LEMME DE KRULL VS AXIOME DU CHOIX

GRÉGORY BERHUY

Table des matières

1. Introduction

Le but de document est de démontrer l'équivalence entre l'axiome du choix et l'existence d'idéaux maximaux dans un anneau commutatif non trivial. Cette équivalence est bien connue des mathématiciens s'intéressant à l'axiome du choix, et il en existe plusieurs démonstrations. Nous suivrons celle de Banaschewski [1], qui est élémentaire et utilise des considérations sur les polynômes en une infinité d'indéterminées et sur la localisation d'un anneau. Dans un souci d'exhaustivité, tous les résultats intermédiaires utilisés, bien que connus, seront redémontrés en détails, quitte à rallonger ce document. Le lecteur qui serait déjà familier avec toutes les notions abordées pourra se reporter directement au dernier paragraphe, qui est le cœur de la démonstration de Banaschewski.

2. L'axiome du choix et ses avatars

L'axiome du choix s'énonce en général comme suit : tout produit d'une famille non vide d'ensembles non vides est non vide. En d'autres termes, pour tout ensemble I non vide, et pour toute famille $(E_i)_{i\in I}$ d'ensembles non vides indexée par I, l'ensemble $\prod_{i\in I} E_i$ est non vide.

Date: 23 octobre 2017.

Donner un élément de ce produit revient à se donner une famille $(x_i)_{i\in I}$, où $x_i \in E_i$ pour tout $i \in I$. Autrement dit, pour tout $i \in I$, on doit choisir un élément $x_i \in I$, d'où le nom de cet axiome. Ceci peut paraître très naturel, et on peut bien se demander ce qui pose problème. Effectivement, lorsque I est fini, il n'y en a pas, puisque l'on peut toujours effectuer un nombre fini de choix. Lorsque I est infini dénombrable, on peut déjà trouver cela plus discutable. Quant au cas où I est infini indénombrable, on se demande bien comment effectuer de tels choix (penser à $I = \mathbb{R}$).

L'axiome du choix étant indépendant des autres axiomes de la théorie des ensembles dans laquelle la plupart des mathématiciens travaillent (les axiomes de Zermelo-Fraenkel), on peut décider librement de l'utiliser ou non. Le problème majeur de l'axiome du choix, et qui est une des raisons pour lesquelles certains mathématiciens se refusent de travailler avec, est que l'utilisation de cet axiome pour démontrer l'existence de certains objets mathématiques fournit une démonstration hautement non constructive. Autrement dit, on peut établir que des objets avec certaines propriétés spécifiques existent, mais on est bien incapable d'en exhiber un seul ! Par exemple, l'utilisation de l'axiome du choix permet de démontrer que tout espace vectoriel sur un corps possède au moins une base. Néanmoins, on serait bien en peine de fournir une base explicite de $\mathbb{R}$, considéré comme $\mathbb{Q}$-espace vectoriel. L'axiome du choix a aussi des conséquences plus incongrues, comme le paradoxe de Banach-Tarski, qui dit en substance que l'on peut découper la boule unité de $\mathbb{R}^3$ en un nombre fini de morceaux, puis recoller ces morceaux sans les déformer pour obtenir deux boules unité.

Néanmoins, une écrasante majorité de mathématiciens travaille avec l'axiome du choix, quitte à se confronter aux difficultés précédentes. Pour finir ce petit laïus introductif, signalons que travailler sans axiome du choix n'est pas dénué d'intérêt. Cela permet de penser les choses autrement, et les démonstrations produites sont en fait des algorithmes qui permettent (du moins en théorie) de construire les objets pas à pas.

Avant d'entrer dans le vif du sujet, nous avons besoin de quelques définitions de théorie des ensembles.

Définition 2.1. Soit E un ensemble non vide. Une *partition* de E est une famille non vide $(E_i)_{i\in I}$ de sous-ensembles **non vides** de E, et vérifiant les deux propriétés suivantes :

(i) pour tous $i, j \in I, i \neq j$, on a $E_i \cap E_j = \emptyset$;

(ii) on a $E = \bigcup_{i\in I} E_i$.

On fait maintenant quelques rappels sur les relations d'ordre.

Définition 2.2. Soit E un ensemble, et soit $\ll \leq \gg$ une relation sur E. On dit alors que $\ll \leq \gg$ est une *relation d'ordre* si l'on a les propriétés suivantes :

(1) réflexivité : pour tout $x \in E$, on a $x \leq x$;

(2) antisymétrie : pour tous $x, y \in E$, $(x \leq y \text{ et } y \leq x) \Longrightarrow x = y$;

(3) transitivité : pour tous $x, y, z \in E$, $(x \leq y \text{ et } y \leq z) \Longrightarrow x \leq z$.

On note alors $x < y$ si $x \leq y$ et $x \neq y$.

On dit que la relation d'ordre $\ll \leq \gg$ est *totale*, ou que $(E, \leq)$ est totalement ordonné, si pour tous $x, y \in E$, on a $x \leq y$ ou $y \leq x$.

Exemples 2.3.

(1) Soit E un ensemble. Alors, la relation d'inclusion est une relation d'ordre sur l'ensemble $\mathcal{P}(E)$ des parties de E. Cette relation d'ordre n'est pas totale dès que E possède au moins deux éléments.

(2) La relation d'ordre usuelle sur l'ensemble $\mathbb{N}$ est une relation d'ordre total.

Définition 2.4. Soit $(E, \leq)$ un ensemble ordonné.

On dit que $z \in E$ est *maximal* si pour tout $x \in E$, on a $z \leq x \Longrightarrow x = z$.

Autrement dit, $z \in E$ est maximal s'il n'existe aucun élément $x \in E$ tel que $z < x$.

On dit que $z \in E$ est un *maximum* (ou un *plus grand élément*) si $x \leq z$ pour tout $x \in E$.

Remarques 2.5.

(1) Un maximum, s'il existe, est unique, et c'est aussi le seul élément maximal.

En effet, si $z, z' \in E$ sont deux maximums de E, on a $z' \leq z$ et $z \leq z'$ par définition d'un maximum, et donc $z' = z$, par définition d'une relation d'ordre.

De plus, si $z \in E$ est un maximum, et si $x \in E$ vérifie $z \leq x$, alors puisque $x \leq z$ par définition d'un maximum, on a $x = z$. D'autre part, si $z' \in E$ est maximal, et puisque $z' \leq z$ par définition d'un maximum, on a $z = z'$.

(2) En revanche, un élément maximal n'est pas nécessairement un maximum. Par exemple, soit E l'ensemble des parties strictes de $X = \{0, 1, 2\}$, ordonné par l'inclusion. Alors, toute partie de X à deux éléments est un élément maximal, mais E ne possède pas d'élément maximum, car il n'existe pas de partie stricte de X qui contienne toutes les autres.

(3) Tout ensemble fini totalement ordonné possède un maximum.

Définition 2.6. Soit $(E, \leq)$ un ensemble ordonné, et soit F une partie non vide de E. On dit que $x \in E$ est un *majorant* de F si l'on a

$$y \leq x \quad \text{pour tout } y \in F.$$

On dit que E est *inductif* si tout sous-ensemble de E totalement ordonné admet un majorant.

Nous pouvons maintenant énoncer le résultat qui nous intéresse.

Théorème 2.7. *Les propriétés suivantes sont équivalentes :*

(1) *pour toute famille non vide $(E_i)_{i\in I}$ d'ensembles non vides, l'ensemble $\prod_{i\in I} E_i$ est non vide ;*

(2) *pour toute famille non vide $(E_i)_{i\in I}$ d'ensembles non vides, il existe une fonction*
$$f : I \longrightarrow \bigcup_{i\in I} E_i$$
telle que pour tout $i \in I$, on a $f(i) \in E_i$;

(3) *pour tout ensemble non vide E, et pour toute partition $(E_i)_{i\in I}$ de E, il existe un sous-ensemble X de E tel que pour tout $i \in I$, l'intersection $X \cap E_i$ soit un singleton ;*

(4) *tout ensemble inductif non vide possède un élément maximal (Lemme de Zorn).*

Démonstration. L'équivalence entre (1) et (4) est la plus délicate. C'est la seule boîte noire que nous nous autoriserons, et renvoyons le lecteur à [3], théorème 1.6.20 pour une démonstration. Démontrons les autres équivalences.

(1) $\Longrightarrow$ (2). Soit $(E_i)_{i\in I}$ une famille non vide d'ensembles non vides. Par hypothèse, l'ensemble $\prod_{i\in I} E_i$ est non vide. Soit $(x_i)_{i\in I} \in \prod_{i\in I} E_i$. On définit alors une fonction $f : I \longrightarrow \bigcup_{i\in I} E_i$ en posant

$$f(i) = x_i \quad \text{pour tout } i \in I.$$

(2) $\Longrightarrow$ (1). Soit $(E_i)_{i\in I}$ une famille non vide d'ensembles non vides. Par hypothèse, il existe une fonction

$$f : I \longrightarrow \bigcup_{i\in I} E_i$$

telle que pour tout $i \in I$, on a $f(i) \in E_i$. La famille $(f(i))_{i\in I}$ est alors un élément de $\prod_{i\in I} E_i$, qui est donc non vide.

(1) $\Longrightarrow$ (3). Soit E un ensemble non vide, et soit $(E_i)_{i\in I}$ une partition de E. Par hypothèse, l'ensemble $\prod_{i\in I} E_i$ est non vide. Soit $(x_i)_{i\in I}$ un élément de $\prod_{i\in I} E_i$. Posons alors

$$X = \{x_k \mid k \in I\} \subset E.$$

Soit $i \in I$. Par définition, $x_i \in X \cap E_i$. Si maintenant $y \in X \cap E_i$, il existe $k \in I$ tel que $y = x_k$. Mais alors, $y \in E_i \cap E_k$, ce qui n'est possible que si $i = k$, puisque $(E_i)_{i\in I}$ est une partition de E. Ainsi, $y = x_i$ et on a $X \cap E_i = \{x_i\}$.

(3) $\Longrightarrow$ (1). Soit $(E_i)_{i\in I}$ une famille non vide d'ensembles non vides. Pour tout $i \in I$, posons $F_i = E_i \times \{i\}$, et soit $F = \bigcup_{i\in I} F_i$. Clairement, pour tout $i \in I, F_i$ est non vide, et pour tous $i, j \in I, i \neq j$, on a $F_i \cap F_j = \emptyset$. Ainsi, $(F_i)_{i\in I}$ est une partition de F. Par hypothèse, il existe $Y \subset F$ tel que, pour tout $i \in I$, l'ensemble $Y \cap F_i$ soit un singleton.

Pour tout $i \in I$, soit $(x_i, i) \in F_i$ l'unique élément de $Y \cap F_i$. La famille $(x_i)_{i\in I}$ est alors un élément de $\prod_{i\in I} E_i$, qui est donc non vide. Ceci achève la démonstration. □

3. Le lemme de Krull

Le lemme de Krull concerne l'existence d'idéaux maximaux dans un anneau commutatif non trivial. Rappelons qu'un anneau A est non trivial si $0_A \neq 1_A$. Cela revient à dire qu'il n'est pas réduit à un élément.

Redonnons la définition d'un idéal maximal.

Définition 3.1. Soit A un anneau commutatif. On dit qu'un idéal $\mathfrak{m}$ de A est *maximal* si $\mathfrak{m} \neq A$, et si pour tout idéal $\mathfrak{a}$ de A, on a

$$\mathfrak{m} \subset \mathfrak{a} \subset A \Longrightarrow \mathfrak{a} = \mathfrak{m} \text{ ou } \mathfrak{a} = A.$$

Autrement dit, $\mathfrak{m}$ est maximal si c'est un élément maximal de l'ensemble des idéaux de A qui sont distincts de A.

L'existence d'idéaux maximaux est assurée par le lemme de Krull, dont la démonstration s'appuie sur le lemme de Zorn (donc l'axiome du choix).

Théorème 3.2 (Krull)**.** *Soit A un anneau commutatif.*

Alors, tout idéal $\mathfrak{a} \neq A$ est contenu dans un idéal maximal. En particulier, tout anneau commutatif non trivial possède au moins un idéal maximal (lemme de Krull).

Démonstration. Considérons l'ensemble E défini par

$$E = \{\mathfrak{b} \mid \mathfrak{b} \neq A \text{ idéal de } A, \mathfrak{a} \subset \mathfrak{b}\}.$$

Alors, E est non vide (car il contient $\mathfrak{a}$), partiellement ordonné par l'inclusion. Soit $(I, \leq)$ un ensemble totalement ordonné, et soit $F = (\mathfrak{b}_i)_{i\in I}$ une famille d'éléments de E totalement ordonnée indexée par I. Autrement dit, pour tous $i, j \in I$ tels que $i \leq j$, on a $\mathfrak{b}_i \subset \mathfrak{b}_j$. Posons

$$\mathfrak{b} = \bigcup_{i\in I} \mathfrak{b}_i.$$

Alors, $\mathfrak{a} \subset \mathfrak{b}$. De plus, $\mathfrak{b}$ est un idéal de l'anneau A. En effet, si $x, y \in \mathfrak{b}$, il existe des indices $i, j \in I$ tels que $x \in \mathfrak{b}_i$ et $y \in \mathfrak{b}_j$. Soit $k = \max(i, j)$. On a ainsi $i \leq k$ et $j \leq k$. Puisque F est totalement ordonné, on a alors

$$x \in \mathfrak{b}_i \subset \mathfrak{b}_k \quad \text{et} \quad y \in \mathfrak{b}_j \subset \mathfrak{b}_k.$$

Puisque $\mathfrak{b}_k$ est un idéal, alors pour tout $a \in A$, on a $x + ay \in \mathfrak{b}_k \subset \mathfrak{b}$. Donc $\mathfrak{b}$ est un idéal de A. De plus, on a $\mathfrak{b} \neq A$. Sinon, $\mathfrak{b}$ contiendrait 1. Mais alors, il existerait $i \in I$ tel que $1 \in \mathfrak{b}_i$ et donc on aurait $\mathfrak{b}_i = A$, ce qui contredirait le fait que $\mathfrak{b}_i \in E$. Ainsi $\mathfrak{b} \in E$, et puisque $\mathfrak{b}_i \subset \mathfrak{b}$ pour tout $i \in I$, $\mathfrak{b}$ est un majorant de F. Ainsi, E est inductif, non vide et donc contient un élément maximal $\mathfrak{m}$ par le lemme de Zorn. On a donc $\mathfrak{m} \neq A$ et $\mathfrak{a} \subset \mathfrak{m}$. Montrons que $\mathfrak{m}$ est un idéal maximal. Soit $\mathfrak{b}'$ un idéal de A tel que $\mathfrak{m} \subset \mathfrak{b}' \subset A$. Supposons que $\mathfrak{b}' \neq A$. Alors, on a $\mathfrak{b}' \in E$ et donc $\mathfrak{b}' = \mathfrak{m}$ par maximalité de $\mathfrak{m}$. Ceci achève la démonstration du premier point. Pour montrer le dernier point, il suffit de prendre $\mathfrak{a} = (0)$, qui est distinct de A, car A est non trivial. □

Le point délicat est donc de démontrer que l'existence d'idéaux maximaux dans un anneau commutatif non trivial implique l'axiome du choix. Pour cela, nous aurons besoin de résultats élémentaires sur la localisation d'un anneau.

4. Localisation d'un anneau

Dans ce paragrpahe, nous introduisons brièvement la notion de localisé d'un anneau. Comme nous n'aurons pas besoin de la théorie générale, nous nous bornerons au cas des anneaux intègres. Le lecteur intéressé par le cas général se reportera à [2], chapitre III, par exemple, qui traite du cas plus général des modules sur un anneau commutatif (le cas du localisé d'un anneau étant le cas où le module en question est l'anneau lui-même).

On commence par définir la notion de partie multiplicative.

Définition 4.1. Soit A un anneau. Une partie S de A est dite *multiplicative* si $1_A \in S$, et si pour tous $s, s' \in S$, on a $ss' \in S$.

Donnons quelques exemples. Commençons par rappeler la notion d'idéal premier.

Définition 4.2. Soit A anneau commutatif. Un idéal $\mathfrak{p}$ de A est dit *premier* si $\mathfrak{p} \neq A$, et si pour tous $x, y \in A$, on a

$$xy \in \mathfrak{p} \Longrightarrow x \in \mathfrak{p} \text{ ou } y \in \mathfrak{p}.$$

Cela revient à dire que $A \setminus \mathfrak{p}$ est non vide, et stable par produit.

Rappelons que tout idéal maximal est premier.

Exemples 4.3. Soit A un anneau commutatif.

(1) Soit $\mathfrak{p}$ un idéal de A. Notons que $A = \mathfrak{p}$ si, et seulement si $1_A \in \mathfrak{p}$. Ainsi, un idéal $\mathfrak{p}$ est premier si, et seulement si, $A \setminus \mathfrak{p}$ est multiplicative.

(2) Soit $(S_i)_{i\in I}$ une famille non vide de parties multiplicatives de A. Alors, $S = \bigcap_{i\in I} S_i$ est une partie multiplicative de A.

En effet, puisque $1 \in S_i$ pour tout $i \in I$, on a $1 \in S$. Si maintenant $s, s' \in S$, alors pour tout $i \in I$, on a $s, s' \in S_i$, et par conséquent $ss' \in S_i$, puisque S_i est multiplicative. Ainsi, $ss' \in S$.

(3) Soit A un anneau, et soit $(\mathfrak{p}_i)_{i\in I}$ une famille non vide d'idéaux premiers de A. Alors, $S = A \setminus \bigcup_{i\in I} \mathfrak{p}_i$ est multiplicative.

En effet, de manière équivalente, on a $S = \bigcap_{i\in I}(A \setminus \mathfrak{p}_i)$, et le résultat découle des deux points précédents.

Si A est un anneau intègre, on rappelle que l'on définit son corps des fractions K_A, de la même manière que l'on construit A à partir de $\mathbb{Z}$. On définit une relation $\sim$ sur $A \times (A \setminus \{0_A\})$ comme suit : on dit que $(a, b) \sim (c, d)$ si $ad - bc = 0_A$.

On vérifie aisément que c'est une relation d'équivalence. On définit K_A comme étant l'ensemble quotient correspondant, et on note $\frac{a}{b}$ la classe d'équivalence de $(a, b) \in A \times (A \setminus \{0_A\})$. On définit une loi d'addition et une loi de multiplication comme dans le cas du corps des rationnels : pour tous $\frac{a}{b}, \frac{c}{d} \in K_A$, on pose

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{cd} \quad \text{et} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ab}{cd}.$$

Comme pour le cas de A, on vérifie que ces deux lois sont bien définies (il faut en effet démontrer que le résultat ne dépend pas du choix des représentants des classes d'équivalence), et confère à K_A une structure de corps, de neutres $\frac{0_A}{1_A}$ et $\frac{1_A}{1_A}$.

On peut maintenant définir le localisé d'un anneau intègre par rapport à une partie multiplicative.

Définition 4.4. Soit A un anneau intègre, et soit S une partie multiplicative de A. L'ensemble

$$S^{-1}A = \{\frac{a}{s} \mid a \in A, s \in S\}$$

est un sous-anneau de K_A, appelé *le localisé de A en S.*

Notons que le fait que $S^{-1}A$ soit un sous-anneau de A découle du fait que S est multiplicative.

Remarquons que l'application

$$\begin{aligned} \iota_S \colon A &\longrightarrow S^{-1}A \\ a &\longmapsto \frac{a}{1} \end{aligned}$$

est un morphisme d'anneaux injectif.

De plus, $S^{-1}A$ est trivial si, et seulement si, $0_A \in S$. En effet, si $0_A \in S$, pour tout $a \in A$ et tout $s \in S$, on a $a0_A - s0_A = 0_A$, et donc $\dfrac{a}{s} = \dfrac{0_A}{0_A}$. Inversement, si $S^{-1}A$ est trivial, alors $\dfrac{1_A}{1_A} = \dfrac{0_A}{1_A}$, et donc $0_A = 1_A \in S$.

On a alors le lemme suivant.

Lemme 4.5. *Soit A un anneau intègre, et soit S une partie multiplicative de A ne contenant pas 0_A. Soit $\mathfrak{M}$ un idéal maximal de $S^{-1}A$. Alors l'idéal $\mathfrak{m} = \iota_S^{-1}(\mathfrak{M})$ est maximal parmi les idéaux de A n'intersectant pas S.*

De plus, $\mathfrak{m}$ est un idéal premier.

Démonstration. Soit $\mathfrak{a}$ un idéal de A n'intersectant pas S, et contenant $\mathfrak{m}$. Posons

$$\mathfrak{M}' = (\iota_S(\mathfrak{m})) \text{ et } \mathfrak{A} = (\iota_S(\mathfrak{a})).$$

Alors, on a $\mathfrak{M}' \subset \mathfrak{A}$.

On a aisément les égalités

$$\mathfrak{M}' = \{\frac{x}{s} \mid x \in \mathfrak{m}, s \in S\} \text{ et } \mathfrak{A} = \{\frac{a}{s} \mid a \in \mathfrak{a}, s \in S\}.$$

Montrons tout d'abord que $\mathfrak{M}' = \mathfrak{M}$. Si $x \in \mathfrak{m}$, alors $\dfrac{x}{1_A} \in \mathfrak{M}$ par définition. Mais alors, pour tout $s \in S$, on a

$$\frac{x}{s} = \frac{1_A}{s} \cdot \frac{x}{1_A} \in \mathfrak{M}.$$

Par conséquent, $\mathfrak{M}' \subset \mathfrak{M}$. Inversement, si $\frac{x}{s} \in \mathfrak{M}$, alors

$$\frac{s}{1_A} \cdot \frac{x}{s} = \frac{x}{1_A} \in \mathfrak{M}.$$

Cela revient à dire que $x \in \mathfrak{m}$, et donc $\mathfrak{M} \subset \mathfrak{M}'$.

On obtient donc que $\mathfrak{M} \subset \mathfrak{A}$. Par maximalité, on a $\mathfrak{A} = \mathfrak{M}$ ou $\mathfrak{A} = S^{-1}A$. Si on avait $\mathfrak{A} = S^{-1}A$, on aurait $\frac{1_A}{1_A} = \frac{a}{s}$, avec $a \in \mathfrak{a}$ et $s \in S$. Mais alors, on aurait $a = s \in \mathfrak{a} \cap S$, ce qui est impossible par choix de $\mathfrak{a}$.

Par conséquent, $\mathfrak{A} = \mathfrak{M}$. Soit $a \in \mathfrak{a}$. Alors, on a $\frac{a}{1_A} \in \mathfrak{A} = \mathfrak{M} = \mathfrak{M}'$. Il existe ainsi $x \in \mathfrak{m}$ et $s \in S$ tels que

$$\frac{a}{1_A} = \frac{x}{s}.$$

On a alors $as = x \in \mathfrak{m}$. Mais alors, $\frac{as}{1_A} \in \mathfrak{M}$, et par suite, on obtient $\frac{a}{1_A} \in \mathfrak{M}$ en multipliant par $\frac{1_A}{s}$. Autrement dit, $a \in \mathfrak{m}$. On obtient finalement $\mathfrak{a} = \mathfrak{m}$, d'où le résultat souhaité.

Il reste à démontrer que $\mathfrak{m}$ est un idéal premier. On a $\mathfrak{m} \neq A$, car sinon on aurait $1_A \in \mathfrak{m} \cap S$. Soient $x, y \in A$ tels que $xy \in \mathfrak{m}$. Alors, on a

$$\frac{x}{1_A}\frac{y}{1_A} = \frac{xy}{1_A} \in \mathfrak{M}.$$

Puisque $\mathfrak{M}$ est maximal, il est premier, et donc on a $\frac{x}{1_A} \in \mathfrak{M}$ ou $\frac{y}{1_A} \in \mathfrak{M}$, soit encore $x \in \mathfrak{m}$ ou $y \in \mathfrak{m}$. Par conséquent, $\mathfrak{m}$ est un idéal premier. □

Remarque 4.6. On peut en fait démontrer que l'ensemble des idéaux maximaux de $S^{-1}A$ est en bijection avec l'ensemble des idéaux de A, maximaux parmi ceux qui n'intersectent pas S. Le lecteur intéressé se reportera à [2, Chapitre III, Proposition 1.13] pour une démonstration.

5. Anneaux de polynômes

Soit A un anneau commutatif, et soit E un ensemble non vide. Pour tout $e \in E$, on considère une indéterminée X_e. Pour toute famille d'entiers naturels $\alpha = (\alpha_e)_{e \in E} \in \mathbb{N}^{(E)}$ presque tous nuls, on pose

$$X^\alpha = \prod_{e \in E} X_e^{\alpha_e}.$$

On note $A[E]$ l'anneau des polynômes à coefficients dans A en les indéterminées $X_e, e \in E$. Tout élément $P \in A[E]$ s'écrit donc de

manière unique

$$P = \sum_{\alpha} a_\alpha X^\alpha,$$

où les éléments $a_\alpha \in A$ sont presque tous nuls et où α parcourt $\mathbb{N}^{(E)}$.

Définition 5.1. Un *monôme* est un élément de $A[E]$ de la forme X^α, avec $\alpha \in \mathbb{N}^{(E)}$.

Soit $P = \sum_{\alpha} a_\alpha X^\alpha \in A[E]$. Le *support* de P est l'ensemble

$$\mathrm{Supp}(P) = \{\alpha \in \mathbb{N}^{(E)} \mid a_\alpha \neq 0\}.$$

Un *monôme de P* est un monôme X^α tel que $\alpha \in \mathrm{Supp}(P)$. Autrement dit, les monômes de P sont exactement ceux qui apparaissent avec un coefficient non nul dans l'écriture de P.

Si 0 désigne la suite nulle, le coefficient $a_0 \in A$ est appelé *le terme constant* de P.

Exemple 5.2. Si $E = \mathbb{N}$, et si $P = -1 + X_1X_2 + 3X_1^2X_3X_5^3$, les monômes de P sont

$$1, X_1X_2, X_1^2X_3X_5^3,$$

et son terme constant est -1.

Remarques 5.3.

(1) On trouve dans la littérature une autre définition de la notion de monôme, à savoir un élément de la forme aX^α, avec $a \in A \setminus \{0\}$. Néanmoins, nous avons choisi de suivre la terminologie de [1], plus adaptée à ce que nous voulons faire ici.

(2) Si $P, Q \in A[X]$, on a

$$\mathrm{Supp}(P+Q) \subset \mathrm{Supp}(P) \cup \mathrm{Supp}(Q).$$

En effet, écrivons $P = \sum_{\alpha} a_\alpha X^\alpha$ et $Q = \sum_{\alpha} b_\alpha X^\alpha$. On a donc

$$P + Q = \sum_{\alpha} (a_\alpha + \beta_\alpha) X^\alpha;$$

Si $\alpha \in \mathbb{N}^{(E)}$ vérifie $a_\alpha = b_\alpha = 0_A$, alors $a_\alpha + b_\alpha = 0_A$. Autrement dit,

$$\mathrm{Supp}(P)^c \cap \mathrm{Supp}(Q)^c \subset \mathrm{Supp}(P+Q)^c,$$

d'où le résultat par passage au complémentaire.

En particulier, l'ensemble des monômes de $P+Q$ est contenu dans la réunion de l'ensemble des monômes de P et de l'ensemble des monômes de Q.

Le lemme suivant nous sera utile dans la suite.

Lemme 5.4. *Soit E' un ensemble non vide. Alors :*

(1) *Si P est dans l'idéal engendré par les $X_e, e \in E'$, alors tout monôme de P est un multiple d'une indéterminée $X_e, e \in E'$ (dépendant du monôme) ;*

(2) *si A est un anneau intègre, alors l'idéal engendré par les $X_e, e \in E'$, est un idéal premier de $A[E']$;*

(3) *si A est un anneau intègre infini, alors pour tous polynômes $P, Q \in A[E']$ non nuls, il existe $a \in A$ tel que l'ensemble des monômes de $P + aQ$ soit la réunion de l'ensemble des monômes de P et de l'ensemble des monômes de Q.*

Démonstration.

(1) Si $R \in A[X]$ et $e \in E'$, alors tout monôme de RX_e est par définition un multiple de X_e. Comme l'ensemble des monômes d'une somme finie de polynômes est contenue dans la réunion de l'ensemble des monômes de chaque terme de la somme, le résultat en découle.

(2) Remarquons que

$$(X_e, e \in E') = \{P \in A[E'] \mid P(0) = 0_A\}.$$

En effet, si $P \in (X_e, e \in E')$, alors $P(0) = 0_A$, et réciproquement, si $P(0) = 0_A$, chaque monôme de P est multiple d'au moins une indéterminée $X_e, e \in E'$.

Remarquons alors que $1_A \notin (X_e, e \in E')$, et donc que $(X_e, e \in E') \neq A[E']$. D'autre part, on vérifie sans peine que pour tous $P, Q \in A[E']$, on a

$$(PQ)(0) = P(0)Q(0).$$

Ainsi, si A est intègre et si $(PQ)(0) = 0_A$, alors $P(0) = 0_A$ ou $Q(0) = 0_A$. Par conséquent, $(X_e, e \in E')$ est un idéal premier.

(3) Écrivons $P = \sum_\alpha a_\alpha X^\alpha$ et $Q = \sum_\alpha b_\alpha X^\alpha$.

Pour tout $\alpha \in \mathrm{Supp}(Q)$, il existe au plus un élément $a \in A$ tel que $a_\alpha + ab_\alpha = 0_A$. En effet, si $a, a' \in A$ vérifient

$$a_\alpha + ab_\alpha = a_\alpha + a'b_\alpha = 0_A,$$

alors $ab_\alpha = a'b_\alpha$. Puisque $\alpha \in \mathrm{Supp}(Q)$, on a $b_\alpha \neq 0_A$, et par intégrité de A, on obtient $a = a'$.

En particulier, l'ensemble $A' = \bigcup_{\alpha \in \mathrm{Supp}(Q)} \{a \in A \mid a_\alpha + ab_\alpha = 0_A\}$ est fini. Puisque A est infini, on peut choisir un élément $a \in A \setminus A'$. Établir le point (3) revient à démontrer l'égalité

$$\mathrm{Supp}(P + aQ) \subset \mathrm{Supp}(P) \cup \mathrm{Supp}(Q).$$

Or, on a

$$P + aQ = \sum_{\alpha} (a_\alpha + ab_\alpha) X^\alpha.$$

Il suffit de vérifier que

$$\mathrm{Supp}(P) \cup \mathrm{Supp}(Q) \subset \mathrm{Supp}(P + aQ),$$

l'autre inclusion étant évidente. Soit $\alpha \in \mathrm{Supp}(P) \cup \mathrm{Supp}(Q)$. Si $\alpha \notin \mathrm{Supp}(Q)$, alors $a_\alpha + ab_\alpha = a_\alpha \neq 0$, puisque $\alpha \in \mathrm{Supp}(Q)$, et si $\alpha \in \mathrm{Supp}(Q)$, alors on a $a_\alpha + ab_\alpha \neq 0$, puisque $a \notin A'$. Ainsi, $\alpha \in \mathrm{Supp}(P + aQ)$ dans tous les cas. Ceci achève la démonstration. □

Corollaire 5.5. *Soit E un ensemble non vide. Alors :*

(1) *Pour toute partie S de E, si P est dans l'idéal de $\mathbb{Q}[E]$ engendré par les $X_s, s \in S$, alors tout monôme de P est un multiple d'une indéterminée X_s, avec $s \in S$ (dépendant du monôme) ;*

(2) *Pour toute partie S de E, l'idéal de $\mathbb{Q}[E]$ engendré par les $X_s, s \in S$, est un idéal premier de $\mathbb{Q}[E]$;*

(3) *pour tous polynômes $P, Q \in \mathbb{Q}[E]$ non nuls, il existe $a \in \mathbb{Q}$ tel que l'ensemble des monômes de $P + aQ$ soit la réunion de l'ensemble des monômes de P et de l'ensemble des monômes de Q.*

Démonstration. Le point (3) découle du lemme précédent, appliqué à $A = \mathbb{Q}$ et $E' = E$. Pour les points (1) et (2), on applique ce même lemme à $A = \mathbb{Q}[S^c]$ et $E' = S$, en remarquant que $\mathbb{Q}[E] = (\mathbb{Q}[S^c])[S]$. □

6. Le lemme de Krull implique l'axiome du choix

Nous en arrivons au cœur de ce document, à savoir la démonstration du fait que le lemme de Krull implique l'axiome du choix. Nous utiliserons la version de l'axiome du choix donnée par le point (3) du théorème 2.7.

On se donne une fois pour toutes un ensemble non vide E, et une partition $(E_i)_{i \in I}$ de E fixée. On peut alors introduire la notion d'éventail de E (relatif à cette partition).

Définition 6.1. Un *éventail* de E est une partie S de E tel que l'on ait

$$|S \cap E_i| \leq 1 \quad \text{pour tout } i \in I.$$

Évidemment, notre but est de démontrer l'existence d'un éventail S tel que $|S \cap E_i| = 1$ pour tout $i \in I$, à partir du lemme de Krull.

Commençons par un lemme.

Lemme 6.2. *Soit S une partie de E. Alors :*

(1) *Si S est un éventail de E, tout sous-ensemble de S est un éventail de E ;*

(2) *l'ensemble S est un éventail de E si, et seulement si, tout partie de S à deux éléments est un éventail de E.*

Démonstration.

(1) Soit S un éventail de E, et soit $S' \subset S$. Alors, pour tout $i \in I$, on a

$$|S' \cap E_i| \leq |S \cap E_i| \leq 1,$$

et S' est donc un éventail de E.

(2) Si S est un éventail de E, toute partie de S à deux éléments est un éventail de E d'après (1). Inversement, soit S une partie de E telle que toute partie de S à deux éléments soit un éventail de E. Supposons qu'il existe $i_0 \in I$ tel que $|S \cap E_{i_0}| \geq 2$, et soient x, y deux éléments de $S \cap E_{i_0}$ distincts. Par hypothèse, $\{x, y\}$ est un éventail de E, et en particulier, on a $|\{x, y\} \cap E_{i_0}| \leq 1$. Ceci est impossible, puisque x et y sont deux éléments distincts de E_{i_0}. Ainsi, pour tout $i \in I$, on a bien

$$|S \cap E_i| \leq 1,$$

et S est un éventail de E. □

On peut maintenant démontrer le théorème suivant.

Théorème 6.3. *L'axiome du choix et le lemme de Krull sont équivalents.*

Démonstration. Le fait que l'axiome du choix implique le lemme de Krull ayant déjà été établi dans le théorème 3.2, il reste donc à démontrer l'autre implication.

On se fixe un ensemble E non vide, et $(E_i)_{i \in I}$ une partition de E. On note $\mathfrak{S}$ l'ensemble des éventails de E. On se place dans l'anneau $\mathbb{Q}[E]$, et on pose

$$T = \bigcup_{S \in \mathfrak{S}} (X_s, s \in S) \quad \text{et} \quad U = T^c.$$

Remarquons que T est une réunion d'idéaux premiers de $\mathbb{Q}[E]$ par le corollaire 5.5 (2). Par conséquent, U est une partie multiplicative de $\mathbb{Q}[E]$ d'après l'exemple 4.3 (3).

On peut donc considérer l'anneau localisé $A = U^{-1}\mathbb{Q}[E]$. Puisque T contient 0, U ne contient pas 0, et l'anneau A est donc non trivial. Par hypothèse, A possède un idéal maximal, ce qui implique qu'il existe un idéal $\mathfrak{m}$ de $\mathbb{Q}[E]$ qui est maximal parmi les idéaux de $\mathbb{Q}[E]$ n'intersectant pas U, d'après le lemme 4.5. Ceci revient à dire que $\mathfrak{m}$ est maximal parmi les idéaux de $\mathbb{Q}[E]$ contenus dans T. Cet idéal $\mathfrak{m}$ est un idéal premier de $\mathbb{Q}[E]$, d'après ce même lemme.

Notons que $\mathfrak{m}$ est non nul, puisqu'il contient toutes les indéterminées $X_e, e \in E$, par exemple.

On pose maintenant

$$S_0 = \{s \in E \mid X_s \in \mathfrak{m}\}.$$

Nous allons démontrer successivement les points suivants :

(i) $(X_s, s \in S_0) = \mathfrak{m}$.

(ii) l'ensemble S_0 est un éventail.

(iii) pour tout $i \in I$, $S_0 \cap E_i$ est un singleton.

Bien entendu, le point (iii) établira la conclusion voulue.

On commence par démontrer (i). Par définition, pour tout $s \in S_0$, on a $X_s \in \mathfrak{m}$, et par conséquent, on a $(X_s, s \in S_0) \subset \mathfrak{m}$. Inversement, soit $P \in \mathfrak{m}$ non nul, et soit X^α un monôme de P. Soit $Q \in \mathfrak{m}$. D'après le corollaire 5.5 (3), il existe $a \in \mathbb{Q}$ tel que l'ensemble des monômes de $P+aQ$ soit la réunion de l'ensemble des monômes de P et de l'ensemble des monômes de Q. Puisque $\mathfrak{m}$ est un idéal, on a $R = P + aQ \in \mathfrak{m}$. En particulier, il existe un éventail S de E tel que $R \in (X_s, s \in S)$. Par le corollaire 5.5, tout monôme de R est multiple d'un X_s, avec $s \in E$ (dépendant du monôme). En particulier, tout monôme de R est dans $(X_s, s \in S)$. Par choix de a, ceci implique que tous les monômes de P et tous les monômes de Q sont dans $(X_s, s \in S)$. Puisque tous les monômes de Q sont dans l'idéal $(X_s, s \in S)$, on en déduit que $Q \in (X_s, s \in S)$. Puisque X^α est un monôme de P, on a $X^\alpha \in (X_s, s \in S)$. Par suite, $Q + VX^\alpha \in (X_s, s \in S)$ pour tout $V \in \mathbb{Q}[E]$. Autrement dit, on a

$$\mathfrak{m} + X^\alpha \mathbb{Q}[E] \subset (X_s, s \in S) \subset T.$$

Par maximalité de $\mathfrak{m}$ pour cette propriété, on en déduit l'égalité

$$\mathfrak{m} + X^\alpha \mathbb{Q}[E] = \mathfrak{m}.$$

Mais alors, $X^\alpha \in \mathfrak{m}$. Comme $\mathfrak{m}$ est un idéal premier, au moins une des indéterminées apparaissant dans X^α avec une puissance non triviale, disons X_{s_0}, est dans $\mathfrak{m}$. Par conséquent, $s_0 \in S_0$, et puisqueX^α est un multiple de X_{s_0}, on a $X^\alpha \in (X_s, s \in S_0)$. Comme c'est vrai pour tout monôme de P, on a $P \in (X_s, s \in S_0)$, ce qu'il fallait démontrer.

Passons au point (ii). D'après le lemme 6.2 (2), il suffit de démontrer que toute partie de S_0 à deux éléments est un éventail. Soient $e, f \in S_0$ deux éléments distincts. Alors, $X_e, X_f \in \mathfrak{m}$, et ainsi $X_e + X_f \in \mathfrak{m}$. Par conséquent, il existe un éventail S de E tel que $X_e + X_f \in (X_s, s \in S)$. Puisque X_e est un monôme de $X_e + X_f$ (car e et f sont distincts), il existe $P \in \mathbb{Q}[E]$ et $s \in S$ tel que $X_e = PX_s$, d'après le corollaire 5.5 (1). Par unicité de l'écriture (en explicitant les termes de P), on obtient que $P = 1$ et $e = s \in S$. De même, on montre que $y \in S$. Comme S est un éventail de E, $\{x, y\}$ est aussi un éventail de E d'après le lemme 6.2 (1), par exemple, d'où le résultat souhaité.

Il reste à établir le point (iii). Supposons qu'il existe $i_0 \in I$ tel que $|S_0 \cap E_{i_0}| = 0$. Autrement dit, $S_0 \cap E_{i_0}$ est vide. Choisissons $e_0 \in E_{i_0}$ (c'est possible car E_{i_0} est non vide), et posons $S = S_0 \cup \{e_0\}$. Alors, S est un éventail de E. En effet, soit $i \in I$. Si $i \neq i_0$, alors $E_i \cap E_{i_0} = \emptyset$, On a donc $e_0 \notin E_i$ et $S \cap E_i = S_0 \cap E_i$, d'où

$$|S \cap E_i| \leq 1,$$

puisque S_0 est un éventail. Enfin, on a

$$S \cap E_{i_0} = (S_0 \cap E_{i_0}) \cup (\{e_0\} \cap E_{i_0}) = \{e_0\},$$

et donc $|S \cap E_{i_0}| = 1$.

Par conséquent, S est bien un éventail de E. Remarquons maintenant que

$$\mathfrak{m} \subsetneq (X_s, s \in S) \subset T.$$

En effet, si on avait égalité, on aurait $X_{e_0} \in \mathfrak{m}$, et donc

$$X_{e_0} \in (X_s, s \in S_0)$$

d'après (i). Par le même argument que précédemment, on aurait $e_0 \in S_0$, d'où une contradiction. Mais alors, cela contredit la maximalité de $\mathfrak{m}$ pour la propriété d'être contenu dans T. On a donc bien $|S_0 \cap E_i| = 1$ pour tout $i \in I$, d'où (iii). Ceci achève la démonstration du théorème. □

Références

[1] B. Banaschewski, *A new proof of « Krull implies Zorn »*. Math. Log. Quat. **40** (1994) 478–480

[2] G. Berhuy, *Modules : théorie, pratique...et un peu d'arithmétique.* Mathématiques en devenir **109**, Calvage & Mounet, 2012.

[3] L. Schwartz, *Analyse I.* Coll. Enseignement des sciences, **42**. Hermann, Paris, 1995.