

# 1 & ()

par Giordano Favi

Sous ce titre pour le moins mystérieux nous reproduirons essentiellement les premiers chapitres d'un lointain diplôme au titre homonyme. Le but de feu ce diplôme était de comprendre les algèbres d'octonions sur un anneau commutatif  $R$ , cependant l'auteur s'est vu poussé inéluctablement vers l'étude des  $R$ -algèbres non nécessairement unitaires ni associatives (ah... mōssieur, ça existe pas ça...vous vous trompez, à moi on m'a toujours dit que c'est associatif une algèbre...) à l'aide de leurs localisés et leurs quotients. Dès lors le lecteur comprendra aisément le choix du titre (prononcez-le comme vous voulez, néanmoins la prononciation officielle est "un et parenthèses"). Comme à son habitude, l'auteur s'est laissé emporter par son zèle vulgarisateur et a essayé de rendre son texte abordable à un public le plus hétérocyte possible.

## 1. Définitions

Pour bien commencer, il est bon de fixer le langage. L'auteur a pu constater que nombreux sont ceux qui froncent leurs sourcils avec effroi lorsqu'ils entendent parler d'algèbres sans unité ou non associatives... La kyrielle de définitions suivantes a pour but de démystifier ces objets et de les faire entrer dans les mœurs des gens.

Pour des raisons qui n'apparaîtront que dans les prochains paragraphes et par respect pour le lecteur, l'anneau de base  $R$  sera supposé commutatif bien que l'on puisse s'affranchir de cette dernière hypothèse pour les présentes définitions.

### Définition 1.

Soit  $R$  un anneau commutatif (un vrai ! un bon vieux anneau avec unité, associatif ; pensez à  $\mathbb{Z}$  si vous êtes perturbés). Une  $R$ -algèbre est un couple  $(A; \mu)$ , où  $A$  est un  $R$ -module et  $\mu : A \times A \rightarrow A$  est une application  $R$ -bilinéaire. (Ouais mais... zêtes vraiment sûr que vous avez rien oublié ?)

Au fait la seule chose que l'on demande dans cette définition est la distributivité de l'addition par rapport à la multiplication (et bien entendu le fait que les éléments de l'anneau ne jouent aucun rôle dans la structure d'algèbre). Ainsi, les êtres que l'on a l'habitude d'appeler "algèbres" habituellement sont des algèbres avec quelques propriétés en plus. On peut donc bien parler de la  $\mathbb{Z}$ -algèbre  $M_2(\mathbb{Z})$  formée des matrices  $2 \times 2$  à coefficients entiers (avec la multiplication matricielle usuelle) ou de la  $\mathbb{R}$ -algèbre  $C(X, \mathbb{R})$  des fonction continues sur un espace topologique  $X$  (avec la multiplication  $f \cdot g(x) = f(x)g(x)$  comme d'habitude) ou encore de la  $\mathbb{Q}$ -algèbre  $\mathbb{Q}^{\mathbb{N}}$  (avec multiplication donnée composante par composante). Il va aussi de soi que tout anneau commutatif  $R$  peut être lui-même vu en tant que  $R$ -algèbre.

**Remarque:** Il est clair que  $\mu$  induit une application  $R$ -linéaire  $\bar{\mu} : A \otimes_R A \rightarrow A$  et réciproquement que toute application  $R$ -linéaire  $\bar{\nu} : A \otimes_R A \rightarrow A$  muni  $A$  d'une structure de  $R$ -algèbre, en posant  $\nu((a, b)) = \bar{\nu}(a \otimes b)$  pour tous  $a, b \in A$ , de sorte que nous confondrons ces applications. (Si vous ne connaissez pas la signification du symbole  $\otimes$  ce n'est pas trop grave)

Lorsqu'aucune confusion n'est à craindre nous dirons algèbre plutôt que  $R$ -algèbre. Pour alléger les écritures (salut Perret !), lorsqu'il n'est fait mention que d'une structure d'algèbre  $\mu$  sur un seul module  $A$ , on écrira le plus souvent  $ab$  au lieu de  $\mu(a \otimes b)$  et on parlera plutôt de l'algèbre  $A$  au lieu de l'algèbre  $(A; \mu)$ .

### Définition 2.

On dit qu'une algèbre  $A$  est **alternative à gauche** (respectivement **à droite**) si  $a^2b = a(ab)$  (respectivement  $ab^2 = (ab)b$ ) pour tous  $a, b \in A$ . Elle sera appelée **alternative** si elle est à la fois alternative à gauche et à droite. Elle sera appelée **associative** si  $a(bc) = (ab)c$  quelques soient  $a, b, c \in A$ , de sorte que toute algèbre associative est aussi alternative. Nous dirons que  $A$  est **commutative** si  $ab = ba$  pour tous  $a, b \in A$ .

Les notions d'alternativité à gauche et à droite se confondent et entraînent l'alternativité lorsque l'algèbre est commutative. En effet  $ab^2 = b^2a = b(ba) = (ba)b = (ab)b$ .

**Définition 3.**

Soit  $A$  une algèbre et  $a \in A$ . On pose  $a^1 = a$  et  $a^n = a(a^{n-1})$  pour tout  $n \in \mathbb{N}$ ,  $n > 0$ .

Cette définition n'est pas nécessaire lorsqu'on travaille avec des algèbres alternatives, en effet  $a^2a = aa^2$  dans de telles algèbres et donc la sous-algèbre engendrée par  $a$  est associative, auquel cas il n'y a pas d'ambiguïté pour la définition de  $a^n$ .

**Exemple:** (Octonions)

Historiquement, la notion d'algèbre alternative a vu le jour grâce à la découverte de l'algèbre des octonions par Cayley (mais il paraît que Graves l'aurait précédé). On la construit sur  $\mathbb{R}$  comme suit :

On prend d'abord la  $\mathbb{R}$ -algèbre des nombres complexes

$$\mathbb{C} = \mathbb{R} \oplus \mathbb{R}i \quad \text{avec} \quad i^2 = -1,$$

non contents, on considère la  $\mathbb{R}$ -algèbre des quaternions

$$\mathbb{H} = \mathbb{C} \oplus \mathbb{C}j \quad \text{avec} \quad j^2 = -1 \quad \text{et} \quad zj = j\bar{z} \quad \forall z \in \mathbb{C}$$

sur laquelle on a une conjugaison  $\overline{x + yj} = \bar{x} - yj$  et, forts de cette astuce, on pose

$$\mathbb{O} = \mathbb{H} \oplus \mathbb{H}\ell \quad \text{avec} \quad \ell^2 = -1 \quad \text{et} \dots$$

...et quoi comme produit ? Et bien, si on se lève de bonne heure, on voit que, pour tous  $u, v, x, y \in \mathbb{H}$ ,

$$(x + y\ell)(u + v\ell) = (xu - \bar{v}y) + (vx + y\bar{u})\ell$$

donne lieu à une structure d'algèbre digne d'intérêt avec elle aussi sa conjugaison :  $\overline{x + y\ell} = \bar{x} - y\ell$  pour tout  $x, y \in \mathbb{H}$ . Cette sympathique algèbre a en effet le bon goût d'être alternative à gauche et à droite mais de ne pas être ni associative ni commutative. Elle est d'une certaine importance car c'est ce qu'on appelle une algèbre de division (c'est-à-dire une algèbre dans laquelle tout élément non nul possède un inverse, un peu comme un corps mais sans demander l'associativité ou la commutativité). On peut démontrer que les seules  $\mathbb{R}$ -algèbres de division, de dimension finie et alternatives sont  $\mathbb{R}$  (de dimension 1), le corps des complexes  $\mathbb{C}$  (de dimension 2), l'algèbre des quaternions  $\mathbb{H}$  (de dimension 4, non commutative, mais associative néanmoins) et finalement  $\mathbb{O}$  (de dimension 8). Et par conséquent on ne peut pas faire les malins en continuant *ad eternam* ce processus (je vous voyais venir en posant  $\mathbb{E} = \mathbb{O} \oplus \mathbb{O}m$  avec  $m^2 = -1\dots$ )

**Définition 4.**

Une algèbre  $A$  est dite **unitaire** s'il existe  $1_A \in A$  tel que  $1_A a = a 1_A = a$  pour tout  $a \in A$ . Dans ce cas  $1_A$  est appelé **l'élément unité** ou **l'unité** de  $A$ . On remarque sans peine que l'existence d'un élément unité entraîne l'unicité de celui-ci.

Voilà donc quelques définitions qui réconcilient le lecteur avec l'auteur. En effet le lecteur aura compris que, dans le langage pompeux qui a été introduit, l'algèbre  $M_2(\mathbb{Z})$  n'est rien d'autre qu'une  $\mathbb{Z}$ -algèbre associative, unitaire, non commutative. D'autre part, des algèbres non unitaires se rencontrent quotidiennement en les personnes des idéaux de l'anneau  $R$  : tout idéal  $I$  de  $R$  est une  $R$ -algèbre pour la multiplication induite de celle de  $R$ . Cette algèbre est associative et non unitaire (à moins que  $I = R\dots$ ) Une autre structure d'algèbre non unitaire peut être associée à n'importe quel  $R$ -module  $A$  : il suffit de déclarer que tous les produits sont nuls i.e.  $\mu(a \otimes b) = 0$  pour tout  $a, b \in A$ .

**Définition 5.**

Soient  $R$  un anneau commutatif,  $(A; \mu)$  et  $(B; \nu)$  deux  $R$ -algèbres. On dit qu'un homomorphisme de  $R$ -modules  $f : A \rightarrow B$  est un **homomorphisme de  $R$ -algèbres** si pour tous  $c, d \in A$  on a

$$f(\mu(c \otimes d)) = \nu(f(c) \otimes f(d))$$

(ou, si l'on préfère,  $f(cd) = f(c)f(d)$ ). Si de plus  $A$  et  $B$  sont unitaires, avec unités notées respectivement  $1_A$  et  $1_B$ , et si  $f(1_A) = 1_B$ , on dit que  $f$  est un **homomorphisme de  $R$ -algèbres unitaires**.

**Définition 6.**

Soit  $A$  une  $R$ -algèbre et  $a \in A$ . L'homomorphisme de  $R$ -modules  $L_a : A \rightarrow A$  défini par  $L_a(b) = ab$  s'appelle la **multiplication à gauche par  $a$** . De même on définit la multiplication à droite par  $a$  que l'on notera  $R_a$ .

**Remarque:** (Adjonction de l'unité)

Si  $(A; \mu)$  est une  $R$ -algèbre non unitaire il existe une  $R$ -algèbre unitaire  $(\tilde{A}; \tilde{\mu})$  et un homomorphisme de  $R$ -algèbres  $\iota_A : A \rightarrow \tilde{A}$  qui a la propriété universelle suivante :

“Pour toute  $R$ -algèbre unitaire  $B$  et pour tout homomorphisme de  $R$ -algèbres  $f : A \rightarrow B$  il existe un unique homomorphisme de  $R$ -algèbres unitaires  $\tilde{f} : \tilde{A} \rightarrow B$  tel que  $\tilde{f} \circ \iota_A = f$ .”

Autrement dit, on a le diagramme commutatif suivant :

$$\begin{array}{ccc} A & \xrightarrow{\iota_A} & \tilde{A} \\ & \searrow f & \downarrow \tilde{f} \\ & & B \end{array}$$

La construction se fait comme suit. On prend le  $R$ -module  $\tilde{A} = A \oplus R$  et, pour tous  $a, b \in A$  et  $r, s \in R$ , on pose

$$\tilde{\mu}((a, r) \otimes (b, s)) = (\mu(a \otimes b) + sa + rb, rs).$$

On vérifie aisément que l'élément  $(0, 1)$  est l'unité de  $\tilde{A}$ . L'homomorphisme  $\iota_A : A \rightarrow \tilde{A}$  est défini par  $\iota_A(a) = (a, 0)$  pour tout  $a \in A$  et  $\tilde{f} : \tilde{A} \rightarrow B$  par  $\tilde{f}((a, r)) = f(a) + r \cdot 1_B$ , où  $1_B$  est l'unité de  $B$ .

Cette construction est fonctorielle. En effet si  $f : A \rightarrow B$  est un homomorphisme de  $R$ -algèbres (non unitaires) en posant  $\tilde{f}(a, r) = (f(a), r)$ , on obtient un homomorphisme de  $R$ -algèbres unitaires  $\tilde{f} : \tilde{A} \rightarrow \tilde{B}$  qui fait commuter le diagramme suivant

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \iota_A \downarrow & & \downarrow \iota_B \\ \tilde{A} & \xrightarrow{\tilde{f}} & \tilde{B} \end{array}$$

Les propriétés de  $A$  se lisent sur  $\tilde{A}$  de telle sorte que  $A$  est alternative, associative, commutative si et seulement si  $\tilde{A}$  l'est. De même  $f$  est injectif (surjectif) si et seulement si  $\tilde{f}$  l'est, ce qui entraîne que  $A \simeq B$  si et seulement si  $\tilde{A} \simeq \tilde{B}$ .

## 2. Spectres

Dans ce qui va suivre nous rappelons la notion de spectre d'un anneau commutatif sans toutefois faire une théorie complète sur le sujet. Seules quelques notions élémentaires seront traitées ici. Le lecteur assoiffé de connaissance pourra avoir de plus amples renseignements dans [1] par exemple.

**Définition 7.**

Soit  $R$  un anneau commutatif. On appelle **spectre de  $R$**  l'ensemble des idéaux premiers de  $R$ . On le notera  $\text{Spec}(R)$ . L'ensemble des idéaux maximaux de  $R$  est noté  $\text{Max}(R)$  et s'appelle le **spectre maximal de  $R$** .

Soit  $f : R \rightarrow R'$  un homomorphisme d'anneaux, si  $\mathfrak{p}$  est un idéal premier de  $R'$ , l'idéal  $f^{-1}(\mathfrak{p})$  est un idéal premier de  $R$ . En effet en considérant le passage au quotient  $\varphi : R \rightarrow R'/\mathfrak{p}$  on voit que  $\ker \varphi = f^{-1}(\mathfrak{p})$  et donc que  $R/f^{-1}(\mathfrak{p}) \simeq \varphi(R) \subset R'/\mathfrak{p}$ . Il s'en suit immédiatement que  $R/f^{-1}(\mathfrak{p})$  est intègre. On définit alors l'application  $\text{Spec}(f) : \text{Spec}(R') \rightarrow \text{Spec}(R)$  en posant  $\mathfrak{p} \mapsto f^{-1}(\mathfrak{p})$  pour tout  $\mathfrak{p} \in \text{Spec}(R')$ .

Sur  $\text{Spec}(R)$  on peut mettre une topologie, dite **la topologie de Zariski**, de la façon suivante :

Si  $I$  est un idéal de  $R$ , on définit l'ensemble  $V(I) = \{\mathfrak{p} \in \text{Spec}(R) \mid I \subseteq \mathfrak{p}\}$ . Si  $I$  et  $J$  sont deux idéaux quelconques de  $R$ , on a que  $V(I) \cup V(J) = V(IJ)$  et, étant donnée une famille  $\{I_s \mid s \in S\}$  d'idéaux de  $R$ , on remarque que

$$\begin{aligned} \bigcap_{s \in S} V(I_s) &= \bigcap_{s \in S} \{\mathfrak{p} \in \text{Spec}(R) \mid I_s \subseteq \mathfrak{p}\} = \{\mathfrak{p} \in \text{Spec}(R) \mid I_s \subseteq \mathfrak{p}, \forall s \in S\} \\ &= \{\mathfrak{p} \in \text{Spec}(R) \mid \sum_{s \in S} I_s \subseteq \mathfrak{p}\} = V\left(\sum_{s \in S} I_s\right). \end{aligned}$$

On voit alors que  $\{V(I) \mid I \text{ idéal de } R\}$  vérifie les conditions pour les fermés d'une topologie sur  $\text{Spec}(R)$ . Les ouverts de la forme  $\text{Spec}(R) - V(\langle f \rangle)$ , où  $f \in R$ , sont appelés les *ouverts distingués* de  $\text{Spec}(R)$  et sont notés  $D(f)$ .

On vérifie aisément que  $\text{Spec}(f)$  est une application continue lorsqu'on munit  $\text{Spec}(R)$  et  $\text{Spec}(R')$  de leur topologie de Zariski. Le lecteur avisé remarquera que cette construction est fonctorielle, i.e.  $\text{Spec}$  est un foncteur de la catégorie des anneaux commutatifs dans celle des espaces topologiques.

**Proposition 1.**

*Pour tout anneau commutatif  $R$ , l'espace topologique  $\text{Spec}(R)$  est compact.*

**Preuve:** Soit  $\{U_s \mid s \in S\}$  un recouvrement quelconque d'ouverts de  $X = \text{Spec}(R)$ . D'après la définition, pour tout  $s \in S$  il existe un idéal  $I_s$  de  $R$  tel que  $U_s = X - V(I_s)$ , donc

$$X = \bigcup_{s \in S} U_s = \bigcup_{s \in S} X - V(I_s) = X - \bigcap_{s \in S} V(I_s) = X - V\left(\sum_{s \in S} I_s\right).$$

Donc  $V\left(\sum_{s \in S} I_s\right) = \emptyset$  et par suite  $\sum_{s \in S} I_s = R$ . Il existe ainsi  $I_1, \dots, I_n$  tels que  $I_1 + \dots + I_n = R$ , ce qui entraîne que  $\{U_1, \dots, U_n\}$  recouvre  $X$  (où  $U_j = X - V(I_j)$  pour  $j = 1, \dots, n$ ).

**Remarque:**  $D(f_1) \cup \dots \cup D(f_n) = \text{Spec}(R) \iff Rf_1 + \dots + Rf_n = R$ .

En effet,  $Rf_1 + \dots + Rf_n \neq R$  si et seulement s'il existe  $\mathfrak{m} \in \text{Spec}(R)$  tel que  $Rf_1 + \dots + Rf_n \subseteq \mathfrak{m}$  ou autrement dit, si et seulement si  $D(f_1) \cup \dots \cup D(f_n) \neq \text{Spec}(R)$ .

Comme conséquence de ce fait, puisque  $D(f) = D(f^k)$  pour tout  $k \in \mathbb{N}$ , nous avons que

$$Rf_1 + \dots + Rf_n = R \iff \text{Spec}(R) = D(f_1) \cup \dots \cup D(f_n) = D(f_1^k) \cup \dots \cup D(f_n^k) \iff Rf_1^k + \dots + Rf_n^k = R.$$

### 3. Localisation

Ce petit rappel est consacré à la localisation d'un module (et d'une algèbre) sur un anneau commutatif. Il est certes incomplet pour des raisons de place et de bon sens, de sorte que nous nous limiterons aux résultats qui nous seront utiles par la suite. Le lecteur avide de détails pourra se régaler dans [2].

**Définition 8.**

*Soit  $R$  un anneau commutatif et  $S \subseteq R$ . On dit que  $S$  est une partie multiplicative de  $R$  si tout produit fini d'éléments de  $S$  appartient à  $S$ .*

Soit  $M$  un  $R$ -module et  $S$  une partie multiplicative de  $R$ . On introduit sur  $M \times S$  la relation suivante :  $(m, s) \sim (m', s')$  s'il existe  $t \in S$  tel que  $t(s'm - sm') = 0$ . Il est facile de vérifier que cette relation est une relation d'équivalence. On notera alors  $S^{-1}M$  le quotient  $M \times S / \sim$  et  $\frac{m}{s}$  la classe de  $(m, s)$ .

Si  $x = \frac{m}{s}$  et  $y = \frac{n}{t}$  appartiennent à  $S^{-1}M$ , on vérifie que  $z = \frac{tm+sn}{st}$  ne dépend que de  $x$  et  $y$  et l'on pose  $x + y = z$ . Si  $r \in R$ , en posant  $r \cdot x = \frac{rm}{s}$ , on fait de  $(S^{-1}M, +, \cdot)$  un  $R$ -module.

L'application  $\iota_S : M \rightarrow S^{-1}M$  qui à tout élément  $m \in M$  fait correspondre  $\frac{m}{1}$  est alors un homomorphisme de  $R$ -modules.

Si  $(A, \mu)$  est une  $R$ -algèbre, on munit  $S^{-1}A$  d'une structure de  $R$ -algèbre en posant  $(S^{-1}\mu)\left(\frac{a}{s} \otimes \frac{b}{t}\right) = \frac{\mu(a \otimes b)}{st}$  pour tout  $\frac{a}{s}, \frac{b}{t} \in S^{-1}A$ . On voit immédiatement que si  $A$  est alternative, associative, commutative, il en est de même de  $S^{-1}A$  et que si  $e$  est unité de  $A$ , alors  $\frac{e}{1}$  est unité de  $S^{-1}A$ .

De cette façon  $S^{-1}R$  est un anneau commutatif et  $S^{-1}M$  est muni d'une structure de  $S^{-1}R$ -module de manière naturelle, tout comme  $S^{-1}A$  devient une  $S^{-1}R$ -algèbre.

Soient  $S \subseteq T$  deux parties multiplicatives de  $R$ . L'application  $\iota_S^T : S^{-1}M \rightarrow T^{-1}M$  définie par  $\iota_S^T(\frac{m}{s}) = \frac{m}{s} \in T^{-1}M$  est un homomorphisme de  $S^{-1}R$ -modules et s'appelle *l'application canonique de changement de partie multiplicative*.

Afin d'alléger quelque peu les écritures (resalut Yves !), nous écrirons  $\frac{ab}{st}$  au lieu de  $(S^{-1}\mu)(\frac{a}{s} \otimes \frac{b}{t})$ . De même,  $\frac{m}{1}$  sera noté  $m$ .

**Définition 9.**

Si  $\mathfrak{p} \in \text{Spec}(R)$ , on voit que  $S = R - \mathfrak{p}$  est une partie multiplicative de  $R$ . Pour tout  $R$ -module  $M$ , on notera par  $M_{\mathfrak{p}}$  le  $S^{-1}R$ -module  $S^{-1}M$ . C'est ce qu'on appelle le *localisé* de  $M$  en  $\mathfrak{p}$ .

**Définition 10.**

On dit qu'un anneau commutatif  $R$  est *local* s'il ne possède qu'un seul idéal maximal. Si  $R$  est un anneau quelconque, l'anneau  $R_{\mathfrak{p}}$  est un anneau local d'unique idéal maximal  $\mathfrak{p}R_{\mathfrak{p}}$ .

**Notation** Si  $f \in R$ , l'ensemble  $S = \{f^k \mid k \in \mathbb{N} \cup \{0\}\}$  est une partie multiplicative de  $R$  et on désigne par  $M_f$  le module  $S^{-1}M$ .

**Lemme 2.** (oh! comme c'est sympa la localisation...)

Soit  $M$  un  $R$ -module et  $m \in M$ . Alors les conditions suivantes sont équivalentes :

- 1)  $m = 0$ ,
- 2)  $m = 0 \in M_{\mathfrak{p}}$  pour tout  $\mathfrak{p} \in \text{Spec}(R)$ ,
- 3)  $m = 0 \in M_{\mathfrak{m}}$  pour tout  $\mathfrak{m} \in \text{Max}(R)$ .

**Preuve:** 1)  $\Rightarrow$  2)  $\Rightarrow$  3) sont évidentes. Il reste à montrer 3)  $\Rightarrow$  1).

Si  $m = 0 \in M_{\mathfrak{m}}$  pour tout  $\mathfrak{m} \in \text{Max}(R)$ , cela signifie qu'il existe  $s \in R - \mathfrak{m}$  tel que  $sm = 0$ , et donc l'idéal  $\text{Ann}(m) = \{r \in R \mid rm = 0\}$  n'est contenu dans aucun idéal maximal de  $R$ . Par conséquent  $\text{Ann}(m) = R$  et donc  $m = 0$ .

**Lemme 3.** (technique)

Soient  $f_1, \dots, f_n \in R$  tels que  $Rf_1 + \dots + Rf_n = R$  et  $M$  un  $R$ -module. Pour tout  $i = 1, \dots, n$ , soient  $x_i \in M_{f_i}$  tels que  $x_i = x_j \in M_{f_i f_j}$  pour tout  $i, j = 1, \dots, n$ . Alors, il existe  $x \in M$  tel que  $x = x_i \in M_{f_i}$  pour tout  $i = 1, \dots, n$ .

**Preuve:** Sans limiter la généralité, on peut écrire  $x_i = \frac{y_i}{f_i^m}$  où  $y_i \in M$ , de sorte que

$$x_i = \frac{f_j^m y_i}{f_i^m f_j^m} \quad \text{et} \quad x_j = \frac{f_i^m y_j}{f_i^m f_j^m} \in M_{f_i f_j}.$$

Puisque ces deux éléments sont égaux dans  $M_{f_i f_j}$ , il existe  $k_{ij} \in \mathbb{N}$  tel que  $(f_i f_j)^{k_{ij}} (f_j^m y_i - f_i^m y_j) = 0$ . Comme  $Rf_1 + \dots + Rf_n = R$ , par la remarque du rappel sur les spectres, on a aussi  $Rf_1^{m+k} + \dots + Rf_n^{m+k} = R$  où  $k = \sum_{i,j=1}^n k_{ij}$ , donc il existe  $r_1, \dots, r_n \in R$  tels que  $r_1 f_1^{m+k} + \dots + r_n f_n^{m+k} = 1$ .

Posons  $x = r_1 f_1^k y_1 + \dots + r_n f_n^k y_n$ .

Il vient alors pour tout  $i = 1, \dots, n$

$$f_i^{m+k} x = \sum_{\ell=1}^n r_{\ell} f_i^{m+k} f_{\ell}^k y_{\ell} = \sum_{\ell=1}^n r_{\ell} f_i^k f_{\ell}^{m+k} y_{\ell} = f_i^k y_i \underbrace{\sum_{\ell=1}^n r_{\ell} f_{\ell}^{m+k}}_{=1} = f_i^k y_i$$

et donc  $f_i^m x = y_i \in M_{f_i}$ , ce qui donne  $x = \frac{y_i}{f_i^m} = x_i \in M_{f_i}$ .

#### 4. Lemme de Nakayama

Dans ce qui va suivre, nous allons nous remémorer quelques résultats classiques de la théorie des anneaux non nécessairement commutatifs. Dans tout ce paragraphe  $A$  désignera un anneau unitaire et associatif.

**Définition 11.**

Le radical de Jacobson de  $A$  (noté  $\text{Rad}(A)$ ) est, par définition, l'intersection de tous les idéaux maximaux à gauche de  $A$ . On montre alors que  $\text{Rad}(A)$  est un idéal bilatère de  $A$ . On dit que  $A$  est **semi-simple** si  $\text{Rad}(A) = 0$ .

**Remarque:** Si  $r \in \text{Rad}(A)$  alors  $1 + r \in A^*$ . En effet, si  $1 + r \notin A^*$ , il existe un idéal maximal à gauche  $\mathfrak{m}$  tel que  $1 + r \in \mathfrak{m}$ . Mais puisque  $r \in \mathfrak{m}$ , il s'ensuit que  $1 \in \mathfrak{m}$ , ce qui est absurde.

**Lemme 4.** (Nakayama)

Soit  $M$  un  $A$ -module à gauche de type fini. Si  $\text{Rad}(A) \cdot M = M$  alors  $M = 0$ .

**Preuve:** Supposons que  $M \neq 0$ . Soient  $x_1, \dots, x_n$  des éléments qui engendrent  $M$  comme  $A$ -module à gauche avec  $n$  minimal. Vu l'hypothèse  $\text{Rad}(A) \cdot M = M$ , il existe  $r_1, \dots, r_n \in \text{Rad}(A)$  tels que

$$x_n = r_1 x_1 + \dots + r_n x_n.$$

Donc

$$(1 - r_n)x_n = r_1 x_1 + \dots + r_{n-1} x_{n-1}.$$

Puisque  $1 - r_n$  est inversible, ceci implique que  $x_n$  peut être écrit comme combinaison linéaire de  $x_1, \dots, x_{n-1}$ , ce qui contredit la minimalité de  $n$ .

**Corollaire 5.**

Soit  $M$  un  $A$ -module de type fini et  $N$  un sous-module de  $M$ . Si  $M = N + \text{Rad}(A) \cdot M$  alors  $M = N$ .

**Preuve:** Clairement, si  $M = N + \text{Rad}(A) \cdot M$ , alors on a  $M/N = (N + \text{Rad}(A) \cdot M)/N = \text{Rad}(A) \cdot (M/N)$ . Par le lemme de Nakayama, il s'ensuit que  $M/N = 0$ .

**Corollaire 6.**

Soient  $P$  et  $Q$  des  $A$ -modules projectifs de type fini. Soit  $\bar{f} : P/\text{Rad}(A) \cdot P \rightarrow Q/\text{Rad}(A) \cdot Q$  un homomorphisme de  $A/\text{Rad}(A)$ -modules. Alors il existe un homomorphisme de  $A$ -modules  $f : P \rightarrow Q$  qui induit  $\bar{f}$ . De plus, si  $\bar{f}$  est un isomorphisme,  $f$  aussi est un isomorphisme.

**Preuve:** L'existence de l'homomorphisme  $f$  découle du fait que  $P$  est projectif.

Si  $\bar{f}$  est surjectif, on a que  $Q = f(P) + \text{Rad}(A) \cdot Q$  et donc, d'après le corollaire 1,  $Q = f(P)$ , ce qui montre la surjectivité de  $f$ .

Supposons en outre que  $\bar{f}$  soit injective et appelons  $K$  le noyau de  $f$ . On a  $\bar{f}(K/K \cap \text{Rad}(A) \cdot P) = 0$  et donc  $K = K \cap \text{Rad}(A) \cdot P$ . Mais  $Q$  est projectif et  $f$  surjectif, donc  $K$  est facteur direct de  $P$ , ce qui montre que  $K$  est de type fini. Il s'ensuit que  $K = K \cap \text{Rad}(A) \cdot P = \text{Rad}(A) \cdot K$  et, d'après le lemme de Nakayama,  $K = 0$ .

**Définition 12.**

Un anneau  $A$  est dit *artinien à gauche* si toute famille non vide d'idéaux à gauche admet un élément minimal.

**Proposition 7.** (ça c'est de la fioriture, on ne l'utilise pas après)

Soit  $A$  un anneau artinien à gauche. Alors  $\text{Rad}(A)$  est un idéal nilpotent.

**Preuve:** On considère la suite d'idéaux emboîtés  $\text{Rad}(A) \supseteq \text{Rad}(A)^2 \supseteq \dots \supseteq \text{Rad}(A)^n \supseteq \dots$ .

Puisque l'anneau est artinien, il existe  $k \in \mathbb{N}$  tel que  $\text{Rad}(A)^k = \text{Rad}(A)^{k+1}$ . Posons  $I = \text{Rad}(A)$  et considérons  $\mathfrak{F} = \{\mathfrak{a} \subseteq A \mid \mathfrak{a} \text{ idéal à gauche de } A \text{ tel que } I^k \mathfrak{a} \neq 0\}$ .

Ab absurdo supposons  $I^k \neq 0$ . Dans ce cas,  $A \in \mathfrak{F}$  et par conséquent  $\mathfrak{F} \neq \emptyset$ . Puisque  $A$  est artinien à gauche, il existe  $\mathfrak{a} \in \mathfrak{F}$  minimal. Dans ce cas  $\mathfrak{a}$  est monogène, i.e. il existe  $a \in A$  tel que  $Aa = \mathfrak{a}$ .

En effet soit  $a \in \mathfrak{a}$  avec  $I^k a \neq 0$ . De  $I^k Aa = I^k a \neq 0$ , il vient que  $Aa \in \mathfrak{F}$  et, comme  $Aa \subseteq \mathfrak{a}$ , la minimalité de  $\mathfrak{a}$  entraîne  $Aa = \mathfrak{a}$ . En particulier  $\mathfrak{a}$  est de type fini.

D'autre part  $I^k I \mathfrak{a} = I^{k+1} \mathfrak{a} = I^k \mathfrak{a} \neq 0$  montre que  $I \mathfrak{a} \in \mathfrak{F}$ . Mais  $I \mathfrak{a} \subseteq \mathfrak{a}$  et  $\mathfrak{a}$  est minimal, donc  $I \mathfrak{a} = \mathfrak{a}$ . Par le lemme de Nakayama  $\mathfrak{a} = 0$  et donc  $I^k \mathfrak{a} = 0$ , ce qui est absurde.

## 5. Résultats (c'est pas trop tôt...)

Lors du passage d'une  $R$ -algèbre  $A$  à ses localisés  $A_{\mathfrak{p}}$  ou à ses quotients  $A/\mathfrak{p}A$  (pour  $\mathfrak{p} \in \text{Spec}(R)$ ), les propriétés d'associativité, d'unité, de commutativité, etc. se retrouvent aisément sur ces derniers.

L'objet du présent paragraphe est donc de traiter le problème inverse, c'est-à-dire d'essayer d'expliquer comment certaines propriétés (associativité, unité essentiellement) des algèbres se lisent à partir de leurs quotients et de quelle agréable façon se comporte la localisation.

### Proposition 8.

Soit  $A$  une  $R$ -algèbre telle que  $A_{\mathfrak{p}}$  soit alternative (resp. associative, commutative) pour tout  $\mathfrak{p} \in \text{Spec}(R)$ . Alors  $A$  est alternative (resp. associative, commutative).

**Preuve:** Soient  $a, b \in A$ . On sait que  $a(ab) - a^2b = 0 \in A_{\mathfrak{p}}$  pour tout  $\mathfrak{p} \in \text{Spec}(R)$  donc  $a(ab) = a^2b$  dans  $A$  par le lemme 2 du rappel sur la localisation. L'alternativité à droite, l'associativité et la commutativité se démontrent de la même manière.

### Théorème 9.

Soit  $R$  un anneau commutatif et  $A$  une  $R$ -algèbre de type fini. Supposons que pour tout  $\mathfrak{p} \in \text{Spec}(R)$  l'algèbre  $A_{\mathfrak{p}}$  soit unitaire. Alors  $A$  est unitaire.

**Preuve:** Soit  $\mathfrak{p} \in \text{Spec}(R)$ . Par hypothèse il existe une unité  $1(\mathfrak{p}) \in A_{\mathfrak{p}}$ . Cette unité s'écrit  $1(\mathfrak{p}) = \frac{u}{s}$  où  $u \in A$  et  $s \in R - \mathfrak{p}$ . Soient  $a_1, \dots, a_n$  des éléments qui engendrent  $A$  comme  $R$ -module. Puisque l'égalité

$$\frac{u}{s} \cdot \frac{a_i}{1} = \frac{a_i}{1} \in A_{\mathfrak{p}}$$

est vérifiée pour tout  $i = 1, \dots, n$ , on en déduit qu'il existe  $t_1, \dots, t_n \in R - \mathfrak{p}$  tels que  $t_i(sa_i - ua_i) = 0$ . Dès lors, en posant  $f = t_1 \cdots t_n$ , on a que

$$\frac{fu}{fs} \cdot \frac{a}{t} = \frac{a}{t} \in A_{fs}$$

pour tout  $a \in A$  et  $t \in \{fs, (fs)^2, \dots\}$ . Il existe donc  $f_{\mathfrak{p}} \in R - \mathfrak{p}$  et  $1(f_{\mathfrak{p}}) \in A_{f_{\mathfrak{p}}}$  unité de  $A_{f_{\mathfrak{p}}}$ , tels que  $1(f_{\mathfrak{p}}) = 1(\mathfrak{p}) \in A_{\mathfrak{p}}$ . Puisque  $\mathfrak{p} \in D(f_{\mathfrak{p}})$  on a que  $\{D(f_{\mathfrak{p}}) \mid \mathfrak{p} \in \text{Spec}(R)\}$  est un recouvrement de  $\text{Spec}(R)$ .

Par compacité, il existe  $\mathfrak{p}_1, \dots, \mathfrak{p}_n \in \text{Spec}(R)$  tels que  $\text{Spec}(R) = D(f_1) \cup \dots \cup D(f_n)$  où  $f_i = f_{\mathfrak{p}_i}$ . Donc  $Rf_1 + \dots + Rf_n = R$ .

Or, pour tout  $i, j = 1, \dots, n$ , l'égalité  $1(f_i) = 1(f_j)$  est vérifiée dans  $A_{f_i f_j}$ . En effet, via les applications canoniques  $A_{f_i} \rightarrow A_{f_i f_j}$  et  $A_{f_j} \rightarrow A_{f_i f_j}$ , les éléments  $1(f_i)$  et  $1(f_j)$  se localisent en l'unité de l'algèbre  $A_{f_i f_j}$ .

Ainsi, d'après le lemme technique, il existe  $u \in A$  tel que  $u = 1(f_i) \in A_{f_i}$  pour tout  $i = 1, \dots, n$ . En particulier, pour tout  $a \in A$  et pour tout  $i = 1, \dots, n$ , on a  $ua = a \in A_{f_i}$ , ce qui entraîne  $ua = a \in A_{\mathfrak{p}}$  pour tout  $\mathfrak{p} \in \text{Spec}(R)$ . Par conséquent  $ua = a$  dans  $A$  et donc  $u$  est une unité de  $A$ .

**Remarque:** Comme c'est souvent le cas dans les procédés de localisation, le raisonnement ci-dessus (et d'ailleurs celui de la proposition précédente aussi) s'applique dans le cas où l'algèbre  $A_{\mathfrak{m}}$  est unitaire pour tout idéal maximal seulement, de sorte qu'il est équivalent de travailler avec le spectre premier et le spectre maximal. C'est en effet le contenu du lemme 2 du rappel sur la localisation. Nous avons donc le corollaire suivant :

**Corollaire 10.**

Soit  $A$  une  $R$ -algèbre de type fini, les trois conditions suivantes sont équivalentes :

- 1)  $A$  est unitaire (resp. alternative, associative, commutative),
- 2)  $A_{\mathfrak{p}}$  est unitaire (resp. alternative, associative, commutative) pour tout  $\mathfrak{p} \in \text{Spec}(R)$ ,
- 3)  $A_{\mathfrak{m}}$  est unitaire (resp. alternative, associative, commutative) pour tout  $\mathfrak{m} \in \text{Max}(R)$ .

La morale de ce qui vient d'être démontré, c'est que l'étude d'une algèbre par le moyen de ses localisés ne donne lieu à aucune perte d'information. Par contre, comme nous pourrons le voir dans le prochain et dernier paragraphe, la connaissance de certaines propriétés sur les quotients d'une algèbre n'entraîne pas souvent la véracité de celles-ci sur l'algèbre elle-même. Malgré tout on peut énoncer un résultat positif.

**Théorème 11.**

Soit  $A$  une  $R$ -algèbre associative de type fini telle que  $A/\mathfrak{p}A$  soit unitaire pour tout  $\mathfrak{p} \in \text{Spec}(R)$ . Alors  $A$  est aussi unitaire.

**Preuve:** Nous commençons la démonstration dans le cas où l'anneau  $R$  est local. Soit  $\mathfrak{m}$  l'unique idéal maximal de  $R$  et soit  $\bar{e}$  l'unité de  $A/\mathfrak{m}A$ . Prenons  $e \in \bar{e}$  un représentant de  $\bar{e}$ . Soit  $L_e : A \rightarrow A$  la multiplication à gauche par  $e$ . On a le diagramme commutatif suivant :

$$\begin{array}{ccc} A & \xrightarrow{L_e} & A \\ \downarrow & & \downarrow \\ A/\mathfrak{m}A & \xrightarrow[\sim]{L_{\bar{e}}} & A/\mathfrak{m}A \end{array}$$

Puisque  $\bar{e}$  est l'unité de  $A/\mathfrak{m}A$  on en déduit que  $L_{\bar{e}}$  est un isomorphisme (l'identité) et donc, par le corollaire 6,  $L_e$  est aussi un isomorphisme. De même  $R_e$ , la multiplication à droite par  $e$ , est un isomorphisme. Il existe donc  $u \in A$  tel que  $ue = e$  et  $v \in A$  tel que  $ev = e$  (car  $L_e$  et  $R_e$  sont surjectives). Soit  $x \in A$ , il existe  $y \in A$  tel que  $x = ey$  et il existe  $z \in A$  tel que  $x = ze$ , de sorte que

$$ux = u(ey) = (ue)y = ey = x,$$

$$xv = (ze)v = z(ev) = ze = x.$$

De plus  $u = uv = v$ , donc  $A$  est unitaire.

Pour traiter le cas global, il suffit de localiser l'algèbre  $A$  en n'importe quel idéal maximal  $\mathfrak{m}$ . L'algèbre  $A_{\mathfrak{m}}$  est une  $R_{\mathfrak{m}}$ -algèbre associative, de plus on a l'isomorphisme suivant

$$A_{\mathfrak{m}}/\mathfrak{m}A_{\mathfrak{m}} \simeq A/\mathfrak{m}A.$$

Or  $A/\mathfrak{m}A$  est unitaire, donc  $A_{\mathfrak{m}}/\mathfrak{m}A_{\mathfrak{m}}$  l'est aussi et, par ce qui a été fait ci-dessus,  $A_{\mathfrak{m}}$  est unitaire. Ceci étant vrai pour n'importe quel idéal maximal de  $R$ , nous en déduisons, par le corollaire 10, que  $A$  est unitaire.

**Corollaire 12.**

Soit  $A$  une  $R$ -algèbre associative de type fini, les conditions suivantes sont équivalentes :

- 1)  $A$  est unitaire,
- 2)  $A/\mathfrak{p}A$  est unitaire pour tout  $\mathfrak{p} \in \text{Spec}(R)$ ,
- 3)  $A/\mathfrak{m}A$  est unitaire pour tout  $\mathfrak{m} \in \text{Max}(R)$ .

## 6. Cas pathologiques

Pour achever cette petite excursion, nous proposons au lecteur quelques exemples (académiques certes, mais exemples tout de même...) d'algèbres qui montrent l'importante perte d'information lors du passage au quotient.

Nous allons notamment donner un contre-exemple au corollaire 12 en construisant, pour tout anneau non semi-simple  $R$ , une  $R$ -algèbre non unitaire  $A$  et dont le quotient  $A/\mathfrak{m}A$  est unitaire pour tout  $\mathfrak{m} \in \text{Max}(R)$  (cette algèbre sera par conséquent non associative).

Soit donc  $R$  un anneau tel que  $\text{Rad}(R) \neq 0$  et prenons  $\epsilon \in \text{Rad}(R)$  avec  $\epsilon \neq 0$ .

1) Soit  $A = R \times R$ . Nous définissons sur  $A$  la structure de  $R$ -algèbre dont les produits sont donnés sur les éléments de base par

$$\begin{aligned}(1, 0) \cdot (1, 0) &= (1, 0) \\ (1, 0) \cdot (0, 1) &= (\epsilon, 1) \\ (0, 1) \cdot (1, 0) &= (\epsilon, 1) \\ (0, 1) \cdot (0, 1) &= (0, 1).\end{aligned}$$

On voit alors que

$$\begin{aligned}((1, 0) \cdot (0, 1)) \cdot (0, 1) &= (\epsilon, 1) \cdot (0, 1) = ((\epsilon, 0) + (0, 1)) \cdot (0, 1) = \epsilon(1, 0) \cdot (0, 1) + (0, 1) \cdot (0, 1) \\ &= (\epsilon^2, \epsilon) + (0, 1) = (\epsilon^2, \epsilon + 1).\end{aligned}$$

Mais que, d'autre part,

$$(1, 0) \cdot ((0, 1) \cdot (0, 1)) = (1, 0) \cdot (0, 1) = (\epsilon, 1).$$

Il s'ensuit que  $A$  n'est pas alternative et donc pas associative.  
De plus, montrons que  $A$  n'est pas unitaire.

Supposons en effet qu'il existe  $(a, b) \in A$  élément unité de  $A$ .  
Dans ce cas, nous avons

$$(1, 0) = (a, b) \cdot (1, 0) = (a(1, 0) + b(0, 1)) \cdot (1, 0) = a(1, 0)^2 + b(0, 1) \cdot (1, 0) = (a, 0) + (\epsilon b, b)$$

et donc  $a = 1$  et  $b = 0$ , ce qui est absurde car  $(1, 0) \cdot (0, 1) \neq (0, 1)$ .

Par contre, la classe de  $(1, 0)$  modulo  $\mathfrak{m}$  est une unité de  $A/\mathfrak{m}A$  pour tout  $\mathfrak{m} \in \text{Max}(R)$ .

En effet, pour tout  $(a, b) \in A$ , nous avons

$$(1, 0) \cdot (a, b) = a(1, 0)^2 + b(1, 0) \cdot (0, 1) = (a, 0) + b(\epsilon, 1) = (a, 0) + b\epsilon(1, 0) + (0, b) = (a, b) + b\epsilon(1, 0)$$

et clairement  $(a, b) + b\epsilon(1, 0) \equiv (a, b) \pmod{\mathfrak{m}}$  pour tout  $\mathfrak{m} \in \text{Max}(R)$ .

2) Sur le même  $R$ -module  $A = R \times R$  nous pouvons mettre une autre structure de  $R$ -algèbre intéressante.  
Nous la présentons encore une fois en décrivant son effet sur les éléments de la base canonique :

$$\begin{aligned}(1, 0) \cdot (1, 0) &= (1, 1) \\ (1, 0) \cdot (0, 1) &= (0, \epsilon) \\ (0, 1) \cdot (1, 0) &= (\epsilon, 0) \\ (0, 1) \cdot (0, 1) &= (\epsilon, \epsilon).\end{aligned}$$

Cette algèbre n'est clairement pas commutative et de plus

$$\begin{aligned}(1, 0) \cdot (1, 0)^2 &= (1, 0) \cdot (1, 1) = (1, 1) + (0, \epsilon) = (1, 1 + \epsilon) \\ (1, 0)^2 \cdot (1, 0) &= (1, 1) \cdot (1, 0) = (1, 1) + (\epsilon, 0) = (1 + \epsilon, 1).\end{aligned}$$

Il s'ensuit qu'elle n'est pas alternative.

Cependant pour tout  $(a, b), (c, d) \in A$  et pour tout  $\mathfrak{m} \in \text{Max}(R)$  on a  $(a, b) \cdot (c, d) \equiv (ac, ac) \pmod{\mathfrak{m}}$ .  
Donc  $A/\mathfrak{m}A$  est associative et commutative pour tout  $\mathfrak{m} \in \text{Max}(R)$ .

Pour tout renseignement complémentaire, toute objection ou réclamation s'adresser à l'auteur qui se fera un plaisir de vous montrer la suite de son diplôme.

## 7. Références

- [1] David Mumford, *The red book of varieties and schemes*, Springer Verlag, 93-108,
- [2] N. Bourbaki, *Algèbre commutative*, Masson Paris, 74-90, 1985