Arithmétique dans un espace vectoriel de dimension fini

Nino Emery

28 Mars 2020

Ceci est une ébauche de recherche, je n'en ai trouvé jusqu'à présent aucune utilité concrète, et relève plus de l'amusement que de l'intérêt. Si un lecteur y trouve une application, envoyez moi un mél, je serai ravi d'en discuter !

1 Introduction

En tant que grand fan d'algèbre linéaire et de la théorie des nombres, je me suis demandé un jour si je pouvais résoudre des problèmes dans des espaces vectoriels en passant par de l'arithmétique. Il fallait alors définir ce qu'était l'arithmétique dans un espace vectoriel, et particulièrement y définir une loi multiplicative (du type euclidienne). Après plusieurs jours de réflexions et d'imagination, je suis arrivé à un résultat que je vais ici décrire.

Notations :

-E est un $\mathbb{K}$-espace vectoriel de dimension n_E.
-$\mathbb{R}^n$ est le $\mathbb{K}$-espace vectoriel usuel et on rappelle $\dim_{\mathbb{K}}(\mathbb{R}^n) = n$
-$\mathbb{R}_{n-1}[X]$ est l'ensemble des polynômes de degré au plus $n-1$. On rappelle $\dim_{\mathbb{K}}(\mathbb{R}_{n-1}[X]) = n$
-$\mathcal{B}$ est la base canonique de $\mathbb{R}^n$
-$\mathcal{C}$ est la base canonique de $\mathbb{R}_{n-1}[X]$
-Φ_i est la forme linéaire telle que $\Phi_i(\vec{x}) = a_i$ avec $\vec{x} = \sum_{j=0}^{n-1} a_j \cdot \vec{e_j}$
-$\mathbb{R}^{\mathbb{N}^*}$ l'ensemble des suites presque nulles
-On notera $A \precsim B$ lorsqu'il existe un plongement f de A dans B. On rappelle qu'un plongement est une application de A dans B telle que $\tilde{f} : A \to f(A)$ soit un homéomorphisme.
-On note π_i la projection sur $< e_1, \cdots, e_i >$

2 Première définition dans $\mathbb{R}^n$

2.1 Lien entre $\mathbb{R}^n$ et $\mathbb{R}_{n-1}[X]$

On se place donc dans $\mathbb{R}^n$ de dimension n. On a $\dim_{\mathbb{K}}(\mathbb{R}_{n-1}[X]) = n$: les deux espaces sont de même dimension, ils sont donc **isomorphes**.
On peu donc définir :

$$\begin{array}{rccc} \varphi_n & : & \mathbb{R}^n & \to & \mathbb{R}_{n-1}[X] \\ & & (a_0, \cdots, a_{n-1}) & \mapsto & \displaystyle\sum_{k=0}^{n-1} a_k \cdot X^k \end{array} \quad \text{isomorphisme d'espace vectoriel}$$

On remarque au passage que $\varphi(\mathcal{B}) = \mathcal{C}$
φ est bijective, elle est donc inversible d'inverse φ^{-1}

On va désormais créer l'anneau $(\mathbb{R}^{\mathbb{N}^*}, +, \times)$ et en particulier y définir la loi $\times$ grâce à φ et l'anneau $(\mathbb{R}[X], +, *)$:

$$\begin{array}{rccc} \times & : & (\mathbb{R}^{\mathbb{N}^*})^2 & \to & \mathbb{R}^{\mathbb{N}^*} \\ & & (a, b) & \mapsto & \varphi^{-1}\left(\varphi(a) * \varphi(b)\right) \end{array}$$

Proposition 1 $(\mathbb{R}^{\mathbb{N}^*}, +, \times)$ est un anneau

Démonstration Soit $(\vec{x}, \vec{y}) \in (\mathbb{R}^{\mathbb{N}^*})^2$. On a par définition de φ :
$(\varphi(\vec{x}), \varphi(\vec{y})) \in \mathbb{R}_{n-1}[X]^2$.
Par stabilité de $*$ dans $(\mathbb{R}[X], +, *)$, $\varphi(\vec{x}) * \varphi(\vec{y}) \in \mathbb{R}[X]$.
Donc $\varphi^{-1}(\varphi(\vec{x}) * \varphi(\vec{y})) \in \mathbb{R}^{\mathbb{N}^*}$, donc $\vec{x} \times \vec{y} \in \mathbb{R}^{\mathbb{N}^*}$
Donc $\mathbb{R}^{\mathbb{N}}$ stable par $\times$
Soit $\vec{x} \in \mathbb{R}^{\mathbb{N}^*}$, on a $\vec{x} \times 1 = \varphi^{-1}(\varphi(\vec{x}) * \varphi(1)) = \varphi^{-1}(\varphi(\vec{x}) * 1) = \varphi^{-1}(\varphi(\vec{x})) = \vec{x}$
Donc 1 est le neutre pour $\times$
On a bien $\times$ loi de composition interne dans $\mathbb{R}^{\mathbb{N}^*}$. La distributivité se démontrerai de la même manière.
$(\mathbb{R}^{\mathbb{N}^*}, +)$ est évidemment un groupe, donc $(\mathbb{R}^{\mathbb{N}^*}, +, \times)$ est un anneau.

Cette démonstration est essentielle, car on va alors utiliser la relation $\mathbb{R}^n \precsim \mathbb{R}^{\mathbb{N}}$ pour définir l'arithmétique.

Définition 1 On définie le degré de $\vec{x}$ dans $\mathbb{R}^n$ comme étant le plus petit entier p tel que $\vec{x} = \pi_p(\vec{x})$. On note $\deg_{\mathbb{R}^n}(\vec{x}) = p$

Remarque 1 C'est l'équivalent du degré dans $(\mathbb{R}[X], +, *)$, la démonstration ne sera pas faite ici.

Remarque 2 On ne cherchera surtout pas à multiplier deux éléments de $\mathbb{R}^n$! La stabilité n'est pas assurée. Cependant en plongeant nos éléments dans $\mathbb{R}^{\mathbb{N}^*}$, cela sera possible, quitte ensuite à retourner en arrière.

2.2 Arithmétique dans $\mathbb{R}^n$

2.2.1 Division euclidienne

Définition 2 On dit que $\vec{x}$ divise $\vec{y}$ ssi il existe $\vec{q} \in \mathbb{R}^n$ tel que $\vec{y} = \vec{q} \times \vec{x}$. On note $\vec{x}|\vec{y}$

Théorème 1 *Soit* $(\vec{x}, \vec{y}) \in (\mathbb{R}^n)^2$, $\exists!(\vec{B}, \vec{R}) \in (\mathbb{R}^n)^2$ / $\vec{x} = \vec{B} \times \vec{y} + \vec{R}$ *et* $\deg_{\mathbb{R}^n}(\vec{R}) < \deg_{\mathbb{R}^n}(\vec{y})$

Démonstration Soit $(\vec{x}, \vec{y}) \in (\mathbb{R}^n)^2$, $\exists!(A, B) \in \mathbb{R}_{n-1}[X]^2 / \varphi(\vec{x}) = A$ et $\varphi(\vec{y}) = B$.
Par théorème de la division euclidienne dans $(\mathbb{R}[X], +, *)$, il existe un unique couple $(R, Q) \in \mathbb{R}_{n-1}[X]^2$ tel que $A = B * Q + R$
φ isomorphisme, donc il existe un unique couple $(\vec{q}, \vec{r}) \in (\mathbb{R}^n)^2$ tel que
$\vec{q} = \varphi^{-1}(Q)$ et $\vec{r} = \varphi^{-1}(R)$.
On a donc $A = B * Q + R$
$\iff \varphi^{-1}(\varphi(\vec{x})) = \varphi^{-1}(\varphi(\vec{q}) * \varphi(\vec{y}) + \varphi(\vec{r}))$
$\iff \vec{x} = \varphi^{-1}(\varphi(\vec{q}) * \varphi(\vec{y})) + \vec{r}$
$\iff \vec{x} = \vec{q} \times \vec{y} + \vec{r}$
On a évidemment $\deg_{\mathbb{R}^n}(\vec{r}) < \deg_{\mathbb{R}^n}(\vec{y})$