Université Paris 6
Année universitaire 2012-2013
Bref résumé des séances du cours *Les outils de la géométrie algébrique*

1 Le langage des catégories

Notion de catégorie. Quelques exemples.

• Les ensembles, les groupes, les espaces vectoriels sur un corps donné, les espaces topologiques, les espaces topologiques pointés, les espaces topologiques ≪à homotopie près≫, les espaces topologiques pointés à homotopie près

• Les deux catégories associées à un groupe G : la catégorie ayant un seul objet X avec $\mathrm{End}(X) = G$, et la catégorie C telle que Ob $\mathsf{C} = G$ et tel qu'il y ait un et un seul morphisme entre deux objets donnés de C.

• La catégorie N telle que Ob $\mathsf{N} = \mathbb{N}$ et $\mathrm{Hom}(m, n) = M_{n,m}(k)$ pour tout (m, n) (ici, k est un corps fixé).

• Catégorie opposée à une catégorie donnée.

Notion de foncteur (covariance et contravariant). Quelques exemples.

• Foncteurs oublis (des groupes vers les ensembles, des espaces topologiques vers les ensembles, etc.).

• Le foncteur dual $M \mapsto \mathrm{Hom}(M, A)$, dans la catégorie des A-modules (pour A anneau commutatif unitaire fixé).

• Le foncteur $(X, x) \mapsto \pi_1(X, x)$ de la catégorie des espaces topologiques pointés à homotopie près vers celle des groupes.

• Le foncteur $n \mapsto k^n$, de la catégorie N décrite ci-dessus vers celle des k-espaces vectoriels (au niveau des morphismes, il envoie une matrice M sur l'application linéaire de matrice correspondante dans les bases canoniques).

Foncteur plein, foncteur fidèle, foncteur pleinement fidèle, sous-catégorie, sous-catégorie pleine.

Notion de morphisme de foncteurs. Exemple : le morphisme naturel du foncteur identité vers le foncteur bidual, dans la catégorie des A-modules. Isomorphisme de foncteurs, équivalence de catégories et quasi-inverses. Un foncteur est une équivalence de catégorie si et seulement si il est pleinement fidèle et essentiellement surjectif. Quelques exemples d'équivalences de catégories.

• Soit K un corps. Soit C la catégorie des $K[X]$-module, et soit D la catégorie dont les objets sont les couples (M, u) où M est un K-ev et u un endomorphisme de M, et où un morphisme de (M, u) vers (N, v) est une application K-linéaire $f : M \to N$ telle que $v \circ f = f \circ u$. Soit F le foncteur qui envoie un $K[X]$-module M sur le K-ev M muni de $m \mapsto Xm$; soit G le foncteur qui envoie un couple (M, u) sur le $K[X]$-module de groupe additif sous-jacent $(M, +)$ et de loi externe $(P, m) \mapsto P(u)(m)$. Les foncteur F induit une équivalence entre les catégories C et D, et G en est un quasi-inverse. En fait, G est même un inverse de F : la composée FG est vraiment *égale* à Id_{D}, et la composée GF est vraiment *égale* à Id_{C}.

• Le foncteur $n \mapsto k^n$ déjà évoqué de N vers la catégorie des k-ev induit une équivalence entre N et la sous-catégorie pleine de celle des k-ev formée des k-ev de dimension finie : c'est une formulation conceptuelle (ou loufoque, ou pédante) de l'existence de bases.

• Soit (X, x) un espace topologique pointé. La catégorie des $\pi_1(X, x)$-ensembles est celle dont les objets sont les ensembles munis d'une action de $\pi_1(X, x)$, et les flèches les applications $\pi_1(X, x)$-équivariantes.

On suppose que X est connexe et semi-localement simplement connexe. Soit F le foncteur qui associe à un revêtement Y de X sa fibre au-dessus de x, laquelle est un $\pi_1(X, x)$-ensemble de façon naturelle. Le foncteur F induit alors une équivalence entre la catégorie des revêtements de X et celle des $\pi_1(X, x)$-ensembles. Un quasi-inverse est donné par le foncteur qui envoie un $\pi_1(X, x)$-ensemble sur son produit contracté avec le revêtement universel de (X, x).

• Soit X un espace topologique compact. On note $F(X)$ son algèbre des fonctions continues à valeurs complexes. C'est une $\mathbb{C}$-algèbre commutative de Banach (pour la norme sup), munie d'une involution $f \mapsto \overline{f}$ prolongeant la conjugaison complexe, et telle que $||f|| = \sqrt{||f\overline{f}||}$ pour tout f ; soit C la catégorie des $\mathbb{C}$-algèbres de Banach munies d'une involution comme ci-dessus, les morphismes étant les morphismes d'algèbres qui contractent la norme et sont compatibles aux involutions de la source et du but ($\varphi(\overline{f}) = \overline{\varphi(f)}$).

On démontre en analyse fonctionnelle (théorie de Gelfand) que le foncteur F induit une anti-équivalence («anti» signifiant simplement qu'il est contravariant) entre la catégorie des espaces topologiques compacts et la catégorie C.

Nous n'avons pas décrit complètement un quasi-inverse G de F. Indiquons simplement que si A est un objet de C, le sous-ensemble sous-jacent à l'espace topologique compact $G(A)$ est l'ensemble des idéaux maximaux de A (un point d'un espace topologique X définit bien un idéal maximal de l'algèbre $F(X)$, à savoir l'ensemble des fonctions qui s'y annulent ; vous pouvez à titre d'exercice vérifier que si X est compact, on obtient bien ainsi une bijection entre X et l'ensemble des idéaux maximaux de $F(X)$).

Notion de couple de foncteurs adjoints. Quelques exemples.

• Le foncteur oubli de la catégorie des k-ev vers celle des ensembles admet un adjoint à gauche, qui envoie un ensemble X sur le k-ev libre de base indexée par X.

• Soit Ab la sous-catégorie pleine de la catégorie Gp des groupes, constituée des groupes *abéliens*. Le foncteur d'inclusion de Ab dans Gp admet un adjoint à gauche, qui envoie un groupe G sur son «abélianisé» $G/\langle ghg^{-1}h^{-1}\rangle_{(g,h)\in G^2}$.

• Soient X, Y et Z trois ensembles. On dispose d'une bijection naturelle $\mathrm{Hom}(X \times Y, Z) \simeq \mathrm{Hom}(X, \mathrm{Hom}(Y, Z))$. Par conséquent, $X \mapsto X \times Y$ est adjoint à gauche de $Z \mapsto \mathrm{Hom}(Y, Z)$.

Foncteurs représentables et lemme de Yoneda

.

Si C est une catégorie et si X est un objet de C, alors $\mathrm{Hom}(X, .) := Y \mapsto \mathrm{Hom}(X, Y)$ est de manière naturelle un foncteur covariant de C vers Ens. On définit de même un foncteur contravariant $\mathrm{Hom}(., X)$.

Un foncteur covariant F de C vers Ens est dit *représentable* s'il existe un objet X de C et un isomorphisme entre $\mathrm{Hom}(X, .)$ et F. Voici quelques exemples.

a) Si A est un anneau et P une partie de A, le foncteur F qui envoie un anneau B sur l'ensemble des morphismes de A dans B s'annulant sur les éléments de P est représentable : en effet, si π désigne l'application quotient $A \to A/\langle P \rangle$, alors $f \mapsto f \circ \pi$ établit une bijection, fonctorielle en B, entre $\mathrm{Hom}(A/\langle P \rangle, B)$ et $F(B)$.

b) Si A est un anneau et n un entier, le foncteur qui envoie une A-algèbre B sur B^n est représentable. En effet, l'application $f \mapsto (f(X_1), \ldots, f(X_n))$ établit une bijection fonctorielle en B entre $\mathrm{Hom}(A[X_1, \ldots, X_n], B)$ et B^n.

c) SiA est un anneau, n un entier et (P_i) une famille de polynômes appartenant à $A[X_1, \ldots, X_n]$, le foncteur G qui envoie une A-algèbre B sur

$$\{(b_1, \ldots, b_n) \in B^n, P_i(b_1, \ldots, b_n) = 0 \; \forall i\}$$

est représentable. En effet, l'application $f \mapsto (f(\overline{X_1}), \ldots, f(\overline{X_n}))$ établit une bijection fonctorielle en B entre $\mathrm{Hom}(A[X_1, \ldots, X_n]/(P_i)_i, B)$ et $G(B)$.

d) Le foncteur $(X, x) \mapsto \pi_1(X, x)$, vu comme défini sur la catégorie des espaces topologiques pointés à homotopie près, est représentable : il s'identifie naturellement, par sa définition même, à $\mathrm{Hom}((S_1, o), .)$, où S_1 est le cercle et o un point quelconque choisi sur S_1.

Soit C une catégorie et soit $F : \mathsf{C} \to \mathsf{Ens}$ un foncteur covariant. Soit X un objet de C et soit $\xi \in F(X)$. La donnée, pour tout objet Y de C, de l'application de $\mathrm{Hom}(X, Y)$ vers $F(Y)$ qui envoie f sur $F(f)(\xi)$ définit un morphisme de $\mathrm{Hom}(X, .)$ vers F.

On démontre que tout morphisme [1] φ de $\mathrm{Hom}(X, .)$ vers F est de cette forme, pour un unique $\xi \in F(X)$ (qui est égal à $\varphi(X)(\mathrm{Id}_X)$. Par conséquent, F est représentable si et seulement si il existe un objet X de C et un élément $\xi \in F(X)$ tel que $f \mapsto F(f)(\xi)$ définisse pour tout objet Y de C une bijection $\mathrm{Hom}(X, .) \to F$. On dit alors que (X, ξ) est un représentant de F et que ξ est un *objet universel* relativement à F.

Revisitons les exemples a), b), c), et d) de ce point de vue. Le foncteur F de l'exemple a) est représenté par le couple $(A/\langle P \rangle, \pi)$;, et π est un morphisme universel s'annulant sur P. Le foncteur $B \mapsto B^n$ est représenté par le couple $(A[X_1, \ldots, X_n], (X_1, \ldots, X_n))$, et $(X_1, \ldots, X_n)$ est un n-uplet universel d'éléments d'une A-algèbre. Le foncteur G de l'exemple c) est représenté par le couple $(A[X_1, \ldots, X_n]/(P_i)_i, (\overline{X_1}, \ldots, \overline{X_n}))$, et $(\overline{X_1}, \ldots, \overline{X_n})$ est un n-uplet universel d'éléments d'une A-algèbre en lequel les P_i s'annulent. Enfin, en ce qui concerne l'exemple d), identifions (S_1, o) à $(\{z \in \mathbb{C}, |z| = 1\}, 1)$. Le couple $((S_1, o), \theta \mapsto e^{2i\pi\theta})$ représente le foncteur π_1, et $\theta \mapsto e^{2i\pi\theta}$ est un lacet universel à homotopie près.

Supposons donnés deux foncteurs représentables F et G, sur la même catégorie C, et soient (X, ξ) et (Y, η) des représentants respectifs de F et G. Tout morphisme f de Y vers X induit par composition un morphisme de foncteurs $\mathrm{Hom}(X, .) \to \mathrm{Hom}(Y, .)$, puis un morphisme $f^\sharp : F \to G$ (*via* les isomorphismes $\mathrm{Hom}(X..) \simeq F$ et $\mathrm{Hom}(Y, .) \simeq G$ fournis par ξ et η).

J'ai énoncé et démontré le lemme de Yoneda sous sa forme suivante : tout morphisme $\varphi : F \to G$ est de la forme $f^\sharp$ pour un unique morphisme $f : Y \to X$, caractérisé par l'égalité $G(f)(\eta) = \varphi(X)(\xi)$.

On en déduit en particulier que si (X, ξ) et (Y, η) sont deux représentants d'un même foncteur F, il existe un unique morphisme $f : Y \to X$ tel

1. Je ne l'ai énoncé en cours que pour les isomorphismes, mais ma preuve marche en fait pour n'importe quel morphisme.

que $F(f)(\eta) = \xi$, et f est un isomorphisme. Il existe donc, à unique isomorphisme près, un unique couple représentant F. On parle ainsi par abus *du* représentant de F. Il arrivera aussi que l'on dise simplement que X représente F (et non que (X, ξ) représente F), mais c'est un abus : en général, plusieurs ξ conviennent pour le même X.

Exemple d'application du lemme de Yoneda. Soient m et n deux entiers. Soit A un anneau, et soient F et G les foncteurs $B \mapsto B^n$ et $B \mapsto B^m$ sur la catégorie des A-algèbres. Ils sont représentables, de représentants respectifs $(A[X_1, \ldots, X_n], (X_1, \ldots, X_n))$ et $(A[Y_1, \ldots, Y_m], (Y_1, \ldots, Y_m))$. Soit φ un morphisme de F vers G. Par le lemme de Yoneda, il provient d'un unique morphisme de $A[Y_1, \ldots, Y_m]$ vers $A[X_1, \ldots, X_n]$. Un tel morphisme est lui-même donné par m polynômes $P_1, \ldots, P_m$ appartenant à $A[X_1, \ldots, X_n]$ (les images des Y_i). On vérifie immédiatement que φ est alors donné par la formule

$$(b_1, \ldots, b_n) \mapsto (P_1(b_1, \ldots, b_n), \ldots, P_m(b_1, \ldots, b_n)).$$

Ce résultat est un sens assez intuitif : la seule façon d'associer de façon naturelle à tout n-uplet d'éléments d'une A-algèbre B un m-uplet d'éléments de B consiste à utiliser une formule polynomiale à coefficients dans A ; on pouvait s'y attendre, puisque les seules opérations que l'on sache effectuer dans une A-algèbre générale sont l'addition, la multiplication interne, et la multiplication par les éléments de A.

Quelques exemples importants de foncteurs représentables

• *Objet initial, objet final.* Soit C une catégorie. Comme il existe une et une seule application d'un singleton dans un autre, la flèche $\mathsf{C} \to \mathsf{Ens}$ qui envoie un objet X sur un singleton $\{*\}$ peut être vue d'une unique manière comme un foncteur covariant F, et d'une unique manière comme un foncteur contravariant G.

Si F est représentable, on appelle *objet initial* de C tout représentant de F. Un objet X de C est initial si et seulement si $\mathrm{Hom}(X, Y)$ est un singleton pour tout objet Y de C.

Si G est représentable, on appelle *objet final* de C tout représentant de F. Un objet X de C est final si et seulement si $\mathrm{Hom}(Y, X)$ est un singleton pour tout objet Y de C.

Quelques exemples.

- Dans la catégorie des ensembles, $\emptyset$ est initial, et $\{*\}$ est final.

- Dans la catégorie des groupes, $\{e\}$ est initial et final.

- Dans la catégorie des modules sur un anneau A donné, $\{0\}$ est initial et final.

- Dans la catégorie des anneaux, $\mathbb{Z}$ est initial, et $\{0\}$ est final.

-La catégorie des corps n'a ni objet initial, ni objet final. Celle des corps de caractéristique nulle a $\mathbb{Q}$ comme objet initial, et n'a pas d'objet final ; celle des corps de caractéristique $p > 0$ a $\mathbb{F}_p$ comme objet initial, et n'a pas d'objet final.

• *Le produit cartésien.* Le produit cartésien ensembliste $X \times Y$ de deux ensembles X et Y est par définition l'ensemble des couples (x, y) où $x \in X$ et $y \in Y$. Si C est une catégorie et si X et Y sont deux objets de C, on dit que le produit cartésien $X \times Y$ existe si le foncteur contravariant $T \mapsto \mathrm{Hom}(T, X) \times$

$\mathrm{Hom}(T, Y)$ est représentable ; si c'est le cas, on note en général $X \times Y$ son représentant. Attention : ce représentant est en réalité constitué de $X \times Y$ et d'un couple (p, q)de morphismes où p va de $X \times Y$ vers X et q de $X \times Y$ vers Y. Ces morphismes n'ont pas de notation standard ; on les appelle les première et seconde projections.

¡la définition du produit cartésien comme représentant d'un foncteur signifie la chose suivante : pour tout objet T de C, tout morphisme $\lambda : T \to X$ et tout morphisme $\mu : Z \to Y$, il existe un et un seul morphisme $\pi : T \to X \times Y$ tel que $\lambda = p \circ \pi$ et $\mu = q \circ \pi$.

Quelques exemples de catégories dans lesquelles les produits cartésiens existent.

- Dans la catégorie des ensembles, le produit cartésien de deux ensembles est leur produit cartésien ensembliste.

- Dans la catégorie des espaces topologiques, le produit cartésien de deux espaces topologiques est leur produit cartésien ensembliste *muni de la topologie produit.*

- Dans la catégorie des groupes (resp. des anneaux, resp. des A-modules), le produit cartésien de deux objets est leur produit cartésien ensembliste, la ou les opérations étant définies coordonnée par coordonnée.

• *Le produit fibré.* Soient X, Y et Z trois ensembles, et soit $f : X \to Z$ et $g : Y \to Z$ deux applications. Le *produit fibré ensembliste* $X \times_{f,g} Y$ (ou plu simplement $X \times_Z Y$ s'il n'y a pas d'ambiguïté sur la définition des flèches f et g) est par définition l'ensemble des couples (x, y) où $x \in X$, où $y \in Y$ et où $f(x) = g(y)$. Il est muni d'une application naturelle h vers z, qui envoie (x, y) sur $f(x) = g(y)$, et l'on a pour tout $z \in Z$ l'égalité $h^{-1}(z) = f^{-1}(z) \times g^{-1}(z)$: ainsi, $X \times_Z Y$ est un «produit cartésien fibre à fibre», d'où l'expression produit fibré.

Si C est une catégorie, si X, Y et Z sont trois objets de C, et si $f : X \to Z$ et $g : Y \to Z$ sont deux morphismes, on dit que le produit fibré $X \times_{f,g} Y$ (ou plus simplement $X \times_Z Y$ s'il n'y a pas d'ambiguïté sur la définition des flèches f et g) existe si le foncteur contravariant $T \mapsto \mathrm{Hom}(T, X) \times_{\mathrm{Hom}(T,Z)} \mathrm{Hom}(T, Y)$ est représentable ; si c'est le cas, on note en général $X \times_Z Y$ ou $X \times_{f,g} Y$son représentant. Attention : ce représentant est en réalité constitué de $X \times_Z Y$ et d'un couple (p, q)de morphismes où p va de $X \times Y$ vers X et q de $X \times Y$ vers Y, et où $f \circ p = g \circ q$. Ces morphismes n'ont pas de notation standard ; on les appelle les première et seconde projections.

La définition du produit fibré comme représentant d'un foncteur signifie la chose suivante : pour tout objet T de C, tout morphisme $\lambda : T \to X$ et tout morphisme $\mu : T \to Y$ tel que $f \circ \lambda = g \circ \mu$, il existe un et un seul morphisme $\pi : T \to X \times_Z Y$ tel que $\lambda = p \circ \pi$ et $\mu = q \circ \pi$.

Notons que $X \times_Z Y$ est muni d'un morphisme naturel vers Z, à savoir $f \circ p = g \circ q$.

Quelques exemples de catégories dans lesquelles les produits fibrés existent.

- Dans la catégorie des ensembles, le produit fibré de deux ensembles au-dessus d'un troisième est leur produit fibré ensembliste.

- Dans la catégorie des espaces topologiques, le produit fibré de deux espaces topologiques au-dessus d'un troisième est leur produit fibré ensembliste *muni de la topologie produit.*

- Dans la catégorie des groupes (resp. des anneaux, resp. des A-modules), le produit fibré de deux objets au-dessus d'un troisième est leur produit ensembliste, la ou les opérations étant définies coordonnée par coordonnée.

Quelques tautologies

Les démonstrations des assertions qui suivent sont laissées en exercice (seule l'une d'elles a été faite en cours à titre d'exemple.)

• Si C est une catégorie admetta nt un objet final S, et si X et Y sont deux objets de C tels que $X \times Y$ existe, alors $X \times_S Y$ existe et s'identifie à $X \times Y$: les produits cartésiens sont donc des produits fibrés, pour peu qu'il existe un objet final.

• Soit C une catégorie et soit S un objet de C. On note C/S la catégorie dite *des objets de* C *au-dessus de* S. Ses objets sont les couples (X, f), où X est un objet de C et f un morphisme de X vers S ; on note parfois aussi $X \to S$ un tel objet (sans nommer le morphisme). Un morphisme de $X \to S$ vers $Y \to S$ est une flèche $X \to Y$ telle que le diagramme

$$\begin{tikzcd} X \arrow[rr] \arrow[dr] & & Y \arrow[dl] \\ & S & \end{tikzcd}$$

commute.

Soient $X \to S$ et $Y \to S$ deux objets de C/S. Alors le produit cartésien de $(X \to S) \times (Y \to S)$ existe dans C/S si et seulement si $X \times_S Y$ existe, et si c'est le cas alors

$$(X \to S) \times (Y \to S) = X \times_S Y$$

(ce dernier est vu comme objet de C/S *via* son morphisme naturel vers S, *cf. supra*).

Soit X un objet de C et supposons que $X \times S$ existe. On le voit comme un objet de C/S *via* la seconde projection. La restriction à C/S du foncteur $\mathrm{Hom}(., X)$ est alors égale à $\mathrm{Hom}\mathsf{C}/S(., X \times S)$.

• Soit C une catégorie dans laquelle les produits fibrés existent, et soient X, Y Z et T des objets de C. Supposons donnés un morphisme $X \to Z$, un morphisme $Y \to Z$, et un morphisme $T \to Y$. On a alors un isomorphisme naturel

$$(X \times_Z Y) \times_Y T \simeq X \times_Z T,$$

où T est vu comme muni du morphisme $T \to Z$ composé de $T \to Y$ et $Y \to Z$.

Sommes disjointes et sommes amalgamées

Il s'agit des notions duales de celles de produit cartésien et de produit fibré.

• *La somme disjointe.* La somme disjointe ensembliste $X \coprod Y$ de deux ensembles X et Y est par définition la réunion d'une copie de X et d'une copie de Y, rendues disjointes (pou rle faire proprement, on peut par exemple la définir comme le sous-ensemble de $X \cup Y) \times \{0, 1\}$ formé des couples de la forme $(x, 0)$ avec $x \in X$ ou $(y, 1)$ avec $y \in Y$). Si C est une catégorie et si X et Y sont deux objets de C, on dit que la somme disjointe $X \coprod Y$ existe si le foncteur covariant $T \mapsto \operatorname{Hom}(X, T) \times \operatorname{Hom}(Y, T)$ est représentable ; si c'est le cas, on note en général $X \coprod Y$ son représentant. Attention : ce représentant est en réalité constitué de $X \coprod Y$ et d'un couple (i, j)de morphismes où i va de X vers $X \coprod Y$ et j de Y vers $X \coprod Y$. Ces morphismes n'ont pas de notation standard.

La définition de la somme disjointe comme représentant d'un foncteur signifie la chose suivante : pour tout objet T de C, tout morphisme $\lambda : X \to T$ et tout morphisme $\mu : Y \to T$, il existe un et un seul morphisme $\sigma : X \coprod Y \to T$ tel que $\lambda = \sigma \circ i$ et $\mu = \sigma \circ j$.

Quelques exemples de catégories dans lesquelles les sommes disjointes existent.

- Dans la catégorie des ensembles, la somme disjointe de deux ensembles est leur somme disjointe ensembliste.

- Dans la catégorie des espaces topologiques, la somme disjointes de deux espaces topologiques X et Y est leur somme disjointe ensembliste $X \coprod Y$ munie de la topologie définie comme suit : sa restriction à X (resp. Y) identifié à une partie de $X \coprod Y$ est la topologie de X (resp. de Y) ; les parties X et Y de $X \coprod Y$ sont toutes deux ouvertes.

-Dans la catégorie des modules sur un anneau donné A, la somme disjointe de deux modules est leur somme directe. L'ensemble sous-jacent n'est donc pas leur somme disjointe ensembliste (on a identifié les zéros des deux modules, et rajouté les sommes d'éléments).

- Dans la catégorie des groupes, le même type de phénomène se reproduit. Si G et H sont deux groupes, leur somme disjointe dans la catégorie des groupes est le *produit libre $G * H$ de G et H*, défini comme suit. Un élément de $G * H$ est une suite finie (x_i) où chaque x_i est un élément non trivial de G ou H, et telle qu'éléments de G et éléments de H alternent. On fait le produit de deux telles suites en les concaténant, puis en contractant s'il y a lieu le résultat obtenu. Notons que le neutre de $G * H$ est la suite vide.

Par exemple, si $G = H = \mathbb{Z}$, et si l'on écrit $G = a^{\mathbb{Z}}$ et $H = b^{\mathbb{Z}}$ pour distinguer les deux groupes, on voit que $G * H$ est constitué des mots en les lettres a et b : c'est le groupe libre sur deux générateurs.

• *La somme amalgamée*. Soient X, Y et Z trois ensembles, et soit $f : Z \to X \to Z$ et $g : Z \to Y$ deux applications. La *somme amalgamée ensembliste* $X \coprod_{f,g} Y$ (ou plu simplement $X \coprod_Z Y$ s'il n'y a pas d'ambiguïté sur la définition des flèches f et g) est par définition le quotient de $X \coprod Y$ par la relation d'équivalence engendrée par les relations $f(z) \sim g(z)$ pour z parcourant Z. On dispose de deux applications naturelles $X \to X \coprod_Z Y$ et $Y \to X \coprod_Z Y$.

Si C est une catégorie, si X, Y et Z sont trois objets de C, et si $f : Z \to X$ et $g : Z \to Y$ sont deux morphismes, on dit que la somme amalgamée $X \coprod_{f,g} Y$. (ou plus simplement $X \coprod_Z Y$ s'il n'y a pas d'ambiguïté sur la définition des flèches f et g) existe si le foncteur covariant $T \mapsto \operatorname{Hom}(X, T) \coprod_{\operatorname{Hom}(Z,T)} \operatorname{Hom}(Y, T)$ est représentable ; si c'est le cas, on note en général $X \coprod_Z Y$ ou $X \coprod_{f,g} Y$son représentant. Attention : ce représentant est en réalité constitué de $X \coprod_Z Y$ et d'un couple (i, j)de morphismes où i va de X

vers $X \coprod Y$ et J de Y vers $X \coprod Y$, et où $i \circ f = j \circ g$. Ces morphismes n'ont pas de notation standard.

La définition de la somme amalgamée comme représentant d'un foncteur signifie la chose suivante : pour tout objet T de C, tout morphisme $\lambda : X \to T$ et tout morphisme $\mu : Y \to T$ tel que $\lambda \circ i = \mu \circ j$, il existe un et un seul morphisme $\sigma : X \coprod_Z Y \to T$ tel que $\lambda = \sigma \circ i$ et $\mu = \sigma \circ j$.

Notons que Z est muni d'un morphisme naturel vers $X \times_Z Y$, à savoir $i \circ f = j \circ g$.

Quelques exemples de catégories dans lesquelles les sommes amalgamées existent.

- Dans la catégorie des ensembles, la somme amalgamée de deux ensembles le long d'un troisième est leur somme amalgamée ensembliste.

- Dans la catégorie des espaces topologiques, le somme amalgamée de deux espaces topologiques X et Y le long d'un troisième espace Z est leur somme amalgamée ensembliste, munie de la topologie quotient (la somme disjointe $X \coprod Y$ étant munie quant à elle de sa topologie décrite plus haut).

- Dans la catégorie des groupes, la somme amalgamée de deux groupes G et H le long d'un groupe K muni de deux morphismes $g : K \to G$ et $h : K \to H$ existe. Elle est notée $G *_K H$ et se décrit d'une façon analogue au produit libre $G * H$, mais un peu plus compliquée.

On choisit un système de représentants S des classes *non triviales* de H modulo $\varphi(K)$. Un élément de $G *_K H$ est alors une suite finie (x_i) où chaque x_i appartient ou bien à $G - \{e\}$, ou bien à S, les deux situations alternant. On fait le produit des suites par concaténation et simplification, en utilisant la règle $h(k) = g(k)$ pour tout $k \in K$.

- Dans la catégorie des anneaux, la somme amalgamée de deux anneaux B et C le long d'un troisième anneau A existe, c'est le produit tensoriel $B \otimes_C A$, que nous verrons un peu plus loin.

J'invite le lecteur à écrire lui-même à propos des sommes disjointes et amalgamées, les ≪quelques tautologies≫ duales de celles vues plus haut sur les produits cartésiens et produits fibrés.

2 Algèbre commutative

Dans tout ce qui suit, ≪anneau≫ signifiera ≪anneau commutatif unitaire≫, et un morphisme d'anneaux sera toujours par définition unitaire.

Idéaux premiers et maximaux

J'ai rappelé les définitions d'anneau intègre, de corps, d'idéal premier et d'idéal maximal. Puis j'ai proposé une approche particulière de la notion d'idéal premier, qui sera utile en théorie des schémas, et que je vais maintenant détailler.

Les idéaux premiers. Soit A un anneau et soit f un morphisme de A vers un corps K. Il est immédiat que le noyau de f est un idéal premier. Réciproquement, soit $\mathfrak{p}$ un idéal premier de A ; la flèche composée $A \to A/\mathfrak{p} \hookrightarrow \mathrm{Frac}(A/\mathfrak{p})$ a pour noyau $\mathfrak{p}$. Ainsi, les idéaux premiers sont exactement *les noyaux de morphismes dont le but est un corps.*

On peut donc décrire un idéal premier de A comme une classe d'équivalence de morphismes $(A \to K)$ où K est un corps, pour la relation d'équivalence «avoir même noyau». Cette relation admet d'ailleurs une description alternative : si K et L sont deux corps, deux morphismes $A \to K$ et $A \to L$ ont même noyau si et seulement si il existe un corps F et un diagramme commutatif

$$\begin{tikzcd} & & K\,. \\ A \arrow[urr] \arrow[r] \arrow[drr] & F \arrow[ur] \arrow[dr] & \\ & & L \end{tikzcd}$$

En effet, si un tel diagramme existe alors

$$\mathrm{Ker}(A \to K) = \mathrm{Ker}(A \to L) = \mathrm{Ker}(A \to F)$$

puisque $F \to K$ et $F \to L$ sont injectifs en tant que morphismes de corps.

Réciproquement, supposons que $A \to K$ et $A \to L$ aient même noyau $\mathfrak{p}$. En vertu des propriétés universelles du quotient et du corps des fractions, la flèche $A \to K$ admet une unique factorisation sous la forme

$$A \to \mathrm{Frac}(A/\mathfrak{p}) \to K,$$

et il en va de même de $A \to L$. Il existe donc un diagramme comme ci-dessus avec $F = \mathrm{Frac}(A/\mathfrak{p})$.

Remarque. Cette preuve montre que la flèche $A \to \mathrm{Frac}(A/\mathfrak{p})$ est en quelque sorte le plus petit élément de la classe d'équivalence de morphismes $A \to K$ qui correspond à $\mathfrak{p}$.

Les idéaux maximaux. Soit $\mathfrak{m}$ un idéal maximal de A. Le quotient $A/\mathfrak{m}$ est un corps, et la flèche $A \to A/\mathfrak{m}$ est surjective.

Réciproquement, si K est un corps et si $f : A \to K$ est surjective, alors comme K s'identifie à $A/\mathrm{Ker} f$, le noyau de f est un idéal maximal de A.

Ainsi, un idéal maximal de A peut être vu comme une classe d'équivalence, de *surjections* $A \to K$, où K est un corps, pour la relation d'équivalence «avoir même noyau». Et si $A \to K$ et $A \to L$ sont deux surjections ayant même noyau $\mathfrak{m}$, les corps K et L s'identifient tous deux à $A/\mathfrak{m}$ comme A-algèbres. Il y a donc en fait à isomorphisme canonique près une seule surjection dans la classe d'équivalence qui correspond à un idéal maximal donné $\mathfrak{m}$: c'est la surjection quotient de A vers $A/\mathfrak{m}$.

Idéaux maximaux au sein des idéaux premiers. Donnons-nous un idéal premier $\mathfrak{p}$ de A. Il correspond à une classe d'équivalence de morphismes $A \to K$, où K est un corps, dont $A \to \mathrm{Frac}(A/\mathfrak{p})$ est le «plus petit élément». Par ce qui précède, l'idéal $\mathfrak{p}$ est maximal si et seulement si il existe, dans la classe d'équivalence qui lui correspond, un morphisme surjectif. Mais cela revient à demander que le «plus petit» morphisme de la classe, à savoir $A \to \mathrm{Frac}(A/\mathfrak{p})$, soit surjectif, c'est-à-dire encore que $\mathrm{Frac}(A/\mathfrak{p}) = A/\mathfrak{p}$, et donc que $A/\mathfrak{p}$ soit un corps (ce qui est la définition usuelle).

Exemple : le cas de $\mathbb{Z}$. Regardons à quoi correspondent les descriptions précédentes lorsque $A = \mathbb{Z}$. Les idéaux premiers de $\mathbb{Z}$ sont :

- l'idéal (0) ; il correspond à la classe des morphismes injectifs $\mathbb{Z} \to K$, c'est-à-dire des morphismes $\mathbb{Z} \to K$ où K est un corps de caractéristique nulle. Le plus petit morphisme de cette classe est l'inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$, laquelle n'est pas surjective : (0) n'est pas maximal ;

- pour tout nombre premier p, l'idéal (p) ; il correspond à la classe des morphismes $\mathbb{Z} \to K$ de noyau $p\mathbb{Z}$, c'est-à-dire des morphismes $\mathbb{Z} \to K$ où K est un corps de caractéristique p. Le plus petit morphisme de cette classe est la flèche naturelle $\mathbb{Z} \to \mathbb{F}_p$, qui est surjective : (p) est maximal.

Fonctorialité contravariante du spectre. Si A est un anneau, on note Spec A le *spectre* de A, c'est-à-dire l'ensemble des idéaux premiers de A (nous verrons plus tard, lors du cours sur les schémas, que Spec A peut être muni d'une topologie, et même d'une structure supplémentaire).

La flèche $A \mapsto \operatorname{Spec} A$ est de manière naturelle un foncteur *contravariant.* Expliquons pourquoi. Soit $f : A \to B$ un morphisme d'anneau. Nous allons construire de deux façons différentes une application de Spec B vers Spec A ; nous laissons au lecteur le soin de vérifier que les deux applications ainsi obtenues sont les mêmes.

1) Point de vue classique. À un idéal premier $\mathfrak{q}$ de B, on associe l'idéal $f^{-1}(\mathfrak{q})$ de A, dont on vérifie qu'il est premier.

2) Point de vue «morphisme vers les corps» : si K est un corps et $B \to K$ un morphisme, le noyau de la flèche composée $A \to B \to K$ ne dépend que de celui de $B \to K$ (c'est son image réciproque dans A). On peut ainsi sans ambiguïté associer à la classe d'équivalence de $B \to K$ la classe d'équivalence de la composée $A \to B \to K$.

Localisation

Soit A un anneau. Lorsqu'on se donne un sous-ensemble P de A, on sait construire un anneau «défini à partir de A, en *décrétant* que les éléments de P sont nuls, et en n'imposant aucune autre contrainte que celle-ci, et ses conséquences découlant de la théorie générale des anneaux» : c'est le quotient $A/(P)$. Celui-ci est caractérisé par sa propriété universelle, c'est-à-dire encore par le foncteur (ici, covariant) qu'il représente.

C'est en fait une illustration d'un phénomène assez général : à chaque fois lorsqu'on veut intuitivement *imposer* une contrainte, et *seulement* cette contrainte, la construction rigoureuse qui répond à ce caprice s'exprime en termes de propriété universelle, ou encore de foncteur à représenter.

Nous allons en voir un nouvel exemple avec ce qu'on appelle la *localisation.* Soit A un anneau, et soit S un sous-ensemble de A. Le but intuitif est de construire un objet à partir de A en imposant aux éléments de S d'être inversibles – et rien d'autre. Techniquement, on s'intéresse au foncteur covariant

$$F : B \mapsto \{f \in \operatorname{Hom}(A, B), f(s) \in B^* \ \ \forall\, s \in S\},$$

et l'on cherche à montrer qu'il est représentable.

Première méthode. On vérifie sans difficulté que

$$(A[T_s]_{s\in S}/(sT_s-1)_{s\in S}, a\mapsto \overline{a})$$

représente F (notons que si $s\in S$ alors $\overline{s}$ est bien inversible, d'inverse $\overline{T_s}$). C'est la méthode la plus économique, et en un sens la plus naturelle : pour forcer les éléments de S à être inversibles, on adjoint formellement à A un symboles T_s pour chaque élément s de S, et l'on décrète que $sT_s=1$, en passant au quotient.

Mais cette construction présente un défaut : il est *en pratique* extrêmement difficile d'arriver à dire quoi que ce soit sur la A-algèbre $A[T_s]_{s\in S}/(sT_s-1)_{s\in S}$: c'est un cas où la connaissance du foncteur représenté par un objet qui, *en théorie*, caractérise l'objet en question à isomorphisme près, n'est pas suffisante.

Par exemple, il semble *a priori* impossible de donner un critère simple permettant de savoir si $A[T_s]_{s\in S}/(sT_s-1)_{s\in S}$ est nul ou non.

Nous allons donc donner une autre construction du représentant de F. Pour cela, on commence par une petite observation. Convenons de dire qu'une partie T de A est *multiplicative* si elle contient 1 et si $ab\in T$ dès que $a\in T$ et $b\in T$ (les amateurs du style bourbakiste peuvent condenser la définition en demandant simplement que T soit stable par produit fini, ce qui la force à contenir 1 puisque ce dernier est le produit vide). L'ensemble $\widehat{S}$ des produits finis d'éléments de S (en incluant 1 qui est le produit vide) est visiblement la plus petite partie multiplicative de A contenant S. Si B est un anneau et si $f:A\to B$ est un morphisme, il est immédiat que $f(s)$ est inversible pour tout $s\in S$ si et seulement si $f(s)$ est inversible pour tout $s\in\widehat{S}$. On peut donc, pour étudier le foncteur F, remplacer S par $\widehat{S}$; autrement dit, on s'est ramené au cas où S est multiplicative.

On définit alors sur $A\times S$ la relation $\mathscr{R}$ suivante : $(a,s)\mathscr{R}(b,t)$ si et seulement si il existe $r\in S$ tel que $r(at-bs)=0$. On vérifie que c'est une relation d'équivalence, et l'on note $S^{-1}A$ le quotient correspondant.

Les formules

$$(a,s);(b,t))\mapsto(at+bs,st) \text{ et } ((a,s);(b,t))\mapsto(ab,st)$$

passent au quotient, et définissent deux lois $+$ et $\times$ sur $S^{-1}A$ qui en font un anneau commutatif.

Si $(a,s)\in A\times S$, on écrira $\frac{a}{s}$ au lieu de $\overline{(a,s)}$. Cette notation permet de disposer des formules naturelles

$$\frac{a}{s}+\frac{b}{t}=\frac{at+bs}{st} \text{ et } \frac{a}{s}\cdot\frac{b}{t}=\frac{as}{bt},$$

et l'on a

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

L'application $a\mapsto\frac{a}{1}$ est un morphisme d'anneaux de A dans $S^{-1}A$. Si $s\in S$ alors $\frac{s}{1}$ est inversible, d'inverse $\frac{1}{s}$. On vérifie aisément que le couple $(S^{-1}A, a\mapsto\frac{a}{1})$ représente aussi le foncteur F. On dit que $S^{-1}A$ est le *localisé* de a par rapport à la partie multiplicative S.

Quelques commentaires.

• La condition d'égalité entre fractions est plus compliquée que le bon vieux produit en croix traditionnel ; c'est le prix à payer pour travailler avec des anneaux quelconques, *i.e.* non nécessairement intègres ni réduits.

Mais si A est intègre et si S *ne contient pas* 0, alors la condition ≪il existe $r \in S$ tel que $r(at - bs) = 0$≫ équivaut à la relation usuelle ≪$at - bs = 0$≫.

• La flèche $A \to S^{-1}A$ n'est pas injective en général, c'est la raison pour laquelle on préfère souvent écrire $\frac{a}{1}$ et non a. Son noyau est facile à décrire : c'est l'ensemble des éléments a de A tels qu'il existe $r \in S$ vérifiant l'égalité $ra = 0$. Une fois encore, les choses se simplifient si A est intègre et si $0 \notin S$: on voit immédiatement que sous ces hypothèses, $a \mapsto \frac{a}{1}$ est injective.

• L'anneau $S^{-1}A$ est nul si et seulement si $1 = 0$ dans $S^{-1}A$, c'est-à-dire encore si et seulement si $\frac{1}{1} = 0$, donc si et seulement si il existe $r \in S$ tel que $r1 = 0$.

Autrement dit, $S^{-1}A$ est nul si et seulement si $0 \in S$.

Exemples.

1) Si A est intègre, $S := A \setminus \{0\}$ est une partie multiplicative, et $S^{-1}A$ est le corps des fractions de A.

2) Soit A un anneau et soit $f \in A$. La partie multiplicative S engendrée par f est $\{f^n\}_{n\in\mathbb{N}}$. Le localisé correspondant est le plus souvent noté A_f. On déduit de la première construction d'un représentant de F que $A_f \simeq A[T]/(fT - 1)$.

Par ce qui précède, $A_f = 0$ si et seulement si S contient 0, c'est-à-dire si et seulement si f est nilpotent. Donnons une preuve alternative de ce fait. L'anneau A_f est nul si et seulement si $A[T]/(Tf - 1) = 0$, c'est-à-dire si et seulement si $1-Tf$ est inversible dans $A[T]$. Or $1-Tf$ est inversible dans $A[[T]]$, d'inverse $g = \sum f^i T^i$. Par unicité de l'inverse (lorsqu'il existe), on voit que $1-Tf$ est inversible dans $A[T]$ si et seulement si $g \in A[T]$, c'est-à-dire si et seulement si f est nilpotent.

3) Si $\mathfrak{p}$ est un idéal premier de A, alors $S := A \backslash \mathfrak{p}$ est une partie multiplicative, et l'anneau $S^{-1}A$ est le plus souvent noté $A_{\mathfrak{p}}$.

Donnons deux exemples.
- Si A est intègre et si $\mathfrak{p} = \{0\}$, l'anneau $A_{\mathfrak{p}}$ est le corps des fractions de A.
- Soit p un nombre premier. Le localisé $\mathbb{Z}_{(p)}$ est le sous-anneau de $\mathbb{Q}$ égal à

$$\{\frac{a}{b}, a \in \mathbb{Z}, b \in \mathbb{Z} \setminus p\mathbb{Z}\}.$$

Formules explicites. Soit A un anneau, soit S une partie multiplicative de A et soit $\varphi : A \to B$ un morphisme tel que $f(S) \subset B^*$. Le morphisme $\psi : S^{-1}A \to B$ induit par f est donné par la formule

$$\psi\left(\frac{a}{s}\right) = \varphi(a)\varphi(s)^{-1}.$$

On remarque : que le noyau de ψ ne dépend que de celui de φ : c'est $\{\frac{a}{s}, a \in \mathrm{Ker}/;\varphi, s \in S\}$; et que le noyau de φ ne dépend que de celui de ψ : c'est $\{a \text{ t.q. } \frac{1}{a} \in \mathrm{Ker}\ \psi\}$.

Fonctorialité. Soit $f : A \to B$ un morphisme d'anneaux. Soit S une partie multiplicative de A, et soit T une partie multiplicative de B telle que $f(S) \subset T$ (par exemple, $T = f(S)$). La flèche composée $A \to B \to T^{-1}B$ envoyant chaque élément de S sur un inversible, elle induit une flèche $S^{-1}A \to T^{-1}B$, donnée par les formules

$$\frac{a}{s} \mapsto \frac{f(a)}{f(s)}.$$

Idéaux premiers. Soit A un anneau et soit S une partie multiplicative de A. Se donner un morphisme de $S^{-1}A$ vers un corps K revient à se donner un morphisme de A vers K qui envoie chaque élément de A sur un inversible de K, c'est-à-dire sur un élément non nul de K ; cela revient donc à se donner un morphisme de A vers K dont le noyau ne rencontre pas S.

Compte-tenu de la description des idéaux premiers en termes de morphismes vers un corps, et de la remarque faite ci-dessus sur les noyaux (au paragraphe ≪formules explicites≫) on en déduit que

$$\mathfrak{p} \mapsto \mathfrak{p}S^{-1}A = \left\{\frac{a}{s}, a \in \mathfrak{p}, s \in S\right\} \text{ et } \mathfrak{q} \mapsto \left\{a \text{ t.q. } \frac{a}{1} \in \mathfrak{q}\right\}$$

établissent une bijection (visiblement croissante) entre l'ensemble des idéaux premiers de A ne rencontrant pas S et l'ensemble des idéaux premiers de $S^{-1}A$.

Anneaux locaux

Soit A un anneau et soit $\mathfrak{p}$ un idéal premier de A. Par ce qui précède, l'ensemble des idéaux premiers de $A_\mathfrak{p}$ est en bijection croissante avec l'ensemble des idéaux premiers de A ne contenant pas $A \setminus \mathfrak{p}$, c'est-à-dire avec l'ensemble des idéaux premiers de A contenus dans $\mathfrak{p}$. Cet ensemble admet un plus grand élément, à savoir $\mathfrak{p}$. Il s'ensuit que $A_\mathfrak{p}$ admet un et un seul idéal maximal, à savoir $\mathfrak{p}A_\mathfrak{p}$.

En termes de morphismes vers les corps, la situation se décrit ainsi : $A \to \mathrm{Frac}(A/\mathfrak{p})$ (qui définit l'idéal premier $\mathfrak{p}$ de A) envoyant $A \setminus \mathfrak{p}$ dans l'ensemble des éléments inversibles de $\mathrm{Frac}(A/\mathfrak{p})$, il induit un morphisme $A_\mathfrak{p} \to \mathrm{Frac}(A/\mathfrak{p})$. On vérifie que ce morphisme est *surjectif*. Il définit donc un idéal maximal de $A_\mathfrak{p}$, qui est précisément $\mathfrak{p}A_\mathfrak{p}$.

On appelle *anneau local* un anneau ayant un et un seul idéal maximal. Si A est un anneau, on démontre que les assertions suivantes sont équivalentes.

i) A est un anneau local.
ii) L'ensemble $\mathfrak{m}$ des éléments non inversibles de A est un idéal de A.

De plus, si elles sont satisfaites, alors $\mathfrak{m}$ est l'unique idéal maximal de A.

Exemples. On a vu plus haut que si A est un anneau et si $\mathfrak{p}$ est un idéal premier de A, alors $A_\mathfrak{p}$ est local.

Donnons maintenant un exemple plus géométrique. Soit X un espace topologique et soit $x \in X$. On considère l'ensemble des couples (U, f) où U est un voisinage ouvert de x et $f \in \mathscr{C}^0(U, \mathbb{R})$, sur lequel on met la relation d'équivalence suivante : $(U, f) \sim (V, g)$ si et seulement si il existe un voisinage ouvert W de x dans $U \cap V$ tel que $f_{|W} = g_{|W}$. L'ensemble quotient A hérite alors d'une structure d'anneau naturelle. En bref, A est l'ensemble des fonctions continues (à valeurs réelles) définies au voisinage de x, deux fonctions étant considérées comme égales si elles coïncident au voisinage de x ; on dit aussi que A est l'anneau des *germes de fonctions continues en x*. L'évaluation en x induit un morphisme $f \mapsto f(x)$ de A dans $\mathbb{R}$.

Ce morphisme est surjectif, grâce aux fonctions constantes. Son noyau $\mathfrak{m}$ est donc un idéal maximal de A. Nous allons montrer que c'est le seul ; il suffit, par le critère donné ci-dessus, de vérifier que $\mathfrak{m}$ est exactement l'ensemble des éléments non inversibles de A. Soit $f \in A \setminus \mathfrak{m}$. Choisissons un voisinage ouvert U de x sur lequel f est définie. Comme $f \notin \mathfrak{m}$, on a $f(x) \neq 0$. Comme f est continue, il existe un voisinage ouvert V de x dans U sur lequel f ne s'annule pas. L'inverse g de f est alors une fonction continue sur V, et l'on a $fg = 1$ dans l'anneau A. Ainsi f est inversible, ce qui achève la preuve.

Remarque. On aurait pu tout aussi bien remplacer X par une variété différentiable, et A par l'anneau des germes de fonctions $\mathscr{C}^\infty$.

Nous verrons par ailleurs lors du cours de géométrie algébrique que le langage des schémas permet, pour tout anneau A et tout idéal premier $\mathfrak{p}$ de A, d'interpréter $A_\mathfrak{p}$ comme un anneau de germes de fonctions.

Endomorphismes d'un modules de type fini sur un anneau

*Très brefs rappels sur les modules.*Je n'ai pas rappelé en cours la définition de module, c'est la même que celle d'espace vectoriel – le corps de base est simplement remplacé par un anneau de base.

On dispose en théorie des modules des analogues des notions usuelles d'algèbre linéaire : applications linéaires, sous-modules, image, noyau, supplémentaires, familles libres, génératrices, bases, sommes directes....

Toutefois, certaines des propriétés vérifiées par les espaces vectoriels ne le sont plus en général par les modules sur un anneau quelconque (il s'agit des propriétés dont la preuve fait appel de manière essentielle à la division par les scalaires non nuls). Ainsi, si un module sur un anneau A possède toujours une partie génératrice génératrice (lui-même), une partie libre (l'ensemble vide), mais pas nécessairement de base. Lorsqu'il en possède une, on dit qu'il est libre.

Si l'anneau A est non nul, les bases d'un module libre sur A ont toutes même cardinal, appelé le *rang* du module en question (ou sa dimension, lorsque A est un corps).

Mais attention : la famille $(e_i)_{i \in I}$ où $e_i = 0$ pour tout i est une base du module nul sur l'anneau nul *quel que soit le cardinal de I* (nul ou non, fini ou infini...).

Venons-en maintenant aux endomorphismes des modules. J'ai démontré et énoncé les résultats suivants ; on fixe un anneau (toujours commutatif et unitaire) A.

Proposition. *Soit M un A-module possédant une famille génératrice de cardinal n, soit I un idéal de A, et soit u un endomorphisme de M tel que $u(M) \subset IM := \{\sum a_i m_i, a_i \in I, m_i \in M\}$. Il existe alors une famille $(a_1, \ldots, a_n)$ telle que $a_j \in I^j$ pour tout j, et telle que*

$$u^n + a_{n-1}u^{n-1} + \ldots + a_1 u + a_0 \mathrm{Id} = 0.$$

Commentaires.

1) La preuve de cette proposition repose *in fine* sur un calcul matriciel (même si M n'a pas besoin d'être libre) ; celle que j'ai donnée en cours utilise le théorème de Cayley-Hamilton.

2) Lorsque $I = A$, la condition $u(M) \subset IM$ est automatiquement satisfaite. La proposition assure donc entre autres que tout endomorphisme de M annule un polynôme unitaire de degré n à coefficients dans A.

En appliquant la proposition précédente lorsque $u = \mathrm{Id}$, on obtient sans difficulté le corollaire suivant.

Corollaire (lemme de Nakayama). *Soit M un A-module de type fini et soit I un idéal de M. Les assertions suivantes sont équivalentes :*

i) $M = IM$;

ii) il existe un élément a de A congru à 1 modulo I et tel que $aM = \{0\}$.

Supposons que A soit local d'idéal maximal $\mathfrak{m}$. Un élément congru à 1 modulo $\mathfrak{m}$ est alors inversible, et le corollaire suivant se décline comme suit : si M est un A-module de type fini, alors $M = \mathfrak{m}M$ si et seulement si $M = \{0\}$ (c'est la formulation originelle du lemme de Nakayama).

Nous allons donner un deuxième corollaire de la proposition ci-dessus, assez spectaculaire, et dont je vais indiquer la preuve qui me semble très élégante.

Corollaire. *Soit M un A-module de type fini et soit u un endomorphisme surjectif de M. L'endomorphisme u est alors bijectif et u^{-1} est un polynôme en u.*

Démonstration. On vérifie immédiatement que la loi externe

$$(P, m) \mapsto P(u)(m)$$

définit sur le groupe abélien $(M, +)$ une structure de $A[X]$-module ; elle prolonge celle de A-module, et la multiplication par X est égale à l'endomorphisme u. Par hypothèse, M est de type fini comme A-module ; il l'est *a fortiori* comme $A[X]$-module.

La surjectivité de u signifie donc que pour tout $m \in M$, il existe $n \in M$ tel que $Xn = m$. En conséquence, $M = (X)M$.

Le lemme de Nakayama assure alors qu'il existe un polynôme P congru à 1 modulo X tel que $PM = 0$. Écrivons $P = 1 + XQ$, avec $Q \in A[X]$. Soit $m \in M$. On a $Pm = 0$, soit $P(u)(m) = 0$, soit encore $(\mathrm{Id} + uQ(u))(m) = 0$. Ceci valant pour tout m, il vient $\mathrm{Id} = u(-Q(u))$. Comme deux polynômes en u commutent, on aussi $\mathrm{Id} = (-Q(u))u$. Ainsi, u est bijectif et $u^{-1} = -Q(u)$. □

Commentaires. Lorsque A est un corps, on dispose d'une preuve plus directe du fait qu'un endomorphisme surjectif d'un espace vectoriel de dimension finie est bijectif : cela provient de la formule du rang. Mais celle-ci n'a pas de sens sur un anneau quelconque, où les modules ne sont en général pas libres.

Par ailleurs, la formule du rang permet aussi de montrer qu'un endomorphisme injectif d'un espace vectoriel de dimension finie est bijectif. Ceci est *faux* en général sur un anneau quelconque. Par exemple, la multiplication par 2 est un endomorphisme injectif du $\mathbb{Z}$-module $\mathbb{Z}$, et elle n'est pas bijective.

On observe donc une certaine dissymétrie entre injections et surjections dans la théorie générale des modules, alors qu'en algèbre linéaire ces deux notions sont plus ou moins duales l'une de l'autre.

Le produit tensoriel : cas de deux modules

Soit A un anneau et soient M et N deux A-modules. Avant de définir rigoureusement le produit tensoriel, expliquons intuitivement le but de sa construction. On cherche à fabriquer la loi bilinéaire *la plus générale possible* de source $M \times N$, c'est-à-dire à donner un sens au produit d'un élément de M par un élément de N, en ne lui imposant rien d'autre que la bilinéarité.

Comme à chaque fois que l'on cherche à construire un objet auquel on impose une liste limitative de contraintes, la définition rigoureuse de l'objet en question s'exprime au moyen d'une propriété universelle ou, si l'on préfère, du foncteur qu'il représente.

Définition – proposition. Soit F le foncteur covariant qui envoie un A-module P sur l'ensemble des applications bilinéaires de $M \times N$ vers P. Ce foncteur est représentable, et son représentant est noté

$$(M \otimes_A N, (m, n) \mapsto m \otimes n).$$

On dit que $M \otimes_A N$ est le *produit tensoriel* de M et N au-dessus de A.

Commentaires et premières propriétés. La construction du produit tensoriel a été faite en cours et n'a aucun intérêt : on «fait ce qu'il faut pour que ça marche», et c'est tout. Elle a tout de même une vertu : elle montre que $M \otimes_A N$ est engendré (comme A-module, ou même comme groupe abélien puisque l'on a $a(m \otimes n) = (am) \otimes n$ pour tout (a, m, n)) par les éléments de la forme $m \otimes n$, qu'on appelle les *tenseurs purs. Exercice : montrez ce fait en utilisant uniquement la propriété universelle du produit tensoriel.*

L'application bilinéaire universelle $(m, n) \mapsto m \otimes n$ a tendance à coder les propriétés (de nature linéaire) vérifiées par *toutes* les applications bilinéaires de source $M \times N$. Par exemple, on démontre facilement, à l'aide de la propriété universelle, que $\sum m_i \otimes n_i = 0$ si et seulement si pour *toute* application bilinéaire $b : M \times N \to P$, on a $\sum b(m_i, n_i) = 0$.

Dans le même esprit, on prouve que $M \otimes_A N$ est nul si et seulement si toute application bilinéaire de source $M \times N$ est nulle.

Premiers exemples. Si M est un A-module, il existe une unique application A-linéaire de $A \otimes_A M$ dans M qui envois $a \otimes m$ sur am pour tout (a, m) (propriété universelle du produit tensoriel : $(a, m) \mapsto am$ est bilinéaire). Elle est bijective, de réciproque $m \mapsto 1 \otimes m$ (la vérification est immédiate).

Montrons que $(\mathbb{Z}/2\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = 0$. Pour cela, il suffit de montrer que $a \otimes b = 0$ pour tout $a \in \mathbb{Z}/2\mathbb{Z}$ et tout $b \in \mathbb{Z}/3\mathbb{Z}$. Donnons-nous donc un tel couple (a, b). On a

$$a \otimes b = (3 - 2)a \otimes b = 3a \otimes b - 2a \otimes b = a \otimes 3b - 2a \otimes b = 0$$

puisque $2a = 0$ et $3b = 0$.

Plus généralement,$(\mathbb{Z}/p\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}/q\mathbb{Z} = 0$ dès que p et q sont premiers entre eux : on raisonne comme ci-dessus, en remplaçant l'égalité $3 - 2 = 1$ par une relation de Bezout entre $p$et q.

Ainsi, on voit que *le produit tensoriel de deux modules non nuls peut très bien être nul.*

Produit tensoriel de deux modules libres. Soient M et N deux A-modules. Supposons que M admet une base (e_i), et que N admet une base (f_j). J'ai démontré en cours que $(e_i \otimes f_j)_{i,j}$ est une base de $M \otimes_A N$.

Ainsi $M \otimes_A N$ est libre, et si A est non nul, on a l'égalité

$$\mathrm{rg}(M \otimes_A N) = \mathrm{rg}(M) \times \mathrm{rg}(N)$$

(le produit est à prendre au sens des cardinaux finis ou non). En particulier, $M \otimes_A N$ est nul si et seulement si M est nul ou N est nul : le phénomène désagréable mis au jour ci-dessus ne peut pas se produire avec des modules libres.

Ce qui précède est particulièrement utile lorsqu'on travaille sur un corps, puisque les espaces vectoriels sont tous libres.

Fonctorialité. Soient $f : M \to M'$ et $g : N \to N'$ des applications A-linéaires. La propriété universelle du produit tensoriel implique immédiatement qu'il existe une unique application linéaire de $M \otimes_A N$ dans $M' \otimes_A N'$ qui envoie $m \otimes n$ sur $f(m) \otimes g(n)$ pour tout (m, n). On la note $f \otimes g$.

En particulier, si l'on fixe M, on obtient un foncteur $N \mapsto M \otimes N$, qui au niveau des morphismes envoie g sur $\mathrm{Id} \otimes g$.

Nous allons maintenant étudier les propriétés de ce foncteur relativement aux *suites exactes*.

Rappelons qu'une suite $\ldots M_i \to M_{i+1} \to M_{i+2} \to \ldots$ (indexée par des entiers relatifs, finie ou infinie d'un côté comme de l'autre) d'applications A-linéaires entre modules est dite *exacte* si elle possède la propriété suivante : pour tout i tel que le module M_i ne soit pas «au bord» de la suite, c'est-à-dire tel qu'il y ait un module M_{i-1} et un module M_{i+1}, le noyau de $M_i \to M_{i+1}$ est égal à l'image de $M_{i-1} \to M_i$.

Par exemple, dire que

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

est exacte signifie que f est injective, que g surjective et que $\mathrm{Ker}\, g = \mathrm{Im}\, f$; dire que

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

est exacte signifie juste que g surjective et que $\mathrm{Ker}\, g = \mathrm{Im}\, f$.

J'ai démontré que pour tout A-module M, le foncteur $M \otimes_A \bullet$ est *exact à droite*, c'est-à-dire qu'il préserve les suites exactes de la forme

$$N' \to N \to N'' \to 0 \ :$$

si l'on se donne une telle suite, alors $M \otimes_A N' \to M \otimes_A N \to M \otimes_A N'' \to 0$ est encore exacte.

Si l'on note f la flèche $N' \to N$, cela revient à dire (exercice : expliquez pourquoi !) que la flèche naturelle

$$(M \otimes_A N)/(\mathrm{Id} \otimes f)(M \otimes_A N') \to M \otimes_A (N/f(N'))$$

est un isomorphisme.

Soit I un idéal de A. On déduit de ce qui précède que $M \otimes_A (N/IN) \simeq (M \otimes_A N)/I(M \otimes_A N)$. Expliquons pourquoi (j'ai esquissé un argument en cours que je ne crois pas, à la réflexion, très convaincant. J'en donne un autre ici).

Soit f l'inclusion de IN dans N. Par ce qui précède,

$$M \otimes_A (N/IN) \simeq (M \otimes_A N)/(1 \otimes f)(M \otimes_A IN).$$

Mais on vérifie immédiatement, à l'aide des définitions et de la bilinéarité de $\otimes$, que $(1 \otimes f)(M \otimes_A IN) = I(M \otimes_A N)$, d'où notre assertion.

Indiquons une autre manière de procéder (ou disons au moins de présenter la preuve) : on peut montrer que $M\otimes_A(N/IN)$ et $M\otimes_A N/I(M\otimes_A N)$ représentent le même foncteur, à savoir celui qui envoie un A-module P sur l'ensemble des applications bilinéaires de $M \times N$ vers P nulles sur $M \times IN$.

On dit que M est un A-module *plat* si $M \otimes_A \bullet$ est *exact*, c'est-à-dire si pour toute suite exacte

$$0 \to N' \to N \to N'' \to 0 ,$$

la suite induite $0 \to M \otimes_A N' \to M \otimes_A N \to M \otimes_A N'' \to 0$ est exacte. Compte-tenu de l'exactitude *à droite* déjà démontrée, on voit que $M \otimes_A \bullet$ est plat si et seulement si il préserve les injections.

La platitude est une notion absolument fondamentale en algèbre commutative et en géométrie algébrique. Pour se convaincre qu'elle n'est pas vide, donnons un exemple simple de module non plat : le $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$.

En effet, soit $f : \mathbb{Z} \to \mathbb{Z}$ la multiplication par 2 ; elle est injective. On vérifie immédiatement que pour tout $\mathbb{Z}$-module N, la flèche de $M \otimes_{\mathbb{Z}} \mathbb{Z} \simeq M$ dans lui-même induite par f est la multiplication par 2. Lorsque $M = \mathbb{Z}/2\mathbb{Z}$, on trouve ainsi l'application nulle de M dans lui-même qui n'est pas injective.

Produit tensoriel et somme directe. Soit (N_i) une famille de A-modules. Rappelons que la somme directe abstraite $\bigoplus N_i$ est définie comme le sous-module de $\prod N_i$ formé des familles (x_i) qui sont presque partout nulles (*i.e.* nulles sauf pour un nombre fini d'indices). L'application h_j qui envoie un élément n de N_j sur la famille (x_i) avec $x_i = 0$ si $i \neq j$ et $x_j = n$ est une injection, et $\bigoplus N_i$ est bien la somme directe (interne) des $h_i(N_i)$; très souvent, on identifie N_i à un sous-module de $\bigoplus N_i$ *via* h_i, et $\bigoplus N_i$ est vraiment la somme directe interne des N_i modulo cet abus.

On peut caractériser la somme directe par une propriété universelle : le couple $(\bigoplus N_i, (h_i)_i)$ représente le foncteur covariant $P \mapsto \prod_i \mathrm{Hom}(N_i, P)$. En d'autres termes, se donner une application linéaire de $\bigoplus N_i$ vers P, c'est se donner une application linéaire de chacun des N_i vers P.

Soit M un A-module. Pour tout indice j, on dispose d'une application A-linéaire $\mathrm{Id} \otimes h_j : M \otimes_A N_j \to M \otimes_A (\bigoplus N_i)$. La famille des $\mathrm{Id} \otimes h_j$ induit une application A-linéaire $\bigoplus(M \otimes_A N_i) \to M \otimes_A (\bigoplus N_i)$, dont j'ai démontré en cours que c'était un isomorphisme, en exhibant sa réciproque.

Suggestion d'une preuve alternative, laissée en exercice : montrer que les A-modules $\bigoplus(M \otimes_A N_i)$ et $M \otimes_A (\bigoplus N_i)$ représentent tous deux le foncteur covariant qui associe à P le produit $\prod_i \mathrm{Bilin}(N_i, P)$.

Platitude des espaces vectoriels. Soit k un corps et soit $j : N \hookrightarrow P$ une injection linéaire de k-espaces vectoriels. Soit M un k-espace vectoriel.

Le sous-espace vectoriel $j(N)$ de P admet un supplémentaire Q. En d'autres termes, il existe un diagramme commutatif

$$\begin{tikzcd} N \arrow[r, "j"] \arrow[d, "i"] & P \\ N \oplus Q \arrow[ur, "\sim"'] & \end{tikzcd}$$

où i est l'injection naturelle. En tensorisant ce diagramme avec M, on obtient le diagramme commutatif

$$\begin{tikzcd} M \otimes_k N \arrow[r, "\mathrm{Id}\otimes j"] \arrow[d, "\mathrm{Id}\otimes i"] & M \otimes_k P \\ M \otimes_k (N \oplus Q) \arrow[ur, "\sim"'] & \end{tikzcd} .$$

Par ce qui précède, on peut identifier $M \otimes_k (N \oplus Q)$ à $(M \otimes_k N) \oplus (M \otimes_k P)$, de sorte que $\mathrm{Id} \otimes i$ corresponde à la flèche canonique $M \otimes_k N \to (M \otimes_k N) \oplus (M \otimes_k P)$, qui est injective. Il s'ensuit que $\mathrm{Id} \otimes j$ est injective. Par conséquent, M est plat.

Donnons une variante de la preuve de l'injectivité de j. Le sous-espace vectoriel $j(N)$ admet un supplémentaire Q ; en composant la projection sur $j(N)$ parallèlement à Q avec la réciproque de l'isomorphisme $N \simeq j(N)$ induit par l'injection j, on obtient une application linéaire $r : P \to N$ telle que $r \circ j = \mathrm{Id}$. Par fonctorialité, il vient $(\mathrm{Id} \otimes r) \circ (\mathrm{Id} \otimes j) = \mathrm{Id}$, ce qui force $(\mathrm{Id} \otimes j)$ à être injective.

Le produit tensoriel : cas d'un module et d'une algèbre

Soit M un A-module et soit B une A-algèbre. J'ai démontré que le A-module $B \otimes_A M$ admet une structure naturelle de B-module (induisant sa structure de A-module), caractérisée par la formule

$$\beta.(b \otimes m) = (\beta b) \otimes m$$

pour tout $(\beta, b, m) \in B^2 \times M$.

On dit que $B \otimes_A M$ est déduit de M par *extension des scalaires de A à B*. Intuitivement, $B \otimes_A M$ est le B-module le plus général fabriqué à partir de M, en autorisant la multiplication externe par les éléments de B, et non plus simplement de A.

Comme toujours, un objet admettant ce type de description informelle est caractérisé par une propriété universelle : j'ai démontré en cours que le couple $(B \otimes_A M, m \mapsto 1 \otimes m)$ représente le foncteur covariant de la catégorie des B-modules vers celle des A-modules qui envoie P sur $\mathrm{Hom}_A(M, P)$.

Autrement dit, se donner une application B-linéaire de $B \otimes_A M$ dans un B-module P, c'est se donner une application A-linéaire de M dans P.

On peut reformuler ces assertions en disant que $M \mapsto B \otimes_A M$ est adjoint à gauche au foncteur qui associe à un B-module le A-module sous-jacent.

Quelques exemples.

1) Soit I un idéal de A et soit M un A-module. Le A-module quotient M/IM est naturellement un A/I-module (la multiplication externe par un scalaire a ne dépend dans ce module que de la classe de a modulo I). On sait par ailleurs qu'on a un isomorphisme naturel de A-modules

$$(A/I) \otimes_A M \simeq M/IM.$$

On vérifie aussitôt que c'est un isomorphisme *de A/I-modules.*

2) Soit S une partie multiplicative de A et soit M un A-module. On définit sur $M \times S$ la relation $\mathscr{R}$ suivante : $(m,s)\mathscr{R}(n,t)$ si et seulement si il existe $r \in S$ tel que $r(tm - sb) = 0$. On vérifie que c'est une relation d'équivalence, et l'on note $S^{-1}M$ le quotient correspondant.

Les formules

$$(m,s);(n,t)) \mapsto (tm + sn, st) \text{ et } ((a,s);(m,t)) \mapsto (am, st)$$

passent au quotient, et définissent une loi $+$ sur $S^{-1}M$ et une loi $\times : S^{-1}A \times S^{-1}M \to S^{-1}M$ qui font de $S^{-1}M$ un $S^{-1}A$-module.

Si $ma,s) \in M \times S$, on écrira $\frac{m}{s}$ au lieu de $\overline{(m,s)}$. Cette notation permet de disposer des formules naturelles

$$\frac{m}{s} + \frac{n}{t} = \frac{sn + tm}{st} \text{ et } \frac{a}{s} \cdot \frac{m}{t} = \frac{am}{bt},$$

et l'on a

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

Toute application linéaire f de M vers un A-module N induit une application $S^{-1}A$-linéaire de $S^{-}M$ vers $S^{-1}N$, qui envoie m/s sur $f(m)/s$.

L'application de $S^{-1}A \times M$ vers $S^{-1}M$ qui envoie $(a/s, m)$ sur am/s étant A-bilinéaire, elle induit une application A-linéaire de $S^{-1}A \otimes_A M$ vers $S^{-1}M$, dont on vérifie que c'est un *isomorphisme de $S^{-1}A$-modules*, fonctoriel en M.

Il résulte de la description explicite de $S^{-1}M$ que si $f : M \to N$ est une application linéaire injective, l'application induitre de $S^{-1}M$ vers $S^{-1}N$ est encore injective. Cela signifie que la A-algèbre $S^{-1}A$ est plate (c'est-à-dire que le A-module sous-jacent à $S^{-1}A$ est plat).

3) Soit M un A-module, et soit $(e_i)_{i \in I}$ une famille génératrice de M. On note $A^{(I)}$ la somme directe de copies de A indexées par I (ou encore le A-module formé des familles $(a_i)_{i \in I}$ d'éléments de A telle que presque tous les a_i soient nuls). Pour tout $j \in I$, notons δ_j^A la famille (a_i) de $A^{(I)}$ avec $a_i = \delta_{ij}$. On a alors $(a_i) = \sum a_i \delta_i^A$ pour toute $(a_i) \in A^{(I)}$.

L'application $p : A^{(I)} \to M$ qui envoie (a_i) sur $\sum a_i e_i$ est surjective. Donnons-nous une famille génératrice $(g_j)_{j \in J}$ du noyau de p, et écrivons $g_j = \sum a_{ij} \delta_i^A$. Soit q l'application de $A^{(J)}$ dans $A^{(I)}$ qui envoie (a_j) sur $\sum a_j g_j$.

On a par construction une suite exacte

$$A^{(J)} \xrightarrow{q} A^{(I)} \xrightarrow{p} M \longrightarrow 0,$$

que l'on peut encore présenter comme un isomorphisme $(A^{(I)}/\text{Im } q) \simeq M$, envoyant $\overline{\delta_i^A}$ sur e_i. Comme Im q est engendré par les g_j, on dit (un peu abusivement) qu'un tel isomorphisme est une *présentation de M par générateurs δ_i^A et relations $g_j = \sum a_{ij}\delta_i^A$.*

Il résulte de la commutation du produit tensoriel aux sommes directes que $B \otimes_A A^{(I)}$ est canoniquement isomorphe comme A-module à $B^{(I)}$; on vérifie aussitôt que cet isomorphisme est B-linéaire, et qu'il envoie $1 \otimes f_j$ sur δ_j^B.

En vertu de l'exactitude à droite du produit tensoriel, la suite

$$B^{(J)} \xrightarrow{\mathrm{Id}\otimes q} B^{(I)} \xrightarrow{\mathrm{Id}\otimes p} B \otimes_A M \longrightarrow 0$$

est exacte.

En conséquence, on dispose d'une présentation de $B \otimes_A M$ par générateurs δ_i^B et relations $g_j = \sum a_{ij}\delta_i^B$ (en écrivant abusivement a_{ij} pour son image dans B).

En d'autres termes, $B \otimes_A M$ est le B-module *décrit de la même manière que le A-module M.* Ou, si l'on préfère, «$B \otimes_A M$ est à B ce que M est à A.»

Effet de l'extension des scalaires sur les familles libres, les familles génératrices et les bases.

Soit M un A-module et soit (e_i) une famille d'éléments de M. Soit $p : A^{(I)} \to M$ le morphisme $(a_i) \mapsto \sum a_i e_i$. La famille (e_i) est génératrice (resp. libre, resp. une base) si et seulement si p est surjective (resp. injective, resp. bijective).

• Supposons que (e_i) soit génératrice. L'application p étant surjective, l'exactitude à droite du produit tensoriel assure que $\mathrm{Id} \otimes p : B^{(I)} \to B \otimes_A M$ est surjective. Ainsi, $(1 \otimes e_i)$ est une famille génératrice de $M \otimes_A B$.

• Supposons que (e_i) soit une base. L'application p étant bijective, $\mathrm{Id} \otimes p$ l'est encore par fonctorialité. Ainsi, $(1 \otimes e_i)$ est une base de $M \otimes_A B$.

• L'extension des scalaires préserve donc les familles génératrices et les bases. Nous allons montrer qu'elle ne préserve pas les familles libres en général. Prenons $A = \mathbb{Z}, B = \mathbb{Z}/7\mathbb{Z}$, et $M = \mathbb{Z}^2$. Posons $e_1 = (1, 0)$ et $e_2 = (0, 1)$. Par préservation des bases, $(\overline{e}_1, \overline{e}_2)$ est une base de $(\mathbb{Z}/7\mathbb{Z}) \otimes_{\mathbb{Z}} M \simeq M/7M$.

Posons $f_1 = 2e_1 + e_2$ et $f_2 = -3e_1 + 2e_2$. La famille (f_1, f_2) est $\mathbb{Z}$-libre (le déterminant de la matrice associée vaut 7, ce qui entraîne que ses colonnes sont $\mathbb{Q}$-libres, et *a fortiori* $\mathbb{Z}$-libres) ; mais $(\overline{f_1}, \overline{f_2})$ n'est pas $\mathbb{Z}/7\mathbb{Z}$-libre car son déterminant dans la base $(\overline{e_1}, \overline{e_2})$ vaut $\overline{7} = 0$.

• Si B est une A-algèbre plate alors $B \otimes_A \bullet$ préserve les injections, et $\mathrm{Id} \otimes p$ est dès lors injective dès que p est injective : dans ce ças particulier, $B \otimes_A \bullet$ préserve les familles libres.

Produit tensoriel de deux algèbres

Soient B et C deux A-algèbres. J'ai démontré qu'il existe une structure d'anneau sur le A-module $B \otimes_A C$, dont l'addition est celle du groupe abélien $B \otimes_A C$, et dont la multiplication est caractérisée par les formules

$$(b \otimes c) \cdot (\beta \otimes \gamma) = (b\beta) \otimes (c\gamma).$$

Les applications $b \mapsto b \otimes 1$ et $c \mapsto 1 \otimes c$ sont des morphismes d'anneaux ; les composées $A \to B \to B \otimes_A C$ et $A \to C \to B \otimes_A C$ coïncident : par A-bilinéarité de $\otimes$, on a en effet $a \otimes 1 = 1 \otimes a$ pour tout $a \in A$ (comme d'habitude, on note encore a les images de a dans B et C).

L'anneau $B \otimes_A C$ hérite ainsi d'une structure de B-algèbre et d'une structure de C-algèbre, qui induisent la même structure de A-algèbre. On vérifie que ses structures de A-module, B-module et C-module sont précisément les structures sous-jacentes à ces structures d'algèbre.

Intuitivement, $B \otimes_A C$ est la A-algèbre la plus générale fabriquée à partir de B et C, en définissant «artificiellement» la multiplication d'un élément b de B par un élément c de C (c'est $b \otimes c$). Comme toujours, ce type de description se traduit rigoureusement en termes de propriété universelle, comme suit.

Pour toute A-algèbre D et tout couple (f, g) où f est un morphisme de A-algèbres de B vers D et g un morphisme de A-algèbres de C vers D, il existe un unique morphisme de A-algèbres de $B \otimes_A C$ vers D tel que le diagramme

$$\begin{tikzcd}
B \arrow[dr] \arrow[drr, "f"] & & \\
& B \otimes_A C \arrow[r] & D \\
C \arrow[ur] \arrow[urr, "g"'] & &
\end{tikzcd}$$

commute. En d'autres termes, la A-algèbre $B \otimes_A C$ est *la somme disjointe de B et C dans la catégorie des A-algèbres.* Il s'ensuit tautologiquement que l'anneau $B \otimes_A C$ est la *somme amalgamée de B et C le long de $A \to B$ et $A \to C$ dans la catégorie des anneaux.*

Selon le contexte, il y a plusieurs façons d'envisager $B \otimes_A C$. On peut y penser comme à un objet symétrique en B et C (c'est le cas lorsqu'on énonce la propriété universelle ci-dessus). Mais on peut faire (psychologiquement) jouer un rôle différent à B et C, en considérant qu'on part d'une A-algèbre C et qu'on la transforme en une B-algèbre $B \otimes_A C$ (ou l'inverse, évidemment). Le slogan à retenir lorsqu'on aborde les choses de ce point de vue est «la B-algèbre $B \otimes_A C$ est à B ce que C est à A».

Illustrons cette pétition de principe par un exemple. Supposons que C est égale à $A[X_i]_{i \in I}/(P_j)_{j \in J}$. On vérifie alors sans peine l'existence d'un isomorphisme canonique de B-algèbres

$$B \otimes_A C \simeq B[X_i]_{i \in I}/(P_j)_{j \in J}$$

(où l'on note encore P_j l'image de P_j dans $B[X_i]_{i \in I}$). En termes concrets, cet isomorphisme envoie $b \otimes \overline{P}$ sur $\overline{bP}$; sa réciproque envoie $\overline{b}$ sur $b \otimes 1$ et $\overline{X}_i$ sur $1 \otimes \overline{X}_i$.

Exemples. Soit A la $\mathbb{Z}$-algèbre $\mathbb{Z}[X]/(6X^2+12X-3)$. Pour toute $\mathbb{Z}$-algèbre B, on a $B \otimes_{\mathbb{Z}} A \simeq B[X]/(6X^2+12X-3)$. L'allure de cette dernière dépend beaucoup de B.

Ainsi :

- si $B = \mathbb{Q}$, elle est égale à $\mathbb{Q}[X]/(6X^2 + 12X - 3)$ qui est un corps de degré 2 sur Q, car $6X^2 + 12X - 3$ est irréductible sur $\mathbb{Q}[X]$ (son discriminant est $144 + 72 = 216$ qui n'est pas un carré dans $\mathbb{Q}$).

- si $B = \mathbb{Z}/2\mathbb{Z}$ elle est égale $(\mathbb{Z}/2\mathbb{Z})[X]/(3) = \{0\}$ car 3 est inversible modulo 2 ;

- si $B = \mathbb{Z}/3\mathbb{Z}$ elle est égale à $(\mathbb{Z}/3\mathbb{Z})[X]/(0) = (\mathbb{Z}/3\mathbb{Z})[X]$;
-si $B = \mathbb{Z}/5\mathbb{Z}$ elle est égale à

$$(\mathbb{Z}/5\mathbb{Z})[X]/(X^2+2X+2) = (\mathbb{Z}/5\mathbb{Z})[X]/(X-1)(X-2)$$

$$\simeq (\mathbb{Z}/5\mathbb{Z})[X]/(X-1) \times (\mathbb{Z}/5\mathbb{Z})[X]/(X-2) \simeq (\mathbb{Z}/5\mathbb{Z})^2.$$

Ainsi, en tensorisant la même $\mathbb{Z}$-algèbre par différents corps on a obtenu un corps, l'anneau nul, un anneau de polynômes, et un produit de corps.

Donnons maintenant un deuxième exemple. Nous allons décrire l'anneau $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$.

Comme $\mathbb{C} \simeq \mathbb{R}[X]/(X^2+1)$, cet anneau s'identifie à

$$\mathbb{C}[X]/(X^2+1) \simeq \mathbb{C}[X]/(X+i)(X-i) \simeq \mathbb{C}[X]/(X+i) \times \mathbb{C}[X]/(X-i) \simeq \mathbb{C} \times \mathbb{C}.$$

À titre d'exercice, vérifiez que l'isomorphisme $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C} \times \mathbb{C}$ ainsi construit envoie $b \otimes \beta$ sur $(b\beta, b\overline{\beta})$.

Remarque. On voit à travers cet exemple qu'un produit tensoriel de deux corps au-dessus d'un troisième n'est pas nécessairement un corps, ni même un anneau intègre. Nous allons voir qu'il peut même arriver qu'un tel produit tensoriel ne soit pas réduit.

Soit k un corps de caractéristique $p > 0$ non parfait, et soit a un élément de k qui n'est pas une puissance p-ième. On vérifie (exercice) que $X^p - a$ est alors un polynôme irréductible. Soit L le corps $k[X]/(X^p - a)$ et soit α la classe de X dans L.

On a

$$L \otimes_k L = L \otimes_k k[X]/(X^p - a) \simeq L[X]/(X^p - a) = L[X]/(X^p - \alpha^p) = L[X]/(X-\alpha)^p$$

car l'élévation à la puissance p est un morphisme d'anneaux en caractéristique p. La classe de $X - \alpha$ modulo $(X-\alpha)^p$ fournit alors un élément nilpotent non nul de $L \otimes_k L$.

Quelques applications du produit tensoriel

Endomorphismes d'un module libre, et forme trace. Soit A un anneau et soit M un A-module. Soit $M^\vee$ le dual de M, c'est-à-dire le A-module $\mathrm{Hom}_A(M, A)$. L'application de $M \times M^\vee$ dans $\mathrm{End}_A M$ qui envoie un couple (m, φ) sur $n \mapsto \varphi(n)m$ est bilinéaire, elle induit donc une application A-linéaire $M \otimes_A M^\vee \to \mathrm{End}_A(M)$.

Supposons que M soit libre de rang fini. Il existe alors une base finie (e_i) de M. Si l'on note e_i^* la i-ème forme linéaire coordonnée dans la base (e_i), alors (e_i^*) est une base de $M^\vee$, et $(e_i \otimes e_j^*)_{i,j}$ est donc une base de $M \otimes_A M^\vee$.

Fixons (i, j). L'image de $e_i \otimes e_j^*$ dans $\mathrm{End}_A(M)$ envoie pour tout ℓ le vecteur e_ℓ sur $e_j^*(e_\ell)e_i$. C'est donc l'endomorphisme u_{ij} de M dont la matrice dans (e_i) est égale à E_{ij}. Comme les u_{ij} forment une base de $\mathrm{End}_A(M)$, l'application $M \otimes_A M^\vee \to \mathrm{End}_A(M)$ est bijective.

Remarque. Le morphisme $M \otimes_A M^\vee \to \mathrm{End}_A(M)$ admet une définition intrinsèque, sans avoir à choisir de base – et il existe d'ailleurs sans supposer M libre. Mais lorsque M est libre de rang fini, on a besoin d'en choisir une base pour montrer, par un *calcul explicite*, que ce morphisme est un isomorphisme. Ce type de situation se rencontre très souvent en algèbre commutative.

La trace. Soit M un A-module. L'application de $M \times M^\vee$ dans A qui envoie un couple (m, φ) sur $\varphi(m)$ est bilinéaire, et induit donc une forme linéaire sur $M \otimes_A M^\vee$. Lorsque M est libre de rang fini on en déduit, *via* l'isomorphisme $\mathrm{End}_A(M) \simeq M \otimes_A M^\vee$, une forme linéaire sur $\mathrm{End}_A(M)$.

Comme l'isomorphisme ci-dessus envoie u_{ij} sur $e_i \otimes e_j^*$, la forme linéaire en question envoie u_{ij} sur $e_j^*(e_i) = \delta_{ij}$. Cette forme n'est donc autre que la trace.

Applications à la théorie des corps : existence d'une extension composée. Soient $k \hookrightarrow F$ et $k \hookrightarrow L$ deux extensions de corps. Il existe alors un corps K et deux plongements $F \hookrightarrow K$ et $L \hookrightarrow K$ tels que le diagramme

$$\begin{tikzcd} & F \arrow[dr] & \\ k \arrow[ur] \arrow[dr] & & K \\ & L \arrow[ur] & \end{tikzcd}$$

commute.

Indiquons la démonstration. Les k-espaces vectoriels F et L sont non nuls, puisque ce sont des corps. Comme ils sont libres sur k (c'est le cas de tout espace vectoriel), leur produit tensoriel est *non nul.* La k-algèbre $F \otimes_k L$ étant non nulle, elle possède un idéal maximal. Si l'on note K le corps quotient correspondant, les flèches composées $F \to F \otimes_k L \to K$ et $F \to F \otimes_k L \to K$ satisfont les conditions requises.

Indiquons maintenant deux applications de ce fait à la théorie des extensions de corps.

Unicité du corps de décomposition. Soit P un polynôme non nul à coefficients dans k, et soient F et L deux corps de décompositions de P sur k (un corps de décomposition de P sur k est une extension de k dans laquelle P est scindé, et qui est engendrée par les racines de P).

Les corps F et L sont alors k-isomorphes. En effet, par ce qui précède, il existe une extension K de k et deux k-plongements $i : F \hookrightarrow K$ et $j : L \hookrightarrow K$. L'image $i(F)$ est isomorphe à F, et est donc un corps de décomposition de P sur k. Il s'ensuit que P est scindé dans K et que $i(F)$ est le sous-corps de K engendré par k et les racines de P.

De même, $j(L)$ est le sous-corps de K engendré par k et les racines de P. Par conséquent, $j(L) = i(K)$. On a donc deux k-isomorphismes $F \simeq i(F)$ et $i(F) = j(L) \simeq L$, d'où un k-isomorphisme $F \simeq L$.

Unicité de la clôture algébrique. Soient F et L deux clôtures algébriques de k (une clôture algébrique de k est une extension algébrique de k qui est algébriquement close).

Les corps F et L sont alors k-isomorphes. En effet, par ce qui précède, il existe une extension K de k et deux k-plongements $i : F \hookrightarrow K$ et $j : L \hookrightarrow K$. L'image $i(F)$ est isomorphe à F, et est donc une clôture algébrique de k. Il s'ensuit que $i(F)$ est nécessairement le sous-corps de K formé des éléments algébriques sur k.

De même, $j(L)$ est le sous-corps de K formé des éléments algébriques sur k. Par conséquent, $j(L) = i(K)$. On a donc deux k-isomorphismes $F \simeq i(F)$ et $i(F) = j(L) \simeq L$, d'où un k-isomorphisme $F \simeq L$.

Remarque. Vous connaissez peut-être des preuves de l'unicité du corps de décomposition d'un polynôme P consistant à construire l'isomorphisme entre deux tels corps F et L en choisissant successivement des racines de diviseurs convenables de P dans F et L. On peut se demander où est passé ce choix de racines dans la preuve proposée ci-dessus, qui peut donner l'impression que ≪rien ne se passe≫. En fait, tout est caché dans le choix de l'idéal maximal de $F \otimes_k L$, effectué lorsqu'on veut exhiber un corps K.

La même chose se produit pour les clôtures algébriques : se donner un isomorphisme entre deux clôtures algébriques F et L de k revient peu ou prou à faire des choix compatibles de racines, dans F et L, de *tous* les polynômes irréductibles de $k[X]$. Là encore, ce choix est pudiquement dissimulé derrière celui de l'idéal maximal de $F \otimes_k L$.

Algèbres finies et algèbres entières

Soit A un anneau et soit B une A-algèbre. On dit que B est *finie* si B est de type fini *comme A-module* (il est alors *a fortiori* de type fini comme A-algèbre). J'ai démontré en cours la proposition suivante.

Proposition-définition. *Soit A un anneau, soit B une A-algèbre et soit $x \in B$. Les assertions suivantes sont équivalentes.*

i) x annule un polynôme unitaire appartenant à $A[X]$.

ii) La A-algèbre $A[x]$ est finie.

iii) Il existe une sous-A-algèbre finie C de B contenant x.

Lorsqu'elles sont satisfaites, on dit que x est entier *sur A. Si tout élément de B est entier sur A, on dit que B est* entière *sur A.*

Remarques.

1) Notons que toute algèbre finie est entière. Nous verrons un peu plus bas que la réciproque est fausse.

2) Au cours de la preuve de iii)⇒i), on voit que si C est engendré par n éléments, alors on peut trouver un polynôme unitaire de $A[X]$ annulant x et de degré n.

J'ai démontré les propriétés suivantes.

a) Transitivité du caractère fini : si B est finie sur A et si C est finie sur B alors C est finie sur A.

b) Si B est une A-algèbre engendrée par un nombre fini d'éléments entiers sur A, elle est finie.

c) Si B est une A-algèbre, l'ensemble des éléments de B entiers sur A est une sous-A-algèbre de B, appelée la *fermeture intégrale* de B dans A.

d) Transitivité du caractère entier : si B est entière sur A et si x est entier sur B alors x est entier sur A.

On peut maintenant donner un exemple d'algèbre entière et non finie. Soit $\overline{\mathbb{Z}}$ la fermeture intégrale de $\mathbb{Z}$ dans $\mathbb{C}$. C'est une $\mathbb{Z}$-algèbre entière, qui n'est pas finie. En effet si elle l'était, il existerait d'après la remarque suivant l'énoncé de la proposition ci-dessus un entier n tel que tout élément de $\overline{\mathbb{Z}}$ soit annulé par un polynôme unitaire de $\mathbb{Z}[X]$ de degré au plus n. Or pour tout entier m, le polynôme $X^m - 2$ est irréductible dans $\mathbb{Q}[X]$ (critère d'Eisenstein), et est donc le polynôme minimal de $\sqrt[m]{2}$, qui ne peut dès lors annuler de polynôme unitaire de degré n à coefficients dans $\mathbb{Z}[X]$ si $m > n$; comme $\sqrt[m]{2} \in \overline{\mathbb{Z}}$ (parce qu'il annule $X^m - 2$), on voit que $\overline{\mathbb{Z}}$ n'est pas finie sur $\mathbb{Z}$.

J'ai démontré les assertions suivantes :

• si B est une A-algèbre entière et si C est une A-algèbre (quelconque) alors $C \otimes_A B$ est une C-algèbre entière ;

• si B est une A-algèbre entière, si I est un idéal de A et si J est un idéal de B contenant IB alors B/J est une A/I-algèbre entière.

Éléments entiers : le cas des corps

Soit $K \hookrightarrow L$ une extension de corps. Au lieu de dire qu'un élément donné de L est entier sur K, on dit plutôt qu'il est *algébrique.* Si tout élément de L est algébrique sur K, on dit que L elle-même est algébrique.

La K-algèbre formée des éléments de L algébrique sur K est en fait un corps ; on a plus généralement le résultat suivant, dont on se servira à plusieurs reprises.

Lemme. *Soit B un anneau intègre et soit A un sous-anneau de B. On suppose que B est entier sur A. Les assertion suivantes sont alors équivalentes.*

i) A est un corps.
ii) B est un corps.

Si K est un corps et A une K-algèbre, on dit d'une famille (x_i) d'éléments de A qu'ils sont *algébriquement indépendants* sur K si le morphisme $K[X_i]_i \to K[x_i]_i$ qui envoie X_i sur x_i pour tout i est bijectif. Il est toujours surjectif ; par conséquent, les x_i sont algébriquement indépendants si et seulement si il est injectif, c'est-à-dire si et seulement si les x_i n'annulent aucun polynôme non trivial à coefficients dans K.

Soit maintenant L une extension de K.

1) Si $x \in L$, la famille singleton $\{x\}$ est algébriquement indépendante sur K si et seulement si x *n'est pas* algébrique. On dit alors que x est *transcendant.*

2) Soit (x_i) une famille d'éléments de L algébriquement indépendants sur K. Elle est maximale, en tant que famille d'éléments de L algébriquement indépendants sur K, si et seulement si L est algébrique sur $K(x_i)$.

Le lemme de Zorn assure qu'il existe une famille d'éléments de L algébriquement indépendants sur K et qui est maximale pour cette propriété. Une telle famille est appelée une *base de transcendance* de L sur K. s

La théorie de l'indépendance algébrique est tout à fait analogue à celle de l'indépendance linéaire. Il existe en fait une théorie générale qui couvre les deux, à savoir celle des *relations de dépendance abstraites* (voir par exemple à ce sujet *Basic Algebra II*, de Jacobson).

On démontre ainsi :

• que si (x_i) est une famille d'éléments de L telle que L soit algébrique sur $K(x_i)_i$, elle contient une base de transcendance ;

• que toutes les bases de transcendances de L sur K ont même cardinal, appelé *degré de transcendance de L sur K* ;

• que si le degré de transcendance de L sur K est fini, toute famille d'éléments de L algébriquement indépendants sur K qui est de cardinal $\deg \operatorname{tr.}(L/K)$ est une base de transcendance.

Par exemple, le degré de transcendance de $K(X_1, \ldots, X_n)$ sur K est égal à n, et $(X_1, \ldots, X_n)$ en est une base de transcendance.

Soit f une fraction rationnelle non constante dans $K(X)$. L'élément X est alors algébrique sur $K(f)$ (exercice facile). En conséquence f est transcendant (sinon, X serait algébrique sur K), et $\{f\}$ est une base de transcendance de L sur K.

Lemme *going-up*, normalisation de Noether et *Nullstellensatz*

J'ai établi le résultat suivant, dit «lemme de *going-up*». Sa preuve consiste essentiellement à se ramener, par passage au quotient et localisation, au lemme du paragraphe précédent sur les injections entières entre anneaux intègres.

Lemme. *Soit $f : A \to B$ un morphisme d'anneaux faisant de B une A-algèbre entière.*

1) Si $\mathfrak{q}$ est un idéal premier de B alors l'idéal premier $f^{-1}(\mathfrak{q})$ de A est maximal si et seulement si $\mathfrak{p}$ est maximal.

2) Si $\mathfrak{q}$ et $\mathfrak{q}'$ sont deux idéaux premiers distincts *de B tels que $f^{-1}(\mathfrak{q}) = f^{-1}(\mathfrak{q}')$, alors $\mathfrak{q}$ et $\mathfrak{q}'$ sont non comparables pour l'inclusion.*

3) Si J est un idéal de B et si l'on pose $I = f^{-1}(J)$ alors pour tout idéal premier $\mathfrak{p}$ de A contenant I il existe un idéal premier $\mathfrak{q}$ de B contenant J tel que $f^{-1}(\mathfrak{q}) = \mathfrak{p}$.

Remarque. Dans le cas où f est injectif, on a $f^{-1}(\{0\}) = \{0\}$ et l'assertion 3) ci-dessus affirme alors que pour tout idéal premier $\mathfrak{p}$ de A, il existe un idéal premier $\mathfrak{q}$ de B tel que $f^{-1}(\mathfrak{q}) = \mathfrak{p}$ (en fait, on ramène la preuve de 3) à celle de ce cas particulier). Autrement dit, si $f : A \to B$ est une injection entière alors $\operatorname{Spec} B \to \operatorname{Spec} A$ est surjective.

J'ai ensuite établi le *lemme de normalisation de Noether.*

Lemme. *Soit k un corps et soit A une k-algèbre non nulle de type fini. Il existe une famille finie $(x_1, \ldots, x_n)$ d'éléments de A qui sont algébriquement indépendants sur k, telle que A soit finie sur sa sous-algèbre $k[x_1, \ldots, x_n]$.*

Ce lemme entraîne, à l'aide du lemme de *going-up*, le «théorème des zéros de Hilbert», également appelé *Nullstellensatz.* Celui-ci peut s'énoncer sous différents formes.

Théorème (*Nullstellensatz*, première version). *Soit k un corps et soit A une k-algèbre de type fini et soit $\mathfrak{p}$ un idéal premier de A. Les assertions suivantes sont équivalentes :*

i) le corps des fractions de $A/\mathfrak{p}$ est une extension algébrique de k ;

ii) le quotient $A/\mathfrak{p}$ est une extension finie de k ;

iii) l'idéal $\mathfrak{p}$ est maximal.

Théorème (*Nullstellensatz*, seconde version). *Soit k un corps et soit $(P_i)_{i\in I}$ une famille de polynômes appartenant à $k[X_1,\ldots,X_n]$. Les assertions suivantes sont équivalentes :*

i) il existe une extension finie L de k et un n-uplet $(x_1,\ldots,x_n)$ d'éléments de L tel que $P_i(x_1,\ldots,x_n)=0$ pour tout i.

ii) il existe une extension L de k et un n-uplet $(x_1,\ldots,x_n)$ d'éléments de L tel que $P_i(x_1,\ldots,x_n)=0$ pour tout i.

iii) Pour toute famille $(Q_i)_{i\in I}$ de polynômes appartenant à $k[X_1,\ldots,X_n]$, on a $\sum Q_iP_i\neq 1$.

Ainsi, si un système d'équations polynomiales à coefficients dans k a une solution dans une extension *quelconque* de k, il en a une dans une extension *finie* ; notez que si k est algébriquement clos, cela signifie qu'il en a une dans k.

Remarque. Supposons qu'un système S d'équations polynomiales à coefficients dans k ait une solution dans une extension L de k, et soit F une extension algébriquement close de K. On a vu plus haut qu'il existe une extension K commune à L et F. Ayant une solution dans L, le système S en a une dans K, et il en a dès lors une dans F par ce qui précède, puisque le corps F est algébriquement clos.

Dimension de Krull

Soit A un anneau et soit $\mathscr{N}$ l'ensemble des entiers n tels qu'il existe une chaîne strictement croissante

$$\mathfrak{p}_0\subsetneq\mathfrak{p}_1\subsetneq\ldots\subsetneq\mathfrak{p}_n$$

où les $\mathfrak{p}_i$ sont des idéaux premiers de A.

On appelle *dimension de Krull* de A la borne supérieure de $\mathscr{N}$ (dans $\mathbb{R}\cup\{-\infty,+\infty\}$).

Remarques et commentaires.

• L'ensemble $\mathscr{N}$ est vide si et seulement si A n'a pas d'idéaux premiers, c'est-à-dire si et seulement si $A=\{0\}$. Dans ce cas, il découle de la définition de la borne supérieure [2] que $\sup\mathscr{N}=-\infty$.

• Si $A\neq 0$ la dimension de Krull de A est ou bien un entier, ou bien égale à $+\infty$ s'il existe des chaînes strictement croissantes arbitrairement longues d'idéaux premiers.

• Le terme «dimension»n'est pas là par hasard : on verra dans le cours sur les schémas que la dimension de Krull a un lien avec la notion intuitive de dimension en géométrie.

Exemples.

1) Dans un corps, il y a un seul idéal premier, l'idéal nul. Il y a donc une seule chaîne strictement croissante d'idéaux premiers, la chaîne singleton $\{0\}$. En conséquence (la numérotation des chaînes commence à 0), la dimension de Krull d'un corps est nulle.

2. La borne supérieure d'une partie d'en ensemble ordonné E est le plus petit de ses majorants dans E, s'il existe. Comme tout élément de E majore $\emptyset$, la borne supérieure de $\emptyset$ dans E est le plus petit élément de E, s'il existe.

2) Soit A un anneau intègre. L'idéal (0) est alors premier. Dire que la dimension de Krull de A est égale à 1 signifie qu'il existe une chaîne d'idéaux premiers $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1$ dans A, mais qu'on ne peut pas trouver de chaîne $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2$.

Autrement dit, cela signifie :

- qu'il existe un idéal premier non nul, c'est-à-dire que A n'est pas un corps ;
- que tout idéal premier non nul de A est maximal.

Ainsi, tout anneau principal qui n'est pas un corps est de dimension 1 ; c'est plus généralement le cas de tout anneau de Dedekind qui n'est pas un corps.

3) Soit k corps. La dimension de Krull de $k[X_i]_{i\in\mathbb{N}}$ est infinie, comme on le voit en considérant par exemple la chaîne

$$(0) \subsetneq (X_0) \subsetneq (X_0, X_1) \subsetneq \ldots \subsetneq (X_0, \ldots, X_i) \subsetneq (X_0, \ldots, X_i, X_{i+1}) \subsetneq \ldots.$$

En ce qui concerne la dimension de Krull, j'ai énoncé deux théorèmes fondamentaux. Le premier concerne les anneaux locaux noethériens ; je ne l'ai pas démontré.

Théorème. *Soit A un anneau local noethérien, et soit $\mathfrak{m}$ son idéal maximal.*

1) La dimension de Krull de A est finie.

2) Toute partie génératrice de $\mathfrak{m}$ a un cardinal au moins égal à la dimension de Krull de A.

Commentaires.

• Il est fondamental que A soit local : Nagata a montré qu'il existe des anneaux noethériens de dimension de Krull égale à $+\infty$.

• Il n'existe pas toujours de partie génératrice de $\mathfrak{m}$ de cardinal égal à la dimension de Krull de A. Lorsque c'est le cas, on dit que l'anneau local noethérien A est *régulier*. Les anneaux locaux réguliers jouent un rôle crucial en géométrie algébrique.

Le second théorème concerne la dimension de Krull des algèbres de type fini sur un corps ; il a été démontré.

Théorème. *Soit k un corps et soit A une k-algèbre intègre et de type fini. La dimension de Krull de A est alors égale au degré de transcendance de* $\mathrm{Frac}(A)$ *sur k (en particulier, elle est finie).*

Exemple. Pour tout n, le degré de transcendance de $k(X_1, \ldots, X_n)$ sur k est égal à n. Par conséquent, la dimension de Krull de $k[X_1, \ldots, X_n]$ vaut n. Notez que

$$(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \ldots \subsetneq (X_1, \ldots, X_n)$$

est une chaîne strictement croissante d'idéaux premiers de $k[X_1, \ldots, X_n]$, ce qui montre déjà que la dimension de Krull de $k[X_1, \ldots, X_n]$ est *au moins* égale à n.

3 Théorie des faisceaux

Préfaisceaux

Notion de préfaisceau (d'ensembles, de groupes abéliens, d'anneaux, de modules, etc.) sur un espace topologique ; morphisme de préfaisceaux ; fibre $\mathscr{F}_x$ d'un préfaisceau $\mathscr{F}$ en un point x.

Exemples.

• Si X est un espace topologique, $U \mapsto \mathscr{C}^0(U, \mathbb{R})$ est un préfaisceau de $\mathbb{R}$-algèbres sur X.

• Si X est une variété différentielle, $U \mapsto \mathscr{C}^\infty(U, \mathbb{R})$ est un préfaisceau de $\mathbb{R}$-algèbres sur X.

• Si X est une variété analytique complexe, $U \mapsto \mathscr{H}(U, \mathbb{C})$ est un préfaisceau de $\mathbb{C}$-algèbres sur X, où $\mathscr{H}(U, \mathbb{C})$ désigne l'anneau des fonctions holomorphes sur U.

• Si X est un espace topologique et E un ensemble, $U \mapsto E$ est un préfaisceau d'ensembles sur X, appelé le *préfaisceau constant associé à E.*

• Sur $\mathbb{C}$, la dérivation des fonctions définit un morphisme de préfaisceaux de $\mathbb{C}$-espaces vectoriels de $\mathscr{H}$ dans lui-même.

Les constructions usuelles au niveau ensembliste se préfaisceautisent : image d'une application, somme directe de groupes abéliens ou de modules, produit tensoriel....

Soit $f : Y \to X$ une application continue entre espaces topologiques.

• Si $\mathscr{F}$ est un préfaisceau sur Y, alors $U \mapsto \mathscr{F}(f^{-1}(U))$ est un préfaisceau sur X noté $f^{-1}(\mathscr{F})$.

• Si $\mathscr{G}$ est un préfaisceau sur X, on définit un préfaisceau $f^{-1}\mathscr{G}$ sur Y comme suit. Pour tout ouvert V de Y, notons $\mathscr{E}_V$ l'ensemble des couples (U, s) où U est un ouvert de X contenant $f(V)$ et où $s \in \mathscr{G}(U)$. On munit $\mathscr{E}_V$ de la relation $\mathscr{R}_V$ définie comme suit : $(U, s)\mathscr{R}_V(U', s')$ si il existe un voisinage ouvert U'' de $f(V)$ dans $U \cap U'$ tel que $s_{|U''} = s'_{|U''}$. On pose alors

$$f^{-1}\mathscr{G}(V) = \mathscr{E}_V / \mathscr{R}_V.$$

Le foncteur f^{-1} est adjoint à gauche au foncteur f_*.

Remarque. La définition de f_* est plus agréable que celle de f^{-1}. Mais en ce qui concerne les fibres, f^{-1} se comporte mieux : si $y \in Y$ alors $f^{-1}\mathscr{G}_y \simeq \mathscr{G}_{f(y)}$, alors qu'il n'existe pas de description commode de $f_*\mathscr{F}_x$ pour $x \in X$.

Remarque. Soit X un espace topologique, soit U un ouvert de X et soit $j : U \hookrightarrow X$ l'inclusion. Si $\mathscr{F}$ est un préfaisceau sur X, alors $j^{-1}\mathscr{F}$ est simplement le faisceau $V \mapsto \mathscr{F}(V)$, où l'on ne considère que des ouverts V contenus dans U. On dit que c'est la *restriction* de $\mathscr{F}$ à U.

Faisceaux

Notion de faisceau (d'ensembles, de groupes abéliens, d'anneaux, de modules, etc.) sur un espace topologique. Si $\mathscr{F}$ et $\mathscr{G}$ sont deux faisceaux , un morphisme de faisceaux de $\mathscr{F}$ vers $\mathscr{G}$ est un morphisme de préfaisceaux de $\mathscr{F}$ vers $\mathscr{G}$: la catégorie des faisceaux est une sous-catégorie pleine de celle des préfaisceaux.

La restriction (comme préfaisceau) d'un faisceau à un ouvert de l'espace ambiant est encore un faisceau.

Remarque. Soit $\mathscr{F}$ un faisceau sur un espace topologique X. En appliquant la définition d'un faisceau au recouvrement ouvert de $\emptyset$ par la *famille vide*, on voit que $\mathscr{F}(\emptyset)$ est un *singleton* (si vous n'aimez pas ça, prenez-le comme une convention).

Exemples.

• Soit E un ensemble et soit X un espace topologique. Le préfaisceau constant qui envoie un ouvert U de X sur l'ensemble E est un faisceau si et seulement si E est un singleton.

• Si X est un espace topologique, $U \mapsto \mathscr{C}^0(U, \mathbb{R})$ est un faisceau de $\mathbb{R}$-algèbres sur X.

• Si X est une variété différentielle, $U \mapsto \mathscr{C}^\infty(U, \mathbb{R})$ est un faisceau de $\mathbb{R}$-algèbres sur X.

• Si X est une variété analytique complexe, $U \mapsto \mathscr{H}(U, \mathbb{C})$ est un faisceau de $\mathbb{C}$-algèbres sur X.

• La dérivation des fonctions holomorphes définit un morphisme de préfaisceaux (et donc de faisceaux) $d : \mathscr{H} \to \mathscr{H}$. Notons $\mathscr{I}$ le préfaisceau image de d. Ce n'est pas un faisceau : en effet, posons $U = \mathbb{C}^*$, $U^+ = \mathbb{C}^* \setminus \mathbb{R}^*_+$, et $U^- = \mathbb{C}^* \setminus \mathbb{R}^*-$. Comme U^+ et U^- sont simplement connexes, $1/z$ appartient à $\mathscr{I}(U^+)$ et $\mathscr{I}(U^-)$, et on a évidemment coïncidence de ces deux sections sur $U^+ \cap U^-$. Mais elles ne se recollent pas en une section de $\mathscr{I}$ sur U : si c'était le cas, cette section serait nécessairement $1/z$, qui n'a pas de primitive sur U (il n'y a pas de logarithme sur $\mathbb{C}^*$) et n'appartient donc pas à $\mathscr{I}(U)$.

Soit X un espace topologique. Le foncteur d'inclusion de la catégorie des faisceaux sur X vers celle des préfaisceaux sur X admet un adjoint à gauche, appelé la *faisceautisation.* Si $\mathscr{F}$ est un préfaisceau, on notera $\widehat{\mathscr{F}}$ son ≪faisceautisé≫.

La définition de $\widehat{\mathscr{F}}$ par sa propriété universelle garantit son unicité à isomorphisme canonique près, et donc son indépendance du procédé particulier utilisé pour le construire. On en trouve plusieurs dans la littérature, je vais décrire succinctement celui que j'ai présenté en cours.

Soit donc $\mathscr{F}$ un préfaisceau sur un espace topologique X. On définit le préfaisceau $\widehat{\mathscr{F}}$ comme suit.

• Pour tout ouvert U de X, on note $\widehat{\mathscr{F}}(U)$ l'ensemble des familles $(s_x)_{x \in U}$, où $s_x \in \mathscr{F}_x$ pour tout x, satisfaisant la propriété suivante : pour tout $y \in U$, il existe un voisinage ouvert V de y dans U et un élément $t \in \mathscr{F}(V)$ tel que $s_x = t_x$ pour tout $x \in V$.

• Si U et V sont deux ouverts de X avec $V \subset U$, on dispose d'une flèche naturelle $\widehat{\mathscr{F}}(U) \to \widehat{\mathscr{F}(V)}$: elle envoie la famille $(s_x)_{x \in U}$ sur $(s_x)_{x \in V}$.

On vérifie que $\widehat{\mathscr{F}}$ est un faisceau. On dispose d'une flèche naturelle $j : \mathscr{F} \to \widehat{\mathscr{F}}$: pour tout ouvert U de X, elle envoie une section s de $\mathscr{F}(U)$ sur la famille de ses germes.

Puis on démontre la propriété universelle : pour tout morphisme de préfaisceaux f de $\mathscr{F}$ dans un faisceau $\mathscr{G}$, il existe un unique morphisme de faisceaux de $\widehat{\mathscr{F}}$ vers $\mathscr{G}$ tel que le diagramme

$$\begin{tikzcd} \mathscr{F} \arrow[r, "f"] \arrow[d, "j"'] & \mathscr{G} \\ \widehat{\mathscr{F}} \arrow[ur] & \end{tikzcd}$$

commute.

Au cours de la preuve, on vérifie que j induit pour tout $x \in X$ une bijection $\mathscr{F}_x = \widehat{\mathscr{F}_x}$: un préfaisceau et son faisceau associé ont les mêmes fibres.

Premiers exemples.

• Si $\mathscr{F}$ est un faisceau, il satisfait la propriété universelle ci-dessus. En conséquence, $\widehat{\mathscr{F}} = \mathscr{F}$.

• Soit E un ensemble et soit X un espace topologique. Pour tout $x \in X$, la fibre en x du préfaisceau constant $U \mapsto E$ est égale à E. Son faisceautisé s'identifie donc, d'après notre construction, au faisceau des applications localement constantes à valeurs dans E. On l'appelle le faisceau constant associé à E, et on le note $\underline{E}$.

Notez que si X est localement connexe, $\underline{E}$ envoie un ouvert U sur $E^{\pi_0(U)}$, où $\pi_0(U)$ est l'ensemble des composantes connexes de U.

• Soit $\mathscr{F}$ un faisceau, et soit $\mathscr{G}$ un sous-*préfaisceau* de $\mathscr{F}$. Le faisceau associé à $\mathscr{G}$ est alors le sous-faisceau de $\mathscr{F}$ formé des sections qui appartiennent localement à $\mathscr{G}$. En termes un peu plus précis, $\mathscr{G}(U)$ est l'ensemble des sections $s \in \mathscr{F}(U)$ satisfaisant la condition suivante : pour tout $x \in U$, il existe un voisinage ouvert V de x dans U tel que $s_{|V} \in \mathscr{G}(V)$.

En général, les constructions usuelles dans la catégorie des préfaisceaux ne préservent pas le fait d'être un faisceau. On est donc amené à les faisceautiser. Nous allons maintenant illustrer ce fait à travers quelques exemples fondamentaux.

Autour des images de morphismes. Si $f : \mathscr{F} \to \mathscr{G}$ est un morphisme de faisceaux, on notera désormais $\mathrm{Im}\, f$ le faisceau associé à l'image préfaisceautique de f, c'est-à-dire le sous-faisceau de $\mathscr{G}$ formé des sections qui appartiennent localement à l'image de f.

Par exemple, soit $\mathscr{H}$ le faisceau des fonctions holomorphes sur $\mathbb{C}$, et soit $d : \mathscr{H} \to \mathscr{H}$ la dérivation. L'image préfaisceautique $\mathscr{I}$ de d envoie un ouvert U sur l'ensemble des fonctions holomorphes de U dans $\mathbb{C}$ qui admettent une primitive ; son image faisceautique $\mathrm{Im}\, f$ envoie U sur l'ensemble des fonctions holomorphes de U dans $\mathbb{C}$ qui admettent *localement* une primitive, ce qui est le cas de toutes les fonctions holomorphes sur U. Autrement dit, $\mathrm{Im}\, f = \mathscr{H}$.

Ce n'est pas le cas de $\mathscr{I}$: comme on l'a déjà signalé plus haut quand on a expliqué que $\mathscr{I}$ n'est pas un faisceau, la fonction $1/z \in \mathscr{H}(U)$ n'appartient pas à $\mathscr{I}(U)$.

Définitions et remarques. On dit qu'un morphisme de faisceaux $f : \mathscr{F} \to \mathscr{G}$ est *surjectif* si $\mathrm{Im}\, f = \mathscr{G}$. Cela ne signifie pas, on vient de le voir, que l'image préfaisceautique de f est égale à $\mathscr{G}$: en d'autres termes, dire que $\mathscr{F} \to \mathscr{G}$ est surjectif n'implique pas que $\mathscr{F}(U) \to \mathscr{G}(U)$ le soit pour tout ouvert U.

On définit par contre l'injectivité et la bijectivité de manière naïve : on dit que $\mathscr{F} \to \mathscr{G}$ est injective (resp. bijective) si $\mathscr{F}(U) \to \mathscr{G}(U)$ est injective (resp. bijective) pour tout U.

Si $\mathscr{F} \to \mathscr{G}$ est injective, on vérifie que son image préfaisceautique est déjà un faisceau (l'unicité des antécédents locaux garantit leur recollement en un antécédent global). Il s'ensuit que $\mathscr{F} \to \mathscr{G}$ est bijectif si et seulement si il est injectif et surjectif.

On vérifie par ailleurs que les notions d'injectivité, surjectivité, et bijectivité se détectent fibre à fibre : un morphisme $\mathscr{F} \to \mathscr{G}$ est injectif (resp. surjectif, resp. bijectif) si et seulement si $\mathscr{F}_x \to \mathscr{G}_x$ est injectif (resp. surjectif, resp. bijectif) pour tout x.

Si $f : \mathscr{F} \to \mathscr{G}$ est un morphisme de faisceaux de groupes, on définit le noyau de f de manière naïve, comme le préfaisceau $U \mapsto \mathrm{Ker}(\mathscr{F}(U) \to \mathscr{G}(U))$. Il se trouve que c'est un faisceau.

Donnons-nous un diagramme de morphismes de faisceaux en groupes

$$\to \mathscr{F}_i \to \mathscr{F}_{i+1} \to \mathscr{F}_{i+2} \to \ldots ...$$

(les indices i appartiennent à $\mathbb{Z}$, et la suite peut être infinie d'un côté ou des deux). On dit que c'est une suite exacte si pour tout i tel que $\mathscr{F}_i$ ne soit pas un terme extrême de la suite, le noyau de $\mathscr{F}_i \to \mathscr{F}_{i+1}$ est égal à l'image (faisceautique !) de $\mathscr{F}_{i-1} \to \mathscr{F}_i$. L'exactitude d'une suite se détecte fibre à fibre.

Si $1 \to \mathscr{F}' \to \mathscr{F} \to \mathscr{F}''$ est une suite exacte de faisceaux en groupe sur un espace topologique X, alors pour tout ouvert U de X la suite

$$1 \to \mathscr{F}'(U) \to \mathscr{F}(U) \to \mathscr{F}''(U)$$

est exacte.

Mais attention : si $1 \to \mathscr{F}' \to \mathscr{F} \to \mathscr{F}'' \to 1$ est une suite exacte, la suite

$$1 \to \mathscr{F}'(U) \to \mathscr{F}(U) \to \mathscr{F}''(U)$$

est exacte par ce qui précède, mais $\mathscr{F}(U) \to \mathscr{F}''(U)$ n'est pas forcément surjectif (on a déjà signalé ce problème lors des discussions sur l'image faisceautique) : le foncteur $\mathscr{F} \mapsto \mathscr{F}(U)$ est exact à gauche, mais n'est pas exact en général.

Exemple de suite exacte de faisceaux. On a vu plus haut que la dérivation $d : \mathscr{H} \to \mathscr{H}$ est surjective. Son noyau est facile à décrire : une application holomorphe sur un ouvert U de $\mathbb{C}$ a une dérivée nulle si et seulement si elle est *localement* constante sur U (l'ouvert U n'est pas forcément connexe !). On dispose donc d'une suite exacte naturelle

$$0 \longrightarrow \underline{\mathbb{C}} \longrightarrow \mathscr{H} \xrightarrow{d} \mathscr{H} \longrightarrow 0 \cdot$$

Décrivons la suite exacte qui lui correspond au niveau des fibres. Soit $x \in \mathbb{C}$. Le développement en série entière en la variable $u = z - x$ fournit un isomorphisme de $\mathbb{C}$-algèbres entre $\mathscr{H}_x$ et l'anneau $\mathscr{C}\{u\}$ des séries entières de rayon > 0. La fibre en x de la suite exacte précédente est la suite exacte de $\mathbb{C}$-espaces vectoriels

$$0 \longrightarrow \mathbb{C} \longrightarrow \mathbb{C}\{u\} \xrightarrow{\partial/\partial u} \mathbb{C}\{u\} \longrightarrow 0 \cdot$$

Fonctorialité. Soit $f : Y \to X$ une application continue entre espaces topologiques. Si $\mathscr{F}$ est un faisceau sur Y, on vérifie que le préfaisceau $f_*\mathscr{F}$ est un faisceau.

Par contre, si $\mathscr{G}$ est un faisceau sur X, le préfaisceau $f^{-1}\mathscr{G}$ n'est pas un faisceau en général. *C'est désormais son faisceautisé que l'on désignera par $f^{-1}\mathscr{G}$.*

On a ainsi défini deux foncteurs : le foncteur f^{-1} qui va de la catégorie des faisceaux sur X vers celle des faisceaux sur Y, et le foncteur f_*, qui va de la catégorie des faisceaux sur Y vers celle des faisceaux sur X. On vérifie que f^{-1} est adjoint à gauche de f_*.

Si $j : U \hookrightarrow X$ est l'inclusion d'un ouvert U dans un espace topologique X, alors pour tout faisceau $\mathscr{F}$ sur X, le faisceau $j^{-1}\mathscr{F}$ n'est autre que la restriction de $\mathscr{F}$ à U.

Produit tensoriel. Soit X un espace topologique et soit $\mathscr{A}$ un faisceau d'anneaux sur X. Soient $\mathscr{F}$ et $\mathscr{G}$ deux faisceaux en $\mathscr{A}$-modules sur X. Le produit tensoriel préfaisceautique de $\mathscr{F}$ et $\mathscr{G}$ au-dessus de $\mathscr{A}$ n'est pas un faisceau en général ; c'est son faisceautisé que l'on notera $\mathscr{F} \otimes_{\mathscr{A}} \mathscr{G}$.

Quotient. Soit $\mathscr{G}$ un faisceau de groupes sur un espace topologique X, et soit $\mathscr{H}$ un sous-faisceau de groupes de $\mathscr{G}$. Le préfaisceau quotient de $\mathscr{G}$ par $\mathscr{H}$ n'est pas un faisceau en général ; c'est son faisceautisé que l'on notera $\mathscr{G}/\mathscr{H}$. On a une suite exacte naturelle

$$1 \to \mathscr{H} \to \mathscr{G} \to \mathscr{G}/\mathscr{H} \to 1.$$

Somme directe. On peut définir la somme directe d'une famille quelconque de faisceaux, en en faisant la somme directe comme préfaisceaux (ouvert par ouvert, donc), puis en faisceautisant. Si on fait la somme directe d'une famille finie de faisceaux, il n'y a pas besoin de faisceautiser : la somme directe préfaisceautique est encore un faisceau.

Espaces annelés

Un *espace annelé* est un espace topologique X muni d'un faisceau d'anneaux $\mathscr{O}_X$.

Par exemple, toute variété différentielle X hérite d'une structure naturelle d'espace annelé : on définit $\mathscr{O}_X$ comme le faisceau des fonctions $\mathscr{C}^\infty$ à valeurs réelles.

Un morphisme d'espaces annelés $f : (Y, \mathscr{O}_Y) \to (X, \mathscr{O}_X)$ consiste en une application continue $f : Y \to X$ et une série de données supplémentaires que l'on peut présenter de trois façons équivalentes.

• *Première façon.* Pour tout couple (V, U) formé d'un ouvert V de Y et d'un ouvert U de X tel que $f(V) \subset U$, on se donne une application $\mathscr{O}_X(U) \to \mathscr{O}_Y(V)$ (attention au sens !), en exigeant que si U et U' sont deux ouverts de X avec $U \subset U'$, et V et V' sont deux ouverts de Y avec $V \subset V'$, $f(V) \subset U$ et $f(V') \subset U'$

alors le diagramme

$$\begin{tikzcd} \mathscr{O}_X(U) \arrow[r] \arrow[d] & \mathscr{O}_Y(V) \arrow[d] \\ \mathscr{O}_X(U') \arrow[r] & \mathscr{O}_Y(V') \end{tikzcd}$$

commute.

- *Deuxième façon.* On se donne un morphisme de $\mathscr{O}_X$ vers $f_*\mathscr{O}_Y$.
- *Troisième façon.* On se donne un morphisme de $f^{-1}\mathscr{O}_X$ vers $\mathscr{O}_Y$.

Remarque. Les deuxièmes et troisièmes façons sont équivalentes par adjonction. Elles sont bien adaptées aux raisonnements théoriques, notamment ceux faisant intervenir des propriétés universelles.

Plus terre à terre, la première façon est très utilisée en pratique.

Exemple. Soit $f : Y \to X$ une application $\mathscr{C}^\infty$ entre variétés différentielles. Elle induit de manière naturelle un morphisme d'espaces annelés de $(Y, \mathscr{O}_Y)$ vers $(X, \mathscr{O}_X)$: si V est un ouvert de Y et si U est un ouvert de X contenant $f(V)$, on envoie une fonction $\varphi \in \mathscr{O}_X(U) = \mathscr{C}^\infty(U, \mathbb{R})$ sur l'élément $\varphi \circ f_{|V}$ de $\mathscr{O}_Y(V) = \mathscr{C}^\infty(V, \mathbb{R})$.

Si $f : (Y, \mathscr{O}_Y) \to (X, \mathscr{O}_X)$ est un morphisme d'espaces annelés, il induit pour tout $y \in Y$ un morphisme d'anneaux $\mathscr{O}_{X,f(y)} \to \mathscr{O}_{Y,y}$.

Espaces localement annelés

Un *espace localement annelé* est un espace annelé $(X, \mathscr{O}_X)$ tel que $\mathscr{O}_{X,x}$ soit pour tout $x \in X$ un anneau local.

Par exemple, si X est une variété différentielle, l'espace annelé correspondant est localement annelé.

Un espace localement annelé ressemble beaucoup, par certains aspects, à un espace topologique muni d'un faisceau de fonctions raisonnables. Nous allons expliquer en quoi, et évoquer également les limites de cette ressemblance.

Soit $(X, \mathscr{O}_X)$ un espace localement annelé. Soit $x \in X$. L'anneau $\mathscr{O}_{X,x}$ est local ; notons $\kappa(x)$ son corps résiduel. On dispose d'une surjection $\mathscr{O}_{X,x} \to \kappa(x)$, dont le noyau est exactement l'ensemble des éléments non inversibles de $\mathscr{O}_{X,x}$. Pour des raisons psychologiques, on décide de noter ce morphisme $f \mapsto f(x)$. On a donc $f \in \mathscr{O}_{X,x}^* \iff f(x) \neq 0$.

Soit U un ouvert de X et soit $x \in U$. On note encore $f \mapsto f(x)$ l'application composée $\mathscr{O}_X(U) \to \mathscr{O}_{X,x} \to \kappa(x)$.

Lemme. *Soit U un ouvert de X et soit $f \in \mathscr{O}_X(U)$.*

i) La fonction f est inversible dans $\mathscr{O}_X(U)$ si et seulement si $f(x) \neq 0$ pour tout $x \in U$.

ii) L'ensemble des points $x \in U$ tels que $f(x) \neq 0$ est un ouvert de U. .

Démonstration. Si f est inversible dans $\mathscr{O}_X(U)$ alors pour tout $x \in U$ l'élément $f(x)$ de $\kappa(x)$ est inversible (un morphisme d'anneaux préserve les inversibles), donc non nul.

Supposons maintenant que $f(x) \neq 0$ pour tout $x \in U$. Soit $x \in U$. Comme $f(x) \neq 0$, le germe de f en x est un élément inversible de $\mathscr{O}_{X,x}$; il existe donc un voisinage ouvert de x dans U sur lequel f est inversible.

Il existe en conséquence un recouvrement ouvert (U_i) de U et, pour tout i, un inverse g_i de $f_{|U_i}$. Par unicité de l'inverse, les restrictions de g_i et g_j à $U_i \cap U_j$ coïncident pour tout (i, j) ; les fonctions g_i se recollent dès lors en une fonction $g \in \mathscr{O}_X(U)$. Comme $gf_{|U_i} = 1$ pour tout i par construction, on a $gf = 1$ et f est inversible, ce qui achève de montrer i).

Montrons ii). Soit x tel que $f(x) \neq 0$. Le germe de f en x est un élément inversible de $\mathscr{O}_{X,x}$; il existe donc un voisinage ouvert V de x dans U sur lequel f est inversible. D'après i), on a alors $f(y) \neq 0$ pour tout $y \in V$, ce qui achève de montrer ii). □

Ce lemme montre donc qu'en ce qui concerne l'inversibilité et la non-annluation, un espace localement annelé se comporte comme un espace muni d'un faisceau de fonctions raisonnables.

Indiquons maintenant quelles sont les limites de cette analogie. La première est que le corps $\kappa(x)$ *dépend* a priori *du point* x, ce qui n'est pas le cas dans les exemples classiques (comme les variétés différentielles, sur lesquelles ce corps est égal à $\mathbb{R}$ pour tout point) ; et on verra dans le cours sur les schémas des exemples naturels d'espaces annelés dans lesquels $\kappa(x)$ varie avec x, éventuellement de façon assez brutale : la caractéristique peut changer.

La seconde concerne l'annulation des fonctions. Si $(X, \mathscr{O}_X)$ est un espace localement annelé, si U est un ouvert de X et si $f \in \mathscr{O}_X(U)$, *il se peut que* $f(x) = 0$ *pour tout* $x \in U$ *sans que* f *soit nulle.*

Supposons par exemple que f soit nilpotente et non nulle. Dans ce cas, $f(x)$ est pour tout $x \in X$ un élément nilpotent d'un corps, et est donc trivial.

Nous allons donner un exemple très simple où une telle f existe. Fixons un corps k, et considérons un espace topologique singleton $\{x\}$. Se donne une structure d'espace localement annelé sur $\{x\}$ revient à choisir un anneau local. Soit $\mathscr{O}$ le quotient $k[T]/(T^2)$ et soit f la classe de T ; elle est non nulle.

L'ensemble des idéaux premiers de $\mathscr{O}$ est en bijection avec l'ensemble des idéaux premiers de $k[T]$ contenant (T^2) ; il n'y en a qu'un, à savoir (T). L'anneau $\mathscr{O}$ est donc local, et son unique idéal maximal est (f). On a ainsi bien défini une structure d'espace localement annelé sur x. Comme f est nilpotente, on a $f(x) = 0$ (ce qu'on peut voir directement ici : l'évaluation en x est la réduction modulo l'idéal maximal de $\mathscr{O}$, c'est-à-dire modulo (f)).

Commentaires. On peut se demander pourquoi autoriser ce genre d'horreurs, alors qu'on a fait en sorte, pour ce qui concerne la non-annulation, que les propriétés usuelles soient satisfaites.

La raison est que la présence de «fonctions» nilpotentes non nulles peut avoir un sens géométrique profond, et c'est notamment le cas dans l'exemple que l'on vient de traiter.

En effet, considérons, un corps k étant fixé, la parabole P d'équation $T^2 = S$ et la droite D d'équation $S = 0$. Leur intersection est le point x de coordonnées $(0, 0)$. En théorie des schémas, cette intersection est un peu plus riche que $\{x\}$: on garde en mémoire le corps de base et les équations, et l'intersection sera donc l'espace topologique $\{x\}$ muni du faisceau (ou de l'anneau, si l'on préfère) $k[S,T]/(S,T^2-S) \simeq k[T]/T^2$: on retrouve l'espace localement annelé évoqué plus haut.

La présence de nilpotents non triviaux parmi les fonctions sur $P \cap D$ s'interprète intuitivement comme suit : l'intersection $P \cap D$ est égale au point x *infinitésimalement épaissi* parce que P et D sont tangentes en x ; le point d'intersection x est en quelque sorte double, et c'est cette multiplicité qui est codée algébriquement par l'existence de nilpotents non triviaux.

Cet exemple est significatif : c'est pour prendre en compte les multiplicités dans la théorie que Grothendieck a décidé d'admettre les ≪fonctions≫ nilpotentes non nulles . Cela se révèle un outil extraordinairement souple, mais il y a un prix à payer : il faut autoriser une fonction à s'annuler en tout point sans être globalement nulle. D'où le choix du formalisme abstrait des espaces localement annelés, qui mime tant que c'est nécessaire le point de vue fonctionnel classique, mais permet ce genre de fantaisies finalement très utiles.

Morphismes d'espaces localement annelés. Soient A et B deux anneaux locaux d'idéaux maximaux respectifs $\mathfrak{m}$ et $\mathfrak{n}$. Soit f un morphisme de A vers B. Si $a \in A$ et si $f(a) \in \mathfrak{n}$ alors $f(a)$ n'est pas inversible, et a n'est donc pas inversible non plus ; autrement dit, $a \in \mathfrak{m}$.

On dit que f est *local* si la réciproque est vraie, c'est-à-dire si $f(\mathfrak{m}) \subset \mathfrak{n}$.

Soient $(Y, \mathscr{O}_Y)$ et $(X, \mathscr{O}_X)$ deux espaces localement annelés. Un *morphisme d'espaces localement annelés* de $(Y, \mathscr{O}_Y)$ vers $(X, \mathscr{O}_X)$ est un morphisme f d'espaces annelés tel que $\mathscr{O}_{X,f(y)} \to \mathscr{O}_{Y,y}$ soit pour tout $y \in Y$ un morphisme local.

Nous allons tout de suite récrire cette condition de façon plus suggestive. Soit $y \in Y$; notons f^* le morphisme induit par f au niveau des anneaux de fonctions.

Dire que $\mathscr{O}_{X,f(y)} \to \mathscr{O}_{Y,y}$ est local signifie que si φ est un élément de $\mathscr{O}_{X,f(y)}$ appartenant à l'idéal maximal de ce dernier, alors $f^*\varphi$ appartient à l'idéal maximal de $\mathscr{O}_{Y,y}$. En termes plus imagés, cela se traduit par l'implication

$$(\varphi(f(y)) = 0) \Rightarrow (f^*\varphi)(y) = 0.$$

Supposons que $(Y, \mathscr{O}_Y)$ et $(X, \mathscr{O}_X)$ soient des variétés différentielles, et que f soit donnée par une application $\mathscr{C}^\infty$. Le morphisme f est alors un morphisme d'espaces localement annelés ; en effet, comme f^* est donné par la composition avec f, l'implication ci-dessus est automatiquement vérifiée.

En fait, si f est un morphisme d'espaces localement annelés, le morphisme f^* ressemble automatiquement à la composition avec f, dans l'exacte mesure où un espace localement annelé ressemble à un espace muni d'un faisceau de fonctions raisonnables.

Précisons ce que j'entends par là. Soit $f : (Y, \mathscr{O}_Y) \to (X, \mathscr{O}_X)$ un morphisme d'espaces localement annelés et soit $y \in Y$. Comme on a affaire à un morphisme d'espaces localement annelés, on a $\varphi(f(y)) = 0 \Rightarrow (f^*\varphi)(y) = 0$ pour toute $\varphi \in \mathscr{O}_{X,f(y)}$. En conséquence, $\mathscr{O}_{X,f(y)} \to \mathscr{O}_{Y,y}$ induit par passage au quotient un plongement $\kappa(f(y)) \hookrightarrow \kappa(y)$, de sorte que le diagramme

$$\begin{tikzcd}
\mathscr{O}_{Y,y} \arrow[r] & \kappa(y) \\
\mathscr{O}_{X,f(y)} \arrow[r] \arrow[u] & \kappa(f(y)) \arrow[u]
\end{tikzcd}$$

commute. Autrement dit, on a pour toute $\varphi \in \mathscr{O}_{X,f(y)}$ l'égalité

$$(f^*\varphi)(y) = \varphi(f(y)) \in \kappa(f(y)) \hookrightarrow \kappa(y).$$

Faisceaux de modules sur un espace annelé

Soit $(X, \mathscr{O}_X)$ un espace annelé. Un faisceau en $\mathscr{O}_X$-modules sera simplement appelé *$\mathscr{O}_X$-module.*

Soit $f : (Y, \mathscr{O}_Y) \to (X, \mathscr{O}_X)$ un morphisme d'espaces annelés. Soit $\mathscr{F}$ un $\mathscr{O}_Y$-module. Le faisceau $f_*\mathscr{F}$ est de manière naturelle un $f_*\mathscr{O}_Y$-module. Comme on dispose d'un morphisme $\mathscr{O}_X \to f_*\mathscr{O}_Y$ (c'est l'une des définitions d'un morphisme d'espaces annelés), le faisceau $f_*\mathscr{F}$ hérite d'une structure naturelle de $\mathscr{O}_X$-module.

Soit $\mathscr{G}$ un $\mathscr{O}_X$-module. Le faisceau $f^{-1}\mathscr{G}$ est de façon naturelle un $f^{-1}\mathscr{O}_X$-module, mais n'a pas *a priori* de structure de $\mathscr{O}_Y$-module : on dispose (là encore d'après l'une des définitions d'un morphisme d'espaces annelés) d'une flèche $f^{-1}\mathscr{O}_X \to \mathscr{O}_Y$, mais elle va dans le mauvais sens. Qu'à cela ne tienne : on le transforme «de force» en un $\mathscr{O}_Y$-module en posant $f^*\mathscr{G} = \mathscr{O}_Y \otimes_{f^{-1}\mathscr{O}_X} f^{-1}\mathscr{G}$.

On ainsi défini deux foncteurs, f_* de $\mathscr{O}_X - \mathsf{Mod}$ vers $\mathscr{O}_Y - \mathsf{Mod}$, et f^* de $\mathscr{O}_Y - \mathsf{Mod}$ vers $\mathscr{O}_X - \mathsf{Mod}$. On vérifie que f^* est adjoint à gauche à f_*.

Soit maintenant $(X, \mathscr{O}_X)$ un espace *localement* annelé et soit $\mathscr{F}$ un $\mathscr{O}_X$-module. Supposons que $\mathscr{F}$ est *localement de type fini*, c'est-à-dire qu'il existe un recouvrement ouvert (U_i) de X et, pour tout i, un entier n_i et une surjection $\bigoplus \mathscr{O}_{U_i}^{n_i} \to \mathscr{F}_{|U_i}$, où $\mathscr{O}_{U_i}$ désigne la restriction de $\mathscr{O}_X$ à U_i pour tout i.

Soit $x \in X$. Par notre hypothèse, $\mathscr{F}_x$ est un $\mathscr{O}_{X,x}$-module de type fini. Lorsqu'on le tensorise avec $\kappa(x)$, on obtient un $\kappa(x)$ espace vectoriel $\mathscr{F} \otimes \kappa(x)$, de dimension finie $r(x)$.

J'ai démontré à l'aide du lemme de Nakayama (dont c'est essentiellement la traduction géométrique) que $x \mapsto r(x)$ est semi-continue supérieurement, c'est-à-dire que pour tout entier n, l'ensemble $\{x \in X, r(x) \geqslant n\}$ est fermé.

Notons une conséquence particulière importante : l'ensemble des x tels que $\mathscr{F} \otimes \kappa(x) = 0$ est *ouvert*, contrairement à ce qu'on pourrait croire à première vue.

Terminons par un exemple. On prend pour X la variété différentielle $\mathbb{R}$. On vérifie que le préfaisceau $\mathscr{F}$ qui envoie U sur $\mathbb{R}$ si $0 \in U$ et sur 0 sinon est un faisceau.

Soit $\mathscr{I}$ le sous-préfaisceau d'idéaux de $\mathscr{O}_X$ tel que $\mathscr{I}(U)$ soit égal à $\mathscr{O}_X(U)$ si $0 \notin U$, et à $\{f \in \mathscr{O}_X(U), f(0) = 0\}$ si $0 \in U$. On voit facilement que $\mathscr{I}$ est un faisceau.

L'application $f \mapsto f(0)$ définit de façon naturelle un morphisme $\mathscr{O}_X \to \mathscr{F}$, qui est surjectif de noyau $\mathscr{I}$. On dispose donc d'une suite exacte

$$0 \to \mathscr{I} \to \mathscr{O}_X \to \mathscr{F} \to 0.$$

Ainsi, $\mathscr{F}$ s'identifie à $\mathscr{O}/\mathscr{I}$ et est en particulier un $\mathscr{O}_X$-module localement de type fini. On vérifie immédiatement que $\mathscr{F} \otimes \kappa(0) = \mathbb{R}$, et que $\mathscr{F} \otimes \kappa(x) = \{0\}$ pour tout $x \neq 0$. La fonction r vaut ainsi 0 sur $\mathbb{R}^*$, et 1 en 0.