $f \in k[t_1, \ldots, t_d]$ s'annule identiquement sur X si et seulement si il est dans I.

Considérons maintenant le morphisme $\Psi\colon k[t_1, \ldots, t_d] \to k^X$ (où k^X désigne la k-algèbre de toutes les fonctions $X \to k$) qui à un polynôme $f \in k[t_1, \ldots, t_d]$ associe la fonction polynomiale correspondante sur X, c'est-à-dire l'application $\Psi(f)\colon X \to k$ donnée par $x \mapsto f(x)$. D'après ce qui vient d'être dit, le noyau de ce morphisme Ψ est I. Par conséquent (cf. 1.1.3), l'image de Ψ s'identifie

à $k[t_1, \ldots, t_d]/I$. L'image de Ψ est par définition l'ensemble des fonctions polynomiales sur X : ce qui vient d'être dit est que la fonction polynomiale $\Psi(f)$ définie par $f \in k[t_1, \ldots, t_d]$ ne dépend que de la classe de f modulo I.

L'anneau $k[t_1, \ldots, t_d]/I$ s'appellera **anneau des fonctions régulières** du fermé de Zariski X. Comme on vient de le signaler, ses éléments peuvent s'identifier aux restrictions à X des fonctions polynomiales sur k^d. On le notera $\mathcal{O}(X)$.

Il sera important de garder à l'esprit les deux points de vue sur les fonctions régulières sur X : on peut les voir soit comme des éléments du quotient $k[t_1, \ldots, t_d]/I$, soit comme des fonctions $X \to k$ qui sont polynomiales.

2.5.2. Par construction, $\mathcal{O}(X)$ est une k-algèbre de type fini (cf. 1.2.7), donc un anneau noethérien (cf. 1.2.8) ; par construction, elle est un anneau *réduit* (puisque I est supposé un idéal radical) ; elle est un anneau *intègre* si et seulement si X est irréductible (cf. 2.4.2) ; et elle est un *corps* si et seulement si X est un singleton (cf. 2.2.2), auquel cas c'est simplement k.

2.5.3. On pourrait refaire une version « relative » des constructions qui ont été faites sur les polynômes : si $\mathscr{F} \subseteq \mathcal{O}(X)$ est un ensemble de fonctions régulières sur X, on peut appeler $Z(\mathscr{F})$ l'ensemble de leurs zéros communs, et si $E \subseteq X$, on peut appeler $\mathfrak{I}_X(E)$ l'ensemble des fonctions régulières sur X qui s'y annulent (c'est simplement l'idéal de $\mathcal{O}(X)$ qui correspond à l'idéal $\mathfrak{I}(E)$ de $k[t_1, \ldots, t_d]$, cf. 1.1.2) ; alors essentiellement tout ce qui a été dit dans les sctions 2.1 et 2.2 vaut encore *mutatis mutandis* : les fonctions Z et $\mathfrak{I}_X$ 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 (cf. 2.3.2) d'autre part. (De plus, si $Y = Z(J)$ est un fermé de Zariski de X défini par un idéal radical J de $\mathcal{O}(X)$, alors $\mathcal{O}(Y) = \mathcal{O}(X)/J$, cf. 1.1.2.) Tout ceci est purement formel, l'intérêt est surtout de se convaincre que les fonctions régulières se comportent bien comme des polynômes.

2.6 L'anneau d'un ouvert relatif : fonctions rationnelles

2.6.1. Si X est une variété algébrique affine (= un fermé de Zariski) et $f \in \mathcal{O}(X)$ une fonction régulière sur X, on a note $D(f) := X \setminus Z(f) = \{x \in X : f(x) \neq 0\}$ l'ensemble des points de X, ou ouvert principal, où f ne s'annule pas (en relevant f de façon quelconque à un polynôme $\tilde{f} \in k[t_1, \ldots, t_d]$, ce $D(f)$ est simplement $X \cap D(\tilde{f})$ où $D(\tilde{f})$ est défini de la même manière sur k^d, cf. 2.3.1).

On définit alors l'**anneau des fonctions régulières** sur $D(f)$ comme le localisé $\mathcal{O}(X)[f^{-1}]$ 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 voir un élément de $\mathcal{O}(X)[f^{-1}]$, disons g/f^n où $g \in \mathcal{O}(X)$ et $n \in \mathbb{N}$, comme une fonction sur $D(f)$: en effet, si $x \in D(f)$, on a $f(x) \neq 0$ par définition, ce qui permet de donner un sens à $g(x)/f(x)^n$. (Par ailleurs, l'identification est légitime car si $g(x)/f(x)^n$ est nul pour tout $x \in D(f)$ alors $g(x)$ aussi, donc $f(x)\,g(x)$ est nul pour tout $x \in X$, ce qui signifie que $g/f^n = 0$ dans $\mathcal{O}(X)[f^{-1}]$ par définition de la localisation.)

Concrètement, donc, une fonction régulière sur $D(f)$ est le quotient d'une fonction régulière sur X (c'est-à-dire la restriction à X d'un polynôme) par une certaine puissance de la fonction f elle-même.

Plus généralement, si $U := D(f_1) \cup \cdots \cup D(f_r)$ est un ouvert relatif quelconque de X, on définit une fonction régulière sur U comme une fonction $U \to k$ dont la restriction à chaque $D(f_i)$ est régulière.

Ces définitions sont assez complexes et peu maniables, donc nous allons considérer le cas beaucoup plus simple où X est irréductible, c'est-à-dire $\mathcal{O}(X)$ intègre, ce qui permet de traiter les localisations comme vivant toutes dans le corps des fractions de $\mathcal{O}(X)$ (cf. 1.3.7).

Index