Table des matières

Anneaux et algèbres

On considère les anneaux commutatifs.

Soit A un anneau. Un *sous-anneau* de A est un sous-groupe de A qui contient 1_A et qui est stable par la multiplication.

Une $A-$*algèbre* est la donnée d'un anneau B et d'un morphisme d'anneaux $i_B : A \to B$. Un morphisme de $A-$algèbres $B \to C$ est un morphisme d'anneaux $\phi : B \to C$ tel que $\phi \circ i_B = i_C$.

Des éléments $x_1, ..., x_n$ de la $A-$algèbre B engendrent B si chaque élément de B est un polynôme en les x_i à coefficients dans $i_B(A)$ *i.e.* le morphisme de $A-$algèbres induit : $A[X_1, ..., X_n] \to B$ est surjectif *i.e.* $B = i_B(A)[x_1, ..., x_n]$.

Un morphisme d'anneaux $A \to B$ est *de type fini* si B est une $A-$ algèbre de type fini.

Un morphisme d'anneaux $A \to B$ est *fini* si B est une $A-$algèbre finie *i.e.* B est un $A-$module de type fini.

Exemples : si k est un corps, $k[X]$ est de type fini sur k et $k[X]/(X^2)$ est finie sur k.

Si k est un corps, si A est une $k-$algèbre,si $1_A \neq 0_A$, alors le morphisme $k \to A$ est injectif et on peut identifier k avec son image dans A.

Conséquences du lemme de Zorn

Soit A un anneau. On dit qu'un idéal I de A est propre si $I \neq A$ *i.e.* si $1 \notin A$.

Un *idéal maximal* est un idéal maximal pour l'inclusion parmi les idéaux propres. Un *idéal premeir* est un idéal propre I tel que

$$xy \in I \Rightarrow x \text{ ou } y \in I$$

pour tous $x, y \in A$.

Rappelons :

$$P \text{ idéal de } A \text{ est premier } \Leftrightarrow A/P \text{ est un anneau non nul intègre}$$

$$\mathfrak{m} \text{ idéal de } A \text{ est maximal } \Leftrightarrow A/m \text{ est un corps (non nul).}$$

Proposition 0.1 Soit A un anneau. Tout idéal propre de A est contenu dans un idéal maximal.

Un élément $x \in A$ est nilpotent si $x^n = 0$ pour un certain $n \geq 0$. Un anneau dont 0 est le seul élément nilpotent est *réduit.*

Exemple : si k est un corps et P est un polynôme à coefficients dans k, alors $k[X]/(P)$ est réduit si et seulement si P est sans facteur carré.

Proposition 0.2 L'idéal des éléments nilpotents de A est $\bigcap_p p$, l'intersection de tous les idéaux premiers de A.

Démonstration : Soit x un élément qui n'est pas nilpotent. La famille des idéaux qui ne contiennent aucune puissance de x est *inductive* donc admet un élément maximal. On vérifie facilement que cet élément maximal est un idéal premier (qui ne contient pas x). *q.e.d.*

1 Nœthériennité

1.1 Anneaux noethériens

Soit A un anneau. Si $x_1, ..., x_n \in A$, on note $(x_1, ..., x_n)$ l'idéal formé des combinaisons $A-$linéaires des x_i. Un tel idéal est de type fini.

Proposition 1.1 Sont équivalentes :

i) tout idéal de A peut être engendré par un nombre fini d'éléments ;

ii) toute une suite croissante d'idéaux $I_0 \subseteq ... \subseteq I_n \subseteq I_{n+1} \subseteq ...$ est stationnaire ;

iii) toute famille non vide d'idéaux de A contient un élément maximal (pour l'inclusion).

Un anneau qui vérifie les assertions de la proposition est appelé *nœthérien.*

Remarques :

— si k est un corps, k est nœthérien. Plus généralement, tout anneau principal est nœthérien car tous ses idéaux peuvent être engendrés par un élément ;

— l'idéal $(X,Y)^n = (X^n, X^{n-1}Y, ..., Y^n)$ de $k[X,Y]$ peut être engendré par $n+1$ éléments mais pas moins ! (*exo*) *Indication : le quotient* $(X,Y)^n/(X,Y)^{n+1}$ *est un* $k-$*espace vectoriel de dimension* $n+1$*, de base les classes de* $X^n, X^{n-1}Y, ..., Y^n$ *modulo* $(X,Y)^{n+1}$.

Proposition 1.2 Le quotient d'un anneau nœthérien est nœthérien.

1.2 Modules nœthériens

Proposition 1.3 Soit A un anneau commutatif. Soit M un $A-$module. Sont équivalentes :

i) tout sous-module de M peut être engendré par un nombre fini d'éléments (en particulier M lui-même) ;
ii) toute une suite croissante de sous-modules $M_0 \subseteq ... \subseteq M_n \subseteq M_{n+1} \subseteq ...$ est stationnaire ;
iii) toute famille non vide de sous-modules de M contient un élément maximal (pour l'inclusion).

On dit qu'un module qui vérifie les assertions de la proposition précédente est *nœthérien.*

Proposition 1.4 Soient $N \leq M$ deux $A-$modules. Alors :

$$M \text{ est nœthérien } \Leftrightarrow N \text{ et } M/N \text{ sont nœthériens.}$$

Corollaire 1.4.1 Soit A un anneau nœthérien. Tout $A-$module de type fini est nœthérien.

Exemple d'application :

Proposition 1.5 Soit A un anneau nœthérien. Soit M un $A-$module de type fini. Il existe une suite finie de sous-modules : :

$$0 = M_0 \subseteq M_1 \subseteq ... \subseteq M_n = M$$

telle que pour tout i, $M_i/M_{i-1} \simeq A/p_i$ pour un certain idéal premier p_i de A.

Démonstration : Si $x \in M$, on note $\mathrm{Ann}(x)$ l'idéal $\{a \in A : ax = 0\}$. L'idéal $\mathrm{Ann}(x)$ est propre si et seulement si $x \neq 0$. Soit $\mathrm{Ann}(x_1)$ un idéal maximal parmi les idéaux de la forme $\mathrm{Ann}(x)$, $x \in M \setminus \{0\}$. L'idéal $P_1 := \mathrm{Ann}(x_1)$ est premier. En effet, si $ab \in P_1$, $abx_1 = 0$. Si par exemple $ax_1 \neq 0$, alors $\mathrm{Ann}(x_1) \underset{\neq}{\subset} \mathrm{Ann}(bx_1)$. Par maximalité, $bx_1 = 0$ *i.e.* $b \in \mathrm{Ann}(x_1)$.

Posons $M_1 := Ax_1$. On a $M_1 \simeq A/P_1$. Le $A-$module M est nœthérien. Il existe donc M' un sous-$A-$module de M maximal parmi ceux qui vérifient l'énoncé de la proposition. On a $M' = M$ sinon on pourrrait trouver $x' \in M$ tel que $\mathrm{Ann}(\overline{x'})$ est premier avec $\overline{x'} := x' \bmod M'$. Le module $M' + Ax'$ contiendrait strictement M' et vérifierait aussi la propriété de l'énoncé :*absurde !* <u>*q.e.d.*</u>

1.3 Théorème de transfert

Théorème 1.6 (de base de Hilbert) Soit A un anneau nœthérien. Alors l'anneau $A[X]$ est aussi nœthérien.

Corollaire 1.6.1 Si k est un anneau nœthérien (par exemple si k est un corps), alors toute $k-$algèbre de type fini est nœthérienne.

Démonstration : En effet, par récurrence sur n, $k[X_1,...,X_n] = k[X_1,...,X_{n-1}][X_n]$ est nœthérien. Si A est une $k-$algèbre de type fini, engendrée par $x_1,...,x_n$, alors il existe un morphisme surjectif :

$$k[X_1,...,X_n] \to k[x_1,...,x_n] \ .$$

donc en notant I le noyau de ce morphisme, on a : $A \simeq k[X_1,...,X_n]/I$. *q.e.d.*

Démonstration du théorème : Soit $\mathscr{A}$ un idéal de $A[X]$. Pour tout $i \geq 0$, soit :

$$\mathscr{A}_i := \{c \in A \ : \ ^\exists f \in A,\ f = cX^i + \underbrace{...}_{\text{termes de degrés } < i} \} \ .$$

Si $cX^i + ... \in \mathscr{A}$, alors $Xf \in \mathscr{A}$. On en déduit que $\mathscr{A}_i \subseteq \mathscr{A}_{i+1}$. Comme A est nœthérien, il existe $d \geq 0$ tel que $\mathscr{A} = \mathscr{A}_i$ si $i \geq d$. Pour tout $i \leq d$, soient

$$c_{i,j},\ 1 \leq j \leq n_i$$

des générateurs de $\mathscr{A}_i$. Pour tous i, j, soit $f_{i,j} = c_{i,j}X^i + ... \in \mathscr{A}$ (les ... sont de degrés $< i$).

Alors $\mathscr{A}$ est engendré par les $f_{i,j}$, $1 \leq i \leq d$, $1 \leq j \leq n_i$. En effet, sinon, il existe $f \in \mathscr{A} \ \setminus \ \sum_{i,j} A[X]f_{i,j}$ de degré minimal. On a :

$$f = cX^n + ...$$

où $n = \deg f$.

Si $n \geq d$, alors $c \in \mathscr{A}_n = \mathscr{A}_d$. Donc il existe des $\lambda_{d,j} \in A$ tels que $c = \sum_j \lambda_{d,j}c_{d,j}$. Mais alors

$$f - X^{n-d}\sum_j \lambda_{d,j}f_{d,j} \in \mathscr{A} \ \setminus \ \sum_{i,j} A[X]f_{i,j}$$

est de degré $< n$: *absurde !*

Si $n \leq d$, alors $c \in \mathscr{A}_n$. Donc il existe des $\lambda_{n,j} \in A$ tels que $c = \sum_j \lambda_{n,j}c_{n,j}$. Mais alors

$$f - \sum_j \lambda_{n,j}f_{n,j} \in \mathscr{A} \ \setminus \ \sum_{i,j} A[X]f_{i,j}$$

est de degré $< n$: *absurde !*

q.e.d.

Soit k un corps.

Contre-exemple : La $k-$algèbre $k(X)$ est nœthérienne (c'est un corps !) mais n'est pas de type fini sur k.

En général, une sous-algèbre d'une $k-$algèbre de type fini n'est pas nœthérienne. Par exemple dans l'anneau $A = k[X, XY, XY^2, ..., XY^n, ...] \subseteq k[X, Y]$, $(X, XY, ..., XY^n) \underset{\neq}{\subseteq} (X, XY, ..., XY^{n+1})$ pour tout n.

Exercice 1 Les sous-$k-$algèbres de $k[X]$ sont de type fini sur k (donc nœthériennes) *Indication : si $P \in k[X]$ est un polynôme non constant, alors le $k[P]-$module $k[X]$ est de type fini.*

1.4 Lemme de Nakayama

Lemme 1.7 (de Nakayama) Soit M un $A-$module de type fini. Soit $\mathfrak{a}$ un idéal de A. Si $\mathfrak{a}M = M$, alors il existe $x \in \mathfrak{a}$ tel que $(1 + x)M = 0$. En particulier, si $\mathfrak{a}$ est contenu dans tous les idéaux maximaux de A et si $\mathfrak{a}M = M$, alors $M = 0$.

Contre-exemple : soient p un nombre premier, $A = \mathbb{Z}_{(p)} := \{m/n : p \text{ ne divise pas } n\}$, $M = \mathbb{Q}$. On a $M = pM$ mais $M \neq 0$.

Corollaire 1.7.1 Soit A un anneau local d'idéal maximal m. On pose $k = A/m$. Soit M un $A-$module de type fini. Si $a_1, ...a_n \in M$, alors $a_1, ..., a_n$ engendrent M comme $A-$module $\Leftrightarrow$ $a_1 + mM, ..., a_n + mM$ engendrent M/mM comme $k-$ev.

Corollaire 1.7.2 Soit A un anneau local d'idéal maximal m. Le nombre minimal de générateur de m est la dimension du $k-$ev m/m^2 où $k = A/m$.

Exercice 2 Soit M un $A-$module de type fini. Soit $u \in \mathrm{End}_A(M)$ un endomorphisme surjectif. Alors u est injectif. *Indication : considérer M comme un $A[X]-$module en posant $P(X).m := P(u)(m)$ pour tout $P(X) \in A[X]$ et vérifier que $(X)M = M$.*

Théorème 1.8 (de l'intersection de Krull) Soit A un anneau nœthérien. Soit $\mathfrak{a}$ un idéal contenu dans tous les idéaux maximaux de A. Alors $\bigcap_{n\geq 1} \mathfrak{a}^n = 0$.

Contre-exemple : Soit A l'anneau des germes des fonctions $\mathscr{C}^\infty$ au voisinage de 0. Soit $\mathfrak{m}$ l'idéal des fonctions nulles en 0. Alors $\bigcap_{n\geq 0} \mathfrak{m}^n \neq 0$. En effet, dans ce cas, $\bigcap_{n\geq 0} \mathfrak{m}^n \neq 0$ est le germe des fonctions $\mathscr{C}^\infty$ au voisinage de 0 dont toutes les dérivées supérieures s'annulent en 0 ; or, il existe une fonction $f\,\mathscr{C}^\infty$ sur $\mathbb{R}$ telle que $f(x) = e^{-1/x}$ si $x \neq 0$ et $f^{(n)}(0) = 0$ pour tout $n \geq 0$.

Démonstration : D'après le lemme de Nakayama, il suffit de vérifier que $\mathfrak{a}\bigcap_{n\geq 1} \mathfrak{a}^n = \bigcap_{n\geq 1} \mathfrak{a}^n$.

Soient $a_1, ..., a_r \in A$ des générateurs de A. Pour tout $m \geq 0$ soit S_m l'ensemble des polynômes $f \in A[X_1, ..., X_r]$ homogènes de degré m tels que :

$$f(a_1, ..., a_r) \in \bigcap_{n\geq 1} \mathfrak{a}^n \ .$$

L'idéal I engendré par tous les S_m est de type fini car $A[X_1, ..., X_r]$ est nœthérien. Soient $f_1, ..., f_k$ des générateurs homogènes (c'est possible de choisir les générateurs homogènes (*exo*)) de I de degrés respectifs $n_1, ..., n_k$. Soit $x \in \bigcap_{n\geq 1} \mathfrak{a}^n$. Soit $m > \max n_i$. Comme $x \in \mathfrak{a}^m$, il existe un polynôme homogène $f \in A[X_1, ..., X_r]$ de degré m tel que $x = f(a_1, ..., a_r)$. On a $f \in I$. Donc il existe des polynômes $\lambda_i \in A[X_1, ..., X_r]$ tels que

$$f = \sum_i \lambda_i f_i \ .$$

Quitte à ne considérer pour chaque i la composante homogène de degré $m-n_i$ de λ_i, on peut supposer chaque λ_i homogène de degré $m-n_i$.

On a alors :

$$x = \sum_i \lambda_i(a_1,...,a_r) f_i(a_1,...,a_r) \in \mathfrak{a} \bigcap_{n\geq 1} \mathfrak{a}^n$$

car $m - n_i > 0$ pour tout i.

<u>*q.e.d.*</u>

Proposition 1.9 Tout idéal d'un anneau nœthérien contient une puissance de son radical. En particulier pour un anneau nœthérien, une certaine puissance de son radical de Jacobson est 0.

2 Localisation

Soit A un anneau. On dit qu'une partie S de A est *multiplicative* si elle contient 1 et est stable par multiplication.

Soit S une partie multiplicative de A. On définit une relation d'équivalence sur $A \times S$ par :

$$(a, s) \sim (b, t)$$

s'il existe $u \in S$ tel que $u(ta - bs) = 0$.

Exercice 3 Vérifier qu'il s'agit bien d'une rela d'équivalence.

On note $\frac{a}{s}$ la classe d'équivalence du couple $(a, s) \in A \times S$. On définit une addition et une multiplication des classes d'équivalences par les règles de calculs suivantes :

$$\frac{a}{s} + \frac{b}{t} := \frac{at + bs}{st} \text{ et } \frac{a}{s}\frac{b}{t} := \frac{ab}{st} \ .$$

Exercice 4 Vérifier que ces règles sont définies sans ambiguïtés.

On obtient un anneau

$$S^{-1}A := \left\{ \frac{a}{s} \ : \ a \in A, s \in S \right\}$$

et un morphisme d'anneaux :

$$i_S : A \to S^{-1}A \, , \ a \mapsto \frac{a}{1}$$

de noyau $\left\{ a \in A \ : \ {}^\exists s \in S, sa = 0 \right\}$.

Remarque : Si S ne contient pas de diviseur de 0, alors i_S est injective. En revanche si $0 \in S$, alors $S^{-1}A$ est l'anneau nul.

Le couple $(S^{-1}A, i_S)$ vérifie la propriété universelle suivante :

Théorème 2.1 Le morphisme i_S envoie tous les éléments de S sur des éléments inversibles de $S^{-1}A$. Si ϕ est un morphisme : $A \to B$ qui a cette même propriété, alors il se factorise de manière unique à travers i_S :

$$\begin{tikzcd} A \arrow[r, "i_S"] \arrow[d, "\phi"'] & S^{-1}A \\ B \arrow[ur, dashed, "\exists!"] & \end{tikzcd} \quad .$$

Exemples :

— si A est l'anneau des fonctions continues $\mathbb{R} \to \mathbb{R}$ et S l'ensemble des fonctions continues $f \in A$ non nulles en 0, alors $S^{-1}A$ est l'anneau des germes de fonctions continues au voisinage de 0 ;

— Si A est intègre, alors $S := A \setminus \{0\}$ est une partie multiplicative de A et $S^{-1}A$ est le corps des fractions de A. De plus si T est une partie multiplicative contenue dans $A \setminus \{0\}$, alors on peut identifier $T^{-1}A$ avec le sous-anneau $\{\frac{a}{t} \,:\, a \in A, t \in T\}$ du corps des fractions de A.

— Soit $h \in A$. La partie $S := \{1, h, ..., h^n, ...\}$ de A est multiplicative et on note $A_h := S^{-1}A$. Si h est nilpotente, $A_h = 0$. Si A est intègre de corps des fractions K, on peut identifier A_h avec le sous-anneau des éléments de K de la forme

$$\frac{a}{h^n},\ n \geq 0\ ;$$

— $\mathbb{Z}_{10} = \{x/(10^k) \,:\, x \in \mathbb{Z}, k \geq 0\}$ c'est l'anneau des décimaux.

— $\mathbb{C}[T]_T = \{p(T)/T^k \,:\, p(T) \in \mathbb{C}[T], k \geq 0\}$ c'est l'anneau des fractions rationnelles définies sur $\mathbb{C} \setminus \{0\}$.

Proposition 2.2 Le morphisme $A[X] \to A_h : \sum_i a_i X^i \mapsto \sum_i a_i/h^i$ induit un isomorphisme d'anneaux :

$$A[X]/(1 - hX) \simeq A_h\ .$$

Démonstration : Comme h est inversible dans $A[X]/(1 - Xh)$, d'inverse $X \bmod (1 - Xh)$, on peut définir, par la propriété universelle de A_h, un morphisme d'anneaux :

$$A_h \to A[X]/(1 - Xh)\ a/h^k \mapsto aX^k$$

qui est clairement le morphisme réciproque du morphisme de l'énoncé. <u>*q.e.d.*</u>

2.1 Idéaux et localisations

Soit S une partie multiplicative de A. Si I est un idéal de A, on note $S^{-1}I$ l'idéal de $S^{-1}A$ engendré par $i_S(I)$.

Proposition 2.3 Si I est un idéal premier de A disjoint de S, alors $i_S^{-1}(S^{-1}I) = I$. De plus, si I est premier, $S^{-1}I$ l'est aussi. Réciproquement, si J est un idéal de $S^{-1}A$, alors $S^{-1}i_S^{-1}(J) = J$.

On a donc une bijection : $I \mapsto S^{-1}I$ entre les idéaux premiers de A disjoints de S et les idéaux premiers de $S^{-1}A$.

Corollaire 2.3.1 Si A est nœthérien, alors $S^{-1}A$ aussi, pour toute partie multiplicative S de A.

2.2 Localisé en un idéal premier

Soit P un idéal premier de A. La partie $S_P := A \setminus P$ de A est multiplicative et on note $A_P := S_P^{-1}A$. L'anneau A_P est local d'idéal maximal $PA_P := \{a/s : a \in P, s \notin P\}$.

Par exemple, si k est un corps, si $A = k[X]$ et $m = (X)$, $A_m = k[X]_{(X)} = \{p/q \ : \ q(0) \neq 0\}$: c'est l'anneau des fractions rationnelles définies en 0.

On a :

$$A_m/(mA_m)^n \simeq k[X]/(X^n)$$

en associant à une fraction rationnelle son développement limité au voisinage de 0 à l'ordre $n-1$.

De même si p est un nombre premier, $\mathbb{Z}_{(p)} = \{m/n \ : \ m, n \in \mathbb{Z}, p \not| n\}$ et $\mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)} \simeq \mathbb{Z}/p^n\mathbb{Z}$.

Proposition 2.4 Soit $\mathfrak{m}$ un idéal maximal de A. On note $\mathfrak{n} := \mathfrak{m}A_{\mathfrak{m}}$.

Pour tout $k \geq 0$, le morphisme d'anneaux :

$$A/\mathfrak{m}^k \to A_{\mathfrak{m}}/\mathfrak{n}^k$$

$$a \bmod \mathfrak{m}^k \mapsto a/1 \bmod \mathfrak{n}^k$$

est un isomorphisme et induit des isomorphismes :

$$\mathfrak{m}^j/\mathfrak{m}^k \simeq \mathfrak{n}^j/\mathfrak{n}^k$$

pour tous couples $j \leq k$.

Démonstration :

Injectivité : si $a/1 \in \mathfrak{n}^k$, alors il existe $s \notin \mathfrak{m}$ tel que $sa \in \mathfrak{m}^k$. Or

$$\mathfrak{m}^k + (s) = (1) \ .$$

donc il existe un $u \in S$ tel que $us = 1 \bmod \mathfrak{m}^k$. Mais alors : $usa = a \bmod \mathfrak{m}^k \in \mathfrak{m}^k$.

Surjectivité : soit $a/s \in A_{\mathfrak{m}}$. Comme ci-dessus, il existe $u \in S$ tel que $us = 1 \bmod \mathfrak{m}^k$. Alors : $a - aus \in \mathfrak{m}^k$ donc : $a/s = ua/1 \bmod \mathfrak{n}^k$.

Pour les derniers isomorphismes, on remarque que :

$$\mathfrak{m}^j/\mathfrak{m}^k = \ker\left(A/\mathfrak{m}^k \to A/\mathfrak{m}^j\right)$$

$$\mathfrak{n}^j/\mathfrak{n}^k = \ker\left(A_{\mathfrak{m}}/\mathfrak{n}^k \to A_{\mathfrak{m}}/\mathfrak{n}^j\right) \ .$$

q.e.d.

Proposition 2.5 Si A est nœthérien, alors :

$$\bigcap_{\mathfrak{m} \text{ maximal}} \bigcap_{n \geq 1} \mathfrak{m}^n = 0 \ .$$

On peut aussi localiser des modules :

2.3 Localisation de modules

Soit S une partie multiplicative de A. Soit M un $A-$module. On définit une relation d'équivalence sur $M \times S$ par :

$$(m, s) \sim (n, t)$$

s'il existe $u \in S$ tel que $u(tm - sn) = 0$.

On note m/s la classe d'équivalence du couple (m, s) et on définit l'addition et la multiplication sur l'ensemble des classes d'équivalences par :

$$m/s + n/t := (tm + sn)/st \text{ et } (a/s) \cdot m/t := (am)/(st) \ .$$

On obtient ainsi un $S^{-1}A-$module :

$$S^{-1}M := \{m/s \ : \ m \in M, s \in S\}$$

et un morphisme de $A--$modules :

$$i_S : M \to S^{-1}M, \ m \mapsto m/1$$

de noyau : $\{m \in M \ : \ ^{\exists}s \in S, \, sm = 0\}$.

Remarque : si $s \in S$, le morphisme de $S^{-1}A-$modules $S^{-1}M \to S^{-1}M$, $m \mapsto sm$ est inversible.

Le couple $(S^{-1}M, i_S)$ vérifie la propriété universelle suivante :

Proposition 2.6 Si $f : M \to N$ est un morphisme de $A-$modules tel que pour tout $s \in S$, $N \to N$, $n \mapsto sn$ est inversible, alors il existe un unique morphisme de $A-$modules : $S^{-1}f : S^{-1}M \to N$ qui fait commuter le diagramme :

$$\begin{tikzcd} M \arrow[r, "i_S"] \arrow[d, "f"] & S^{-1}M \arrow[dl, dashed, "S^{-1}f"] \\ N & \end{tikzcd} \ .$$

Démonstration : Soit $s \in S$, on note $n \mapsto s^{-1}n$ l'inverse de $N \to N$, $s \mapsto sn$. Il suffit de poser :

$$S^{-1}f(m/s) := s^{-1}f(m) \ .$$

q.e.d.

En particulier, pour tout morphisme de $A-$modules $f : M \to N$, il existe un unique morphisme $S^{-1}f : S^{-1}M \to S^{-1}N$ tel que :

$$\begin{tikzcd} M \arrow[r, "i_S"] \arrow[d, "f"] & S^{-1}M \arrow[d, "S^{-1}f"] \\ N \arrow[r, "i_S"] & S^{-1}N \end{tikzcd} \ .$$

Proposition 2.7 Le foncteur $M \mapsto S^{-1}M$ est exact *i.e.* si la suite $M' \stackrel{\alpha}{\to} M \stackrel{\beta}{\to} M''$ est exacte, alors la suite induite :

$$S^{-1}M' \stackrel{S^{-1}\alpha}{\to} S^{-1}M \stackrel{S^{-1}\beta}{\to} M''$$

l'est aussi.

Démonstration : Soit $m/s \in \ker S^{-1}\beta$. On a $s'\beta(m) = 0$ pour un certain $s' \in S$. Donc $\beta(s'm) = 0$ *i.e.* $s'm \in \ker \beta = \operatorname{Im} \alpha$. Il existe alors un $m' \in M'$ tel que $\alpha(m') = s'm$. On a alors $S^{-1}\alpha(m'/(ss')) = m/s$. *q.e.d.*

3 Anneaux factoriels

Soit A un anneau. Soit un élément $a \in A$ qui n'est ni 0 ni inversible. On dit que a est *irréductible* si :

$$a = bc \Rightarrow b \text{ ou } c \text{ inversible} \ .$$

On dit que a est premier si l'idéal (a) est premier.

Exercice 5 Premier $\Rightarrow$ irréductible

Définition 1 (Anneau factoriel) On dit qu'un anneau A est factoriel s'il est intègre et si :

i) tout élément $a \in A$ se décompose :
$$a = \prod_i a_i$$
où les a_i sont irréductibles ;

ii) si $\prod_{i \in I} a_i = \prod_{j \in J} b_j$ pour certains a_i, b_j irréductibles, alors il existe une bijection : $I \to J$, $i \mapsto j(i)$ telle que $a_i = b_{j(i)}$ à un facteur inversible près pour chaque i.

Voici un fait bien connu :

Proposition 3.1 Un anneau principal est factoriel.

Proposition 3.2 Dans un anneau factoriel, tout élément irréductible est premier.

Exercice 6 Si k est un corps, alors $k[X]$ contient une infinité de polynômes irréductibles deux à deux non associés.

Proposition 3.3 Si A est factoriel, alors $A[X]$ aussi.

Si $0 \neq f \in A[X]$, on note $c(f)$ le *contenu* de f : c'est le pgcd des coefficients de f. Les éléments irréductibles de $A[X]$ sont les $a \in A$ irréductibles et les $f \in A[X]$ de contenu $c(f) = 1$ et irréductible dans $K[X]$ où K est le corps des fractions de A.

Corollaire 3.3.1 L'anneau $k[X_1, ..., X_n]$ est factoriel.

Corollaire 3.3.2 Dans l'anneau $k[X_1, ..., X_n]$, tout polynôme irréductible engendre un idéal premier.

Exemple : dans l'anneau $k[T_{i,j} \ : \ 1 \leq i, j \leq n]$, le polynôme $\text{dét}\,(T_{i,j}) - 1$ est irréductible. En effet, c'est un polynôme de degré 1 en $T_{1,1}$, donc irréductible sur le corps $k(T_{i,j} \ : \ (i,j) \neq (1,1))$ et en raisonnant par récurrence, on voit que ses coefficients dans $k[T_{i,j} \ : \ (i,j) \neq (1,1)]$ sont premiers entre eux. En particulier, l'idéal $(\text{dét}\,(T_{i,j}) - 1)$ est premier et l'anneau $k[T_{i,j}]/(\text{dét}\,(T_{i,j}) - 1)$ est premier.

4 Éléments entiers

Soit A un sous-anneau d'un anneau B. On dit que $b \in B$ est *entier* sur A si :

$$b^n + a_1 b^{n-1} + ... + a_n = 0$$

pour certains $a_i \in A$. On dit que B est entier sur A si tous ses éléments le sont.

Exercice 7 Soient $A \subseteq B$ deux anneaux intègres. Alors A est un corps si et seulement si B est un corps.

Proposition 4.1 Soit A un sous-anneau d'un anneau B. Un élément $b \in B$ est *entier* sur A si et seulement s'il existe un $A[b]-$module fidèle M (*i.e.* $xM = 0$, $x \in A[b] \Rightarrow x = 0$) tel que M soit un $A-$ module de type fini.

Proposition 4.2 Soit A un sous-anneau d'un anneau B. Le $A-$module B est de type fini si et seulement si la $A-$algèbre B est de type fini et entière sur A.

On en déduit le :

Théorème 4.3 Soit A un sous-anneau d'un anneau B. L'ensemble des $b \in B$ qui sont entiers sur A est un sous-anneau de B.

Démonstration : Soient $\alpha, \beta \in B$ entiers sur A. Il existe $m, n \geq 1$, $a_1, ..., a_m \in A$, $b_1, ..., b_n \in A$ tels que :

$$\alpha^m + a_1\alpha^{m-1} + ... + a_m = \beta^n + b_1\beta^{n-1} + ... + b_n = 0 \ .$$

Alors on a :

$$A[\alpha, \beta] = A[\alpha][\beta] = A[\alpha] + ... + A[\alpha]\beta^{n-1}$$

$$= A + A\alpha + ... + A\alpha^{m-1}\beta^{n-1}$$

c'est un $A-$module de type fini. Donc tout élément de $A[\alpha, \beta]$ est entier sur A. *q.e.d.*

L'ensemble des $b \in B$ entiers sur A est la *fermeture intégrale* de A dans B. On note par exemple $\overline{\mathbb{Z}}$ la fermeture intégrale de $\mathbb{Z}$ dans $\mathbb{C}$. C'est l'anneau des *entiers algébriques.*

Proposition 4.4 Soit A un anneau intègre de corps des fractions K. Soit L une extension de corps de K. Si $x \in L$ est algébrique sur K, alors il existe $0 \neq d \in A$ tel que dx est entier sur A.

Corollaire 4.4.1 Soit A un anneau intègre de corps des fractions K. Soit L une extension de corps de K. La fermeture intégrale de A dans L a pour corps des fractions L.

Définition 2 (intégralement clos) Un anneau intègre A est intégralement clos s'il est égal à sa fermeture intégrale dans son corps des fractions.

Proposition 4.5 Factoriel $\Rightarrow$ intégralement clos.

Exemples : Les anneaux $\mathbb{R}[\cos t, \sin t], k[X_1, X_2, X_3, X_4]/(X_1X_2 - X_3X_4)$, ($k$ corps), $\overline{\mathbb{Z}}$ sont intégralement clos mais non factoriels. Soit k un corps. Soit $f \in k[X, Y]$ tel que $(f, \partial_X f, \partial_Y f) = (1)$. Alors l'anneau $k[X, Y]/(f)$ est intégralement clos.

Proposition 4.6 Soit A un anneau intégralement clos de corps des fractions K. Soit L une extension finie de A. Un élément $x \in L$ est entier sur A si et seulement si son polynôme minimal est à coefficients dans A.

Corollaire 4.6.1 Soit A un anneau intégralement clos de corps des fractions K. Soit $f(X) \in A[X]$ un polynôme unitaire. Les facteurs irréductibles unitaires de $f(X)$ dans $K[X]$ sont dans $A[X]$.

Théorème 4.7 (normalisation de Nœther) Soit k un corps. Soit A une $k-$algèbre de type fini. Il existe $a_1, ..., a_r \in A$ tels que A est entière sur $k[a_1, ..., a_r]$ et $a_1, ..., a_r$ sont $k-$algébriquement indépendants (*i.e.* : pour tout $P \in k[T_1, ..., T_r]$, $P(a_1, ..., a_r) = 0 \Rightarrow P = 0$).

Remarque : Si $A = k[x_1, ..., x_n]$ et si k est infini, alors il existe $f_1, ..., f_r$ des combinaisons $k-$linéaires des x_i telle que les f_i sont algébriquement indépendants sur k et A est entière sur $k[f_1, ..., f_r]$.

5 Degré de transcendance

Soit A une $k-$algèbre.
On pose

$$\partial_k(A) := \sup\{m \geq 0 \ : \ {}^\exists a_1, ..., a_m \in A \text{ algébriquement indépendants sur } k\} \ .$$

Rappels (définitions) : soit K/k une extension de corps ; on dit qu'une famille $a_1, ..., a_m$ d'éléments de K est une base de transcendance de K sur k si les a_i sont algébriquement indépendants sur k et si l'extension $K/k(a_1, ..., a_m)$ est algébrique.

S'il existe une base de transcendance finie, alors toutes les bases de transcendance ont le même cardinal : c'est le degré de transcendance de K/k noté $\text{degtr}_k K$ (*cf. Jacobson, Basic algebra II, §3.6 et 8.12*).

On a aussi :

Théorème de la base incomplète : Soient $a_1, ..., a_m, a_{m+1}, ...a_{m+n} \in K$ tels que :

— les $a_1, ..., a_m$ sont algébriquement indépendants sur k,

— $K/k(a_1, ..., a_{m+n})$ est algébrique,

alors on peut compléter les $a_1, ..., a_m$ en une base de transcendance de K sur k en prenant certains a_j, $m < j \leq m + n$. En particulier, toute extension de corps de type fini admet une base de transcendance finie.

Propriétés : si $K_1 \subseteq K_2 \subseteq K_3$, si K_3/K_1 est de type fini alors K_2/K_1 aussi et : $\partial_{K_1}(K_3) = \partial_{K_1}(K_2) + \partial_{K_2}(K_3)$.

Si A est intègre, alors $\partial_k(A) = \text{degtr}_k(\text{Frac}(A))$.

Exemples : $\partial_k(k(X_1, ..., X_n)) = n$, $\partial_k(k[X, Y, Z, T]/(XY - ZT - 1)) = 3$, $\partial_k(k[T, T^{-1}]) = \partial_k(k[X, Y]/(X^2 + Y^2 - 1) = 1$, plus généralement, si $f \in k[X_1, ..., X_n]$ est non constant, alors $\partial_k(k[X_1, ..., X_n]/(f)) = n - 1$.

6 Produit tensoriel

Soit A un anneau. Soient M, N, P des $A-$modules. On dit qu'une application

$$\phi : M \times N \to P$$

est $A-$bilinéaire si :

$$\forall x, x' \in M, \forall y \in N, \phi(x + x', y) = \phi(x, y) + \phi(x', y)$$

$$\forall x \in M, \forall y, y' \in N, \phi(x, y + y') = \phi(x, y) + \phi(x, y')$$

$$\forall a \in A, \forall x \in M, \forall y \in N, \phi(ax, y) = \phi(x, ay) = a\phi(x, y)$$

i.e. ϕ est $A-$linéaire en chaque variable.

Soient M, N deux $A-$modules.

6.1 Propriété universelle

Théorème 6.1 Il existe un $A-$module noté $M \otimes_A N$ engendré par des éléments notés $m \otimes n$, $(m, n) \in M \times N$ tel que $\mu : M \times N \to M \otimes_A N$, $(m, n) \mapsto m \otimes n$ est bilinéaire et pour tout morphise bilinéaire de $A-$modules : $\phi : M \times N \to P$ il existe un unique morphisme linéaire $\widetilde{\phi} : M \otimes_A N \to P$ tel que $\widetilde{\phi}(m \otimes n) = \phi(m, n)$.

Remarque : un tel module est unique à isomorphisme près.

6.2 Construction du produit tensoriel

Soit $A^{(M \times N)}$ le $A-$module libre de base $M \times N$. Chaque élément de $A^{(M \times N)}$ est une somme finie de la forme :

$$\sum_i a_i (x_i, y_i)$$

pour certains $a_i \in A$, $(x_i, y_i) \in M \times N$.

Soit R le sous-$A-$module de $A^{(M \times N)}$ engendré par :

$$(x + x', y) - (x, y) - (x', y),\ x, x' \in M, y \in N$$

$$(x, y + y') - (x, y) - (x, y'),\ x \in M, y, y' \in N$$

$$(ax, y) - a(x, y),\ a \in A, x \in M, y \in N$$

$$(x, ay) - a(x, y),\ a \in A, x \in M, y \in N\ .$$

On note $m \otimes n$ la classe de $(m, n) \bmod R$. On pose alors $M \otimes_A N := A^{(M \times N)}/R$.

Exercice 8 Vérifier que cette construction démontre le théorème.

6.3 Propriétés exemples

Proposition 6.2 Si M est un $A-$ module libre de base $(e_i)_{i\in I}$ et N un $A-$module libre de base $(f_j)_{j\in J}$, alors $M\otimes_A N$ est un $A-$module libre de base $(e_i\otimes f_j)_{(i,j)\in I\times J}$. En particulier, si E, F sont des $k-$espaces vectoriels, $\dim_k(E\otimes_k F)=\dim_k E.\dim_k F$.

Exemples : — $A\otimes_A M\simeq M$; — si s est une partie multiplicative de A, alors $S^{-1}A\otimes_A M\simeq S^{-1}M$; — si I est un idéal de A, alors $A/I\otimes_A M\simeq M/IM$; — si $k\subseteq K$ sont des corps, alors $K\otimes_k k[X]\simeq K[X]$;

— si m, n sont des entiers de pgcd d, alors : $\mathbb{Z}/m\otimes_{\mathbb{Z}}\otimes\mathbb{Z}/n\simeq\mathbb{Z}/d$.

— si E, F sont des $k-$espaces vectoriels de dimension finie, alors $E^*\otimes_k F\simeq \mathrm{Hom}_k(E,F)$.

— Soient $A\in M_{m,n}(k), B\in M_{p,q}(k)$; on peut définir une application linéaire : $A\otimes B : k^n\otimes k^q\to k^m\otimes k^p$, $x\otimes y\mapsto Ax\otimes By$. Soient (e_i), (e'_j), (f_k), (f'_l) les bases canoniques de k^n, k^m, k^q, k^p. La matrice de $A\otimes B$ dans les bases $(e_i\otimes f_k)$, $(e'_j\otimes f'_l)$ est

$$(A_{i,j}B)_{i,j}\in M_{mp,nq}(k)$$

(c'est le produit de Kronecker de A et B) ;

— $\mathbb{Q}\otimes_{\mathbb{Z}}\mathbb{Q}/\mathbb{Z}=0$;

— si M est un $A-$module de type fini, alors $M\otimes_A M\neq 0$ (en revanche, $\mathbb{Q}/\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Q}/\mathbb{Z}=0$).

6.4 Produit tensoriel d'algèbres

Soient A, B deux $k-$algèbres. On peut munir $A\otimes_k B$ d'une structure de $k-$algèbres en posant :

$$(a\otimes b).(a'\otimes b'):=aa'\otimes bb'$$

pour tous $a, a'\in A, b, b'\in B$. Justifier !

Exercice 9 a) si k est un corps, alors $k[X]\otimes_k k[X]\simeq k[X,Y]$;

b) si I, J sont des idéaux de A, $A/I\otimes_A A/J\simeq A/(I+J)$;

c) $\mathbb{Q}\otimes_{\mathbb{Z}}\mathbb{Q}\simeq\mathbb{Q}$;

6.5 Algèbre tensorielle, algèbre symétrique d'un module

Pour $r\geq 0$, on pose

$$T^rM:=\underbrace{M\otimes_A ...\otimes_A M}_{r}\ .$$

On pose $TM:=\oplus_r T^rM$. On peut munir TM d'une structure de $A-$algèbre (non commutative) en requérant que la multiplication soit induite par les applications bilinéaires :

$$T^rM\times T^sM\to T^{r+s}M$$

$$(m_1\otimes...\otimes m_r, m_{r+1}\otimes ..., \otimes m_{r+s})\mapsto m_1\otimes ...\otimes m_{r+s}$$

Exercice 10 La paire $(M, i : M \to TM)$ vérifie la propriété universelle suivante :

$$\begin{tikzcd} M \arrow[r, "i"] \arrow[dr, "\forall A-\text{lin}"'] & TM \arrow[d, dashed, "\exists! A-\text{alg}"] \\ & R \end{tikzcd}$$

pour toute $A-$algèbre R (non nécessairement commutative).

Remarque : Si M est un $A-$module libre de base $x_1, ..., x_n$, alors TM est isomorphe à l'algèbre polynomiale non commutative en n variables.

Algèbre symétrique :

pour tout $r \geq 0$, on note $S^r M$ le quotient de $T^r M$ par le sous-$A-$module engendré par les

$$m_1 \otimes ... \otimes m_r - m_{\sigma(1)} \otimes ... \otimes m_{\sigma(r)},\ \sigma \in S_r\ .$$

On note $m_1 \cdots m_r$ la classe de $(m_1, ..., m_r)$.

On peut vérifier que pour toute application $r-$linéaire symétrique : $f : M^r \to N$, il existe une unique application linéaire $\widetilde{f} : S^r M \to N$ telle que $\widetilde{f}(m_1 \cdots m_r) = f(m_1, ..., m_r)$.

On pose $\mathrm{Sym}(M) := \oplus_r S^r M$.

Vérifier que $\mathrm{Sym}(M)$ peut être munie d'une structure de $A-$algèbre commutative en posant :

$$(m_1 \cdots m_r) \cdot (m_{r+1} \cdots m_{r+s}) := m_1 \cdots m_{r+s}\ .$$

Vérifier aussi ue la paire $(\mathrm{Sym}(M), i) : M \to \mathrm{Sym}(M)$ vérifie la propriété universelle suivante :

$$\begin{tikzcd} M \arrow[r, "i"] \arrow[dr, "\forall A-\text{lin}"'] & TM \arrow[d, dashed, "\exists! A-\text{alg}"] \\ & R \end{tikzcd}$$

pour toute $A-$algèbre R commutative.

Exercice 11 Si M est un $A-$module libre de base $e_1, ...e_n$, on a un isomorphisme de $A-$algèbres :

$$A[X_1, ..., X_n] \simeq \mathrm{Sym}(M),\ P(X_1, ..., X_n) \mapsto P(e_1, ..., e_n)\ .$$

7 Le théorème des zéros de Hilbert

7.1 Lemme de Zariski

Exercice 12 Si k est un corps, alors il y a une infinité d'éléments irréductibles dans $k[X]$.

Lemme 7.1 (Zariski) Soient $k \subseteq K$ deux corps. Si K est une $k-$algèbre de type fini, alors K est algébrique sur k (et donc finie). En particulier si k est algébriquement clos, $K = k$.

Démonstration :

Première méthode :

Lemme 7.2 Soient $A \subseteq B \subseteq C$ trois anneaux tels que :

i) A est nœthérien ;

ii) C est une $A-$algèbre de type fini ;

iii) C est une $B-$ algèbre finie ;

alors, B est aussi une $A-$algèbre de type fini.

Démonstration : $C = A[c_1, ..., c_n]$, $C = Be_1 + ... + Be_r$. Soient $b_{i,j}, b_{i,j,k} \in B$ tels que :

$$c_i = \sum_{i,j} b_{i,j} e_j$$

$$e_i e_j = \sum_{i,j,k} b_{i,j,k} e_k$$

alors : $C = A'e_1 + ... + A'e_r$ où $A' = A[b_{i,j}, b_{i,j,k}]$ est nœthérien. Donc B est aussi un $A'-$module nœthérien. *q.e.d.*

Exercice 13 En déduire qu'un corps qui est une $\mathbb{Z}-$algèbre de type fini est un corps fini.

On raisonne par récurrence sur le nombre minimal de générateurs de la $k-$algèbre K.

Si $K = k[x_1, ..., x_r]$, alors par hypothèse de récurrence, $k(x_1)[x_2, ..., x_r] = K$ est algébrique sur $k(x_1)$. Donc, d'après le lemme, $k(x_1)$ est aussi une $k-$algèbre de type fini. Donc $k(x_1)$ n'est pas isomorphe à $k(T)$ *i.e.* x_1 est algébrique sur k.

Deuxième méthode :

Lemme 7.3 Si A est un anneau intègre, si $f \in A[X]$, alors $A[X]_f$ n'est pas un corps.

Lemme 7.4 Soient $A \subseteq B$ deux anneaux. Si B est entier sur A, alors $A \cap B^\times = A^\times$. En particulier, B est un corps si et seulement si A l'est.

Proposition 7.5 Soit A un anneau intègre. Supposons qu'il existe m un idéal maximal de $A[X_1, ..., X_n]$ tel que $A \cap m = 0$. Alors, il existe $0 \neq a \in A$ tel que A_a est un corps et $A[X_1, ..., X_n]/m$ est une extension finie de A_a.

On en déduit le lemme de Zariski.

q.e.d.

7.2 Théorème des zéros

Soit k un corps. Notons k^a une clôture algébrique de k.

Théorème 7.6 (nullstellensatz) Si I est un idéal propre de $k[X_1, ..., X_n]$, alors il existe $a := (a_1, ..., a_n) \in (k^a)^n$ tel que pour tout $f \in I$, $f(a) = 0$.

Corollaire 7.6.1 Si k est algébriquement clos, les idéaux maximaux de $k[X_1, ..., X_n]$ sont de la forme $(X_1 - x_1, ..., X_n - x_n)$ pour certains $x_i \in k$.

Contre-exemple : l'idéal (X^2+1) est maximal dans $\mathbb{R}[X]$.
On a donc une correspondance bijective :

$$\text{idéaux maximaux de } k[X_1, ..., X_n] \overset{1:1}{\longleftrightarrow} \text{points de } k^n$$

si k est algébriquement clos.

Théorème 7.7 (forme forte du nullstellensatz) Soit I un idéal de $k[X_1, ..., X_n]$. Soit $Z(I)$ l'ensemble des $x \in (k^a)^n$ tels que $f(x) = 0$ pour tout $f \in I$. Si $h \in k[X_1, ..., X_n]$ est nul sur $Z(I)$, alors $h^m \in I$ pour un certain $m \geq 0$.

Si I est un idéal d'un anneau A, on note $\sqrt{I} := \{h \in A \,:\, {}^{\exists}n,\, h^n \in I\}$: c'est le radical de I et c'est encore un idéal de A.

Un *idéal radical* est un idéal égal à son radical.
Remarques :

a) $\sqrt{\sqrt{I}} = \sqrt{I}$, si I est premier, $\sqrt{I} = I$.

b) À partir de $Z(I)$, on peut retrouver $\sqrt{I}$.

c) Si k est algébriquement clos, on a une correspondance bijective :

$$\text{idéaux maximaux de } k[X_1, ..., X_n] \text{ qui contiennent } I \overset{1:1}{\longleftrightarrow} \text{points de } Z(I)$$

Proposition 7.8 Le radical d'un idéal I d'une $k-$algèbre de type fini A est l'intersection des idéaux maximaux qui le contiennent :

$$\sqrt{I} = \cap_{m \supseteq I} m \ .$$

En particulier, si A est réduite, $\cap_{m \,\text{maximal}} m = 0$.

Contre-exemple : dans l'anneau $k[T]_{(T)}$, l'idéal nul est premier donc égal à son radical mais n'est pas l'intersection du seul idéal maximal qui le contient : (T).

Définition 3 Un anneau de Jacobson est un anneau où chaque idéal premier est l'intersection des idéaux maximaux le contenant.

Les $k-$algèbres de type fini sont de Jacobson.

Exercice 14 $\mathbb{Z}$ est un anneau de Jacobson.

8 Ensembles algébriques

On suppose ici que k est un corps algébriquement clos.

8.1 Définitions

Un *ensemble algébrique* de k^n est une partie de la forme :

$$Z(S) = \{x \in k^n \ : \ {}^{\forall}f \in S, f(x) = 0\}$$

où $S \subseteq k[X_1, ..., X_n]$.
Remarque : soit I l'idéal engendré par S. On a $Z(S) = Z(I)$. En particulier les ensembles algébriques peuvent être définis par un nombre fini d'équations polynômiales.

Proposition 8.1 Les faits suivants sont vrais :

i) $I \subseteq J \Rightarrow Z(I) \supseteq Z(J)$;

ii) $Z(0) = \mathrm{Spec_m}(A)$, $Z((1)) = \emptyset$;

iii) $Z(IJ) = Z(I \cap J) = Z(I) \cup Z(J)$;

iv) $Z(\sum_\alpha I_\alpha) = \cap_\alpha Z(I_\alpha)$.

Exemples : les sous-espaces vectoriels de k^n. Si $f \in k[X, Y]$ est irréductible, on dit que $Z(f)$ est une courbe algébrique plane irréductible.

Exercice 15 L'ensemble $\{(t, t^2, t^3)\ :\ t \in k\}$ est un ensemble algébrique de k^3.

Si $Z \subseteq k^n$, on définit $I(Z) = \{f \in k[X_1, ..., X_n]\ :\ f|_Z = 0\}$.
On a :

Proposition 8.2 i) si Z est un sous-ensemble algébrique de k^n, alors $Z = Z(I(Z))$;

ii) si I est un idéal de $k[X_1, ..., X_n]$, alors $I(Z(I)) = \sqrt{I}$.

8.2 Topologie de Zariski

L'ensemmble des sous-ensembles algébriques de k^n vérifie les axiomes d'un ensemble de fermés pour une topologie : c'est la *topologie de Zariski.*

Exemples : les fermés de k sont k, $\emptyset$ et les ensembles finis de points ; les fermés de k^2 sont k^2, $\emptyset$ et les réunions finies de points et de courbes irréductibles.

Proposition 8.3 Soit Z un sous-ensemble algébrique de k^n muni de la topologie de Zariski induite.

i) les points de Z sont fermés ;

ii) toute suite décroissante de fermés est stationnaire ;

iii) de tout recouvrement ouvert on peut extraire un sous-recouvrement fini.

On dit qu'un espace topologique est *nœthérien* s'il vérifie ii).

8.3 Anneau des coordonnées

Soit Z un sous-ensemble algébrique de k^n. On note $k[Z] := \{P|_Z\ :\ P \in k[X_1, ..., X_n]\}$

Remarque : l'anneau $k[Z]$ est une $k-$algèbre réduite de type fini.

Si I est un idéal de $k[Z]$, on pose $Z(I) := \{x \in Z\ :\ {}^\forall f \in I, f(x) = 0\}$. Si $h \in k[Z]$, on pose $D(h) := \{x \in Z\ :\ h(x) \neq 0\}$.

Proposition 8.4 i) Les points de Z sont en bijection avec les idéaux maximaux de $k[Z]$;

ii) les fermés de Z sont en bijection avec les idéaux radicaux de $k[Z]$;

iii) Les $D(h)$, $h \in k[Z]$, forment une base d'ouverts de la topologie de Zariski de Z.

Remarque : on peut reformuler i) : l'application

$$Z \to \mathrm{Hom}_{k-\mathrm{alg}}(k[Z], k),\ x \mapsto \mathrm{ev}_x$$

est bijective.

8.4 Composantes irréductibles

On dit qu'un espace topologique non vide est *irréductible* s'il n'est pas l'union de deux fermés propres *i.e.* si deux ouverts non vides quelconques s'intersectent toujours *i.e.* si tout ouvert non vide est dense.

Par exemple, les espaces séparés irréductibles sont réduits à un seul point.

Proposition 8.5 Soit Z un sous-ensemble algébrique de k^n. Alors Z est irréductible si et seulement si $I(Z)$ est premier *i.e.* si et seulement si $k[Z]$ est intègre.

Les sous-ensembles algébriques irréductibles de k^n correspondent donc aux idéaux premiers de $k[X_1, ..., X_n]$.

En particulier, si $f \in k[X_1, ..., X_n]$, le sous-ensemble algébrique $Z(f)$ est irréductible si et seulement si f est irréductible dans $k[X_1, ..., X_n]$ ou $f = 0$. Par exemple k^n est irréductible.

Si $f \in k[X_1, ..., X_n]$ se décompose en $f = f_1^{\alpha_1}...f_r^{\alpha_r}$ avec des polynômes f_i irréductibles deux à deux premiers entre eux, alors :

$$Z(f) = \cup_i Z(f_i) \ .$$

Plus généralement, on a :

Proposition 8.6 Si X est un espace topologique nœthérien, alors X est une réunion finie de fermés irréductibles :

$$X = \cup_i X_i$$

et cette décomposition est unique (à permutation près des termes) s'il n'y a pas d'inclusion entre les X_i. On dit que les X_i sont les composantes irréductibles de X.

Exemple : $(xy = 0) = (x = 0) \cup (y = 0)$.

Exercice 16 Si Z est un ensemble algébrique fini, alors $|Z| = \dim_k k[Z]$.

9 Spectre maximal d'un anneau

9.1 Cas général

Soit A un anneau. On note $\mathrm{Spec_m}(A)$ l'ensemble des idéaux maximaux de A (*spectre maximal de* A). Pour tout idéal I de A, on pose :

$$V(I) := \{m \in \mathrm{Spec_m}(A) \ : \ I \subseteq m\} \ .$$

Proposition 9.1 Les faits suivants sont vrais :

i) $I \subseteq J \Rightarrow V(I) \supseteq V(J)$;
ii) $V(0) = \mathrm{Spec_m}(A)$, $V((1)) = \emptyset$;
iii) $V(IJ) = V(I \cap J) = V(I) \cup V(J)$;
iv) $V(\sum_\alpha I_\alpha) = \cap_\alpha V(I_\alpha)$.

9.1.1 Topologie de Zariski

L'ensemble des parties de $\mathrm{Spec_m}(A)$ de la forme $V(I)$, I idéal de A, vérifie les axiomes qui définissent les fermés d'une topologie de $\mathrm{Spec_m}(A)$. C'est la *topologie de Zariski de* $\mathrm{Spec_m}(A)$.

Exercice 17 Si $A = k[T]$, déterminer les fermés de $\mathrm{Spec_m}(A)$.

Si $h \in A$, on note $D(h) := \{m \in \mathrm{Spec_m}(A) \ : \ h \notin m\}$.

Les $D(h)$ sont des ouverts de $\mathrm{Spec_m}(A)$ pour la topologie de Zariski et en forment une base d'ouverts. En effet, si I est un idéal engendré par une partie S, alors :

$$\mathrm{Spec_m}(A) \setminus V(I) = \cup_{h \in S} D(h) \ .$$

Proposition 9.2 i) Soit $h \in A$, on a un homéomorphisme :

$$D(h) \simeq \mathrm{Spec_m}(A_h),\ m \mapsto mA_h \ .$$

ii) soit I un idéal de A. On a un homéomorphisme d'espaces topologiques :

$$V(I) \simeq \mathrm{Spec_m}(A/I),\ J \mapsto J/I \ .$$

iii) Si $A = A_1 \times ... \times A_n$ est un produit d'anneaux, alors $\mathrm{Spec_m}(A) = \cup_i \mathrm{Spec_m}(A_i)$, réunion disjointe d'ouverts.

Exercice 18 Soit u un endomorphisme d'un $\mathbb{C}-$espace vectoriel de dimension finie. Vérifier que $\mathrm{Spec_m}(\mathbb{C}[u]) = \{(u - \lambda \mathrm{Id}) \ : \ \lambda \in \mathrm{sp}(u)\}$.

Étudions plus précisément la topologie de Zariski :

si $S \subseteq A$, on note $V(S) := \{m \in \mathrm{Spec_m}(A) \ : \ S \subseteq m\}$ et si $W \subseteq \mathrm{Spec_m}(A)$, on note $I(W) := \cap_{m \in W} m$.

Proposition 9.3 i) Les $V(S)$ sont fermés dans $\mathrm{Spec_m}(A)$, $I(W)$ est un idéal radical de A.

ii) $V(I(W))$ est l'adhérence de W dans $\mathrm{Spec_m}(A)$. En particulier, si W est fermé, $V(I(W)) = W$.

Exercice 19 Si A est nœthérien, l'espace topologique $\mathrm{Spec_m}(A)$ aussi.

9.2 Applications entre spectres maximaux

Soit $\phi : A \to B$ un morphisme de $k-$algèbres.

Proposition 9.4 Si m est un idéal maximal de B, alors $\phi^{-1}(m)$ est un idéal maximal de A.

Remarque : cette proposition est fausse si A, B ne sont pas des $k-$algèbres dte type fini. Par exemple, si $A = k[T]_{(T)}$, $B = A[X]$, $m = (XT - 1)$, alors $m \cap A = 0$ n'est pas maximal.

On pose $\phi^* : \mathrm{Spec_m}(B) \to \mathrm{Spec_m}(A)$, $m \mapsto \phi^{-1}(m)$.

Proposition 9.5 L'application $\phi^* : \mathrm{Spec_m}(B) \to \mathrm{Spec_m}(A)$ est continue.

9.3 Cas des $k-$algèbres de type fini

Soit k un corps algébriquement clos. Soit A une $k-$algèbre de type fini. On supposera k algébriquement clos. Si $\phi : A \to k$ est un morphisme de $k-$algèbres, alors $\ker \phi$ est un idéal maximal de A car $A/\ker\phi \simeq k$.

Proposition 9.6 On a une bijection :

$$\mathrm{Hom}_{k-alg}(A,k) \stackrel{1:1}{\longleftrightarrow} \mathrm{Spec_m}(A),\ \phi \mapsto \ker\phi\ .$$

On en déduit que si A est une $k-$algèbre de type fini réduite, k algébriquement clos, on peut identifier A à une sous-algèbre des fonctions : $\mathrm{Spec_m}(A) \to k$ en posant $a(\ker\phi) := \phi(a)$ (*exo*) .

Définition 4 Une variété algébrique affine est un couple $(X, k[X])$ où X est un ensemble, $k[X]$ est une sous-$k-$algèbre des fonctions $X \to k$, contenant 1, réduite (c'est automatique) et de type fini tel que $X \to \mathrm{Hom}_{k-alg}(k[X], k)$, $x \mapsto \mathrm{ev}_x$ est bijective

Exemples :
— $(\mathrm{Spec_m}(A), A)$, si A est une $k-$algèbre réduite de type fini.
— Si Z est un sous-ensemble algébrique de k^n, alors $(Z, k[Z])$ est une variété algébrique affine.

Remarque : une variété algébrique affine est entièrement déterminée par $k[X]$.

Exercice 20 Vérifier que $(k^\times, k[T, T^{-1}])$ sont des variétés algébriques affines.

Un *morphisme* entre les variétés algébriques affines $(X, k[X])$ et $(Y, k[Y])$ est une application $\phi : X \to Y$ telle que $f \circ \phi \in k[X]$ pour toute $f \in k[Y]$.

Exercice 21 Supposons que A et B sont des $k-$algèbres de type fini. Montrer que l'on peut identifier l'ensemble des morphismes $(\mathrm{Spec_m}(B), B) \to (\mathrm{Spec_m}(A), A)$ et l'ensemble des morphismes de $k-$algèbres $A \to B$.

Proposition 9.7 Soit $(X, k[X])$ une variété algébrique affine, alors il existe un $n \geq 1$ et un sous-ensemble algébrique Z de k^n tel que $(X, k[X]) \simeq (Z, k[Z])$.

9.4 Faisceau des fonctions régulières

On suppose maintenant k algébriquement clos.

Soit A une $k-$algèbre de type fini réduite.

Si $a \in A$ et si $m = \ker\phi$ est un idéal maximal de A, ϕ un morphisme de $k-$algèbres : $A \to k$, on pose :

$$a(\ker\phi) := \phi(a)$$

De cette façon, la $k-$algèbre A s'identifie à une sous-algèbre des fonctions de $\mathrm{Spec_m}(A)$ dans k. (Il suffit de vérifier que si $\phi(a) = 0$ pour tout $\phi \in \mathrm{Hom}_{k-\mathrm{alg}}(A,k)$, alors $a = 0$ (*exo*)).

Avec cette notation, vérifier :

Exercice 22 Si $h \in A$, alors $V(h) = \{x \in \mathrm{Spec_m}(A) \,:\, h(x) = 0\}$, $D(h) = \{x \in \mathrm{Spec_m}(A) \,:\, h(x) \neq 0\}$.

Exercice 23 Si $A = k[X_1, ..., X_n]$, si $a \in A$, si $m = (X_1 - x_1, ..., X_n - x_n)$, alors :

$$a(m) = a(x_1, ..., x_n) \ .$$

Soit U un ouvert de $\mathrm{Spec_m}(A)$.

On dira qu'une application $f : U \to k$ est régulière sur U s'il existe un recouvrement ouvert $U = \cup_i U_i$, des éléments $a_i, b_i \in A$, tels que :

$$^\forall i,\ ^\forall x \in U_i, b_i(x) \neq 0 \text{ et } f(x) = a_i(x)/b_i(x) \ .$$

On notera $\mathscr{O}(U)$ la $k-$algèbre des fonctionsrégulières sur U.

Par exemple, si $a \in A$, alors $x \mapsto a(x)$ est régulière sur $\mathrm{Spec_m}(A)$ et $x \mapsto 1/a(x)$ est régulière sur $D(a)$.

On a les isomorphismes suivants :

Proposition 9.8 i) $A \simeq \mathscr{O}(\mathrm{Spec_m}(A))$;
ii) $A_h \simeq \mathscr{O}(D(h))$, pour tout $h \in A$.

Par exemple, si $A = k[X]$, si $U = \mathrm{Spec_m}(A) \setminus V((X - x_1)...(X - x_n))$ pour certains $x_i \in k$ deux à deux distincts, U est homéomorphe à $\mathbb{A}^1 \setminus \{x_1, ..., x_n\}$ et les fonctions régulières sur U sont les :

$$\frac{p(X)}{(X - x_1)^{\alpha_1}...(X - x_n)^{\alpha_n}},$$

$p(X) \in k[X]$, $\alpha_1, ..., \alpha_n \geq 0$.

Soit $\phi : A \to B$ un morphisme entre $k-$algèbres réduites. On note $f : \mathrm{Spec_m}(B) \to \mathrm{Spec_m}(A)$ l'application (continue) induite.

Proposition 9.9 Si U est un ouvert de $\mathrm{Spec_m}(A)$, alors pour tout $h \in \mathscr{O}_{\mathrm{Spec_m}(A)}(U)$, $h \circ f \in \mathscr{O}_{\mathrm{Spec_m}(B)}(f^{-1}(U))$.

Exercice 24 Soit $x \in \mathrm{Spec_m}(A)$. On note $\mathscr{O}_x$ l'algèbre des germes de fonctions régulières au voisinage de x *i.e.* :

$$\mathscr{O}_x = \{(f, U) \,:\, x \in U \subseteq \mathrm{Spec_m}(A) \text{ ouvert et } f \text{ régulière sur } U\} / \sim$$

où $(f, U) \sim (g, V)$ s'il existe un ouvert $x \in W \subseteq U \cap V$ tel que $f|_W = g|_W$. Vérifier que l'isomorphisme $A \simeq \mathscr{O}(\mathrm{Spec_m}(A))$ induitun isomorphisme $A_x \simeq \mathscr{O}_x$.