III Introduction à la géométrie algébrique

1. Un peu d'algèbre commutative

Convention : anneau = anneau commutatif avec 1
morphisme d'anneau = morph. compatible avec la multiplication et qui préserve 1.

Exemple : $A \longrightarrow A \times A$, $a \longmapsto (a,0)$ est un morphisme d'anneaux ssi $A = 0$.

1.1 Radical de Jacobson, racine d'un idéal, nilradical

Soit A un anneau non nul.

Déf : Le radical de Jacobson de A est l'ensemble

$$\mathrm{Rad}A := \{x \in A \mid 1 + ax \text{ est inversible pour tout } a \in A\}.$$

Lemme 1 : a) $\mathrm{Rad}A$ est un idéal de A. On a $1 + \mathrm{Rad}A \subseteq A^*$ et $\mathrm{Rad}A$ est le plus grand idéal avec cette propriété.

b) $\mathrm{Rad}A$ est l'intersection des idéaux maximaux de A.

Dém. : a) Pour $x \in \mathrm{Rad}A$ et $a \in A$, on a $ax \in \mathrm{Rad}A$, par définition.
Soient $x, y \in \mathrm{Rad}A$. On a

$$1 + (x+y) = (1+x) + y \quad \text{et donc} \quad (1+x)^{-1}(1+x+y) = 1 + (1+x)^{-1}y$$

ce qui montre que $1+x+y$ est inversible. Donc $\mathrm{Rad}A$ est un idéal.
Le reste est clair.

b) Montrons que le complémentaire de $\mathrm{Rad}A$ est égal au complémentaire de l'intersection des idéaux maximaux :

$y \notin \mathrm{Rad}A \Rightarrow \exists\, a \in A$ t.q. $1 + ay \notin A^* \Rightarrow A \cdot (1+ay) \neq A$

$\Rightarrow \exists\, \mathfrak{m}$ idéal max. t.q. $(1+ay)\cdot A \subseteq \mathfrak{m}$

$\Rightarrow 1+ay \in \mathfrak{m} \Rightarrow y \notin \mathfrak{m}$ (sinon, on aurait $1 \in \mathfrak{m}$).

$y \notin \bigcap_{\mathfrak{m} \text{ max.}} \mathfrak{m} \Rightarrow \exists\, \mathfrak{m}_0$ max. t.q. $y \notin \mathfrak{m}_0$

$\Rightarrow \exists\, a$ t.q. $1+ay \in \mathfrak{m}_0$ (car $A/\mathfrak{m}_0$ est un corps)

$\Rightarrow 1+ay$ n'est pas inversible

$\Rightarrow y \notin \operatorname{Rad} A$. ✓

<u>Déf</u> : Soit I un idéal de A. La <u>racine</u> de I (="radical" de I) est l'ensemble

$$\sqrt{I} = \{ a \in A \mid \exists\, n \geq 1 \text{ t.q. } a^n \in I \}$$

L'idéal I est <u>radical</u> si $I = \sqrt{I}$.

<u>Lemme 2</u> : a) $\sqrt{I}$ est un idéal, c'est le plus petit idéal radical contenant I. Tout idéal premier est radical.

b) On a $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ pour tout idéal J.

c) $\sqrt{I}$ est l'intersection des idéaux premiers contenant I.

Dém. : a) Clairement si $x \in I$ et $a \in A$, alors $ax \in I$. Soient $x, y \in \sqrt{I}$ et $n, m \geq 1$ t.q. $x^n \in I$ et $x^m \in I$. Alors

$$(x+y)^{n+m} = \sum_{p+q=n+m} \binom{p}{n+m} \underbrace{x^p y^q}_{\in I \text{ car } p \geq n \text{ ou } q \geq m.} \in I$$

Si $x \in \sqrt{\sqrt{I}}$, alors $x^n \in \sqrt{I}$ et $(x^n)^m \in I$ pour des $n, m \geq 1$. Donc $x \in \sqrt{I}$ et on a $\sqrt{\sqrt{I}} = \sqrt{I}$. Si $J \supseteq I$ est radical et $x^n \in I$, alors $x^n \in J$, donc $x \in J$. Donc $J \supseteq \sqrt{I}$. Si $\mathfrak{p}$ est premier et $x^n \in \mathfrak{p}$, alors $x^n = 0$ dans $A/\mathfrak{p}$, qui est intègre. Donc $x = 0$ dans $A/\mathfrak{p}$ et $x \in \mathfrak{p}$. b) Exercice !

c) Montrons que le complémentaire de $\sqrt{I}$ est égal au complémentaire de l'intersection des idéaux premiers contenant I. Si x n'est pas dans l'intersection, alors $x \notin \mathfrak{p}$ pour un premier $\mathfrak{p}$ contenant I. Donc $x^n \notin \mathfrak{p}$, $\forall n \geq 1$, et $x \notin \sqrt{I}$. Réciproquement, supposons que $x \notin \sqrt{I}$. Alors $x^n \notin I$, $\forall n \geq 0$. Considérons l'ens. ordonné $\mathcal{E}$ des idéaux J contenant I t.q. $x^n \notin J$, $\forall n \geq 1$. Alors $\mathcal{E}$ est non vide (car $I \in \mathcal{E}$) et toute famille non vide d'éléments de $\mathcal{E}$ admet une borne supérieure (la réunion). Soit J_0 maximal dans $\mathcal{E}$ (Zorn). Montrons que J_0 est premier. Soient $a, b \in A$ t.q. $a \notin J_0$ et $b \notin J_0$. Alors il existe $n, m \geq 1$ t.q. $x^n \in (a) + J_0$ et $x^m \in (b) + J_0$, par la maximalité de J. Donc $x^{n+m} \in (ab) + J_0$ et $ab \notin J_0$ car $x^{n+m} \notin J_0$. On a montré que $x \notin \sqrt{I}$ implique que $x \notin J_0$ pour l'idéal premier J_0. ✓

<u>Corollaire 3</u> : Soit $S \subseteq A$ une <u>partie multiplicative</u>, i.e. $1 \in S$ et $SS \subseteq S$. Si J_0 est maximal dans l'ens. ordonné des idéaux qui ne rencontrent pas S, alors J_0 est premier.

<u>Déf</u> : Le <u>nilradical</u> de A est l'ensemble des éléments nilpotents de A.

<u>Rque</u> : Le nilradical est donc égal à $\sqrt{(0)}$ et on a

$$\sqrt{(0)} = \bigcap_{\mathfrak{p} \text{ premier}} \mathfrak{p}$$

par le lemme 2. Notons que $\sqrt{(0)} \subseteq \operatorname{Rad} A$.

1.2 Théorème de Cayley-Hamilton et lemme de Nakayama

Soit A un anneau commutatif.

<u>Thm 1</u> (Cayley-Hamilton*, 1858 resp. 1853): Soient M un A-module de type fini et $u: M \to M$ un endomorphisme. Alors il existe un polynôme <u>unitaire</u> qui annule u, i.e. on a

$$u^n + a_1 u^{n-1} + \dots + a_n 1_M = 0$$

pour des $a_i \in A$. De plus, si l'on a $u(M) \subseteq JM$ pour un idéal J de A, on peut trouver $a_i \in J^i$.

Dém.: Supposons que M est engendré par $m_1, \dots, m_n$ et que $u(M) \subseteq JM$ (p.ex. $J = A$). Nous avons

$$(1) \qquad u(m_i) = \sum_{j=1}^{n} a_{ij} m_j$$

pour des $a_{ij} \in J$. Considérons M comme un module sur $A[X]$, où X agit par u. Ecrivons

$$m = \begin{bmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{bmatrix} \in M^n, \quad I_n = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix} \in M_n(A).$$

Alors (1) nous donne

$$(2) \qquad (X \cdot I_n - A) \cdot m = 0$$

dans M^n considéré comme $A[X]$-module. Soit $B \in M_n(A[X])$ la transposée de la comatrice de $X \cdot I_n - A$. Si on multiplie (2) à gauche par B, on obtient

---

*Arthur Cayley, 1821 (Richmond) – 1895 (Cambridge)
Sir William Rowan Hamilton, 1805 (Dublin) – 1865 (Dublin)

$$\det(X\cdot I_n - A)\cdot I_n \cdot m = 0.$$

Mais alors on a

$$\det(X\cdot I_n - A)\, m_i = 0, \quad 1 \leq i \leq n,$$

et $P(X) = \det(X\cdot I_n - A)$ annule M considéré comme $A[X]$-module.
Donc $P(u)$ est nul en tant qu'endomorphisme de M. ✓

<u>Cor. 2</u> : Soit M un A-module de type fini.
a) Tout endomorphisme surjectif de M est bijectif.
b) Si M est libre de rang fini n, toute famille génératrice formée de n éléments est une base.

<u>Rque</u> : Par b), on a : $A^n \cong A^m \Longrightarrow n = m$.
Ceci n'est pas vrai en général pour les anneaux non-commutatifs. Par exemple, si $\Lambda = \mathrm{End}_A(A^{(\mathbb{N})})$, on a un isom. de Λ-modules (à droite)

$$\Lambda \xrightarrow{\sim} \Lambda \oplus \Lambda$$

induit par tout isomorphisme de A-modules $A^{(\mathbb{N})} \xrightarrow{\sim} A^{(\mathbb{N})} \oplus A^{(\mathbb{N})}$

Dém. du cor. : a) Soit $f : M \longrightarrow M$ un endom. surjectif. On considère M comme un $A[X]$-module, où X agit par f. Pour $J = (X)$, on a $JM = M$ car f est surjectif. On applique le théorème de Cayley-Hamilton à $u = \mathbb{1}_M$. On a

$$u^n + a_1 u^{n-1} + \dots + a_n = 0$$

pour des $a_i \in (X)$. Cela se réécrit

$$\mathbb{1}_M - f\cdot Q(f) = 0$$

pour un $Q \in A[X]$. Alors $Q(f)$ est inverse de f.

b) résulte de a) : Si M est libre de base $e_1, \dots, e_n$ et $m_1, \dots, m_n$ est génératrice, alors l'endomorphisme

$$M \longrightarrow M, \; e_i \longmapsto m_i$$

est surjectif, donc bijectif, donc $m_1, \dots, m_n$ est une base. ✓

<u>Cor. 3</u> : Si M est de type fini et $I \subseteq A$ un idéal t.q. $IM = M$, alors il existe $x \in I$ t.q. $(1-x)M = 0$.

Dém. : On applique le thm de Cayley-Hamilton à $u = 1_M$. On obtient

$$1_M + a_1 1_M + \dots + a_n 1_M = 0$$

et on pose $x = -a_1 - \dots - a_n$. ✓

<u>Cor. 4</u> ("Lemme de Nakayama*", 1951) Soient I un idéal contenu dans $\operatorname{Rad} A$ et M un A-module <u>de type fini</u>.

a) Si $IM = M$, alors $M = 0$.

b) Si les images de $m_1, \dots, m_n \in M$ engendrent M/IM, alors $m_1, \dots, m_n$ engendrent M.

⚠ En général, le fait que M/IM soit de type fini n'implique pas que M soit de type fini (p.ex. k corps, $A = k[[X]]$, $I = (X)$, $M = \operatorname{Frac} A$)

Dém. du cor. : a) Par le corollaire précédent, il existe $x \in \operatorname{Rad} A$ t.q. $(1-x)M = 0$. Or l'élément $1-x$ est inversible. Donc $M = 0$.

b) Soit $N = M/Am_1 + \dots + Am_n$. Alors

$$N/IN = M/(IM + Am_1 + \dots + Am_n) = 0.$$

Donc $N = IN$ et $N = 0$ par a). Cela donne $M = Am_1 + \dots + Am_n$. ✓

---

* Nakayama, Tadashi (中山正), 1912 (Tokyo) – 1964 (Nagoya)

1.3 Extensions finies et entières

Soient A un anneau et B une A-algèbre.

Déf : B est une <u>A-algèbre de type fini</u> si, <u>en tant que A-algèbre</u>, elle est engendrée par un nombre fini d'éléments.

B est une <u>A-algèbre finie</u> si, <u>en tant que A-module</u>, elle est engendrée par un nombre fini d'éléments.

Un élément $x \in B$ est <u>entier sur A</u> s'il est annulé par un polynôme <u>unitaire</u> à coefficients dans A.

B est <u>entier sur A</u> si tout élément de B est entier sur A.

B est une <u>extension entière</u> de A si de plus l'appl. can. $A \to B$ est injective.

Rqu : B est une A-alg. de type fini ssi elle est quotient d'une algèbre de polynômes $A[X_1, \dots, X_n]$. Elle est finie ssi en tant que A-module, elle est quotient d'un module libre de type fini A^n.

Prop. 1 : Soit $A \hookrightarrow B$ une extension d'anneaux et $x \in B$.

$\Updownarrow$

i) x est entier sur A.

ii) $A[x]$ est une A-algèbre finie, libre comme A-module.

iii) Il existe une A-algèbre finie A' t.q. $A \subseteq A[x] \subseteq A' \subseteq B$.

Dém : i) $\Rightarrow$ ii) Si x est annulé par un polynôme unitaire P à coeff. dans A et de degré n, alors le A-module $A[x]$ est engendré librement par $1, x, \dots, x^{n-1}$ (division euclidienne par P !).

ii) $\Rightarrow$ iii) On prend $A' = A[x]$.

iii) $\Rightarrow$ i) On considère la multiplication par x :

$$u : A' \longrightarrow A', \; a' \longmapsto xa'.$$

Comme A' est un A-module de type fini, d'après le thm de Cayley-Hamilton, il existe un polynôme unitaire $P \in A[X]$ t.q. $P(u) = 0$. Mais alors $P(x) = P(u).1$ s'annule. ✓

<u>Cor. 2</u>: Toute extension finie $A \hookrightarrow B$ est entière.

<u>Prop. 3</u>: Soient $A \hookrightarrow B \hookrightarrow C$ des homomorphismes d'anneaux injectifs.

a) $A \hookrightarrow B$ finie et $B \hookrightarrow C$ finie $\Rightarrow$ $A \hookrightarrow C$ finie

b) $y_1, \dots, y_n \in B$ entiers sur A $\Rightarrow$ $A[y_1, \dots, y_n]$ finie sur A.

c) $A \hookrightarrow B$ entier et $B \hookrightarrow C$ entier $\Rightarrow$ $A \hookrightarrow C$ entier.

Dém.: a) Si B est engendré par $x_1, \dots, x_p$ comme A-module et C engendré par $y_1, \dots, y_q$ comme B-module, alors C est engendré par $x_i y_j$, $1 \leq i \leq p$, $1 \leq j \leq q$, comme A-module.

b) résulte de a) par récurrence sur n.

c) Soit $c \in C$. Comme c est entier sur B, on a

$$c^n + b_1 c^{n-1} + \dots + b_n = 0$$

pour des $b_i \in B$. Donc $A[c]$ est fini sur $A[b_1, \dots, b_n]$, qui est fini sur A, par b). Donc $A[c]$ est fini sur A, par a), et c entier sur A. ✓

Déf: Soit $A \hookrightarrow B$ une extension d'anneaux. La <u>clôture entière</u> de A dans B est l'ensemble $\tilde{A}$ des éléments de B entiers sur A.

A est <u>intégralement clos dans B</u> si $\tilde{A} = B$.

Si A est intègre, A est <u>intégralement clos</u> si A est intégralement clos dans son corps de fractions.

<u>Lemme 4</u> : a) $\tilde{A}$ est une ss-algèbre de B.

b) $A \subseteq \tilde{A}$ est une extension entière.

c) On a $\tilde{\tilde{A}} = \tilde{A}$.

Dém. : a) Clairement, on a $A \subseteq \tilde{A}$. Pour $b_1, b_2 \in \tilde{A}$, on sait que $A[b_1, b_2]$ est fini sur A. Donc $1_A, b_1+b_2, -b_1, b_1 b_2$ sont dans $\tilde{A}$.

b) Par définition des extensions entières.

c) On a $\tilde{A} \subseteq \tilde{\tilde{A}}$. Comme les extensions $A \subseteq \tilde{A}$ et $\tilde{A} \subseteq \tilde{\tilde{A}}$ sont entières, $\tilde{\tilde{A}}$ est entier sur A. Donc $\tilde{\tilde{A}} \subseteq \tilde{A}$. ✓

<u>Lemme 5</u> : Tout anneau factoriel est intégralement clos.

Dém. : Soient C un anneau factoriel et $r/s \in \mathrm{Frac}(C)$, où r et s sont premiers entre eux. Supposons que

$$(r/s)^n + c_1 (r/s)^{n-1} + \dots + c_n = 0$$

Alors on a

$$r^n + s \cdot (c_1 r^{n-1} + \dots + c_n s^{n-1}) = 0$$

Comme r et s sont premiers entre eux, s doit être inversible dans C. ✓

<u>Prop. 6</u> : Soit $A \subseteq B$ une extension et P un polynôme <u>unitaire</u> à coefficients dans A. Si on a

$$P = Q \cdot R$$

pour des polynômes <u>unitaires</u> Q et R dans $B[X]$, alors les coefficients de Q et R sont entiers sur A.

Dém. : Soient $C_1 = B[T]/(Q)$ et $\alpha_1 \in C_1$ l'image de T. Alors $Q(\alpha_1) = 0$ et comme Q est unitaire, on a $Q = (X - \alpha_1) \cdot Q_1$ dans $C_1[X]$. Notons que C_1 est un B-module <u>libre</u> de base

$1, \alpha_1, \dots, \alpha_1^{(\deg Q)-1}$ puisque Q est unitaire (division euclidienne). En particulier, l'homomorphisme can. $B \to C$, est injectif. En itérant cette construction on construit une extension d'anneaux $B \hookrightarrow C$ telle que

$$Q = \prod (X - \alpha_i), \quad R = \prod (X - \beta_j)$$

dans $C[X]$. Les α_i et β_j sont entiers sur A (car annulés par P). Donc les coeff. de Q et R sont entiers sur A. ✓

<u>Cor. 7</u> ("Lemme de Gauss*"): Supposons A intégralement clos. Si $P \in A[X]$ est unitaire et se factorise $P = QR$ pour des polynômes unitaires Q, R à coeff. dans $\mathrm{Frac}(A)$, alors Q et R sont à coeff. dans A.

<u>Prop. 8</u>: A intégralement clos $\Rightarrow$ $A[X]$ intégralement clos.

<u>Rque</u>: La réciproque est vraie aussi (!).

Dém.: Nous avons $\mathrm{Frac}(A[X]) \cong K(X)$, où $K = \mathrm{Frac}(A)$. Soit $F \in K(X)$ entier sur $A[X]$. Alors F est en particulier entier sur $K[X]$. Comme $K[X]$ est factoriel, on a $F \in K[X]$. Supposons que

$$F^n + a_1 F^{n-1} + \dots + a_n = 0$$

pour des $a_i \in A[X]$. Alors

$$F \cdot (F^{n-1} + a_1 F^{n-2} + \dots + a_{n-1}) = -a_n$$

dans $A[X]$. Pour pouvoir appliquer le lemme de Gauss, on aimerait

---

* Johann Carl Friedrich Gauss, 1777 (Brunswick) – 1855 (Göttingen)

remplacer F et $(F^{n-1}+\dots+a_{n-1})$ par des polynômes unitaires. Ecrivons

$$F = X^r + G$$

où r est un entier $> \deg F$ et $> \deg a_i$ pour $1 \leq i \leq n$. Alors

$$(X^r+G)^n + a_1 (X^r+G)^{n-1} + \dots + a_n = 0$$

et donc

$$G^n + b_1 G^{n-1} + \dots + b_n = 0,$$

où

$$-b_n = X^{rn} + a_1 X^{r(n-1)} + \dots + a_n.$$

On a

$$-b_n = (-G)(-G^{n-1} - a_1 G^{n-2} - \dots - a_{n-1})$$

et c'est une factorisation en un produit de deux polynômes unitaires. Par le lemme de Gauss, on a $-G \in A[X]$. Donc $F \in A[X]$. ✓

1.4 Lemme de normalisation de Noether

Soit k un corps. Soit A une k-algèbre.

Déf. : Des éléments $a_1, \dots, a_n$ de A sont

- <u>algébriquement liés</u> s'il existe un polynôme $0 \neq P \in k[X_1, \dots, X_n]$ t.q. $P(a_1, \dots, a_n) = 0$;
- <u>algébriquement indépendants</u> s'ils ne sont pas alg. liés, i.e. $\forall P \in k[X_1, \dots, X_n]$: $P(a_1, \dots, a_n) = 0 \Rightarrow P = 0$.

A est une <u>extension algébrique pure</u> si $A = k[a_1, \dots, a_n]$ pour des éléments alg. indép. $a_1, \dots, a_n$ de A.

<u>Thm 9</u> ("Lemme de normalisation de E. Noether*", 1926): Soit A une k-algèbre de type fini. Alors il existe des éléments algébriquement indépendants $y_1, \dots, y_m$ dans A tels que A soit une extension finie de $k[y_1, \dots, y_m]$.

<u>Rque</u>: On a donc

$$\begin{array}{c} A \\ \cup\!\!\mid \text{ finie} \\ k[y_1, \dots, y_m] \\ \cup\!\!\mid \text{ algébrique pure} \\ k \end{array} \quad \text{type fini}$$

<u>Lemme 10</u>: Soit A une k-alg. de type fini engendrée par des éléments $x_1, \dots, x_n$ alg. liés. Alors il existe $x_1', \dots, x_{n-1}'$ dans A t.q. x_n est entier sur $A' = k[x_1', \dots, x_{n-1}']$ et $A = A'[x_n]$.

Dém. du thm à partir du lemme: Supposons que A est engendrée par des éléments $x_1, \dots, x_n$. On procède par récurrence sur n. Pour $n = 0$, on prend $m = 0$. Supposons $n \geq 1$. Si $x_1, \dots, x_n$ sont alg. indép., on prend $m = n$, $y_i = x_i$, $1 \leq i \leq n$. Sinon, le lemme s'applique: il existe $x_1', \dots, x_{n-1}'$ t.q. x_n est entier sur $A' = k[x_1', \dots, x_{n-1}']$ et que $A = A'[x_n]$. Par l'hypothèse de récurrence, il existe $y_1, \dots, y_m$ alg. indép. dans A' t.q. A' est finie sur $k[y_1, \dots, y_m]$. Alors $A = A'[x_n]$ est finie sur $k[y_1, \dots, y_m]$. ✓

Dém. du lemme: Soit $0 \neq P \in k[X_1, \dots, X_n]$ t.q. $P(x_1, \dots, x_n) = 0$.

<u>Première méthode</u> (Nagata, 1962): On cherche les x_i' sous la forme

$$x_i' = x_i - x_n^{e_i}, \quad 1 \leq i \leq n-1,$$

---

* Emmy Amalie Noether, 1882 (Erlangen) - 1935 (Bryn Mawr, Pennsylvania)

pour un entier e assez grand. Pour tout choix de $e \geq 1$, on a $k[x_1', \dots, x_{n-1}', x_n] = A$. En outre, on a

$$0 = P(x_1, \dots, x_n) = P(x_1' + x_n^e, x_2' + x_n^{e^2}, \dots, x_{n-1}' + x_n^{e^{n-1}}, x_n)$$
$$= Q(x_1', x_2', \dots, x_{n-1}', x_n)$$

pour un $Q \in k[X_1', \dots, X_{n-1}', X_n]$. On aimerait que le coeff. dominant de $Q(x_1', \dots, x_{n-1}', X_n) \in A'[X_n]$ soit une constante inversible (car cela impliquerait que x_n soit entier sur A). Pour tout monôme $X_1^{a_1} \dots X_n^{a_n}$ apparaissant dans P, on a

$$X_1^{a_1} \dots X_n^{a_n} = \left(\prod_{i=1}^{n-1} (X_i' + X_n^{e^i})^{a_i}\right) X_n^{a_n}$$
$$= X_1'^{a_1} \dots X_{n-1}'^{a_{n-1}} X_n^{a_n} + \dots + X_n^{a_1 e + a_2 e^2 + \dots + a_{n-1} e^{n-1} + a_n}$$

Le dernier terme est l'unique terme de plus haut degré en X_n. Si e est strictement plus grand que tous les exposants a_i qui apparaissent dans les monômes de P, alors le degré

$$a_1 e + a_2 e^2 + \dots + a_{n-1} e^{n-1} + a_n \quad (*)$$

détermine les a_i : ce sont les chiffres de l'écriture de $(*)$ en base e. Donc des monômes distincts de P fournissent des puissances distinctes de X_n dans $Q(x_1', \dots, x_{n-1}', X_n)$. Une seule de ces puissances est maximale et elle apparaît avec un coeff. dans k^*.

<u>Deuxième méthode</u> (E. Noether) : Cette méthode ne s'applique que quand k est infini, ce qu'on suppose maintenant. On cherche les x_i' sous la forme

$$x_i' = x_i - c_i x_n, \quad 1 \leq i \leq n-1,$$

pour des $c_i \in k$ à déterminer. Soit d le degré total de P et soit Q la somme des termes de degré d de P. Alors les coefficients dominants de X_n dans

$$P(x_1' + c_1 X_n, \dots, x_{n-1}' + c_{n-1} X_n, X_n)$$

et $Q(x_1' + c_1 X_n, \dots, x_{n-1}' + c_{n-1} X_n, X_n)$

sont égaux. On a

$$Q(x_1' + c_1 X_n, \dots, x_{n-1}' + c_{n-1} X_n, X_n) = X_n^d \, Q(c_1, \dots, c_{n-1}, 1) + R,$$

R de degré $< d$ en X_n. Comme $Q(X_1, \dots, X_{n-1}, 1)$ est un polynôme non nul (car le polynôme homogène $Q(X_1, \dots, X_{n-1}, X_n)$ est non nul) il existe des $c_1, \dots, c_{n-1} \in k$ t.q. $Q(c_1, c_2, \dots, c_{n-1}, 1) \neq 0$, par le lemme suivant. ✓

<u>Lemme 11</u> : Soient k un corps infini et $P \in k[X_1, \dots, X_n]$ un polynôme non nul. Alors il existe $x_1, \dots, x_n \in k$ t.q. $P(x_1, \dots, x_n) \neq 0$.

Dém. : Montrons par récurrence sur n que

$$P(x_1, \dots, x_n) = 0, \ \forall x \in k^n \Longrightarrow P = 0.$$

C'est bien connu pour $n = 1$. Supposons $n \geq 2$. Écrivons $P = \sum_{i=0}^{N} A_i X^i$ où $A_i \in k[X_1, \dots, X_{n-1}]$, $0 \leq i \leq n$. Pour tous $x_1, \dots, x_{n-1} \in k$, le polynôme

$$P(x_1, \dots, x_{n-1}, X_n) = \sum_{i=1}^{N} A_i(x_1, \dots, x_{n-1}) \cdot X^i$$

s'annule en tout $x_n \in k$. Donc les $A_i(x_1, \dots, x_{n-1})$ s'annulent (cas $n = 1$). Donc les A_i s'annulent (récurrence). ✓

1.5 Nullstellensatz (théorème des zéros)

<u>Lemme 1</u> : Soit $A \subseteq B$ une extension entière d'anneaux intègres.
Alors A est un corps ssi B est un corps.

Dém. : "$\Rightarrow$" Soit $0 \neq x \in B$. Comme x est entier sur A, le A-espace vectoriel $A[x]$ est de dimension finie. La mult. par x est un endomorphisme injectif donc bijectif de $A[x]$. Elle atteint donc 1.

"$\Leftarrow$" Soit $0 \neq x \in A$. Soit $y \in B$ l'inverse de x. Comme y est entier sur A, on a

$$y^n + a_1 y^{n-1} + \dots + a_n = 0$$

pour des $a_i \in A$. En multipliant par x^{n-1} on trouve

$$y + a_1 + a_2 x + \dots + a_n x^{n-1} = 0$$

ce qui montre que y est dans A. ✓

<u>Théorème 2</u> (Nullstellensatz faible, Hilbert*, 1893) : Soient k un corps et K une k-algèbre <u>de type fini</u> qui est un corps. Alors l'extension $K \supseteq k$ est <u>finie</u>.

Dém. : Par le lemme de normalisation, il existe $y_1, \dots, y_m$ algébriquement indépendants dans K tels que K est fini sur $k[y_1, \dots, y_m]$. Par le lemme 1, $k[y_1, \dots, y_m]$ doit être un corps. Donc $m = 0$ et K est fini sur k. ✓

<u>Rques</u> : 1) Si k est non dénombrable, ce théorème est "une trivialité" : Si K n'est pas fini sur k, il n'est pas algébrique. Donc il existe

---

* David Hilbert, 1862 (Königsberg = Калининград) – 1943 (Göttingen)

$x \in K$ qui est transcendant sur k. Mais alors les éléments

$$\frac{1}{x-\alpha}, \quad \alpha \in k,$$

sont linéairement indépendants sur k (unicité de la décomposition en éléments simples). Donc K est de dimension non dénombrable sur k. C'est absurde car K est quotient d'une algèbre de polynômes en un nombre fini de variables.

2) Le Nullstellensatz affirme : les idéaux maximaux de $k[X_1, \dots, X_n]$ sont de codimension finie. Si k est alg. clos, ils sont même de codimension 1 (car alors k n'admet pas d'extension finie non triviale).

<u>Cor. 3</u> : Si k est un corps alg. clos, les idéaux maximaux de $k[X_1, \dots, X_n]$ sont exactement les idéaux

$$m_x = (X_1 - x_1, X_2 - x_2, \dots, X_n - x_n)$$

associés aux points $x = (x_1, x_2, \dots, x_n)$ de k^n.

Dém. : Pour $x \in k^n$, l'évaluation

$$k[X_1, \dots, X_n] \longrightarrow k, \quad P \longmapsto P(x)$$

induit un isomorphisme

$$k[X_1, \dots, X_n]/m_x \xrightarrow{\sim} k.$$

Donc les m_x sont bien maximaux. Si m est maximal quelconque, on a un isomorphisme

$$\varphi : k[X_1, \dots, X_n]/m \xrightarrow{\sim} k$$

grâce au Nullstellensatz et au fait que k soit alg. clos. Soit $x_i = \varphi(X_i)$, $1 \leq i \leq n$. Alors clairement $m_x \subseteq m$. Donc $m_x = m$ par maximalité. ✓

<u>Cor. 4</u> : Un système d'équations polynomiales

$$\left.\begin{array}{c} F_1(x_1,\dots,x_n)=0 \\ \vdots \\ F_r(x_1,\dots,x_n)=0 \end{array}\right\} (*)$$

à coeff. dans un corps alg. clos k n'admet aucune solution $x \in k^n$ ssi il existe des $G_i \in k[X_1,\dots,X_n]$, $1 \leq i \leq r$, t.q.

$$\sum_{i=1}^{r} G_i F_i = 1.$$

Dém. : Soit I l'idéal de $k[X_1,\dots,X_n]$ engendré par les F_i.

Alors

$$\begin{aligned} (*) \text{ n'a pas de solution} &\iff I \not\subset m_x, \quad \forall x \in k^n \\ &\iff I \not\subset m, \quad \forall m \text{ max. de } k[X_1,\dots,X_n] \\ &\iff I = k[X_1,\dots,X_n] \\ &\iff 1 \in I. \end{aligned}$$

✓

2. Variétés algébriques affines

2.1 Parties algébriques et idéaux

Soit k un corps.

<u>Déf</u> : Une partie $X \subseteq k^n$ est <u>algébrique</u> (ou : est une <u>ss-variété alg. fermée de k^n</u>) s'il existe une famille de polynômes P_i, $i \in I$, $P_i \in k[X_1,\dots,X_n]$, t.q.

$$X = \{x \in k^n \mid P_i(x) = 0, \ \forall i \in I\}.$$

Si J est un idéal de $k[X_1,\dots,X_n]$, le <u>lieu d'annulation</u> de J est la partie algébrique

$$V(J) = \{x \in k^n \mid P(x) = 0, \ \forall P \in J\} \subseteq k^n$$

(V = "variété" = "vanishing set"). Si $Y \subseteq k^n$ est une partie

quelconque, <u>l'idéal associé à Y</u> est

$$I(Y) = \{ P \in k[X_1, \dots, X_n] \mid P(y) = 0, \ \forall y \in Y \}.$$

<u>Rques</u> : 1) Une famille de polynômes $(P_i)_{i \in I}$ et l'idéal J qu'elle engendre ont même lieu d'annulation. Donc toute partie algébrique de k^n est de la forme $V(J)$ pour un idéal J.

3) Les applications

$$\{\text{parties de } k^n\} \underset{V}{\overset{I}{\rightleftarrows}} \{\text{idéaux de } k[X_1, \dots, X_n]\}$$

sont décroissantes. On a

$$I(\emptyset) = k[X_1, \dots, X_n], \quad I(k^n) = (0) \text{ si } k \text{ est infini (L1.4.11)}$$

$$V(k[X_1, \dots, X_n]) = \emptyset, \quad V((0)) = k^n$$

4) Pour toute partie $X \subseteq k^n$, on a $V(I(X)) \supseteq X$ et on a l'égalité ssi X est algébrique ("$\Rightarrow$" clair, "$\Leftarrow$" : si $X = V(J)$, alors $J \subseteq I(X)$ donc $V(I(X)) \subseteq V(J) = X \subseteq V(I(X))$)

2) Tout idéal J de $k[X_1, \dots, X_n]$ est de type fini (car $k[X_1, \dots, X_n]$ est noethérien). Donc toute partie alg. de k^n est le lieu d'annulation d'une famille <u>finie</u> de polynômes.

5) Soit J un idéal de $k[X_1, \dots, X_n]$. On a $I(V(J)) \supseteq J$.

Deux obstructions à l'égalité :

- si k n'est pas alg. clos, on peut avoir $J \subsetneq k[X_1, \dots, X_n]$ et $V(J) = \emptyset$ donc $I(V(J)) = k[X_1, \dots, X_n] \supsetneq J$.
- on a $V(J) = V(\sqrt{J})$, donc $J \subseteq \sqrt{J} \subseteq I(V(J))$ et $J = \sqrt{J}$ est une cond. nécessaire pour avoir $J = I(V(J))$.

<u>Thm 1</u> (Nullstellensatz fort) : Supposons k alg. clos. Alors on a $I(V(J)) = \sqrt{J}$ pour tout idéal J de $k[X_1, \dots, X_n]$.

Dém (astuce de Rabinowitch, 1929) : Soient $F_1, \dots, F_m$ des générateurs de J et soit $P \in I(V(J))$. Alors les polynômes

$$F_1, \dots, F_m, \quad X_{n+1} \cdot P - 1 \in k[X_1, \dots, X_{n+1}]$$

n'ont pas de racine commune dans k^{n+1}. Donc (cor. 1.5.4), il existe $G_1, \dots, G_{m+1}$ dans $k[X_1, \dots, X_{n+1}]$ tels que

$$1 = G_1 F_1 + \dots + G_m F_m + G_{m+1} \cdot (X_{n+1} P - 1). \qquad (*)$$

On a un homomorphisme d'anneaux

$$\begin{aligned} k[X_1, \dots, X_{n+1}] &\longrightarrow k(X_1, \dots, X_n) \\ X_i &\longmapsto X_i, \quad 1 \leq i \leq n \\ X_{n+1} &\longmapsto 1/P. \end{aligned}$$

L'image de l'équation $(*)$ par cet homomorphisme est

$$1 = G_1(X_1, \dots, X_n, 1/P) \cdot F_1 + \dots + G_m(X_1, \dots, X_m, 1/P) \cdot F_m.$$

Si on multiplie des deux côtés par une puissance assez élevée P^N, on obtient une équation dans $k[X_1, \dots, X_n]$, qui montre que P^N est dans l'idéal engendré par $F_1, \dots, F_m$. ✓

2.2 Topologie de Zariski

Soient k un corps algébriquement clos et n un entier naturel.

<u>Lemme 1</u> : a) On a $V(k[X_1,\dots,X_n]) = \emptyset$ et $V((0)) = k^n$.

b) Pour tous idéaux J_1, J_2 de $k[X_1,\dots,X_n]$, on a
$$V(J_1) \cup V(J_2) = V(J_1 \cap J_2) = V(J_1 J_2).$$

c) Pour toute famille d'idéaux $(J_i)_{i\in I}$ de $k[X_1,\dots,X_n]$, on a
$$\bigcap_{i\in I} V(J_i) = V\Big(\sum_{i\in I} J_i\Big).$$

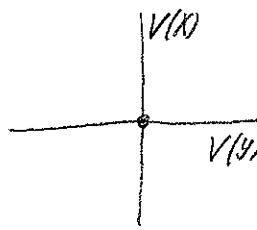
Dém. : a) et c) sont faciles. Montrons b) : on a $J_1 J_2 \subseteq J_1 \cap J_2 \subseteq J_i$ pour $i = 1,2$. Donc
$$V(J_1) \cup V(J_2) \subseteq V(J_1 \cap J_2) \subseteq V(J_1 J_2).$$

Réciproquement, si $x \in k^n$ est dans le complémentaire de $V(J_1) \cup V(J_2)$, il existe $P_i \in J_i$ t.q. $P_i(x) \neq 0$, $i = 1,2$. Donc $P_1 P_2(x) \neq 0$ et x est dans le complémentaire de $V(J_1 J_2)$. ✓

<u>Déf</u> : La <u>topologie de Zariski</u>* sur k^n est la topologie dont les fermés sont les $V(J)$, où J parcourt les idéaux de $k[X_1,\dots,X_n]$. La <u>topologie de Zariski</u> sur une partie algébrique $X \subseteq k^n$ est la topologie induite.

<u>Exemples</u> : 1) Les parties fermées propres de k (muni de la top. de Zariski) sont les parties finies. Donc k n'est pas réunion de deux fermés propres (et deux ouverts non vides ont toujours une intersection non vide).

2) La partie alg. $V(XY) \subseteq k^2$ est réunion deux deux fermés propres : $V(X)$ et $V(Y)$.



---

*Oscar Zariski, 1899 (Kobrin, Bélorussie) – 1986 (Brookline, É.-U.)

Déf. : Un espace topologique est <u>irréductible</u> s'il n'est pas réunion de deux fermés propres.

<u>Lemme 2</u> : Soit X un espace topologique. On a équivalence entre

i) X est irréductible.

ii) Si X_1 et X_2 sont des fermés de X, alors
$$X = X_1 \cup X_2 \implies X = X_1 \text{ ou } X = X_2$$

iii) Deux ouverts non vides de X ont une intersection non vide.

iv) Tout ouvert non vide de X est dense.

Dém. : exercice ! ✓

<u>Rques</u> : 1) Tout espace irréductible est connexe (mais la réciproque est fausse).

2) Un ss-espace d'un esp. top. est irréd. ssi son adhérence l'est (exo).

3) Un ouvert non vide d'un espace irréd. est irréd.

<u>Lemme 3</u> : Soit $X \subseteq k^n$ une partie algébrique.
$$X \text{ est irréductible} \iff I(X) \text{ est première.}$$

Dém. : Montrons que X est réductible ssi $I(X)$ n'est pas première.

"$\Leftarrow$" : Il existe des polynômes P_1, P_2 n'appartenant pas à $I(X)$ t.q. $P_1 \cdot P_2 \in I(X)$. Alors X est réunion de ses fermés propres $X \cap V(P_1)$ et $X \cap V(P_2)$.

"$\Rightarrow$" : Soient $X_1, X_2 \subsetneq X$ des fermés propres tels que $X = X_1 \cup X_2$. Alors on a $I(X) = I(X_1) \cap I(X_2)$ et $I(X_i)$ contient strictement $I(X)$, $i = 1, 2$, (k est algébriquement clos). Mais alors $I(X)$ n'est pas première. ✓

<u>Exemples</u> : k^n est irréductible ; $Gl_n(k) \subset M_n(k)$ est irréductible car ouvert non vide dans $M_n(k)$ (identifié à $k^{n \times n}$).

<u>Déf.</u> : Un espace top. est <u>noethérien</u> si toute suite croissante d'ouverts $U_0 \subseteq U_1 \subseteq \dots \subseteq U_p \subseteq \dots$, $p \in \mathbb{N}$, devient stationnaire : $U_r = U_{r+1}$, $\forall r \gg 0$.

<u>Rques</u> : 1) C'est le cas ssi toute suite décroissante de fermés devient stationnaire ssi toute famille d'ouverts contient un élément maximal ssi toute famille de fermés contient un élément minimal.

2) Tout ss-espace d'un espace noethérien est noethérien.

<u>Lemme 4</u> : k^n est noethérien.

Dém. : Les suites décroissantes de fermés correspondent bijectivement aux suites croissantes d'idéaux radicaux de $k[X_1, \dots, X_n]$. Ces suites deviennent stationnaires car $k[X_1, \dots, X_n]$ est noethérien. ✓

<u>Déf.</u> : Une <u>composante irréductible</u> d'un espace top. est une partie irréductible maximale.

<u>Exemple</u> : Les compos. irréd. d'un espace séparé sont ses parties ponctuelles.

<u>Lemme 5</u> : Soit X un espace top.

a) Les compos. irréd. de X sont fermées et X est leur réunion.

b) Si $X = F_1 \cup \dots \cup F_r$ pour des fermés irréd. F_i t.q. $F_i \not\subseteq F_j$ pour tous $i \neq j$, alors les F_i sont les compos. irréd. de X.

c) Si X est noethérien, il n'admet qu'un nombre fini de composantes irréductibles.

Dém. : a) Soit $Y \subseteq X$ une compos. irréd.. Alors $\overline{Y}$ est encore irréd.. Donc on a $Y = \overline{Y}$ par maximalité de Y. Soit $x \in X$. Alors $\{x\}$ est irréductible donc contenue dans une compos. irréd. de X (Zorn).

b) Soit $Y \subseteq X$ une compos. irréd.. Alors Y est la réunion

finie des fermés $Y \cap F_i$, $1 \leq i \leq r$. Comme Y est irréd., on a $Y = Y \cap F_i$ pour un i. Donc $Y \subseteq F_i$. Comme Y est irréd. maximal et F_i irréd., on a $Y = F_i$. Réciproquement, montrons que chaque F_i est une compos. irréd.. On a $F_i \subseteq Y$ pour une compos. irréd. Y. Or $Y = F_j$ pour un $1 \leq j \leq r$. Donc $F_i \subseteq Y = F_j$ ce qui entraîne $i = j$ et $F_i = Y$.

c) Par b), il suffit de montrer que X est réunion finie de parties fermées irréductibles. Soit C l'ensemble des fermés de X qui ne sont pas réunion finie de fermés irréductibles. On suppose $C \neq \emptyset$. Comme X est noethérien, C contient un élément minimal F. Comme $F \in C$, F est réductible : on a $F = F_1 \cup F_2$ pour deux fermés propres F_1 et F_2 de F. Par minimalité de F, les F_i sont des réunions finies de fermés irréductibles. Donc F l'est. ↯. ✓

<u>Cor. 6</u> : Tout idéal radical de $k[X_1, \dots, X_n]$ est intersection finie d'idéaux premiers.

Dém. : Soit J un idéal radical. Alors on a $J = I(X)$ pour $X = V(J)$ par le Nullstellensatz fort (Thm 2.1.1). Comme $X \subseteq k^n$ est noethérien (L4), il est réunion finie de ses composantes irréductibles (L5c)

$$X = Y_1 \cup \dots \cup Y_r .$$

Donc $J = I(X) = I(Y_1) \cap \dots \cap I(Y_r)$ et les $I(Y_i)$ sont premiers (L3). ✓

<u>Exemple</u> : Soit $P \in k[X_1, \dots, X_n]$ un polynôme non nul. La partie $V(P) \subseteq k^n$ est l'<u>hypersurface</u> définie par P. Supposons que

$$P = c P_1^{n_1} P_2^{n_2} \dots P_r^{n_r}$$

est la décomposition en facteurs irréductibles ($c \in k^*$).

Alors

$$V(P) = V(P_1 \cdots P_r) = V(P_1) \cup V(P_2) \cup \cdots \cup V(P_r)$$

est la décomposition en composantes irréductibles et

$$(P_1 \cdots P_r) = (P_1) \cap (P_2) \cap \cdots \cap (P_r)$$

l'écriture de l'idéal radical $(P_1 \cdots P_r)$ comme intersection d'idéaux premiers.

<u>Résumé</u> : Soit $Y \subseteq k^n$ une partie fermée et $A = k[X_1, \ldots, X_n]/I(Y)$.

On a la bijection

$$\{\text{fermés de } Y\} \xrightarrow{\sim} \{\text{idéaux radicaux de } A\}$$
$$Z \longmapsto \text{image de } I(Z)$$

Elle renverse les inclusions et induit des bijections

$$\text{points de } Y \longleftrightarrow \text{idéaux max. de } A$$
$$\text{fermés irréd. de } Y \longleftrightarrow \text{idéaux premiers de } A$$
$$\text{compos. irréd. de } Y \longleftrightarrow \text{idéaux premiers minimaux}$$

<u>Déf</u> : La <u>dimension</u> (combinatoire) <u>d'un espace top.</u> Y est le sup des longueurs l de chaînes $F_0 \supsetneq F_1 \supsetneq \cdots \supsetneq F_l$ de fermés irréd. de Y. La <u>dimension</u> (de Krull*) <u>d'un anneau</u> com. A est le sup des longueurs l de chaînes $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_l$ d'idéaux premiers de A.

<u>Rque</u> : Dans les notations du résumé ci-dessus, on a $\dim Y = \dim A$.

<u>Exemple</u> : On a la chaîne $Y = k^n \supsetneq k^{n-1} \supsetneq \cdots \supsetneq k^0 = \{0\}$.

Donc $\dim k^n \geq n$.

<u>But</u> : $\dim k^n = n$.

---

* 1928, Wolfgang Krull, 1899 (Baden-Baden) – 1971 (Bonn)

2.3 Localisation

Anneaux

Soient A un anneau commutatif et $S \subseteq A$ une partie multiplicative, i.e. $1 \in S$ et $S \cdot S \subseteq S$.

But : construire un morph. d'anneaux $A \xrightarrow{can} A_S$ qui envoie les éléments de S sur des inversibles et qui est universel pour cette propriété :

$$\begin{tikzcd} A \arrow[d, "can"'] \arrow[dr, "\forall f \text{ t.q. } f(S) \subseteq B^\times"] & \\ A_S \arrow[r, dashed, "\exists 1\ \tilde{f}"'] & B \end{tikzcd}$$

Construction

Sur $A \times S$, on définit la relation $\sim$ par :

$$(a,s) \sim (b,t) \iff \exists\, r \in S \text{ t.q. } r(at - bs) = 0$$

Exercice : C'est une relation d'équivalence.

Notations : a/s = classe d'équivalence de (a,s)

A_S = ensemble des classes d'équivalence.

Lemme 1 et Déf. : a) Pour $a/s,\ b/t \in A_S$, les éléments

$$a/s + b/t := \frac{at+bs}{st}, \quad a/s \cdot b/t = ab/st$$

ne dépendent pas des choix des représentants.

b) les lois $+$ et $\cdot$ font de A_S un anneau commutatif avec unité $1/1$.

c) L'appl. $A \xrightarrow{can} A_S$, $a \mapsto a/1$ est un morphisme d'anneaux qui rend inversibles les éléments de S et qui est universel pour cette propriété.

d) Le noyau de $can : A \longrightarrow A_S$ est $\{a \in A \mid \exists s \in S \text{ t.q. } as = 0\}$.

Dém : exercice ! ✓

<u>Déf</u> : A_S est le <u>localisé de A par rapport à S</u>.

<u>Exemples</u> : 1) Supposons A intègre. Si $S = A \setminus \{0\}$, alors $A_S = \mathrm{Frac}(A)$.

Si S est quelconque, l'appl. can. $A_S \longrightarrow \mathrm{Frac}(A)$, $a/s \longmapsto a/s$ identifie A_S à un ss-anneau de $\mathrm{Frac}(A)$.

2) Si B est un autre anneau com., alors $S = A^\times \times B$ est une partie mult. de $A \times B$ et $(A \times B)_S \xrightarrow{\sim} A$ (!).

<u>Notation</u> : On note $\mathrm{Spec}(A)$ l'ensemble (ordonné) des idéaux premiers de A.

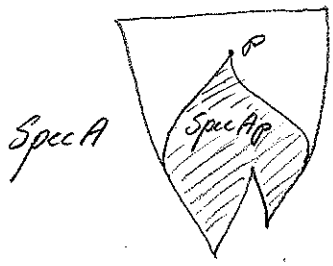
<u>Lemme 2</u> : a) L'application

$$\mathrm{Spec}(A_S) \longrightarrow \mathrm{Spec}(A), \quad \mathfrak{p} \longmapsto can^{-1}(\mathfrak{p})$$

est injective d'image l'ens. des idéaux premiers de A qui ne rencontrent pas S.

b) Un idéal $\mathfrak{p}$ de A est premier ssi $S = A \setminus \mathfrak{p}$ est multiplicative. Dans ce cas, <u>l'anneau</u>

$$A_{\mathfrak{p}} := A_S \quad (!)$$



est <u>local</u>, i.e. admet un unique idéal maximal, à savoir l'idéal $\mathfrak{p}A_{\mathfrak{p}} := \{x/s \mid x \in \mathfrak{p}, s \notin \mathfrak{p}\}$

Dém. : a) Exercice.

b) Par a), les idéaux premiers de $A_{\mathfrak{p}}$ sont en bijection avec les idéaux de A contenus dans $A \setminus S$. Or $A \setminus S = \mathfrak{p}$. ✓

Modules

Rque : Soit M un A_S-module. Par restriction des scalaires le long de $A \to A_S$, M devient un A-module dans lequel les éléments de S agissent par des endom. inversibles. Réciproquement, si N est un A-module où les éléments $s \in S$ agissent par des endom. inversibles λ_s, alors N devient un A_S-module par

$$a/s \cdot x = a\,\lambda_s^{-1}(x), \quad a/s \in A_S, \ x \in N.$$

Donc

A_S-module " = " A-module où les él. de S agissent de façon inversible.

Soit M un A-module. Sur $M \times S$, on définit la relation $\sim$ par :

$$(m,s) \sim (n,t) \iff \exists\, r \in S \text{ t.q. } r(tm - sn) = 0.$$

Exercice : c'est une relation d'équivalence.

Notation : m/s = classe d'équivalence de (m,s)

M_S = ensemble des classes d'équivalence.

Lemme 3 et Déf. : a) Pour $m/s, n/t \in M_S$ et $a/r \in A_S$, les éléments

$$m/s + n/t := \frac{mt+ns}{st} \quad \text{et} \quad a/r \cdot m/s = \frac{am}{rs}$$

ne dépendent pas du choix des représentants.

b) Les lois $+$ et $\cdot$ font de M_S un A_S-module.

c) L'application $M \to M_S$, $m \mapsto m/1$ est un morphisme de A-modules, universel parmi les morphismes dans un module où les éléments de S agissent de façon inversible.

c) Le noyau de $M \to M_S$ est $\{m \in M \mid \exists s \in S \text{ t.q. } sm = 0\}$.

Dém. : Exercice. ✓

<u>Lemme 4</u> : On a un isomorphisme canonique de A-modules

$$\varphi : A_S \otimes_A M \xrightarrow{\sim} M_S \,,\ \frac{a}{s} \otimes m \longmapsto \frac{am}{s}$$

En particulier, si M est libre (resp. de type fini) sur A, alors M_S est libre (resp. de type fini) sur A_S.

Dém. : On vérifie que l'appl. $\psi : \frac{m}{s} \longmapsto \frac{1}{s} \otimes m$ est bien définie et inverse de φ. ✓

<u>Exemple</u> : Soit M un $\mathbb{Z}$-module.

$$M \otimes_{\mathbb{Z}} \mathbb{Q} = 0 \underset{L4}{\Longleftrightarrow} M_S = 0 \text{ où } S = \mathbb{Z} \setminus \{0\}$$

$$\underset{L3c)}{\Longleftrightarrow} \forall m \in M \ \exists\, a \in \mathbb{Z} \setminus \{0\} \text{ t.q. } am = 0.$$

$$\Longleftrightarrow M \text{ est de torsion.}$$

<u>Lemme 5</u> : Si

$$0 \longrightarrow L \xrightarrow{i} M \xrightarrow{p} N \longrightarrow 0$$

est une suite exacte de A-modules, alors

$$0 \longrightarrow L_S \xrightarrow{i_S} M_S \xrightarrow{p_S} N_S \longrightarrow 0$$

est une suite exacte de A_S-modules.

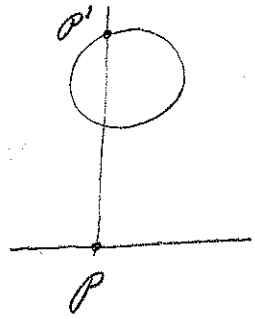
Dém. : La suite $L_S \longrightarrow M_S \longrightarrow N_S \longrightarrow 0$ est exacte car isomorphe à la suite $A_S \otimes_A L \longrightarrow A_S \otimes_A M \longrightarrow A_S \otimes_A N \longrightarrow 0$, qui est exacte par les propriétés du produit tensoriel. Il reste à montrer que i_S est injective. En effet, si $l/s \in L_S$ et $i_S(l/s) = 0$, alors $i_S(l/1) = 0$, donc $t\, i(l) = 0$ pour un $t \in S$. Mais alors $i(tl) = 0$ et $tl = 0$ car i est injective. Donc $l/1 = 0$ et $l/s = 0$ dans L_S. ✓

2.4 Dimension

Soit $A \hookrightarrow B$ une extension finie (i.e. un morph. d'anneaux injectif qui fait de B un A-module de type fini). On va étudier l'application induite

$$\begin{array}{ccc} B & \mathfrak{p}' & \operatorname{Spec} B \\ \updownarrow & \downarrow & \downarrow \\ A & \mathfrak{p}' \cap A & \operatorname{Spec} A \end{array}$$

p. ex.



$$\begin{array}{c} k[X,Y]/(X^2+Y^2-1) \\ \updownarrow \\ k[X] \end{array}$$

On obtiendra le

<u>Thm 1</u> (Cohen[1]-Seidenberg[2], 1946) : $\dim A = \dim B$

<u>Prop. 2</u> : a) Pour tout $\mathfrak{p} \in \operatorname{Spec} A$, il existe $\mathfrak{p}' \in \operatorname{Spec} B$ t.q. $\mathfrak{p}' \cap A = \mathfrak{p}$.

b) Pour tous $\mathfrak{p}' \subseteq \mathfrak{p}'' \in \operatorname{Spec} B$ t.q. $\mathfrak{p}' \cap A = \mathfrak{p}'' \cap A$, on a $\mathfrak{p}' = \mathfrak{p}''$.

c) Un idéal $\mathfrak{p}' \in \operatorname{Spec} B$ est maximal ssi $\mathfrak{p}' \cap A$ est max. dans A.

Dém. : c) On a l'extension finie $A/\mathfrak{p}' \cap A \hookrightarrow B/\mathfrak{p}'$.
Donc $B/\mathfrak{p}'$ est un corps ssi $A/\mathfrak{p}' \cap A$ en est un (L 1.5.1).

b) Soit $\mathfrak{p} = \mathfrak{p}' \cap A = \mathfrak{p}'' \cap A$. Soit $S = A \setminus \mathfrak{p}$. On a l'extension finie $A_S \hookrightarrow B_S$. On a

$$\mathfrak{p}'_S \cap A_S = \mathfrak{p}''_S \cap A_S = \mathfrak{p}_S$$

et c'est (l'unique) idéal maximal de $A_S = A_{\mathfrak{p}}$. Donc $\mathfrak{p}'_S$ et $\mathfrak{p}''_S$ sont maximaux (par c) et $\mathfrak{p}'_S = \mathfrak{p}''_S$. Comme $S \cap \mathfrak{p}' = \emptyset = S \cap \mathfrak{p}''$, il s'ensuit que $\mathfrak{p}' = \mathfrak{p}''$.

a) B est un A-module de type fini. Si $\mathfrak{p}B = B$, alors, par le lemme de Nakayama, il existe $x \in \mathfrak{p}$ t.q. $(1-x)B = 0$. Mais alors $(1-x)A = 0$ et $1-x = 0$. ↯. Donc $\mathfrak{p}B$ est un

---

[1] I.S. Cohen

[2] Abraham Seidenberg, 1918 (Washington) – 1988 (Milan)

idéal propre. On choisit un idéal $\mathfrak{p}'$ de B qui contient $\mathfrak{p}B$, évite $S = A \setminus \mathfrak{p}$ et qui est maximal avec ces propriétés. Alors $\mathfrak{p}'$ est premier (P1.1.3) et, par construction, $\mathfrak{p}' \cap A = \mathfrak{p}$. ✓

<u>Prop. 3</u> : a) Si
$$\mathfrak{p}_0' \subsetneq \mathfrak{p}_1' \subsetneq \cdots \subsetneq \mathfrak{p}_\ell'$$
est une chaîne d'idéaux premiers de B, alors les $\mathfrak{p}_i = \mathfrak{p}_i' \cap A$ forment une chaîne strictement croissante d'idéaux premiers de A.

b) Soit
$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_\ell$$
une chaîne d'idéaux premiers de A. Alors il existe une chaîne d'idéaux premiers de B
$$\mathfrak{p}_0' \subsetneq \cdots \subsetneq \mathfrak{p}_\ell'$$
t.q. $\mathfrak{p}_i' \cap A = \mathfrak{p}_i$, $1 \leq i \leq \ell$.

Dém. du thm 1 : Les deux inégalités résultent des parties a) et b) de la prop. 3. ✓

Dém. de la prop. 3 : a) résulte de la partie b) de la prop. 2.

b) On procède par récurrence sur ℓ. Pour $\ell = 0$, on utilise la partie a) de la prop. 2. Pour $\ell > 0$, l'hypothèse de récurrence donne un relèvement $\mathfrak{p}_0' \subsetneq \cdots \subsetneq \mathfrak{p}_{\ell-1}'$ de la chaîne $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_{\ell-1}$. On considère l'extension finie
$$A/\mathfrak{p}_{\ell-1} \hookrightarrow B/\mathfrak{p}_{\ell-1}'$$
et on applique la partie a) de la prop. 2 pour obtenir $\mathfrak{p}_\ell'/\mathfrak{p}_{\ell-1}'$ qui relève $\mathfrak{p}_\ell/\mathfrak{p}_{\ell-1}$. ✓

<u>Thm 4</u> : Soient k un corps et $n \in \mathbb{N}$. On a

a) $\dim k[X_1, \dots, X_n] = n$.

b) Si k est alg. clos, on a $\dim k^n = n$ (k^n considéré comme espace top. pour la top. de Zariski).

Dém. : b) résulte de a). Notons $A = k[X_1, \dots, X_n]$.

a) On a la chaîne d'idéaux premiers $(0) \subset (X_1) \subset (X_1, X_2) \subset \dots \subset (X_1, \dots, X_n)$. Donc $\dim A \geq n$. Montrons l'égalité par récurrence. Elle est claire pour $n=0$. Supposons donc $n > 0$. Soit $0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_l$ une chaîne d'idéaux premiers dans A. Soit f un élément non nul de $\mathfrak{p}_1$. Alors

$$\mathfrak{p}_1/(f) \subsetneq \mathfrak{p}_2/(f) \subsetneq \dots \subsetneq \mathfrak{p}_l/(f)$$

est une chaîne d'idéaux premiers de $A/(f)$. Donc $\dim A/(f) \geq l-1$. Soient $x_1, \dots, x_n$ les images des X_i dans $A/(f)$. Les x_i sont algébriquement liés. Donc il existe $x_1', \dots, x_{n-1}'$ dans $A/(f)$ t.q. x_n soit entier sur la ss-algèbre $A' = k[x_1', \dots, x_{n-1}']$ de $A/(f)$ et $A/(f) = A'[x_n]$ (L 1.4.10, Noether, Nagata)

Par le thm 1, on a

$$\dim A/(f) = \dim k[x_1', \dots, x_{n-1}'].$$

Comme $k[x_1', \dots, x_{n-1}']$ est un quotient de $k[Y_1, \dots, Y_{n-1}]$, on a

$$\dim k[x_1', \dots, x_{n-1}'] \leq \dim k[Y_1, \dots, Y_{n-1}],$$

et $\dim k[Y_1, \dots, Y_{n-1}] = n-1$ par l'hypothèse de récurrence. Donc $l-1 \leq \dim A/(f) \leq n-1$ et $l \leq n$. ✓

<u>Déf.</u> : Soit $L \supseteq K$ une extension de corps. Une partie $B \subseteq L$ est une <u>base de transcendance</u> de L sur K si

a) les éléments de B sont algébriquement indépendants sur K et

b) le corps L est algébrique sur $K(B)$.

<u>Lemme 5 et déf.</u> : Soient K un corps et $L \supseteq K$ une extension engendrée par un nombre fini d'éléments $x_1, \dots, x_r$.

a) Le corps L a une base de transc. finie sur K.

b) Deux bases de trans. de L sur K ont même cardinal.

Le <u>degré de transcendance</u> $\operatorname{degtr}_K L$ est ce cardinal.

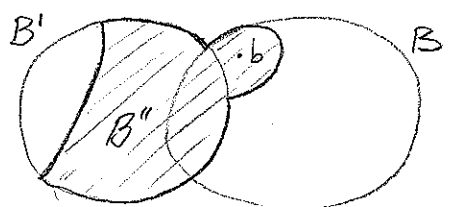
Dém. : a) Un ensemble maximal d'éléments alg. indép. $B \subseteq \{x_1, \dots, x_r\}$ est une base de transcendance de L sur K.

b) Soient B, B' deux bases de transcendance. Supposons que B' est finie (ce qui est légitime grâce à a). Montrons par récurrence descendante sur $|B \cap B'|$ que B et B' ont même cardinal :

- Si $|B \cap B'| = |B|$, alors $B' \subseteq B$ et $B' = B$ car $K(B) \supseteq K(B')$ est alg.
- Supposons $|B \cap B'| < |B|$. Soit $b \in B \setminus B'$. Alors $B' \cup \{b\}$ n'est plus une base de transcendance. Il existe alors un ensemble max. B'' t.q.

$$(B \cap B') \cup \{b\} \subseteq B'' \subsetneq B' \cup \{b\}$$

et qui est une base de transcendance. Alors $|B \cap B'| < |B \cap B''|$. Donc, par l'hypothèse de récurrence, B'' est fini et $|B| = |B''| \leq |B'|$. En échangeant les rôles de B et B' on trouve $|B'| \leq |B|$. ✓



<u>Corollaire 6</u> : Soit k un corps et A une k-algèbre intègre de type fini. Alors $\dim A = \operatorname{degtr}_k \operatorname{Frac}(A)$.

Dém. : D'après le lemme de Noether (Thm 1.4.9), il existe des éléments alg. indép. $y_1, \dots, y_m$ de A tels que A est une extension finie de $k[y_1, \dots, y_m]$. Alors $y_1, \dots, y_m$ est une base de transc. de $\operatorname{Frac}(A)$ sur k et

$$\operatorname{degtr}_k \operatorname{Frac}(A) = m \underset{\text{Thm 4}}{=} \dim k[y_1, \dots, y_m] \underset{\text{Thm 1}}{=} \dim A. \quad \checkmark$$

<u>Corollaire 7</u> : Soient k un corps et $f \in k[X_1, \dots, X_n]$ un polynôme non nul et non constant. Alors

$$\dim k[X_1, \dots, X_n]/(f) = n-1.$$

<u>Rque</u> : Si k est algébriquement clos, cela signifie que l'hypersurface $V(f) \subset k^n$ est de dimension $n-1$.

Dém : On peut supposer f irréductible (si $(f) \subseteq \mathfrak{p}$ pour un idéal premier $\mathfrak{p}$ de $k[X_1, \dots, X_n]$, alors $(f') \subseteq \mathfrak{p}$ pour un facteur irréd. f' de f). Quitte à renuméroter $X_1, \dots, X_n$, on peut supposer que $f \notin k[X_1, \dots, X_{n-1}]$. Alors le morphisme canonique

$$k[X_1, \dots, X_{n-1}] \longrightarrow k[X_1, \dots, X_n]/(f) = A$$

est injectif. D'où une extension de corps

$$k(X_1, \dots, X_n) \hookrightarrow \operatorname{Frac}(A),$$

qui est en fait finie. Donc

$$n-1 = \operatorname{degtr} k(X_1, \dots, X_{n-1}) = \deg \operatorname{Frac} A = \dim A. \quad \checkmark$$

2.5 Variétés affines et quasi-affines

Soient k un corps algébriquement clos et $n \in \mathbb{N}$.

Notation : $\mathbb{A}^n$ = espace affine de dim. n
= espace k^n muni de la top. de Zariski.

Rques : 1) Un espace top. est noethérien ssi tous ses ouverts sont quasi-compacts (!). Donc $\mathbb{A}^n$ et tous ses ss-espaces sont quasi-compacts.

2) Tout fermé de $\mathbb{A}^n$ est intersection de fermés $V(f)$, $f \in k[X_1, \dots, X_n]$. Donc tout ouvert de $\mathbb{A}^n$ est réunion d'ouverts principaux $D(f) := \mathbb{A}^n \setminus V(f)$, $f \in k[X_1, \dots, X_n]$, et les ouverts principaux forment une base de la topologie de $\mathbb{A}^n$.

Déf : Une variété affine est un ss-espace fermé $X \subseteq \mathbb{A}^n$; une fonction polynomiale sur X est la restriction d'une fonction polynomiale sur k^n. On note $A(X)$ l'algèbre des fonctions polynomiales sur X.

Rque : On a un isomorphisme naturel $k[X_1, \dots, X_n]/I(X) \xrightarrow{\sim} A(X)$.

Déf : Soient $X \subseteq \mathbb{A}^n$ et $Y \subseteq \mathbb{A}^m$ des variétés affines. Un morphisme $f : X \longrightarrow Y$ est une application

$$x \longmapsto f(x) = (f_1(x), \dots, f_m(x))$$

dont les composantes f_i sont polynomiales. On note $\mathrm{Mor}(X, Y)$ l'ensemble des morphismes de X dans Y.

Exemples : 1) $\mathrm{Mor}(X, k) \xrightarrow{\sim} A(X)$.

2) $X = \mathbb{A}^1$, $Y = V(X_1^2 - X_2^3) \subseteq \mathbb{A}^2$, $f : \mathbb{A}^1 \longrightarrow Y$, $t \longmapsto (t^3, t^2)$.

<u>Rque</u>: L'identité de toute var. affine est un morphisme ; le composé de deux morphismes est un morphisme.

<u>Déf.</u> : Un morphisme de var. affines $f : X \to Y$ est un <u>isomorphisme</u> s'il existe un morphisme $g : Y \to X$ t.q. $fg = 1_Y$ et $gf = 1_X$.

<u>Rque</u>: L'exemple 2) montre qu'un morphisme bijectif n'est pas toujours un isom

<u>Déf</u>: Le <u>comorphisme</u> d'un morphisme $f : X \to Y$ est le morphisme d'algèbres $f^* : A(Y) \to A(X)$, $u \mapsto u \circ f$.

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[dr, bend right, "f^*(u)"'] & Y \arrow[d, "u"] \\ & k \end{tikzcd}$$

<u>Rque</u> : On a $1_X^* = 1_{A(X)}$ et $(f \circ g)^* = g^* \circ f^*$.

<u>Prop 1</u> : a) Soient $X \subseteq \mathbb{A}^n$ et $Y \subseteq \mathbb{A}^m$ deux var. affines.

L'application $\mathrm{Mor}(X, Y) \xrightarrow{\sim} \mathrm{Hom}_{alg}(A(Y), A(X))$, $f \longmapsto f^*$

est bijective.

b) Pour toute k-algèbre A qui est réduite (i.e. $\mathrm{nil}(A) = 0$) et de type fini, il existe une var. affine $X \subseteq \mathbb{A}^n$ telle que $A \simeq A(X)$.

<u>Rque</u> : La proposition montre que l'étude des variétés affines et de leurs morphismes est équivalente à celle des k-algèbres réduites de type fini et de leurs morphismes.

<u>Dém.</u> : b) On a $A \simeq k[X_1, \dots, X_n]/J$ pour un idéal <u>radical</u> J donc $X = V(J)$ convient ($J = I(V(J))$ par le Nullstellensatz).

a) Injectivité : soit $f : X \to Y$ un morphisme et soient $f_1, \dots, f_m$ ses composantes. Soient $y_i : Y \to \mathbb{A}^1$, $1 \leq i \leq m$, les fonctions coordonnées restreintes à Y. On a

$f_i = y_i \circ f = f^*(y_i)$. Donc f^* détermine f.

Surjectivité : soit $\varphi : A(Y) \to A(X)$ un morphisme d'algèbres. Alors φ est déterminé par les $f_i := \varphi(y_i)$ car les y_i engendrent $A(Y)$ (y_i est l'image de $Y_i \in k[Y_1, \dots, Y_m]$).

Montrons que $\tilde{f} : X \to \mathbb{A}^m$, $x \mapsto (f_1(x), \dots, f_m(x))$ se factorise en $\tilde{f} = j \circ f$, où $j : Y \hookrightarrow \mathbb{A}^m$ est l'inclusion.

$$\begin{tikzcd} & \mathbb{A}^m \\ X \arrow[ur, "\tilde{f}"] \arrow[r, dashed, "f"'] & Y \arrow[u, hook, "j"'] \end{tikzcd}$$

On aura alors $f^* = \varphi$ car $f^*(y_i) = \varphi(y_i)$, $1 \leq i \leq m$.

Il s'agit de montrer que pour tout $x \in X$ et tout $u \in I(Y)$, on a $u(\tilde{f}(x)) = 0$. Or on a $u \circ \tilde{f} = \tilde{f}^*(u) = \varphi \circ j^*(u) = 0$.

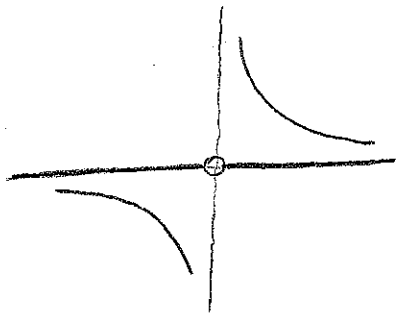
$$\begin{tikzcd} & A(\mathbb{A}^m) \arrow[dl, "\tilde{f}^*"'] \arrow[d, "j^*"] \\ A(X) & A(Y) \arrow[l, "\varphi"] \end{tikzcd}$$

✓

<u>But</u> : Etendre les notions de "variété" et de "morphisme" de façon que, par exemple, la droite épointée $\mathbb{A}^1 \setminus \{0\}$ devienne une "variété" et l'application

$$\mathbb{A}^1 \setminus \{0\} \longrightarrow \{X_1 X_2 = 1\}, \quad t \mapsto (t, 1/t)$$

un "isomorphisme" sur l'hyperbole $X_1 X_2 = 1$.



<u>Déf</u> : Une <u>variété quasi-affine</u> est un ouvert d'une variété affine.
Une fonction $f : X \to k$ sur une var. quasi-affine X est <u>régulière</u> en un point $x \in X$ si, <u>au voisinage</u> de x, elle s'écrit $f = g/h$ pour des $f, g \in A(\bar{X})$ t.q. $g(x) \neq 0$.
Elle est <u>régulière sur</u> X si elle est régulière en tout point de X.

Si $X \subseteq \mathbb{A}^n$ et $Y \subseteq \mathbb{A}^m$ sont des variétés quasi-affines, une application $f : X \to Y$ de composantes $f_1, \dots, f_m$ est <u>régulière</u> si les $f_i : X \to k$ sont régulières sur X.

<u>Rques</u>: Les applications régulières sont continues (l'image réciproque d'un fermé est fermée au voisinage de tout point de X). La composée de deux appl. régulières est régulière. Les identités sont régulières.

<u>Thm 2</u>: Si $X \subseteq \mathbb{A}^n$ est affine, toute appl. régulière $X \xrightarrow{f} \mathbb{A}^1$ (Serre, 1955) est polynomiale.

<u>Rque</u>: Il s'ensuit que toute appl. régulière d'une var. affine X dans une var. quasi-affine Y a des composantes polynomiales et que les appl. rég. entre var. affines sont exactement les morphismes de variétés affines.

<u>Déf</u>: Un <u>morphisme</u> de variétés quasi-affines est une appl. régulière. Un <u>isomorphisme</u> est un morph. f t.q. il existe un morph. g t.q. $f \circ g = \mathbb{1}$ et $g \circ f = \mathbb{1}$.

<u>Exemples</u>: 1) L'hyperbole est isomorphe à la droite épointée.

2) Si $f \in k[X_1, \dots, X_n]$, l'ouvert principal $X = D(f)$ est une variété quasi-affine isomorphe à la var. affine

$$Y = V(X_{n+1} \cdot f - 1) \subseteq \mathbb{A}^{n+1}$$

via $(x_1, \dots, x_n) \longmapsto (x_1, \dots, x_n, 1/f(x_1, \dots, x_n))$.

3) $Gl_n(k) = \{ M \in M_n(k) \mid \det(M) \neq 0 \}$ est un ouvert principal, donc une variété affine (à isom. près). De même, $Gl_n(k) \times Gl_n(k)$ est affine. La mult. et le passage à l'inverse sont des morphismes. $Gl_n(k)$ est un <u>groupe algébrique affine</u>.

Dém. du thm 2 : 1ère étape : l'affirmation pour X irréductible.

Il existe un recouvrement (qu'on peut choisir fini car X est quasi-compact) par des ouverts denses U_i, $1 \leq i \leq r$, et des g_i, h_i dans $A(X)$ tels que h_i est partout non nul sur U_i et

$$f|_{U_i} = g_i/h_i|_{U_i}, \quad 1 \leq i \leq r.$$

Les h_i n'ont pas de zéro commun dans X. Donc ils engendrent l'idéal $A(X)$ et il existe des $l_j \in A(X)$ t.q.

$$\sum_{j=1}^{r} l_j h_j = 1.$$

Soit $U = \bigcap_{i=1}^{r} U_i$. Alors on a

$$f|_U = g_i/h_i|_U = \sum_{j=1}^{r} l_j g_j|_U \quad \left(\text{car } g_i|_U = \sum_{j=1}^{r} l_j h_j g_i|_U = \sum_{j=1}^{r} l_j h_i g_j|_U\right).$$

Donc $f = \sum_{j=1}^{r} l_j g_j$ sur X car U est dense et f et la somme sont continues.

2e étape : Soit $0 \neq H \in A(\mathbb{A}^n)$. Alors

a) Toute fonction régulière sur $D(h)$ s'écrit F/H^m pour un $F \in A(\mathbb{A}^n)$ et un $m \in \mathbb{N}$.

b) Toute fonction régulière sur $D(H)$ et nulle sur X s'écrit F/H^m pour un $F \in I(X)$ et un $m \in \mathbb{N}$.

Les applications

$$D(h) \underset{\sim}{\rightleftarrows} V(H \cdot X_{n+1} - 1) =: Y$$

$$x \longmapsto (x, 1/H(x))$$

$$(y_1, \dots, y_n) \longleftarrow\!\shortmid \; y = (y_1, \dots, y_{n+1})$$

sont régulières et inverses l'une de l'autre. Elles induisent des bijections entre les fct. régulières $D(H) \longrightarrow k$ et $V(H \cdot X_{n+1} - 1) \longrightarrow k$. L'espace $D(H)$ est irréductible. Donc $V(H \cdot X_{n+1} - 1)$ est irréductible. Par la première étape, toute fct. régulière sur $V(H \cdot X_{n+1} - 1)$ s'écrit

$$g = P(X_1, \dots, X_{n+1}) / V(X_{n+1} h - 1)$$

Donc toute fct. régulière sur $D(H)$ s'écrit

$$f = F(X_1, \dots, X_n) / H^m .$$

De plus, si f s'annule sur $X \cap D(H)$, il est clair que F s'annule sur $X \cap D(H)$ et $H \cdot F$ s'annule sur X. Donc $H \cdot F \in I(X)$ et $f = F \cdot H / H^{m+1}$.

3e étape : l'affirmation dans le cas général.

On peut trouver un nombre fini d'ouverts $U_i = X \cap D(H_i)$ qui recouvrent $\mathbb{A}^n$ et un entier N tels que

a) Sur $U_i \cap X$, on a $f = L_i / H_i^N$, $L_i \in A(\mathbb{A}^n)$

b) Sur $U_{ij} = U_i \cap U_j$, on a

$$\frac{L_i}{H_i^N} - \frac{L_j}{H_j^N} = \frac{L_{ij}}{(H_i H_j)^N} , \quad L_{ij} \in I(X).$$

Les H_i^N n'ont pas de zéro en commun dans $\mathbb{A}^n$. Donc il existe des R_i tels que $\sum R_i H_i^N = 1$ dans $A(\mathbb{A}^n)$.

Sur U_i, considérons la fonction régulière $v_i := \sum_s R_s \frac{L_{is}}{H_i^N}$.

Alors v_i s'annule sur $U_i \cap X$ et sur U_{ij}, on a

$$v_i - v_j = \sum_s R_s \frac{L_{is}}{H_i^N} - \sum_t R_t \frac{L_{jt}}{H_j^N}$$

$$= \sum_s R_s H_s^N \frac{L_{is}}{(H_s H_i)^N} - \sum_t R_t H_t^N \frac{L_{jt}}{(H_t H_j)^N}$$

$$= \sum_s R_s H_s^N \left(\frac{L_i}{H_i^N} - \frac{L_s}{H_s^N}\right) - \sum_t R_t H_t^N \left(\frac{L_j}{H_j^N} - \frac{L_t}{H_t^N}\right)$$

$$= \frac{L_i}{H_i^N} - \frac{L_j}{H_j^N} .$$

D'où

$$\frac{L_i}{H_i^N} - v_i = \frac{L_j}{H_j^N} - v_j \quad \text{sur } U_{ij}.$$

Par la première étape, il existe donc $P \in A(A^n)$ tel que

$$P|_{U_i} = \left(\frac{L_i}{H_i^N} - v_i\right)\Big|_{U_i}$$

On a alors $f = P|_X$ et f est bien polynomiale. ✓