AUTOMORPHISMES DES ALGÈBRES DE MATRICES SUR UN ANNEAU COMMUTATIF

G.BERHUY

Table des matières

Dans cet article, on supposera le lecteur familier avec les notions de base sur les modules, en particulier avec la notion de module libre, même si nous feront de très brefs rappels.

1. Introduction

Dans tout ce qui suit, R est un anneau commutatif unitaire et $n \geq 1$ est un entier. On s'intéresse à la question suivante :

quels sont les automorphismes de la R-algèbre $\mathrm{M}_n(R)$?

Commençons par donner une famille d'exemples.

Lemme 1.1. *Soit $P \in \mathrm{GL}_n(R)$ une matrice inversible*[1] *de $\mathrm{M}_n(R)$ Alors, l'application*

$$\begin{array}{rcl} \mathrm{Int}(P)\colon \mathrm{M}_n(R) & \longrightarrow & \mathrm{M}_n(R) \\ A & \longmapsto & PAP^{-1} \end{array}$$

est un automorphisme d'algèbre.

Démonstration. C'est un simple calcul. □

Définition 1.2. Un automorphisme de $\mathrm{M}_n(R)$ de la forme $\mathrm{Int}(u)$ est appelé un *automorphisme intérieur*.

Date: 6 mars 2024.

1. On rappelle que cela équivaut à demander que $\det(P) \in R^\times$.

Lorsque R est un corps, le théorème suivant montre que ce sont les seuls automorphismes possibles.

Thm. Soit K un corps. Alors, tout automorphisme de K-algèbre de $\mathrm{M}_n(K)$ est intérieur.

Nous reléguons la démonstration de ce théorème au paragraphe suivant.

Au vu de ce résultat, il est légitime de se pose la question suivante : tout automorphisme de R-algèbre de $\mathrm{M}_n(R)$ est-il intérieur ?

L'exemple suivant montre que la réponse est négative.

Exemple 1.3. Soit $R = \mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5} \mid a, b, \in \mathbb{Z}\}$. On rappelle que $R^\times = \{\pm 1\}$.

En effet, si $z = a + b\sqrt{-5} \in R^\times$, il existe $z \in R$ tel que $zz' = 1$. Mais alors, $|z|^2|z'|^2 = 1 \in \mathbb{N}$. On a donc $|z|^2 = 1 = a^2 + 5b^2$. Si $b \neq 0$, c'est impossible, puisque $a + 5b^2 \geq 5 > 1$. Ainsi, $b = 0$, puis $a^2 = 1$, et enfin $z = a = \pm 1$.

Posons $Q = \begin{pmatrix} 2 & \omega \\ \overline{\omega} & 2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}(i\sqrt{5}))$. Notons que $\det(Q) = -2 \notin R^\times$, et donc Q n'est pas inversible dans $\mathrm{M}_2(R)$. Néanmoins, on a $QAQ^{-1} \in \mathrm{M}_2(R)$ et $Q^{-1}AQ \in \mathrm{M}_2(R)$ pour tout $A \in \mathrm{M}_2(R)$.

En effet, si $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{M}_2(R)$, on a

$$QAQ^{-1} = \begin{pmatrix} -2\alpha - \gamma\omega + \beta\overline{\omega} + \dfrac{\omega\overline{\omega}}{2}\delta & -2\beta + (\alpha - \delta)\omega + \dfrac{\omega^2}{2}\gamma \\ -2\gamma + (\delta - \alpha)\overline{\omega} + \dfrac{\overline{\omega}^2}{2}\beta & -2\delta + \gamma\omega - \beta\overline{\omega} + \dfrac{\omega\overline{\omega}}{2}\alpha \end{pmatrix},$$

ainsi que

$$Q^{-1}AQ = \begin{pmatrix} -2\alpha + \gamma\omega - \beta\overline{\omega} + \dfrac{\omega\overline{\omega}}{2}\delta & -2\beta + (\delta - \alpha)\omega + \dfrac{\omega^2}{2}\gamma \\ -2\gamma + (\alpha - \delta)\overline{\omega} + \dfrac{\overline{\omega}^2}{2}\beta & -2\delta - \gamma\omega + \beta\overline{\omega} + \dfrac{\omega\overline{\omega}}{2}\alpha \end{pmatrix}.$$

On conclut en remarquant que

$$\frac{\omega^2}{2} = -2 + i\sqrt{5}, \ \frac{\overline{\omega}^2}{2} = -2 - i\sqrt{5} \ \text{ et } \frac{\omega\overline{\omega}}{2} = 3.$$

Il s'ensuit que la restriction de $\mathrm{Int}(Q)$ à $\mathrm{M}_2(R)$ induit un automorphisme de R-algèbre de $\mathrm{M}_2(R)$, que l'on notera θ.

Autrement dit, on a $\theta(A) = QAQ^{-1}$ pour tout $A \in \mathrm{M}_2(R)$.

Démontrons maintenant que θ n'est pas un automorphisme intérieur de $\mathrm{M}_2(R)$.

Supposons au contraire que $\theta = \mathrm{Int}(P)$, avec $P \in \mathrm{GL}_2(R)$. Pour tout $A \in \mathrm{M}_2(R)$, on a donc $QAQ^{-1} = PAP^{-1}$, et ainsi $P^{-1}Q$ commute avec toute matrice $\mathrm{M}_2(R)$. Comme on peut toujours écrire un élément de $\mathbb{Q}(i\sqrt{5})$ s'écrit $\dfrac{r}{m}$, avec $r \in R$ et $m \geq 1$ est un entier, on en déduit que $P^{-1}Q$ commute avec toute matrice de $\mathrm{M}_2(\mathbb{Q}(i\sqrt{5}))$. Par conséquent, on a $P^{-1}Q = \lambda I_2$, avec

$\lambda \in \mathbb{Q}(i\sqrt{5})$. Puisque $P^{-1}Q$ est à coefficients dans R (P étant inversible dans $\mathrm{M}_2(R)$, on a $\lambda \in R$. En prenant les déterminants, et en tenant compte du fait que $\det(P) \in R^\times = \{\pm 1\}$, on a donc $\pm 2 = \lambda^2$. Ainsi, $|\lambda|^2 = 2$. Mais, cette équation n'a pas de solution dans R, d'où une contradiction.

Le but de cet article est, entre autres, de comprendre ce qui se cache derrière ce contre-exemple, ainsi que donner des exemples d'anneaux R pour lesquels tout automorphisme de $\mathrm{M}_n(R)$ est intérieur.

2. Brefs rappels sur les modules

Dans ce cours paragraphe, on rappelle brièvement les notions sur les modules que nous utiliserons dans la suite.

Un *R-module* (à gauche) est la structure que l'on obtient lorsque l'on remplace le corps de base K par un anneau R dans la définition d'un K-espace vectoriel.

Les notions de sous-module, d'application R-linéaire, d'isomorphisme, de famille libre, de famille génératrice, et de base se définissent alors de la même manière.

Contrairement au cas des espaces vectoriels, un R-module n'admet pas nécessairement de base. Un R-module possédant au moins une base s'appelle un *R-module libre*. Lorsque R est commutatif (ce qui est le cas dans cet article), on démontre que si M est un R-module libre de type fini (i.e. possédant une famille génératrice finie), toutes les bases de M ont même cardinal.[2] Ce cardinal commun est appelé le *rang* de M, et noté alors $\mathrm{rg}(M)$.

L'exemple type d'un R-module libre de rang n est R^n, dont une base est la base canonique (qui est définie de manière similaire à celle de K^n).

On démontre comme dans le cas des espaces vectoriels qu'un R-module M est libre de rang n si et seulement si $M \simeq R^n$.

Si $f : M \longrightarrow N$ est une application R-linéaire, et si M est un R-module libre, alors f est déterminée de manière unique par les images des éléments d'une base de M.

De plus, si f est un isomorphisme, alors N est libre si et seulement si M l'est, et f envoie alors une base de M sur une base de N.

Enfin, si on a une décomposition en somme directe $M = M_1 \oplus \cdots \oplus M_r$, et si chaque M_i est libre, alors M est libre, et la concaténation d'une base de chaque M_i fournit une base de M. En particulier, le rang d'une somme directe (interne ou externe) de modules est égal à la somme des rangs.

On laisse le lecteur consulter la littérature existante pour les détails.

3. Une condition nécessaire et suffisante

Dans ce paragraphe, on se fixe un automorphisme d'algèbre θ de $\mathrm{M}_n(R)$.

2. Ce n'est plus nécessairement le cas lorsque R n'est pas commutatif.

On se propose de donner une condition nécessaire et suffisante pour que θ soit intérieur en termes de sous-modules de R^n.

Commençons par introduire une définition commode.

Définition 3.1. Un *système de matrices élémentaires* de $\mathrm{M}_n(R)$ est une famille de n^2 matrices $(F_{ij})_{i,j}$ deux à deux distinctes vérifiant les relations

$$F_{ij}F_{k\ell} = \delta_{j,k}F_{i\ell} \text{ pour tous } i,j,k,\ell \in [\![1,n]\!] \quad \text{et} \quad \sum_{i=1}^{n} F_{ii} = I_n.$$

Exemples 3.2.

(1) Pour tous $i,j \in [\![1,n]\!]$, on note $E_{ij} \in \mathrm{M}_n(R)$ la matrice dont tous les coefficients sont nuls, sauf celui en position (i,j), qui vaut 1.

Alors, $(E_{ij})_{i,j}$ est un système de matrices élémentaires.

(2) L'image d'un système de matrices élémentaires par un automorphisme d'algèbre de $\mathrm{M}_n(R)$ est encore un système de matrices élémentaires.

On a alors le lemme utile suivant.

Lemme 3.3. *Soit $(F_{ij})_{i,j}$ un système de matrices élémentaires de $\mathrm{M}_n(R)$. Pour tout $j \in [\![1,n]\!]$, on pose $M_j = \mathrm{Im}(F_{j1})$. Alors, on a une décomposition en somme directe*

$$R^n = M_1 \oplus \cdots \oplus M_n.$$

De plus, pour tout $j \in [\![1,n]\!]$, l'application

$$\begin{aligned} \mu_{F_{j1}} \colon R^n &\longrightarrow R^n \\ v &\longmapsto F_{j1}v \end{aligned}$$

induit par double restriction un isomorphisme de R-modules $M_1 \simeq M_j$.

En particulier, l'application

$$\begin{aligned} \varphi \colon \quad M_1^n &\longrightarrow R^n \\ (x_1,\dots,x_n) &\longmapsto \sum_{j=1}^{n} F_{j1}x_j \end{aligned}$$

est un isomorphisme de R-modules.

Démonstration. Commençons par établir la somme directe. Si $v \in R^n$, on a

$$v = I_n v = \sum_{j=1}^{n} F_{jj}v = \sum_{j=1}^{n} F_{j1}(F_{1j}v),$$

d'où l'existence de la décomposition. Supposons maintenant que $\sum_{j=1} y_j = 0$, avec $y_j \in \mathrm{Im}(F_{j1})$. Écrivons $y_j = F_{j1}v_j$, avec $v_j \in R^n$. En appliquant F_{kk} à l'égalité précédente, et en tenant compte de la relation $F_{kk}F_{j1} = \delta_{k,j}F_{k1}$, on obtient $F_{k1}v_k = 0$, soit encore $y_k = 0$, d'où l'unicité.

Passons à la deuxième partie du lemme. Soit $j \in [\![1,n]\!]$. Pour tout $v \in R^n$, on a $F_{j1}(F_{11}v) = F_{j1}v$, si bien que $\mu_{F_{j1}}$ induit une application linéaire $\varphi_j : M_\theta \longrightarrow M_j$.

De même, on a $F_{1j}(F_{j1}v) = F_{11}v$, et $\mu_{F_{1j}}$ induit donc une application linéaire $\psi_j : M_j \longrightarrow M_\theta$. Or, pour tout $v \in R^n$, on a

$$\varphi_j(\psi_j(F_{j1}v)) = F_{j1}F_{1j}F_{j1}v = F_{j1}v,$$

ainsi que

$$\psi_j(\varphi_j(F_{11}v)) = F_{1j}F_{j1}F_{11}v = F_{11}v,$$

ce qui démontre que φ_j et ψ_j sont inverses l'une de l'autre.

Le dernier point découle alors des deux points précédents, puisque par définition, on a

$$\varphi(x_1, \ldots, x_n) = \sum_{j=1}^{n} \varphi_i(x_j)$$

pour tous $x_1, \ldots, x_n \in M_\theta$. □

Revenons maintenant à notre problème.

Dans la suite, on note E_{ij} la matrice élémentaire standard.

On notera $\mathscr{B} = (e_1, \ldots, e_n)$ la base canonique de R^n, et on notera implicitement les éléments de R^n sous forme de vecteurs colonne.

On commence par un lemme classique.

Lemme 3.4. *Soient $A_1, A_2 \in \mathrm{M}_n(R)$ et soit $P \in \mathrm{GL}_n(R)$. Si $A_2 = PA_1P^{-1}$, alors l'application*

$$\begin{aligned} \mu_P \colon R^n &\longrightarrow R^n \\ v &\longmapsto Pv \end{aligned}$$

induit par double restriction un isomorphisme de R-modules $\mathrm{Im}(A_1) \simeq \mathrm{Im}(A_2)$.

Démonstration. L'application μ_P est clairement R-linéaire. Si de plus $v = A_1x$, avec $x \in R^n$, alors $Pv = PA_1x = A_2(Px)$. Ainsi, μ_P envoie bien un élément de $\mathrm{Im}(A_1)$ sur un élément de $\mathrm{Im}(A_2)$, et se restreint donc en une application linéaire $f : \mathrm{Im}(A_1) \longrightarrow \mathrm{Im}(A_2)$. On démontre de même que $\mu_{P^{-1}}$ se restreint en une application linéaire $f : \mathrm{Im}(A_2) \longrightarrow \mathrm{Im}(A_1)$. Il est alors clair que f et g sont inverses l'une de l'autre. □

On peut alors démontrer le théorème suivant.

Théorème 3.5. *Soit θ un automorphisme d'algèbre de $\mathrm{M}_n(R)$.*

Pour tous $i, j \in [\![1, n]\!]$, on pose $F_{ij} = \theta(E_{ij})$ et $M_j = \mathrm{Im}(F_{j1})$. Enfin, soit $M_\theta = \mathrm{Im}(F_{11})(= M_1)$.

Alors :

(1) *on a $R^n = M_1 \oplus \cdots \oplus M_n$*

(2) *pour tout $j \in [\![1, n]\!]$, l'application*

$$\begin{aligned} \mu_{F_{j1}} \colon R^n &\longrightarrow R^n \\ v &\longmapsto F_{j1}v \end{aligned}$$

induit par double restriction un isomorphisme de R-modules $M_\theta \simeq M_j$

(3) *l'application*

$$\begin{array}{rccl} \varphi\colon & M_\theta^n & \longrightarrow & R^n \\ & (x_1,\dots,x_n) & \longmapsto & \displaystyle\sum_{j=1}^n F_{j1}x_j \end{array}$$

est un isomorphisme de R-modules.

De plus, θ est un automorphisme intérieur si et seulement si M_θ est un module libre de rang 1.

Dans ce cas, si v_1 est une base de M_θ, alors $\theta = \mathrm{Int}(P)$, où P est la matrice dont la j-ième colonne est $F_{j1}v_1$ pour tout $j \in [\![1,n]\!]$.

Démonstration. La première partie découle du fait que les matrices F_{ij} forment un système de matrices élémentaires d'après l'exemple 3.2 (2) et du lemme 3.3.

Supposons que $\theta = \mathrm{Int}(P)$. Alors, $F_{11} = \theta(E_{11}) = PE_{11}P^{-1}$, et le lemme précédent implique que $M_\theta = \mathrm{Im}(F_{11}) \simeq \mathrm{Im}(E_{11})$.

Mais on a clairement $\mathrm{Im}(E_{11}) = R{\cdot}e_1$, où e_1 est le premier vecteur de la base canonique. Or, il est facile de constater e_1 est une base de $R{\cdot}e_1$. Ainsi, $\mathrm{Im}(E_{11})$ est aussi libre de rang 1.

Supposons maintenant que M_θ soit libre de rang 1. Le lemme 3.3 montre que F_{j1} induit par double restriction un isomorphisme entre M_θ et M_j, si bien que, si v_1 est une base M_θ, $F_{j1}v_1$ est une base de M_j. La somme directe précédente montre alors que $(F_{11}v_1,\dots,F_{j1}v_1)$ est une base de R^n. Ainsi, la matrice P dont la j-ième colonne est $F_{j1}v_1$ pour tout $j \in [\![1,n]\!]$ est une matrice inversible.

Montrons que $\theta = \mathrm{Int}(P)$. Puisque les matrices E_{ij} forment une base de $\mathrm{M}_n(R)$, il suffit de montrer que $\theta(E_{ij}) = PE_{ij}P^{-1}$ pour tous $i,j \in [\![1,n]\!]$, soit encore $\theta(E_{ij})P = PE_{ij}$. Comme deux matrices sont égales si et seulement les colonnes correspondantes sont égales, cela équivaut finalement à montrer que $\theta(E_{ij})Pe_k = PE_{ij}e_k$ pour tous $i,j,k \in [\![1,n]\!]$.

Par définition de P et E_{ij}, on a $PE_{ij}e_k = \delta_{j,k}Pe_i = \delta_{j,k}v_i$. Mais, on a aussi

$$\theta(E_{ij})Pe_k = F_{ij}Pe_k = F_{ij}v_k = F_{ij}F_{k1}v_1 = \delta_{j,k}F_{i1}v_1 = \delta_{j,k}v_i,$$

d'où le résultat voulu. □

Remarque 3.6. Dans l'énoncé précédent, on peut remplacer la condition « M_θ est libre de rang 1 » par la condition a priori plus faible « M_θ est libre ».

En effet, le lemme 3.3 montre que $R^n = M_1 \oplus \cdots \oplus M_n$, et que chaque M_j est isomorphe à M_θ. En particulier, M_j est libre, de même rang que M_θ, et on a donc $\mathrm{rg}(R^n) = n = n\mathrm{rg}(M_\theta)$, d'où $\mathrm{rg}(M_\theta) = 1$. Autrement dit, si M_θ est libre, il est nécessairement de rang 1.

Lorsque R est un corps, un R-module n'est rien d'autre qu'un espace vectoriel. Comme tout espace vectoriel possède une base, on obtient alors le résultat suivant, déjà énoncé dans l'introduction.

Théorème 3.7. *Soit K un corps. Alors, pour tout $n \geq 1$, tout automorphisme de K-algèbre de $\mathrm{M}_n(K)$ est intérieur.*

4. Réinterprétation dans le cas d'un anneau intègre

On va maintenant s'intéresser de plus près au contre-exemple exposé dans l'introduction.

Dans ce paragraphe, R sera un anneau intègre, et K sera son corps des fractions. On identifiera canoniquement R à un sous-anneau de K afin d'éviter les lourdeurs de notation.

Soit θ un automorphisme de $\mathrm{M}_n(R)$. D'après le lemme 3.3, on a $R^n = M_1 \oplus \cdots \oplus M_n$, où $M_j = \mathrm{Im}(F_{j1})$.

Notons V_j l'image de la matrice F_{j1}, mais vue cette fois comme matrice à coefficients dans K. Le lemme 3.3 montre alors que $K^n = V_1 \oplus \cdots \oplus V_n$, et $V_1 \simeq V_j$. En particulier, V_1 est de dimension 1.

On fixe alors un vecteur $v_0 \in R^n$ tel que $V_1 = K{\cdot}v_0$. Si maintenant $v \in R^n$, alors en voyant v comme un élément de K^n et F_{11} comme une matrice à coefficients dans K, on constate qu'il existe un unique $\lambda \in K$ tel que $F_{11}v = \lambda{\cdot}v_0$.

Cela nous conduit à poser

$$I_\theta = \{\lambda \in K \mid \text{ il existe } v \in R^n \text{ tel que } F_{11}v = \lambda v_0\}.$$

Puisque $e_j \in R^n$, on a donc $F_{11}e_j = \lambda_j v_0$.

Notons que la classe d'isomorphisme de I_θ ne dépend pas du choix de v_0. En effet, si v_0' est un autre vecteur de R^n qui engendre V_1, alors $v_0' = \lambda' v_0$ pour un certain $\lambda' \in K^\times$. Si I_θ' est le R-module obtenu avec cet autre choix, on constate aisément que la multiplication par λ' induit un isomorphisme de R-modules $I_\theta' \simeq I_\theta$.

Remarquons aussi que l'on a alors

$$F_{11}(\sum_{j=1}^{n} r_j e_j) = (\sum_{j=1} r_j \lambda_j){\cdot}v_0.$$

On en conclut donc que

$$I_\theta = \sum_{j=1}^{n} R{\cdot}\lambda_j.$$

En réduisant au même dénominateur, on peut écrire $\lambda_j = \dfrac{a_j}{d}$ pour tout $j \in [\![1, r]\!]$, avec $a_1, \ldots, a_r, d \in R$. Si $\mathfrak{A}$ est l'idéal engendré par $a_1, \ldots, a_r$, on a donc $I_\theta = d^{-1}\mathfrak{A}$.

Cela conduit à la définition suivante.

Définition 4.1. Soit R un anneau intègre, de corps des fractions K. Un *idéal fractionnaire* de R est un sous-module du R-module K de la forme $x\mathfrak{A}$, où $x \in K^\times$ et $\mathfrak{A}$ est un idéal de R.

Un idéal fractionnaire de R est dit *principal* s'il est de la forme

$$R{\cdot}\alpha = \{r\alpha \mid r \in R\},$$

avec $\alpha \in K$.

Remarque 4.2. Si $I = x\mathfrak{A}$ est un idéal fractionnaire de K, alors I est principal si et seulement si $\mathfrak{A}$ est un idéal principal de R, ce qui explique le choix des mots employés dans la définition précédente.

En effet, si $\mathfrak{A}$ est principal, engendré par a, alors $I = R{\cdot}ax$. Inversement, si $I = R{\cdot}\alpha$, avec $\alpha = \dfrac{a}{d} \in K$, alors $I = d^{-1}\mathfrak{A}$, où $\mathfrak{A}$ est l'idéal de R engendré par a.

Lemme 4.3. *L'application K-linéaire*

$$\begin{aligned} K &\longrightarrow V_1 \\ \lambda &\longmapsto \lambda{\cdot}v_0 \end{aligned}$$

induit par double restriction un isomorphisme de R-modules $I_\theta \simeq M_\theta$.

En particulier, θ est un automorphisme intérieur si et seulement si l'idéal fractionnaire I_θ est principal.

Démonstration. Par définition même de I_θ, l'application linéaire de l'énoncé induit par double restriction une application R-linéaire $f : I_\theta \longrightarrow M_\theta$. Le fait que v_0 soit une K-base de V_1 entraîne l'injectivité de f. Si maintenant $x \in M_\theta$, alors il existe $v \in R^n$ tel que $F_{11}v = x$. Mais alors, $F_{11}v = \lambda{\cdot}v_0$, pour un certain $\lambda \in K$, comme on l'a déjà constaté, et ainsi $f(\lambda) = \lambda{\cdot}v_0 = F_{11}v = x$, d'où la surjectivité de f.

D'après le théorème 3.5, θ est un automorphisme intérieur si et seulement si M_θ est libre de rang 1.

Si M_θ est libre de rang 1, de base x_0, alors $I_\theta = f(M_\theta) = f(R{\cdot}v_0) = R{\cdot}f(v_0)$. Ainsi, I_θ est un idéal fractionnaire principal. Inversement, si $I_\theta = R{\cdot}\alpha$, alors $M_\theta = R{\cdot}x_0$, avec $x_0 = f^{-1}(\alpha)$. Mais M_θ est non nul. En effet, $\theta(E_{11})$ n'est pas nul car θ est un automorphisme et $E_{11} \neq 0$. Si maintenant $r{\cdot}x_0 = 0$ pour un certain $r \in R$, alors $r = 0$, car sinon, la multiplication par $\dfrac{1}{r} \in K$ donnerait $x_0 = 0$. Ainsi, x_0 est une base de M_θ, qui est bien libre de rang 1. □

On peut maintenant revenir à l'exemple cité dans l'introduction.

Exemple 4.4. Soit $R = \mathbb{Z}[i\sqrt{5}]$, soit $\omega = 1+i\sqrt{5}$, et soit θ l'automorphisme de $\mathrm{M}_2(R)$ défini par

$$\theta(A) = QAQ^{-1} \quad \text{pour tout } A \in \mathrm{M}_2(R),$$

avec $Q = \begin{pmatrix} 2 & \omega \\ \overline{\omega} & 2 \end{pmatrix}$.

Un simple calcul montre que $F_{11} = \theta(E_{11}) = \begin{pmatrix} -2 & \omega \\ -\overline{\omega} & 3 \end{pmatrix}$.

Posons $v_0 = \begin{pmatrix} 2 \\ \overline{\omega} \end{pmatrix}$, si bien que $F_{11}e_1 = -v_0$ et $F_{11}e_2 = \dfrac{\omega}{2}v_0$.

On a donc $I_\theta = R(-1) + R\frac{\omega}{2} = R + R\frac{\omega}{2} = \frac{1}{2}\mathfrak{A}$, où $\mathfrak{A} = (2, \omega)$.

Le lemme 4.3 et la remarque 4.2 montrent alors que θ est intérieur si et seulement si $\mathfrak{A}$ est un idéal principal de R.

Supposons que $\mathfrak{A} = Rz, z \in R$. Alors, $2 = zz_1$ et $\omega = zz_2$ avec $z_1, z_2 \in R$. En particulier, $|z|^2 \mid |2|^2$ et $|z|^2 \mid |\omega|^2$ dans $\mathbb{N}$, si bien que $|z|^2 \mid \mathrm{pgcd}(4, 6)$, i.e. $|z|^2 \mid 2$ dans $\mathbb{N}$.

On a déjà constaté que l'équation $|z|^2 = 2$ n'a pas de solutions dans R. Ainsi, $|z|^2 = 1$, ce qui implique comme on l'a vu que $z = \pm 1$. En particulier, $1 \in \mathfrak{A}$ et il existe $r_1, r_2 \in R$ tels que $1 = 2r_1 + \omega r_2$. En multipliant par $\overline{\omega}$ et en se rappelant que $\omega\overline{\omega} = 6$, on en déduit que $\overline{\omega} \in 2R$. En calculant le module au carré, on en déduit que $4 \mid 6$ dans $\mathbb{N}$, d'où une contradiction.

Ainsi, I_θ n'est pas un idéal fractionnaire principal et M_θ n'est pas un R-module libre, ce qui explique d'une manière un peu plus conceptuelle le fait que θ ne soit pas intérieur.

5. Le cas d'un anneau factoriel

On continue à supposer l'anneau R intègre. Le lemme 4.3 et la remarque 4.2 permettent alors d'obtenir immédiatement le résultat suivant.

Théorème 5.1. *Soit R un anneau principal. Alors, pour tout $n \geq 1$, tout automorphisme d'algèbre de $\mathrm{M}_n(R)$ est intérieur.*

Ce théorème peut se démontrer beaucoup plus rapidement en utilisant le fait bien connu que si R est un anneau principal, alors tout sous-module de R^n est libre. Néanmoins, notre approche a l'avantage de ne pas utiliser ce théorème non trivial. Elle va également permettre de généraliser ce résultat au cas d'un anneau factoriel.

Pour cela, nous allons étudier plus en détail les propriétés de l'idéal fractionnaire I_θ introduit dans le paragraphe précédent.

On commence par introduire une notation. Si I, J sont deux idéaux fractionnaires, on note IJ le sous-module de K engendré par les produits de la forme xy, avec $x \in I$ et $y \in J$.

C'est encore un idéal fractionnaire. En effet, si $I = x\mathfrak{A}$ et $J = y\mathfrak{B}$, alors IJ est le R-module engendré par les produits de la forme $xyab, a \in A, b \in B$. Ce R-module n'est rien d'autre que $xy(\mathfrak{A}\mathfrak{B})$, par définition de l'idéal produit $\mathfrak{A}\mathfrak{B}$.

Définition 5.2. Si I et J sont des idéaux fractionnaires de R, l'idéal fractionnaire IJ est appelé le *produit* de I et J.

Le produit définit une loi interne associative et commutative sur l'ensemble des idéaux fractionnaires de R, de neutre R, puisque $IR = RI = I$. Ceci motive la définition suivante.

Définition 5.3. Un idéal fractionnaire I est *inversible* s'il existe un idéal fractionnaire tel que $IJ = R$.

Dans ce cas, l'idéal fractionnaire J est unique et est noté I^{-1}. De plus, I^{-1} est alors inversible, d'inverse I.

Remarques 5.4. (1) Si I est un idéal fractionnaire inversible, on a nécessairement $I^{-1} = \{\mu \in K \mid \mu I \subset R\}$.

En effet, posons $J = \{\mu \in K \mid \mu I \subset R\}$. Par définition de J et du produit IJ, on a $IJ \subset R$. On a alors $J = I^{-1}IJ \subset I^{-1}R = I^{-1}$. D'autre part, pour tout $\mu \in I^{-1}$, on a $\mu I \subset I^{-1}I = R$, et donc $\mu \in J$, d'où $I^{-1} \subset J$.

(2) Un idéal fractionnaire inversible est nécessairement de type fini comme R-module.

En effet, par définition, il existe $\lambda_1, \ldots, \lambda_r \in I$ et $\mu_1, \ldots, \mu_r \in I^{-1}$ tels que $\displaystyle\sum_{i=1}^{r} \lambda_i \mu_i = 1$.

Mais alors, pour tout $x \in I$, et pour tout $i \in [\![1, r]\!]$, on a $x\mu_i \in R$, et par conséquent

$$x = \sum_{i=1}^{r} (x\mu_i)\lambda \in R{\cdot}\lambda_1 + \cdots + R{\cdot}\lambda_r.$$

Comme d'autre part, $\lambda_1, \ldots, \lambda_r \in I$, on a l'autre inclusion, et par conséquent, $I = R{\cdot}\lambda_1 + \cdots + R{\cdot}\lambda_r$.

Exemples 5.5.

(1) Si $\alpha \in K^\times$, $R\alpha$ est un idéal fractionnaire inversible, d'inverse $R\alpha^{-1}$.

(2) L'idéal $I = (2, X)$ n'est pas un idéal fractionnaire inversible. En fait, si c'était le cas, d'après la remarque précédente, on aurait $IJ = \mathbb{Z}[X]$, avec $J = \{\mu \in \mathbb{Q}(X) \mid \mu I \subset \mathbb{Z}[X]\}$.

Écrivons $\mu = \dfrac{P}{Q}$, avec $P \in \mathbb{Z}[X]$ et $Q \in \mathbb{Z}[X] \setminus \{0\}$. On peut toujours supposer que P et Q sont premiers entre eux, puisque $\mathbb{Z}[X]$ est un anneau factoriel.

Alors, $\mu \in J$ si et seulement si $2\mu \in \mathbb{Z}[X]$ et $X\mu \in \mathbb{Z}[X]$, soit encore $2P \in Q\mathbb{Z}[X]$ et $XP \in Q\mathbb{Z}[X]$. Cela revient à demander $Q \mid 2P$ et $Q \mid XP$, et comme P et Q sont premiers entre eux, cela à équivaut à $Q \mid 2$ et $Q \mid X$, d'après le lemme de Gauss. La première relation de divisibilité entraîne que $Q = \pm 1, \pm 2$, et la seconde force $Q = \pm 1$. Autrement dit, $J = \mathbb{Z}[X]$. Mais alors, $IJ = I \neq \mathbb{Z}[X]$ (En effet, les éléments de I sont de terme constant pair, donc $1 \notin I$).

On a alors le lemme suivant.

Lemme 5.6. *L'idéal fractionnaire I_θ est inversible.*

Démonstration. Rappelons que I_θ est engendré par $\lambda_1, \ldots, \lambda_n \in K^\times$, où λ_i est défini par l'égalité $F_{11}e_i = \lambda_i{\cdot}v_0$.

Écrivons $v_0 = \displaystyle\sum_{j=1}^{n} \mu_j e_j$, avec $\mu_j \in R$ (rappelons que $v_0 \in R^n$), et posons $J = R\mu_1 + \ldots + R\mu_n$. Nous allons démontrer que $IJ = R$.

Puisque $v_0 \in \mathrm{Im}(F_{11})$ et que $F_{11}^2 = F_{11}$, on a $F_{11}v_0 = v_0$, soit $(\sum_{j=1}^{n} \lambda_j\mu_j)\cdot v_0 = v_0$, d'où $\sum_{j=1}^{n} \lambda_j\mu_j = 1$. En particulier, $1 \in IJ$, d'où $R \subset IJ$.

D'autre part, $F_{11}e_i = \lambda_i v_0 = \sum_{j=1}^{n}(\lambda_i\mu_j)\cdot e_j$. Comme $F_{11}e_i \in R^n$, on a donc $\lambda_i\mu_j \in R$ pour tous $i, j \in [\![1, n]\!]$, et on en déduit aisément que $IJ \subset R$. □

Le lemme précédent prend tout son intérêt au vu de la proposition qui suit.

Proposition 5.7. *Soit R un anneau factoriel. Alors, un idéal fractionnaire de R est inversible si et seulement s'il est non nul et principal.*

Démonstration. Un idéal fractionnaire non nul principal est inversible d'après l'exemple 5.5 (1).

Soit I un idéal fractionnaire inversible. Il est alors non nul, puisque $II^{-1} = R \neq 0$ (un anneau factoriel étant intègre, donc non trivial), et de type fini comme R-module d'après la remarque 5.4 (2).

Soient $\lambda_1, \ldots, \lambda_r \in K$ des générateurs de I, que l'on peut supposer tous non nuls. Écrivons $\lambda_i = \dfrac{a_i}{d}$, avec $a_i, d \in R \setminus \{0\}$.

Soit $\mu = \dfrac{b}{e} \in K$, avec $b \in R$ et $e \in R \setminus \{0\}$. On a alors $\mu \in I^{-1}$ si et seulement si $de \mid a_i b$ dans R pour tout $i \in [\![1, n]\!]$. Puisque R est factoriel, un pgcd $a \in R$ de $a_1, \ldots, a_r$ existe, et de plus ab est un pgcd de $a_1b, \ldots, a_rb$. Notons que a est non nul puisque les a_i le sont. On a alors $\mu \in I^{-1}$ si et seulement si $de \mid ab$ dans R, ce qui équivaut à $\mu \in R\dfrac{d}{a}$.

Autrement dit, $I^{-1} = R\dfrac{d}{a}$, d'où $I = R\cdot\dfrac{a}{d}$. □

Comme dans le cas d'un anneau principal, on en déduit immédiatement le théorème suivant.

Théorème 5.8. *Soit R un anneau factoriel. Alors, pour tout $n \geq 1$, tout automorphisme d'algèbre de $\mathrm{M}_n(R)$ est intérieur.*

6. Le cas d'un anneau local

On donne maintenant une autre famille d'anneaux pour laquelle tout automorphisme de $\mathrm{M}_n(R)$ est intérieur.

Définition 6.1. Un anneau commutatif R est dit *local* si R possède un unique idéal maximal.

Exemples 6.2.

(1) Tout corps est un anneau local.

(2) Si R est un anneau commutatif, et si $\mathfrak{m}$ est un idéal maximal, pour tout $n \geq 1$, l'anneau $R/\mathfrak{m}^n$ est un anneau local.

En effet, les idéaux maximaux de $R/\mathfrak{m}^n$ sont en bijection avec les idéaux maximaux $\mathfrak{m}'$ de R contenant $\mathfrak{m}^n$.

Supposons que $\mathfrak{m}' \neq \mathfrak{m}$. Alors, par maximalité de $\mathfrak{m}$, on a $\mathfrak{m} + \mathfrak{m}' = R$. Il existe donc $x \in \mathfrak{m}$ et $y \in \mathfrak{m}'$ tels que $x + y = 1$. En élevant l'égalité à la puissance n, on obtient une relation de la forme $x^n + z = 1$, avec $z \in \mathfrak{m}'$. Comme $x^n \in \mathfrak{m}^n$, on a donc $\mathfrak{m}^n + \mathfrak{m}' = R$. Par conséquent, $R = \mathfrak{m}^n + \mathfrak{m}' \subset \mathfrak{m}'$, d'où une contradiction. Ainsi, $\mathfrak{m}' = \mathfrak{m}$, d'où la conclusion.

Avant de continuer, nous allons introduire une nouvelle notion.

Définition 6.3. On dit qu'un R-module P est *projectif de type fini* s'il est isomorphe à un facteur direct d'un R-module libre de rang fini. Autrement dit, P est projectif de type fini s'il existe un R-module libre de rang fini L, et deux sous-modules P' et Q de L vérifiant :

(1) $P \simeq P'$

(2) $L = P' \oplus Q$.

Remarques 6.4.

(1) On peut toujours supposer que $L = R^n$ dans la définition. En effet, si L, P' et Q vérifient les conditions de la définition, et si $\varphi : L \xrightarrow{\sim} R^n$ est un isomorphisme de R-modules, on peut vérifier aisément que $R^n = \varphi(P') \oplus \varphi(Q)$.

De plus, φ étant injective, on a $\varphi(P') \simeq P' \simeq P$.

(2) Un R-module projectif de type fini est de type fini au sens usuel. En effet, on a $P \simeq P' \simeq L/Q$, qui est de type fini, puisque L l'est.

On peut définir de manière plus générale un R-module projectif comme étant un R-module isomorphe à un facteur direct d'un R-module libre (non nécessairement de rang fini). On peut alors démontrer qu'un R-module à la fois projectif et de type fini est projectif de type fini au sens de la définition précédente : autrement dit, si P est de type fini et projectif, on peut s'arranger pour choisir L de rang fini.

Comme nous n'aurons pas besoin de ceci dans cet article, nous renvoyons le lecteur à la littérature existante.

Exemples 6.5.

(1) Tout R-module libre de rang fini est projectif de type fini, mais la réciproque est fausse (cf. (3)).

(2) Si $S \in \mathrm{M}_n(R)$ vérifie $S^2 = S$, alors on démontre comme dans le cas d'un corps que $R^n = \mathrm{Im}(S) \oplus \mathrm{Ker}(S)$.

Ainsi, l'image et le noyau de S sont projectifs de type fini.

(3) Si θ est un automorphisme de R-algèbre de $\mathrm{M}_n(R)$, les considérations du paragraphe précédent montrent que le module M_θ est projectif de type fini.

En particulier, le R-module M_θ associé à l'automorphisme θ de l'exemple 1.3 est projectif de type fini, mais n'est pas libre.

Introduisons maintenant quelques notations.

Soit R un anneau commutatif, et soit $\mathfrak{m}$ l'unique idéal maximal de R. Si M est un R-module, on note $\mathfrak{m}{\cdot}M$ le sous-module de M engendré par les éléments de la forme $a{\cdot}x$, avec $a \in \mathfrak{m}$ et $x \in M$. Lorsque M est de type fini, engendré par des éléments $x_1, \ldots, x_m$, on constate aisément que $\mathfrak{m}{\cdot}M$ est combinaison linéaire de $x_1, \ldots, x_m$ à coefficients dans $\mathfrak{m}$.

On vérifie que l'application

$$\begin{aligned} R/\mathfrak{m} \times M/\mathfrak{m}{\cdot}M &\longrightarrow M/\mathfrak{m}{\cdot}M \\ (\overline{a}, \overline{x}) &\longmapsto \overline{a{\cdot}x} \end{aligned}$$

est bien définie, et induit sur le groupe abélien $M/\mathfrak{m}{\cdot}M$ une structure de $R/\mathfrak{m}$ -espace vectoriel, qui est de dimension finie dès que M est un R-module de type fini.

Si $p, q \geq 1$ sont des entiers, pour tout $A = (a_{ij})_{i,j} \in \mathrm{M}_{p\times q}(R)$, et tous $x_1, \ldots, x_q \in M$, on pose

$$A * \begin{pmatrix} x_1 \\ \vdots \\ x_q \end{pmatrix} = \begin{pmatrix} \displaystyle\sum_{k=1}^{q} a_{1k}{\cdot}x_k \\ \vdots \\ \displaystyle\sum_{k=1}^{q} a_{pk}{\cdot}x_k \end{pmatrix}.$$

On vérifie alors que si $A \in \mathrm{M}_{p\times q}(R)$ et $B \in \mathrm{M}_{q\times r}(R)$, alors, pour tous $x_1, \ldots, x_r \in M$, on a

$$A * (B * \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix}) = AB * \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix}.$$

Nous avons alors le théorème suivant.

Théorème 6.6. *Soit R un anneau local d'unique idéal maximal $\mathfrak{m}$, et soit P un R-module de type fini.*

Si $(\overline{v}_1, \ldots, \overline{v}_r)$ est une famille génératrice du $R/\mathfrak{m}$-espace vectoriel $P/\mathfrak{m}{\cdot}P$, alors $(v_1, \ldots, v_r)$ est une famille génératrice de P.

Si de plus P est un facteur direct de R^n et $(\overline{v}_1, \ldots, \overline{v}_r)$ est une $R/\mathfrak{m}$-base de $P/\mathfrak{m}{\cdot}P$, alors $(v_1, \ldots, v_r)$ est une R-base de P.

En particulier, tout R-module projectif de type fini est libre de rang fini.

Démonstration. Notons $\kappa = R/\mathfrak{m}$. Soit P un R-module de type fini, et soit $(x_1, \ldots, x_m)$ une famille génératrice de P.

Notons $(\overline{v}_1, \ldots, \overline{v}_r)$ une famille κ-génératrice de $P/\mathfrak{m}{\cdot}P$.

Pour tout $i \in [\![1, n]\!]$, on peut donc écrire

$$\overline{x}_i = \sum_{k=1}^{r} \overline{b}_{ik}{\cdot}\overline{v}_k, \ b_{ik} \in R.$$

On a alors $x_i - (\sum_{k=1}^{r} b_{ik}\cdot e_k) \in \mathfrak{m}\cdot P$, et par conséquent, on a

$$x_i = \sum_{\ell=1}^{m} a_{i\ell}\cdot x_\ell + \sum_{k=1}^{r} b_{ik}\cdot e_k,\ a_{i\ell} \in \mathfrak{m}.$$

Cela se récrit de manière plus compacte de la manière suivante :

$$(I_m - A) * \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = B * \begin{pmatrix} e_1 \\ \vdots \\ e_r \end{pmatrix},$$

où $A \in \mathrm{M}_m(R)$ est une matrice à coefficients dans $\mathfrak{m}$, et $B \in \mathrm{M}_{m\times r}(R)$.

En faisant agir $\mathrm{com}(I_m - A)^t$, on obtient

$$(\det(I_m - A)I_n) * \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \begin{pmatrix} \det(I_m - A)\cdot x_1 \\ \vdots \\ \det(I_m - A)\cdot x_m \end{pmatrix} = C * \begin{pmatrix} e_1 \\ \vdots \\ e_r \end{pmatrix},$$

où $C \in \mathrm{M}_{m\times r}(R)$. En réduisant modulo $\mathfrak{m}$, ou en développant le déterminant, on voit que $\det(I_m - A) = 1 + a$, avec $a \in \mathfrak{m}$. En particulier, $\det(I_m - A) \in A \setminus \mathfrak{m}$. Comme $\mathfrak{m}$ est l'unique idéal maximal de $\mathfrak{m}$, $\det(I_m - A) \in R^\times$. Mais alors, on obtient

$$\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \det(I_m - A)^{-1} C * \begin{pmatrix} e_1 \\ \vdots \\ e_r \end{pmatrix}.$$

Ainsi, $x_1, \ldots, x_m$ sont des combinaisons R-linéaires de $e_1, \ldots, e_r$. Comme $x_1, \ldots, x_m$ engendrent P, on en déduit que $e_1, \ldots, e_r$ engendrent P.

Supposons maintenant $R^n = P \oplus Q$. Il est donc en particulier de type fini d'après la remarque 6.4 (2). De même, Q est de type fini puisque $Q \simeq R^n/P$.

Il est facile de constater que $\mathfrak{m}\cdot R^n = \mathfrak{m}\cdot P \oplus \mathfrak{m}\cdot Q$, si bien que l'application évidente $P/\mathfrak{m}\cdot P \times Q/\mathfrak{m}\cdot Q \longrightarrow R^n/\mathfrak{m}\cdot R^n$ est un isomorphisme de κ-espaces vectoriels. Si r et s dénotent respectivement les dimensions de $P/\mathfrak{m}\cdot P'$ et $Q/\mathfrak{m}\cdot Q$, on a donc $r + s = n$, puisque $R^n/\mathfrak{m}\cdot R^n \simeq \kappa^n$.

Notons que $P/\mathfrak{m}\cdot P$ et $Q/\mathfrak{m}\cdot Q$ s'injectent canoniquement dans $R^n/\mathfrak{m}\cdot R^n$ et on peut identifier la classe d'un élément de P modulo $\mathfrak{m}\cdot P$ avec sa classe modulo $\mathfrak{m}\cdot R^n$, et de même pour Q.

Soit maintenant $(\overline{v}_1, \ldots, \overline{v}_r)$ une κ-base de $P/\mathfrak{m}\cdot P$ et soit $(\overline{v}_{r+1}, \ldots, \overline{v}_n)$ une κ-base de $Q/\mathfrak{m}\cdot Q$. L'isomorphisme canonique précédent montre alors que $(\overline{v}_1, \ldots, \overline{v}_n)$ est une κ-base de $R^n/\mathfrak{m}\cdot R^n$.

D'après le premier point, $v_1, \ldots, v_r$ engendrent P et $v_{s+1}, \ldots, v_n$ engendrent Q. Comme $R^n = P \oplus Q$, $v_1, \ldots, v_n$ engendrent R^n.

Si $(e_1, \ldots, e_n)$ est la base canonique de R^n, $(\overline{e}_1, \ldots, \overline{e}_n)$ est clairement une κ-base de $R^n/\mathfrak{m}\cdot R^n$. Si $A \in \mathrm{M}_n(R)$ est la matrice dont la j-ème colonne est v_j, sa réduction modulo $\mathfrak{m}$ est donc inversible. On a alors $\det(\overline{A}) \neq 0 \in A/\mathfrak{m}$.

Comme, $\det(\overline{A})$ n'est rien d'autre que la classe de $\det(A)$ modulo $\mathfrak{m}$, on a $\det(A) \in A \setminus \mathfrak{m}$. Comme précédemment, on en déduit que $\det(A) \in R^\times$ et A est donc inversible. Par conséquent, $(v_1, \ldots, v_n)$ est une R-base de R^n. En particulier, $(v_1, \ldots, v_r)$ est R-libre, et comme elle engendre P, c'est une base de P.

Enfin, supposons que P soit un R-module projectif de type fini.

En utilisant la remarque 6.4 (1), on peut donc écrire $R^n = P' \oplus Q$, où $P' \simeq P$. D'après le point précédent, P' est libre et a fortiori, P est libre. □

Puisque M_θ est projectif de type fini, le lemme 4.3 et la remarque 4.2 permettent alors d'obtenir immédiatement le résultat suivant.

Théorème 6.7. *Soit R un anneau local. Alors, pour tout entier $n \geq 1$ un entier, tout automorphisme d'algèbre de $\mathrm{M}_n(R)$ est intérieur.*

7. Rappels sur la localisation

On fait ici quelques rappels sur la localisation d'anneaux et de modules. le contenu de ce paragraphe peut être passé sans que cela nuise à la compréhension de la suite, pour peu qu'il admette la démonstration du lemme 8.2.

Définition 7.1. Soit R un anneau commutatif. Une partie S de R est dite *multiplicative* si elle est non vide et stable par multiplication.

Exemples 7.2.

(1) Si R est intègre, $R \setminus \{0\}$ est multiplicative

(2) Si R est un anneau commutatif non trivial et $\mathfrak{p}$ est un idéal premier, $R \setminus \mathfrak{p}$ est multiplicative, par définition même d'un idéal premier

(3) Si R est un anneau commutatif et $s \in R$, $\{s^n \mid n \geq 0\}$ est multiplicative.

Soit R un anneau commutatif, et soit S une partie multiplicative de R. Si M est un R-module, on définit une relation $\sim$ sur l'ensemble $M \times S$ de la façon suivante.

Pour tous $(x_1, s_1), (x_2, s_2) \in M \times S$, on dit que $(x_1, s_1) \sim (x_2, s_2)$ s'il existe $s' \in S$ tel que $s' \cdot (s_2 \cdot x_1 - s_1 \cdot x_2) = 0$.

On démontre que $\sim$ est une relation d'équivalence sur l'ensemble $M \times S$. La classe d'équivalence de (x, s) est notée $\dfrac{x}{s}$.

On vérifie alors que l'application

$$\begin{aligned} S^{-1}M \times S^{-1}M &\longrightarrow S^{-1}M \\ (\frac{x_1}{s_1}, \frac{x_2}{s_2}) &\longmapsto \frac{x_1}{s_1} + \frac{x_2}{s_2} = \frac{s_2 \cdot x_1 + s_1 \cdot x_2}{s_1 s_2} \end{aligned}$$

est bien définie, et induit sur $S^{-1}M$ une structure de groupe abélien, de neutre $\dfrac{0}{1}$.

En particulier, en considérant le R-module R, on obtient une loi interne sur $S^{-1}R$ définie par

$$\begin{aligned} S^{-1}R \times S^{-1}R &\longrightarrow S^{-1}R \\ (\frac{r_1}{s_1}, \frac{r_2}{s_2}) &\longmapsto \frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{s_2 r_1 + s_1 r_2}{s_1 s_2}, \end{aligned}$$

qui confère à $S^{-1}R$ une structure de groupe abélien. On vérifie alors que l'application

$$\begin{aligned} S^{-1}R \times S^{-1}R &\longrightarrow S^{-1}R \\ (\frac{r_1}{s_1}, \frac{r_2}{s_2}) &\longmapsto \frac{r_1}{s_1}\frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2} \end{aligned}$$

est bien définie, et induit sur le groupe abélien $(S^{-1}A, +)$ une structure d'anneau commutatif, de neutre multiplicatif $\frac{1}{1}$.

Enfin, on vérifie que l'application

$$\begin{aligned} S^{-1}R \times S^{-1}M &\longrightarrow S^{-1}M \\ (\frac{r}{s}, \frac{y}{t}) &\longmapsto \frac{r}{s}.\frac{y}{t} = \frac{r.y}{st} \end{aligned}$$

est bien définie et induit sur le groupe abélien $(S^{-1}M, +)$ une structure de $S^{-1}R$-module.

Définition 7.3. Soit S une partie multiplicative d'un anneau commutatif R, et soit M un R-module. L'anneau $S^{-1}R$ est appelé *le localisé de R en S*. De même, $S^{-1}M$ est appelé *le localisé de M en S*.

Exemples 7.4.

(1) Si R est un anneau intègre et $S = R \setminus \{0\}$, $S^{-1}R$ n'est rien d'autre que le corps des fractions de R.

En effet, notons que la relation d'équivalence définissant le corps de fractions est bien celle qui définit $S^{-1}R$ dans ce cas, puisque que l'on peut simplifier par s' par intégrité.

(2) Si R est un anneau commutatif et $S = R \setminus \mathfrak{p}$, où $\mathfrak{p}$ est un idéal premier, on note $R_{\mathfrak{p}}$ l'anneau obtenu.

L'anneau $R_{\mathfrak{p}}$ est alors un anneau local, d'unique idéal maximal $\mathfrak{p}R_{\mathfrak{p}} = \{\frac{r}{s} \mid r \in \mathfrak{p}, s \in R \setminus \mathfrak{p}\}$.

Remarquons tout d'abord que $\frac{1}{1} \notin \mathfrak{p}R_{\mathfrak{p}}$. En effet, dans le cas contraire, on aurait $\frac{1}{1} = \frac{r}{s}$, avec $r \in \mathfrak{p}, s \notin \mathfrak{p}$, et il existerait $s' \notin \mathfrak{p}$ tel que $s'(s - r) = 0$, soit $rs' = ss'$. Mais alors, on a une contradiction, puisque le membre de gauche est dans $\mathfrak{p}$, puisque $\mathfrak{p}$ est un idéal tandis que le membre de droite ne l'est pas, puisque $R \setminus \mathfrak{p}$ est multiplicative.

Si $\mathfrak{a}$ est un idéal de R contenant strictement $\mathfrak{p}R_{\mathfrak{p}}$, alors il contient un élément de la forme $\frac{r}{s}$, avec $r, s \notin \mathfrak{p}$. Mais un tel élément est inversible dans $R_{\mathfrak{p}}$, d'inverse $\frac{s}{r}$. Ainsi, $\mathfrak{a} = R_{\mathfrak{p}}$.

Si maintenant $\mathfrak{m}$ est un idéal maximal de $R_{\mathfrak{p}}$, le même genre d'arguments montre que $\mathfrak{m} \subset \mathfrak{p}R_{\mathfrak{p}}$ (car un idéal maximal est distinct de $R_{\mathfrak{p}}$, et donc ne peut contenir d'élément inversible). Par maximalité, $\mathfrak{m} = \mathfrak{p}R_{\mathfrak{p}}$.

Rappelons maintenant que si $f : M \longrightarrow N$ est une application R-linéaire, l'application

$$\begin{array}{rccc} S^{-1}f\colon & S^{-1}M & \longrightarrow & S^{-1}N \\ & \frac{x}{s} & \longmapsto & \frac{f(x)}{s} \end{array}$$

est bien définie, et est $S^{-1}R$-linéaire. Si de plus f est injective/surjective/bijective, il en est de même de $S^{-1}f$.

Si N est un sous-module d'un R-module M, l'inclusion $N \subset M$ induit donc une application $S^{-1}N \longrightarrow S^{-1}M$ injective, si bien que $S^{-1}N$ s'identifie canoniquement à un sous-module de $S^{-1}M$.

Enfin, si $M = M_1 \oplus \cdots \oplus M_r$, après identification canonique de chaque $S^{-1}M_i$ à un sous-module de $S^{-1}M$, on a alors $S^{-1}M = S^{-1}M_1 \oplus \cdots \oplus S^{-1}M_r$.

La même propriété vaut pour le produit direct externe : si on a un isomorphisme de R-modules $M \simeq M_1 \times \cdots \times M_r$, alors on a un isomorphisme de $S^{-1}R$-modules $S^{-1}M \simeq S^{-1}M_1 \times \cdots \times S^{-1}M_r$.

En particulier, $S^{-1}M^n \simeq (S^{-1}M)^n$.

Notations. Si R est un anneau et $S = R$
pp, où $\mathfrak{p}$ est un idéal premier de R, $S^{-1}R, S^{-1}M$ et $S^{-1}f$ seront respectivement notés $R_{\mathfrak{p}}$, $M_{\mathfrak{p}}$ et $f_{\mathfrak{p}}$.

On finit ce paragraphe en définissant le rang d'un module projectif. D'après le théorème 6.6 et l'exemple 7.4 (2), si P est un R-module projectif de type fini, pour tout idéal premier $P_{\mathfrak{p}}$ est un $R_{\mathfrak{p}}$-module libre de rang fini.

Si $\mathrm{Spec}(R)$ est l'ensemble des idéaux premiers de R, on obtient alors une application

$$\begin{array}{rccc} \mathrm{rg}(P)\colon & \mathrm{Spec}(R) & \longrightarrow & \mathbb{N} \\ & \mathfrak{p} & \longmapsto & \mathrm{rg}_{R_{\mathfrak{p}}}(P_{\mathfrak{p}}). \end{array}$$

Définition 7.5. Soit P un R-module projectif de type fini. On dit que P est *de rang constant* si l'application $\mathrm{rg}(P) : \mathrm{Spec}(R) \longrightarrow \mathbb{N}$ est constante.

Dans ce cas, on confondra l'application $\mathrm{rg}(P)$ avec sa valeur constante.

Autrement dit, un R-module projectif de type fini P sera de rang (constant) r si pour tout idéal premier $\mathfrak{p}$ de R, $P_{\mathfrak{p}}$ est un $R_{\mathfrak{p}}$-module libre de rang r.

Exemples 7.6.

(1) Supposons que l'on ait une décomposition en somme directe

$$R^n = M_1 \oplus \cdots \oplus M_n,$$

où tous les sous-modules M_i sont isomorphes à un même module M.

Alors, M est projectif de type fini de rang 1.

En effet, la projectivité de M découle de la définition. De plus, si $\mathfrak{p}$ est un idéal premier de R, on a

$$(R^n)_\mathfrak{p} = (M_1)_\mathfrak{p} \oplus \cdots \oplus (M_n)_\mathfrak{p}.$$

Mais, chaque M_i est isomorphe à M, et donc chaque $(M_i)_\mathfrak{p}$ est isomorphe à $M_\mathfrak{p}$. Ainsi, $\mathrm{rg}_{R_\mathfrak{p}}(M_i) = \mathrm{rg}_{R_\mathfrak{p}}(M)$ pour tout $i \in [\![1, n]\!]$. De plus, $(R^n)_\mathfrak{p} \simeq R_\mathfrak{p}^n$ est de rang n, d'où $n = n\mathrm{rg}_{R_\mathfrak{p}}(M_\mathfrak{p})$, soit $\mathrm{rg}_{R_\mathfrak{p}}(M) = 1$.

(2) Tout R-module M vérifiant $M^n \simeq R^n$ est un R-module projectif de type fini de rang 1.

En effet, si $\varphi : M^n \xrightarrow{\sim} R^n$ est un isomorphisme de R-modules, on vérifie que $R^n = M_1 \oplus \cdots \oplus M_n$, où $M_i = \{\varphi(0, \ldots, 0, x_i, 0, \ldots, 0) \mid x_i \in M\}$, chaque M_i étant isomorphe à M. On applique alors (1).

(3) Si θ est un automorphisme d'algèbre de $\mathrm{M}_n(R)$, M_θ est un module projectif de type fini de rang 1.

Cela découle en effet du point précédent et du théorème 3.5.

8. Le cas général

On revient au cas général. Le but de ce paragraphe est d'approfondir le lien entre les automorphismes d'algèbre de $\mathrm{M}_n(R)$ et les R-modules M vérifiant $M^n \simeq R^n$.

Dans la suite, on note $\mathscr{P}_n(R)$ l'ensemble des classes d'isomorphisme de R-modules M vérifiant $M^n \simeq R^n$, et on note $\mathrm{Out}(\mathrm{M}_n(R))$ l'ensemble des classes à gauche $\mathrm{Aut}(\mathrm{M}_n(R))/\mathrm{Int}(\mathrm{M}_n(R))$.

On se propose d'établir une bijection entre $\mathrm{Out}(\mathrm{M}_n(R))$ et $\mathscr{P}_n(R)$.

On sait déjà associer un élément de $\mathscr{P}_n(R)$ à un automorphisme d'algèbre θ de $\mathrm{M}_n(R)$, à savoir la classe de M_θ. Le lemme suivant montre la classe d'isomorphisme de M_θ ne dépend que de la classe de θ dans $\mathrm{Out}(\mathrm{M}_n(R))$.

Lemme 8.1. *Soient θ_1, θ_2 deux automorphismes d'algèbre de $\mathrm{M}_n(R)$. Supposons qu'il existe $P \in \mathrm{GL}_n(R)$ tel que $\theta_2 = \theta_1 \circ \mathrm{Int}(P)$. Alors, $M_{\theta_1} \simeq M_{\theta_2}$.*

Démonstration. Gardons les notations de l'énoncé. On a alors

$$\theta_2(E_{11}) = \theta_1(PE_{11}P^{-1}) = \theta_1(P)\theta_1(E_{11})\theta_1(P)^{-1}.$$

Le lemme 3.4 montre alors que $M_{\theta_1} \simeq M_{\theta_2}$. □

Si $[M]$ désigne la classe d'isomorphisme d'un R-module M, on a donc une application

$$\begin{array}{rccc} \alpha\colon & \mathrm{Out}(\mathrm{M}_n(R)) & \longrightarrow & \mathscr{P}_n(R) \\ & \overline{\theta} & \longmapsto & [M_\theta], \end{array}$$

bien définie en vertu du lemme précédent.

Nous allons maintenant construire une application en sens inverse. Pour cela, nous aurons besoin d'un lemme concernant l'anneau des endomorphismes d'un R-module vérifiant $M^n \simeq R^n$.

Lemme 8.2. *Soit M un R-module vérifiant $M^n \simeq R^n$. Alors, l'application*

$$\begin{aligned} R &\longrightarrow \mathrm{End}_R(M) \\ r &\longmapsto r{\cdot}\mathrm{Id}_M \end{aligned}$$

est un isomorphisme.

Démonstration. L'application de l'énoncé étant clairement linéaire, il reste donc à montrer sa bijectivité.

Soit $f : M \longrightarrow M$ un endomorphisme de M, et soit $\mathfrak{m}$ un idéal maximal de R. On sait que M est de type fini. Soient $x_1, \ldots, x_r \in M$ des générateurs de M.

Comme $M_\mathfrak{m}$ est un R-module libre de rang 1 d'après l'exemple 7.6 (2), on a $f_\mathfrak{m} = \lambda_\mathfrak{m}{\cdot}\mathrm{Id}_{M_\mathfrak{m}}$, avec $\lambda_\mathfrak{m} \in R_\mathfrak{m}$.

Écrivons $\lambda_\mathfrak{m} = \dfrac{r_\mathfrak{m}}{s_\mathfrak{m}}$, avec $s_\mathfrak{m} \in R \setminus \mathfrak{m}$. En calculant $f_\mathfrak{m}(\dfrac{x_i}{1})$, on en déduit que, pour tout $i \in [\![1, r]\!]$, il existe $t_{i,\mathfrak{m}} \in R \setminus \mathfrak{m}$ tel que $t_{i,\mathfrak{m}}{\cdot}(s_\mathfrak{m}{\cdot}f(x_i) - r_\mathfrak{m}{\cdot}x_i) = 0$.

Posons $t_\mathfrak{m} = t_{1,\mathfrak{m}} \cdots t_{r,\mathfrak{m}}$. Alors, $t_\mathfrak{m} \in R \setminus \mathfrak{m}$ et, en faisant agir $\prod_{j \neq i} t_{j,\mathfrak{m}}$, on peut écrire l'égalité précédente sous la forme

$$t_\mathfrak{m} s_\mathfrak{m}{\cdot}f(x_i) = t_\mathfrak{m} r_\mathfrak{m}{\cdot}x_i,$$

cette égalité étant valable pour tout $i \in [\![1, r]\!]$.

Remarquons que l'idéal engendré par les éléments $t_\mathfrak{m} s_\mathfrak{m}$ lorsque $\mathfrak{m}$ parcourt l'ensemble des idéaux maximaux, n'est contenu dans aucun idéal maximal de R, puisque pour chaque idéal maximal $\mathfrak{m}$, cet idéal contient au moins un élément en dehors de $\mathfrak{m}$, à savoir $t_\mathfrak{m} s_\mathfrak{m}$. Cet idéal est donc l'anneau R tout entier. On en déduit qu'il existe des éléments $u_\mathfrak{m} \in R$ presque tous nuls tels que $\sum_\mathfrak{m} u_\mathfrak{m}(t_\mathfrak{m} s_\mathfrak{m}) = 1$.

Mais alors, on obtient $f(x_i) = r{\cdot}x_i$ pour tout $i \in [\![1, r]\!]$, avec $r = \sum_\mathfrak{m} u_\mathfrak{m}(t_\mathfrak{m} s_\mathfrak{m})$.

Comme $x_1, \ldots, x_r$ engendrent M, on en déduit l'égalité $f(x) = r{\cdot}x$ pour tout $x \in M$, i.e. $f = r{\cdot}\mathrm{Id}_M$.

Il reste à démontrer que si $r{\cdot}\mathrm{Id}_M = 0$, alors $r = 0$. Si $r{\cdot}\mathrm{Id}_M = 0$, on a en particulier

$$r{\cdot}(x_1, \ldots, x_n) = (r{\cdot}x_1, \ldots, r{\cdot}x_n) = 0 \quad \text{pour tous } x_1, \ldots, x_n \in M.$$

En appliquant φ, on en déduit que $r{\cdot}v = 0$ pour tout $v \in R^n$. En prenant $v = (1, 0, \ldots, 0)$, on en déduit $r = 0$. □

Remarque 8.3. Pour le lecteur ayant lu le paragraphe sur la localisation : ce lemme est en fait valable pour tout R-module projectif de rang 1.

Corollaire 8.4. *Soit M un R-module vérifiant $M^n \simeq R^n$.*

Pour tout $A = (a_{ij}) \in \mathrm{M}_n(R)$, l'application

$$\begin{array}{rccl} \mu_A\colon & M^n & \longrightarrow & M^n \\ & (x_1,\dots,x_n) & \longmapsto & (\sum_{j=1}^n a_{1j}\cdot x_j,\dots,\sum_{j=1}^n a_{nj}\cdot x_j) \end{array}$$

est un endomorphisme de M^n, et l'application

$$\begin{array}{rcl} \mu\colon \mathrm{M}_n(R) & \longrightarrow & \mathrm{End}_R(M^n) \\ A & \longmapsto & \mu_A \end{array}$$

est un isomorphisme de R-algèbres.

Démonstration. Il est clair que μ_A est R-linéaire, et de simples calculs montrent que μ est un morphisme d'algèbres. Il reste donc à vérifier sa bijectivité.

Soit $u \in \mathrm{End}_R(M^n)$. Il existe donc des applications linéaires $u_1,\dots,u_n : M^n \longrightarrow M$ telles que $u(x) = (u_1(x),\dots,u_n(x))$ pour tout $x \in M^n$. Pour tous $x_1,\dots,x_n \in M$, on a

$$u(x_1,\dots,x_n) = \sum_{i=1}^n\sum_{j=1}^n (0,\dots,0,u_i(0,\dots,0,x_j,0,\dots,0),0,\dots,0).$$

L'application

$$\begin{array}{rcl} u_{ij}\colon M & \longrightarrow & M \\ x_j & \longmapsto & u_i(0,\dots,x_j,0,\dots,0) \end{array}$$

est un endomorphisme de M, donc de la forme $a_{ij}\cdot\mathrm{Id}_M$ d'après le lemme 8.2. On a alors

$$u(x_1,\dots,x_n) = \sum_{i=1}^n (0,\dots,0,\sum_{j=1}^n a_{ij}\cdot x_j,0,\dots,0) = (\sum_{j=1}^n a_{1j}\cdot x_j,\dots,\sum_{j=1}^n a_{nj}\cdot x_j)$$

pour tous $x_1,\dots,x_n \in M$, soit $u = \mu_A$. Ainsi, μ est surjective.

Montrons l'injectivité de μ. Supposons que $\mu_A = 0$. En calculant $\mu_A(0,\dots,0,x,0,\dots,0)$, où x est en k-ème position, on en déduit que $a_{ik}\cdot x = 0$ pour tous $i,k \in [\![1,n]\!]$ et tout $x \in M$, i.e. $a_{ik}\cdot\mathrm{Id}_M = 0$ pour tous $i,k \in [\![1,n]\!]$. Le lemme 8.2 montre alors que $a_{ik} = 0$ pour tous $i,k \in [\![1,n]\!]$. Ainsi, $A = 0$. □

Soit M un R-module vérifiant $M^n \simeq R^n$. On se fixe un isomorphisme $\varphi : M^n \xrightarrow{\sim} R^n$. Pour tout $A \in \mathrm{M}_n(R)$, on pose $\theta_{M,\varphi}(A) = \varphi \circ \mu_A \circ \varphi^{-1} \in \mathrm{End}_R(R^n)$. Autrement dit, c'est l'unique endomorphisme de R^n tel que

$$\theta_{M,\varphi}(A)(\varphi(x_1,\dots,x_n)) = (\sum_{j=1}^n a_{1j}\cdot x_j,\dots,\sum_{j=1}^n a_{nj}\cdot x_j) \text{ pour tous } x_1,\dots,x_n \in M.$$

Dans la suite, on confondra un endomorphisme de R^n avec sa matrice représentative dans la base canonique, si bien que l'on peut voir $\theta_{M,\varphi}$ comme une application de $\mathrm{M}_n(R)$ dans elle-même.

Lemme 8.5. *L'application $\theta_{M,\varphi}$ est un automorphisme d'algèbre de $\mathrm{End}_R(R^n)$, dont la classe dans $\mathrm{Out}(\mathrm{M}_n(R))$ ne dépend que de la classe d'isomorphisme de M.*

Démonstration. On vérifie aisément que $\theta_{M,\varphi}$ est un morphisme de R-algèbres. L'isomorphisme $\varphi : M^n \xrightarrow{\sim} R^n$ induit un isomorphisme d'algèbres

$$\begin{aligned}\mathrm{End}_R(M^n) &\xrightarrow{\sim} \mathrm{End}_R(R^n)\\ u &\longmapsto \varphi \circ u \circ \varphi^{-1}.\end{aligned}$$

Montrer la bijectivité de $\theta_{M,\varphi}(A)$ revient donc à vérifier que tout endomorphisme $u \in \mathrm{End}_R(M^n)$ s'écrit de manière unique sous la forme $u = \mu_A$, ce qui est donné par le corollaire 8.4.

Montrons maintenant que $\overline{\theta}_{M,\varphi}$ est indépendante de φ.

Soient $\varphi_1, \varphi_2 : M^n \xrightarrow{\sim} R^n$ deux isomorphismes. Posons $\rho = \varphi_1^{-1} \circ \varphi_2$. C'est un automorphisme de M^n. Comme un automorphisme d'algèbre induit par double restriction un isomorphisme entre les groupes des inversibles, le lemme 8.2 montrer que $\rho = \mu_P$, où $P \in \mathrm{GL}_n(R)$.

On a donc $\varphi_2 = \varphi_1 \circ \mu_P$ et $\varphi_2^{-1} = \mu_{P^{-1}} \circ \varphi_1^{-1}$. Mais alors, pour tout $A \in \mathrm{M}_n(R)$, on a

$$\theta_{M,\varphi_2}(A) = \varphi_1 \circ \mu_P \circ \mu_A \circ \mu_{P^{-1}} \circ \varphi_1^{-1} = \varphi_1 \circ \mu_{PAP^{-1}} \circ \varphi_1^{-1} = \theta_{M,\varphi_1}(PAP^{-1}).$$

Autrement dit, $\theta_{M,\varphi_2} = \theta_{M,\varphi_1} \circ \mathrm{Int}(P)$ et ainsi $\overline{\theta}_{M,\varphi_2} = \overline{\theta}_{M,\varphi_1}$.

Revenons au cas général. Soit M un R-module vérifiant $M^n \simeq R^n$. Nous voulons démontrer que si $M \simeq N$, alors pour tout isomorphisme $\varphi : M^n \xrightarrow{\sim} R^n$ et tout isomorphisme $\psi : N^n \xrightarrow{\sim} R^n$, on a $\overline{\theta}_{M,\varphi} = \overline{\theta}_{N,\psi}$.

D'après le point précédent, on peut remplacer φ par un isomorphisme de notre choix. Soit $f : M \xrightarrow{\sim} N$ un isomorphisme. On pose

$$\begin{aligned}\varphi\colon \quad M^n &\longrightarrow R^n\\ (x_1, \dots, x_n) &\longmapsto \psi(f(x_1), \dots, f(x_n)).\end{aligned}$$

Nous allons montrer l'égalité $\theta_{M,\varphi} = \theta_{N,\psi}$ pour ce choix de φ. Comme l'image de φ est R^n tout entier, il suffit de montrer l'égalité

$$\theta_{M,\varphi}(A)(\varphi(x_1, \dots, x_n)) = \theta_{N,\psi}(A)(\varphi(x_1, \dots, x_n))$$

pour tout $A \in \mathrm{M}_n(R)$, et tous $x_1, \dots, x_n \in M$.

Or, en utilisant la définition de φ et la linéarité de f, on a

$$\theta_{M,\varphi}(A)(\varphi(x_1, \dots, x_n)) = \varphi(\sum_{j=1}^n a_{1j} \cdot x_j, \dots, \sum_{j=1}^n a_{nj} \cdot x_j) = \psi(\sum_{j=1}^n a_{1j} \cdot f(x_j), \dots, \sum_{j=1}^n a_{nj} \cdot f(x_j))$$

d'une part, et d'autre part

$$\theta_{N,\psi}(A)(\varphi(x_1, \dots, x_n)) = \theta_{N,\psi}(A)(\psi(f(x_1), \dots, f(x_n))) = \psi(\sum_{j=1}^n a_{1j} \cdot f(x_j), \dots, \sum_{j=1}^n a_{nj} \cdot f(x_j)),$$

d'où l'égalité voulue. □

Le lemme précédent montre que l'on peut définir une application

$$\begin{aligned}\beta\colon \mathscr{P}_n(R) &\longrightarrow \mathrm{Out}(\mathrm{M}_n(R))\\ [M] &\longmapsto \overline{\theta}_{M,\varphi},\end{aligned}$$

où M est n'importe quel représentant de la classe d'isomorphisme $[M]$ et $\varphi : M^n \xrightarrow{\sim} R^n$ est un isomorphisme arbitraire.

On a alors le théorème suivant.

Théorème 8.6. *L'application*

$$\begin{array}{rcl} \alpha\colon \mathrm{Out}(\mathrm{M}_n(R)) & \longrightarrow & \mathscr{P}_n(R) \\ \overline{\theta} & \longmapsto & [M_\theta], \end{array}$$

est bijective, d'inverse

$$\begin{array}{rcl} \beta\colon \mathscr{P}_n(R) & \longrightarrow & \mathrm{Out}(\mathrm{M}_n(R)) \\ [M] & \longmapsto & \overline{\theta}_{M,\varphi}. \end{array}$$

Démonstration. Commençons par démontrer que $\alpha \circ \beta = \mathrm{Id}_{\mathscr{P}_n(R)}$. Soit M un R-module tel que $M^n \simeq R^n$, et soit $\varphi : M^n \xrightarrow{\sim} R^n$ un isomorphisme. On doit démontrer que $M_{\theta_{M,\varphi}} \simeq M$, soit encore $\mathrm{Im}(\theta_{M,\varphi}(E_{11})) \simeq M$. Par définition, on a

$$\theta_{M,\varphi}(E_{11})(\varphi(x_1,\dots,x_n)) = \varphi(x_1,0,\dots,0) \ \text{ pour tous } x_1,\dots,x_n \in M.$$

Ainsi, l'image de $\theta_{M,\varphi}(E_{11})$ est égale à l'image de l'application linéaire

$$\begin{array}{rcl} M & \longrightarrow & R^n \\ x & \longmapsto & \varphi(x,0,\dots,0). \end{array}$$

Or, cette application est injective, puisque φ l'est. Ainsi, son image est isomorphe à M, d'où le résultat voulu.

Il découle de l'égalité $\alpha \circ \beta = \mathrm{Id}_{\mathscr{P}_n(R)}$ que β est injective. Nous allons maintenant montrer que $\beta \circ \alpha = \mathrm{Id}_{\mathrm{Out}(\mathrm{M}_n(R))}$.

Il faut donc montrer que si θ est un automorphisme de $\mathrm{M}_n(R)$, $\theta_{M_\theta,\varphi}$ est conjugué à θ, où $\varphi : M_\theta^n \xrightarrow{\sim} R^n$ est un isomorphisme de R-modules.

Soit θ un automorphisme d'algèbre de $\mathrm{M}_n(R)$. D'après le théorème 3.5, l'application

$$\begin{array}{rcl} \varphi\colon \quad M_\theta^n & \longrightarrow & R^n \\ (x_1,\dots,x_n) & \longmapsto & \displaystyle\sum_{k=1}^n F_{k1}x_k \end{array}$$

est un isomorphisme de R-modules, où $F_{j1} = \theta(E_{j1})$.

Pour tous $x_1,\dots,x_n \in M_\theta$, on a

$$\theta_{M_\theta,\varphi}(E_{ij})(\varphi(x_1,\dots,x_n)) = \varphi(0,\dots,0,x_j,0,\dots,0),$$

où x_j est en i-ème position. Par conséquent,

$$\theta_{M_\theta,\varphi}(E_{ij})(\varphi(x_1,\dots,x_n)) = F_{i1}x_j.$$

Mais on a aussi

$$F_{ij}\varphi(x_1,\dots,x_n) = F_{ij}\sum_{k=1}^n F_{k1}x_k = F_{ij}F_{j1}x_j = F_{i1}x_j.$$

On en déduit donc l'égalité $\theta_{M,\varphi}(E_{ij}) = F_{ij} = \theta(E_{ij})$, et ce, pour tous $i,j \in [\![1,n]\!]$. Comme les matrices élémentaires E_{ij} forment une base de $\mathrm{M}_n(R)$, on en conclut que $\theta_{M,\varphi} = \theta$, ce qui suffit à conclure. $\square$