Quelques applications des algèbres de matrices à la théorie des corps non commutatifs*

Erwan Biland

28 février 2002

On appelle algèbre à division, ou «corps non commutatif», un anneau unitaire tel que tout élément non nul y ait un inverse.

Dans toute la suite, le mot «corps», employé seul, signifiera corps commutatif. Tous les anneaux et algèbres seront supposés unitaires.

Première partie

Une conséquence d'un théorème de Burnside

1 Théorème de Burnside

Soit K un corps (commutatif), et E un espace vectoriel sur K. Une sous-algèbre (unitaire) A de $\mathcal{L}(E)$ est dite irréductible si et seulement si les seuls sous-espaces vectoriels de E stables par A sont $\{0\}$ et E.

Théorème 1 *Si K est algébriquement clos, et E de dimension finie sur K, alors $\mathcal{L}(E)$ n'admet pas d'autre sous-algèbre irréductible qu'elle même.*

Démonstration.

1. Supposons E de dimension finie, et soit A une sous-algèbre irréductible de $\mathcal{L}(E)$.
   Alors A agit transitivement sur $E-\{0\}$ et $E^*-\{0\}$. Plus précisément,
   $$\forall x \in E-\{0\} \quad \{a(x), a \in A\} = E$$
   $$\forall \varphi \in E^*-\{0\} \quad \{\varphi \circ a, a \in A\} = E^*.$$
2. On en déduit que si A contient un élément de rang 1, il les contient tous, auquel cas $A = \mathcal{L}(E)$
3. Il reste à montrer que si K est algébriquement clos, A contient un élément de rang 1, ce qui achève la démonstration.

2 Théorème d'Artin-Wedderburn

Soit K un corps, et A une K-algèbre. A est dite simple si ses seuls idéaux bilatères sont $\{0\}$ et A.

Théorème 2 *Supposons K algébriquement clos, et A de dimension finie sur K. Si A est simple, alors il existe un espace vectoriel E de dimension finie sur K tel que A soit isomorphe à $\mathcal{L}(E)$*

Démonstration. Soit J un idéal à gauche non nul de A, et de dimension minimale pour cette propriété. Alors l'action à gauche de A sur J fournit un morphisme $\rho : A \to \mathcal{L}(J)$, qui est un isomorphisme.

*Cet exposé est tiré du cours de préparation à l'agrégation assuré par Richard Antetomaso à l'ENS au deuxième semestre de l'année 2000-2001.

3 Théorème de Wedderburn

Théorème 3 *Soit E une algèbre à division de dimension finie sur son centre K, alors $\dim_K E$ est un carré parfait.*

Démonstration.

1. Soit k une clôture algébrique de K, et $A = k \otimes_K E$. Etant donné $a \in A$, il existe $p \in \mathbb{N}$ et deux familles $(\lambda_i) \in k^p$ et $(x_i) \in E^p$ tels que
$$a = \sum_{i=1}^{p} \lambda_i \otimes x_i.$$
On notera $p(a)$ le plus petit tel p.
2. On a les résultats suivants :
   (a) Si $a \in A$ et $p(a) = 1$, alors a est inversible.
   (b) Si $a \in A$ et $a = \sum_{i=1}^{p(a)} \lambda_i \otimes x_i$, alors les familles (λ_i) et (x_i) sont K-libres dans k et E respectivement.
   (c) Si $0 = \sum_{i=1}^{p} \lambda_i \otimes x_i$ et si la famille (λ_i) est K-libre dans k (resp. (x_i) dans E), alors tous les x_i (resp. λ_i) sont nuls.
3. Ceci montre qu'une base de E sur K fournit une base de A sur k, d'où
$$dim_K E = dim_k A.$$
4. Soit I un idéal bilatère non nul de A. Alors il existe $a \in I$ tel que $p(a) = 1$, et ainsi $I = A$.
A est donc une k-algèbre simple et de dimension finie : on en déduit le résultat.

Deuxième partie
Construction de $\mathbb{Q}$-algèbres à division

Théorème 4 (Dirichlet) *Soient a et b des entiers naturels non nuls et premiers entre eux. Alors il existe un nombre premier $p \in \mathbb{N}$ tel que*
$$p \equiv a \bmod b.$$

4 Extensions cyclotomiques d'indice premier

1. Soit $p \in \mathbb{N}$ un nombre premier, et $\Phi_p = 1 + X + ... + X^{p-1}$ le p-ième polynôme cyclotomique. On sait que Φ_p est irréductible sur $\mathbb{Q}$.
D'autre part, le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique. Le théorème de Dirichlet montre qu'il existe un nombre premier $q \in \mathbb{N}$ dont la classe modulo p engendre $(\mathbb{Z}/p\mathbb{Z})^*$. Alors Φ_p est également irréductible sur $\mathbb{F}_q$.
2. Le corps K désignera ici soit $\mathbb{Q}$, soit $\mathbb{F}_p$. Soit L un corps de rupture de Φ_p sur K. On a $L = K[u]$, pour u une racine de Φ_p dans L. Il existe alors un unique K-automorphisme σ de L tel que $\sigma(u) = u^q$. Il vérifie les propriétés suivantes :
   (a) σ est d'ordre $p-1$.
   (b) Les éléments de L stables par σ sont les éléments de K.
   (c) La famille $\left(\sigma^i(u)\right)_{0 \leqslant i \leqslant p-2}$ est une base de L sur K.
3. Pour $\alpha \in L$, on pose
$$N(\alpha) = \prod_{i=0}^{p-2} \sigma^i(\alpha).$$

On a $N(\alpha) \in K$ et $N(\alpha) = 0 \iff \alpha = 0$.
De plus, il existe un polynôme $P \in \mathbb{Z}[X_0 ... X_{p-2}]$, ne dépendant pas du choix de K, tel que,

$$\text{si} \quad \alpha = \sum_{i=0}^{p-2} x_i \sigma^i(u), \quad \text{avec} \quad x_i \in K, \quad \text{alors} \quad N(\alpha) = P(x_0 ... x_{p-2})$$

4. On se place ici dans le cas $K = \mathbb{Q}$. On a alors le

Lemme 1 *Soit $(x_i)_{0 \leqslant i \leqslant p-2} \in \mathbb{Z}^{p-1}$, et $\alpha = \sum_{i=0}^{p-2} x_i \sigma^i(u) \in L$. Alors $N(\alpha) \in \mathbb{Z}$. De plus*

$$N(\alpha) \equiv 0 \bmod q \quad \Rightarrow \quad \forall i \in \{0 ... p-2\} \quad x_i \equiv 0 \bmod q.$$

5 Construction d'une $\mathbb{Q}$-algèbre à division de dimension $(p-1)^2$

1. On se place dans le cas $K = \mathbb{Q}$, et on travaille dans $\mathcal{M}_{p-1}(L)$, considérée comme $\mathbb{Q}$-algèbre. On a alors une application

$$M : \begin{array}{ccccc} L & \to & \mathcal{M}_{p-1}(L) & & \\ \alpha & \mapsto & M(\alpha) & = & diag\left(\alpha, \sigma(\alpha), ..., \sigma^{p-2}(\alpha)\right) \end{array}.$$

On a aussi la matrice

$$A = \begin{bmatrix} 0 & & & & q \\ 1 & \ddots & & 0 & \\ & \ddots & \ddots & & \\ & 0 & \ddots & \ddots & \\ & & & 1 & 0 \end{bmatrix}.$$

On pose

$$E = \left\{ \sum_{i=0}^{p-2} M(\alpha_i) A^i \quad , \quad (\alpha_i) \in L^{p-1} \right\} \subset \mathcal{M}_{p-1}(L).$$

2. Ces objets vérifient :
   (a) M est un morphisme d'algèbres unitaires.
   (b) $A^{p-1} = q I_{p-1}$.
   (c) $\forall \alpha \in L \quad M(\alpha)\ A = A\, M(\sigma(\alpha))$

   Ainsi E est une sous-$\mathbb{Q}$-algèbre de $\mathcal{M}_{p-1}(L)$ de dimension $(p-1)^2$. Son centre est $\mathbb{Q}$.
3. Après avoir remarqué que

$$\det\left(\sum_{i=0}^{p-2} M(\alpha_i) A^i \right) \equiv N(\alpha_0) \bmod q,$$

et en appliquant le lemme 1, on montre que

$$\forall N \in E \quad \det N = 0 \ \Rightarrow \ N = 0.$$

Ceci prouve que E est intègre, c'est donc un «corps non commutatif».

6 Amélioration de la construction précédente et résultat définitif

1. On a montré l'existence, pour tout $p \in \mathbb{N}$ premier, d'une algèbre à division de dimension $(p-1)^2$ sur son centre $\mathbb{Q}$, et on veut maintenant en déduire le

Théorème 5 *Soit n un entier naturel non nul, alors il existe un «corps non commutatif» de centre $\mathbb{Q}$ et de dimension n^2 sur $\mathbb{Q}$.*

2. On va pour cela considérer une sous-algèbre F de l'algèbre E construite précédemment. n étant fixé, on choisit p premier tel que
   (a) n divise $p-1$. On note $r = \frac{p-1}{n}$.
   (b) n et r sont premiers entre eux.

   L'existence d'un tel p est assurée par le théorème de Dirichlet : on peut prendre $p \equiv (n+1) \bmod n^2$.
3. Soit M le sous-corps des éléments de L invariants par σ^n, et τ le $\mathbb{Q}$-automorphisme de M induit par σ^r. Posons $v = \sum_{j=0}^{r-1} \sigma^j(u)$. On a
   (a) τ est d'ordre n.
   (b) Les éléments de M stables par τ sont exactement ceux de $\mathbb{Q}$.
   (c) La famille $\left(\tau^i(v)\right)_{0 \leqslant i \leqslant n-1}$ est une base de M sur $\mathbb{Q}$.

   Soit d'autre part $B = A^r$, qui vérifie :
   (d) $B^n = q\, I_{p-1}$
   (e) $\forall \beta \in M \quad M(\beta)\ B = B\, M(\tau\beta)$.
4. On pose enfin
$$F = \left\{ \sum_{i=0}^{n-1} M(\beta_i)\, B^i \quad , \quad (\beta_i) \in M^n \right\} \ \subset\ E\ \subset\ \mathcal{M}_{p-1}(L)\,.$$
   Les propriétés précédentes montrent que c'est une $\mathbb{Q}$-algèbre à division de dimension n^2 et de centre $\mathbb{Q}$.