## 2. Classes d'équivalence de matrices sur un anneau principal

Soient $A$ un anneau *commutatif* et $n \geqslant 1$ un entier. On rappelle l'anneau des matrices $\mathrm{M}_n(A)$, ainsi que son groupe des inversibles $\mathrm{GL}_n(A) := \mathrm{M}_n(A)^\times$. Dans cette généralité on dispose d'une application polynomiale

$$\det : \mathrm{M}_n(A) \to A,\ (m_{i,j}) \mapsto \sum_{\sigma \in \mathrm{S}_n} \varepsilon(\sigma) \prod_{j=1}^{n} m_{\sigma(j),j},$$

qui généralise la définition bien connue pour $A = \mathbb{C}$ (voire $A$ un corps). Par définition, $M \mapsto \det M$ est une fonction multi-$A$-linéaire des lignes et des colonnes de $M$, qui est également alternée pour la même raison que dans le cas des corps.

Lemme 2.1. *Pour tout anneau commutatif $A$, et tout $M, N \in \mathrm{M}_n(A)$ on a*

$$\det MN \ = \ \det M \det N \ \text{ et } \ M\,{}^t\mathrm{Co}(M) \ = \ {}^t\mathrm{Co}(M)\,M = \det M \ 1_n.$$

Démonstration — Ce sont des identités polynomiales en les $2n^2$ entrées $m_{i,j}$ et $n_{i,j}$ de $M$ et $N$, à coefficients entiers. Elle sont bien connues pour $A = \mathbb{C}$. En utilisant qu'un polynôme $P \in \mathbb{C}[X_1, \ldots, X_r]$ est identiquement nul si, et seulement si, on a $P(x_1, \ldots, x_r) = 0$ pour tout $x_1, \ldots, x_r \in \mathbb{C}$, on en déduit que le lemme vaut pour tout anneau $A$ de la forme $\mathbb{Z}[X_1, \ldots, X_r]$.

Si on a un morphisme d'anneaux commutatifs $\varphi : A \to B$, et si on note $\varphi_n : \mathrm{M}_n(A) \to \mathrm{M}_n(B)$ le morphisme d'anneaux défini par $\varphi_n((m_{i,j}) = (\varphi(m_{i,j}))$, alors pour tout $M \in \mathrm{M}_n(A)$ on a $\det \varphi_n(M) = \varphi(\det M)$ et $\varphi_n({}^t\mathrm{Co}(M)) = {}^t\mathrm{Co}(\varphi_n(M))$. On en déduit que si le lemme est vrai pour le triplet $(A, M, N)$, il est vrai pour le triplet $(B, \varphi_n(M), \varphi_n(N))$.

Soient enfin $B$ un anneau commutatif général ainsi que $M', N' \in \mathrm{M}_n(B)$. Posons $A = \mathbb{Z}[\{X_{i,j}\}_{1 \leqslant i,j \leqslant n}, \{Y_{i,j}\}_{1 \leqslant i,j \leqslant n}]$, $M = (X_{i,j})_{1 \leqslant i,j \leqslant n}$ et $N = (Y_{i,j})_{1 \leqslant i,j \leqslant n}$ : le lemme est vrai pour le triplet $(A, M, N)$ par le premier paragraphe. Soit $\varphi : A \to B$ le morphisme d'anneaux envoyant $X_{i,j}$ sur $m_{i,j}$ et $Y_{i,j}$ sur $n_{i,j}$. On a $\varphi_n(M) = M'$, $\varphi_n(N) = N'$ et donc le lemme est vrai pour le triplet $(B, M', N')$. □

Proposition 2.2. *Pour tout anneau commutatif $A$ on a*

$$\mathrm{GL}_n(A) = \{M \in \mathrm{M}_n(A) \mid \det M \in A^\times\}.$$

Démonstration — Pour $M \in \mathrm{M}_n(A)$, il existe $N \in \mathrm{M}_n(A)$ avec $MN = 1_n$. On en déduit $\det M \det N = \det 1_n = 1$ par le Lemme 2.1. Comme on a $\det M, \det N \in A$, on en déduit $\det M \in A^\times$. Réciproquement, si on a $\det M \in A^\times$ on constate que $N := (\det M)^{-1}\ {}^t\mathrm{Co}(M)$ est un inverse de $M$ dans $\mathrm{M}_n(A)$ par le Lemme 2.1. □

Par le Lemme 2.1, on dispose d'un morphisme de groupes $\det : \mathrm{GL}_n(A) \to A^\times$, manifestement surjectif (considérer des matrices diagonales). Son noyau est particulièrement important :

Définition 2.3. *On note $\mathrm{SL}_n(A)$ le noyau du morphisme $\det : \mathrm{GL}_n(A) \to A^\times$. C'est un sous-groupe distingué de $\mathrm{GL}_n(A)$.*

On fixe $p, q \geqslant 1$ et on s'intéresse à l'action du groupe $\mathrm{GL}_p(A) \times \mathrm{GL}_q(A)$ sur $\mathrm{M}_{p,q}(A)$, définie par $(P, Q).M = PMQ^{-1}$. Deux matrices $M, N \in \mathrm{M}_{p,q}(A)$ dans la même orbite pour cette action sont dites *équivalentes* (à ne pas confondre avec la conjugaison !). Le résultat principal de cette section est la description des classes d'équivalence quand $A$ est un anneau principal. Cette énoncé a une riche histoire, avec des contributions de Gauss, Smith, Frobenius, Jordan...

THÉORÈME 2.4. (Forme normale de Smith) *Soient $A$ un anneau principal et $M \in \mathrm{M}_{p,q}(A)$ avec $p, q \geqslant 1$, et $r = \min(p, q)$. Il existe $P \in \mathrm{GL}_p(A)$, $Q \in \mathrm{GL}_q(A)$, ainsi que $a_1, a_2, \dots a_r \in A$ uniques modulo association, avec $a_1 \mid a_2 \mid \cdots \mid a_r$ et*

$$PMQ = \begin{bmatrix} a_1 & & & & \\ & a_2 & & & \\ & & \ddots & & \\ & & & a_r & \end{bmatrix} \text{ (avec des 0 partout ailleurs).} \tag{66}$$

(La situation dessinée est celle avec $r = p$.) Noter qu'il est très possible d'avoir $a_i = 0$, par exemple pour $M = 0$ !, mais qu'alors on a $a_j = 0$ pour tout $j \geqslant i$.

DÉFINITION 2.5. *Les éléments $a_i \in A$ non nuls ci-dessus, uniques modulo $A^\times$, sont appelés* facteurs invariants *de la matrice $M \in \mathrm{M}_{p,q}(A)$.*

Avant de débuter la démonstration du théorème, revisitons les *opérations sur les lignes et les colonnes*. Pour $\lambda \in A$, et pour $1 \leqslant i \neq j \leqslant n$, on dispose des *transvections standards* $\mathrm{T}_{i,j}(\lambda) := \mathrm{I}_n + \lambda \mathrm{E}_{i,j}$. Ce sont des éléments de $\mathrm{SL}_n(A)$. Pour $M \in \mathrm{M}_{n,m}(A)$, la matrice $\mathrm{T}_{i,j}(\lambda)M$ est obtenue à partir de $M$ en ajoutant à la ligne $i$ de $M$, $\lambda$ fois la ligne $j$ de $M$. De même (en transposant !), pour $M \in \mathrm{M}_{m,n}(A)$, $M\,\mathrm{T}_{i,j}(\lambda)$ est obtenue à partir de $M$ en ajoutant à la colonne $j$ de $M$, $\lambda$ fois la colonne $i$ de $M$. Pour $1 \leqslant i < j \leqslant n$, on dispose d'un morphisme de groupes naturel

$$f_n^{i,j} : \mathrm{GL}_2(A) \to \mathrm{GL}_n(A),\ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{array}{c} \\ i \\ \\ j \\ \\ \end{array} \begin{array}{c} \begin{array}{cccc} i & & j & \end{array} \\ \begin{bmatrix} \mathrm{I}_{i-1} & \vdots & & \vdots & \\ \cdots & a & & b & \\ & & \mathrm{I}_{j-i-1} & & \\ \cdots & c & & d & \\ & & & & \mathrm{I}_{n-j} \end{bmatrix} \end{array}. \tag{67}$$

On a par exemple $f_n^{i,j}(\begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}) = \mathrm{T}_{i,j}(\lambda)$ et $f_n^{i,j}(\begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix}) = \mathrm{T}_{j,i}(\lambda)$ pour $\lambda \in A$. De plus, pour $M \in \mathrm{M}_{n,m}(A)$ et $\tau = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, on constate que $f_n^{i,j}(\tau)M$ est la matrice obtenue à partir de $M$ en échangeant les lignes $i$ et $j$. Idem pour $Mf_n^{i,j}(\tau)$ quand $M \in \mathrm{M}_{m,n}(A)$.

DÉMONSTRATION — (de l'existence) Pour $a \in A$ non nul on note $\nu(a) \in \mathbb{N}$ le nombre de facteurs irréductibles de $a$, et on pose $\nu(0) = +\infty$. On peut supposer $M = (m_{i,j})$ non nulle et on pose aussi $\nu(M) = \inf_{i,j} \nu(m_{i,j})$. On procède par récurrence sur le couple $(p + q, \nu(M)) \in \mathbb{N}^2$ pour l'ordre lexicographique, qui est un bon ordre. [3] On a $p + q \geqslant 2$. Le cas $p + q = 2$ (initialisation), qui force $p = q = 1$, est trivial. Soit

3. Merci aux étudiants d'avoir suggéré ceci en classe !

$(i_0, j_0)$ tel que $\nu(m_{i_0,j_0}) = \nu(M)$. Quitte à effectuer des transpositions des lignes $1, i_0$ et des colonnes de $1, j_0$ de $M$, on peut supposer $(i_0, j_0) = (1, 1)$.

**(Cas 1)** Il existe $j > 1$ tel que $m_{1,1}$ ne divise pas $m_{1,j}$. Comme $A$ est principal, $m_{1,1}$ et $m_{1,j}$ ont un pgcd, disons $d$, et on a alors $\nu(d) < \nu(m_{1,1})$. De plus, il existe $u, v \in A$ avec $m_{1,1}u - m_{1,j}v = d$. La matrice

$$Q = \begin{bmatrix} u & m_{1,j}/d \\ v & m_{1,1}/d \end{bmatrix}$$

est donc dans $\mathrm{SL}_2(A)$, et le coefficient $(1, 1)$ de $M' := Mf_q^{1,j}(Q)$ vaut $d$. On a donc $\nu(M') < \nu(M)$ et $M' \sim M$, et on conclut par récurrence.

**(Cas 2)** Il existe $i > 1$ tel que $m_{1,1}$ ne divise pas $m_{i,1}$. On conclut de même par récurrence (ou en transposant l'argument ci-dessus).

**(Cas 3)** Dans le cas restant, $m_{1,1}$ divise $m_{i,1}$ et $m_{1,j}$ pour tout $1 \leqslant i \leqslant q$ et $1 \leqslant j \leqslant p$. En multipliant $M$ à gauche successivement par les transvections $\mathrm{T}_{1,i}(-m_{i,1}/m_{1,1})$ pour $i = 2, \ldots, p$, ce qui ne modifie à chaque fois que la $i$-ème ligne de $M$, on peut alors supposer successivement sans changer la première ligne (et en particulier $m_{1,1}$), que l'on a $m_{1,j} = 0$ pour $j = 2, \ldots, q$. Puis en multipliant de même des transvections bien choisies à droite, on peut supposer en plus $m_{1,j} = 0$ pour $j = 2, \ldots, q$, sans changer $m_{1,1}$. Noter qu'après chacune des $p + q - 2$ opérations ci-dessus, on peut toujours supposer que la matrice $M'$ obtenue vérifie $\nu(M') = \nu(m_{1,1})$. En effet, $m_{1,1}$ en est un coefficient, et si on a $\nu(M') < \nu(m_{1,1})$ on conclut par récurrence.

Dans les cas particulier $p = 1$ ou $q = 1$, on a manifestement terminé. Considérons un coefficient $m_{k,l}$ avec $k, l > 1$ n'est pas divisible par $m_{1,1}$. S'il on ajoute à $M$ sa $k$-ème ligne, on obtient une matrice équivalente $M'$ avec de coefficients $(1, 1)$ et $(1, l)$ égaux à $m_{1,1}$ et $m_{k,l}$, avec $m_{1,1}$ ne divisant pas $m_{k,l}$. L'argument du Cas 1 montre que $M'$ est équivalente à une matrice $M''$ avec $\nu(M'') < \nu(m_{1,1})$, et on conclut par récurrence.

On peut donc supposer que tous les coefficients $m_{k,l}$ avec $k, l > 1$ sont divisibles par $m_{1,1}$. Alors le bloc $[2, p] \times [2, q]$ de $M$ est de la forme $m_{1,1}N$ avec $N \in \mathrm{M}_{p-1,q-1}(A)$. On applique alors l'hypothèse de récurrence à $N$, et on conclut par un calcul par blocs immédiat. □

La démonstration de l'unicité nécéssitera une définition préliminaire. L'anneau $A$ y est à nouveau commutatif quelconque. Fixons $M = (m_{i,j}) \in \mathrm{M}_{p,q}(A)$. Rappelons que pour $1 \leqslant k \leqslant \min(p, q)$, un *mineur de taille* $k$ de $M$ est un élément de $A$ de la forme $\pm \det M_{I,J}$, où $I \subset \{1, \ldots, p\}$ et $J \subset \{1, \ldots, q\}$ sont des sous-ensembles de cardinal $k$ et $M_{I,J}$ désigne la matrice extraite $(m_{i,j})_{(i,j) \in I \times J}$.

Définition 2.6. *Soit $A$ un anneau commutatif, $M \in \mathrm{M}_{p,q}(A)$ et $k \in \mathbb{Z}$. Le contenu d'ordre $k$ de $M$ l'idéal $\mathrm{c}_k(M)$ de $A$ engendré par les mineurs de taille $k$ de $M$, avec les conventions $\mathrm{c}_k(M) = A$ pour $k \leqslant 0$ et $\mathrm{c}_k(M) = \{0\}$ pour $k > \min(p, q)$.*

Par exemple, on a $\mathrm{c}_1(M) = \sum_{i,j} A\, m_{i,j}$ (*idéal pgcd des coefficients de $M$*).

Lemme 2.7. *Soient $A$ un anneau commutatif, ainsi que $M, N \in \mathrm{M}_{p,q}(A)$ deux matrices équivalentes. Pour tout $k \in \mathbb{Z}$ on a $\mathrm{c}_k(M) = \mathrm{c}_k(N)$.*

Démonstration — On peut supposer $k \leqslant \min(p,q)$. Vérifions $\mathrm{c}_k(MN) \subset \mathrm{c}_k(M)$ pour tout $M \in \mathrm{M}_{p,q}(A)$ et tout $N \in \mathrm{M}_q(A)$. On a $(MN)_{i,j} = \sum_{r=1}^{q} m_{i,r} n_{r,j}$, de sorte que si $\mathrm{col}_j(X)$ désigne la $j$-ème colonne de la matrice $X$, cette égalité s'écrit aussi $\mathrm{col}_j(MN) = \sum_{r=1}^{q} n_{r,j}\,\mathrm{col}_r(M)$. Le caractère multi-$A$-linéaire alterné de det montre alors que pour $I \subset \{1,\dots,p\}$ et $J \subset \{1,\dots,q\}$ de tailles $k$ on a

$$\det(MN)_{I,J} \quad \in \quad \sum_{K \subset \{1,\dots,q\}} A\ \det M_{I,K},$$

la somme portant sur les parties $K$ à $k$ éléments[4] de $\{1,\dots,q\}$. On en déduit $\mathrm{c}_k(MN) \subset \mathrm{c}_k(M)$. On en tire $\mathrm{c}_k(M) = \mathrm{c}_k(MQ)$ pour $Q \in \mathrm{GL}_q(A)$, car $\mathrm{c}_k(M) = \mathrm{c}_k(MQQ^{-1}) \subset \mathrm{c}_k(MQ) \subset \mathrm{c}_k(M)$. On a de même en travaillant sur les lignes (ou en transposant) $\mathrm{c}_k(PM) = \mathrm{c}_k(M)$ pour $P \in \mathrm{GL}_p(A)$. □

Démonstration — (Assertion d'unicité du Théorème 2.4, seule l'hypothèse $A$ intègre sera utilisée) Par le Lemme 2.7, et comme $A$ est intègre, il suffit de montrer que pour $D \in \mathrm{M}_{p,q}(A)$ diagonale de coefficients $a_1 \,|\, a_2 \,|\, \dots \,|\, a_r$ on a $\mathrm{c}_k(D) = a_1 a_2 \dots a_k A$ pour $1 \leqslant k \leqslant r$. L'inclusion $a_1 a_2 \dots a_k A \subset \mathrm{c}_k(M)$ est évidente en considérant le mineur d'indices $1 \leqslant i,j \leqslant k$. Réciproquement, pour $I, J$ de taille $k$ quelconques on a $\det D_{I,J} = 0$ sauf pour $I = J$, auquel cas on a $\det D_{I,I} = \prod_{i \in I} a_i$, qui est bien divisible par $a_1 a_2 \dots a_k$ dans $A$. □

## 3. Modules de type fini sur un anneau principal

Soient $A$ un anneau commutatif, ainsi que $E$ et $F$ deux $A$-modules. On suppose $E$ et $F$ libres de rangs finis, disons respectivement $q$ et $p$, et on se donne $u : E \to F$ une application $A$-linéaire. Soit $e_1,\dots,e_q$ une base de $E$ et $f_1,\dots,f_p$ une base de $F$. Il existe une unique matrice $(u_{i,j}) \in \mathrm{M}_{p,q}(A)$ telle que $u(e_j) = \sum_{i=1}^{p} u_{i,j} f_i$ pour tout $1 \leqslant j \leqslant q$. C'est la *matrice de $u$ dans les bases $e$ et $f$*, notée $\mathrm{Mat}_{e,f} u$. Bien sûr, comme $e$ et $f$ sont des bases de $E$ et $F$, toute $M \in \mathrm{M}_{p,q}(A)$ est même la matrice d'une unique application $A$-linéaire $F \to E$. Cette discussion matricielle est strictement identique à celle bien connue dans le cadre des espaces vectoriels. En particulier, si on a une autre application $A$-linéaire $v : F \to G$ avec $G$ libre de rang $o$, et $g = (g_1,\dots,g_o)$ une $A$-base de $G$, on vérifie immédiatement l'identité matricielle

$$\mathrm{Mat}_{e,g}\, v \circ u \;=\; \mathrm{Mat}_{f,g} v\ \mathrm{Mat}_{e,f} u.$$

Cette formule implique d'abord que pour $E = F$ et $u$ l'identité alors $\mathrm{P}_{e,f} := \mathrm{Mat}_{e,f}\mathrm{id}_E$ est dans $\mathrm{GL}_p(A)$ (*matrice de passage de $f$ vers $e$*), et d'inverse $\mathrm{P}_{f,e}$. Ensuite, elle montre que si $e'$ est une autre base à $q$ éléments de $E$, et si $f'$ est une autre base à $p$ éléments de $F$, on a

$$\mathrm{Mat}_{e',f'} u \;=\; P\ \mathrm{Mat}_{e,f}\, u\ \ Q,$$

avec $Q = \mathrm{P}_{e',e} \in \mathrm{GL}_q(A)$ et $P = \mathrm{P}_{f,f'} \in \mathrm{GL}_p(A)$. On déduit de cette discussion et du Théorème 2.4 le :

4. On peut raffiner l'analyse ci-dessus pour obtenir une formule plus précise appelée *formule de Cauchy-Binet*.

THÉORÈME 3.1. (Théorème de la base adaptée pour les applications linéaires) *Soient $E$ et $F$ des $A$-modules et $u : E \to F$ une application $A$-linéaire. On suppose $A$ principal, $E$ et $F$ libres sur $A$ de rangs respectifs $q$ et $p$. Alors il existe une base $e = (e_1, \dots, e_q)$ de $E$, une base $f = (f_1, \dots, f_p)$ de $F$, et des éléments non nuls $a_1, \dots, a_r \in A$ avec $r = \min(p, q)$ et $a_1 \,|\, a_2 \,|\, \dots \,|\, a_r$, vérifiant*

$$u(f_i) = a_i e_i \text{ pour } i \leqslant r, \text{ et } u(f_i) = 0 \text{ pour } i > r.$$

Une seconde version de ce théorème concerne les sous-modules d'un module libre de type fini sur un anneau principal.

THÉORÈME 3.2. (Théorème de la base adaptée pour les sous-modules) *Soient $A$ un anneau principal, $M$ un $A$-module libre de rang fini $m$, et $N$ un sous-module de $M$. Il existe une base $e_1, \dots, e_m$ de $M$, un entier $0 \leqslant s \leqslant m$, et des éléments $a_1, \dots, a_s \in A$ non nuls, tels que :*

*(i) $a_1 e_1,\ a_2 e_2,\ \dots,\ a_s e_s$ est une base de $N$.*

*(ii) $a_1 \mid a_2 \mid \cdots \mid a_s$.*

*En particulier, $N$ est libre sur $A$ de rang $s \leqslant n$.*

Le cas particulier $A = \mathbb{Z}$ du Théorème 3.2 est déjà intéressant, et n'avait pas été démontré au chapitre 3.

DÉMONSTRATION — On peut supposer $M$ non nul, et donc $n \geqslant 1$, sinon il n'y a rien à démontrer. Comme un anneau principal est noethérien, on sait que $N$ est de type fini par le Théorème 1.17. On peut donc trouver un entier $n \geqslant 1$ une application $A$-linéaire $u : A^n \to M$ avec $\operatorname{Im} u = N$. Posons $r = \min(m, n)$. D'après le Théorème 3.1, il existe une base $e_1, \dots, e_n$ de $A^n$, et une base $f_1, \dots, f_m$ de $M$, ainsi que $a_1 \mid a_2 \mid \cdots \mid a_r$, tels que $u(e_i) = a_i f_i$ pour $i \leqslant r$ et $u(e_i) = 0$ pour $i > r$. Soit $s$ le plus grand entier $1 \leqslant i \leqslant r$ tel que $a_i$ est non nul (s'il n'en existe pas, on pose $s = 0$, et c'est que l'on a $N = \{0\}$). On a $N = u(\sum_{i=1}^m Af_i) = \sum_{i=1}^p Aa_i e_i$, et les $a_i e_i$ sont $A$-libres car les $e_i$ le sont (et les $a_i$ sont non nuls). □

THÉORÈME 3.3. *Soient $A$ un anneau principal et $M$ un $A$-module de type fini. Il existe un unique entier $r \geqslant 0$, appelé rang de $M$, un unique entier $s \geqslant 0$, et des éléments non nuls $a_1, \dots, a_s \in A$, uniques modulo association, avec*

$$M \simeq A^r \times A/a_1A \times A/a_2A \times \cdots \times A/a_sA,\ \ a_1 \mid a_2 \mid \cdots \mid a_s \text{ et } a_1 \notin A^\times$$

Les éléments $a_i$ ci-dessus sont appelés *facteurs invariants de $M$*. Quand $s = 0$, l'énoncé signifie simplement $M \simeq A^r$, *i.e.* que $M$ est libre de rang $r$.

DÉMONSTRATION — (de la partie existence) Comme $M$ est un $A$-module de type fini, on peut trouver un entier $m \geqslant 1$ et une application $A$-linéaire surjective $u : A^m \to M$. Cela montre $M \simeq A^m/\ker u$. On conclut [5] l'existence en appliquant le théorème de la base adaptée au sous-module $\ker u$ du $A$-module libre $A^m$. □

5. Il est clair que que si on a $M = \prod_{i=1}^m M_i$ avec les $M_i$ des $A$-modules, et si pour tout $i$ on a $N_i$ un sous-$A$-module de $M_i$, alors la projection canonique $M \to \prod_{i=1}^m M_i/N_i, (m_i) \mapsto (m_i + N_i)$, a pour noyau $N := \prod_{i=1}^m N_i$, et donc induit un isomorphisme $M/N \simeq \prod_{i=1}^m M_i/N_i$.

Pour démontrer l'unicité, nous pourrions procéder par un argument très similaire à celui du cas $A = \mathbb{Z}$ démontré en détail dans le Chapitre 3, c'est pourquoi l'argument a été omis en classe. Nous renvoyons au Complément 5 pour deux démonstrations détaillées. Terminons plutôt par une application à la réduction des endomorphismes.

THÉORÈME 3.4. *Soient $k$ un corps et $V$ un $k$-espace vectoriel de dimension finie.*

*(i) Pour tout endomorphisme $u$ de $V$, il existe une unique entier $s \leqslant \dim V$ et une unique suite de polynômes $P_1, \dots, P_s \in k[X]$ unitaires de degré $\geqslant 1$ avec $P_1 \,|\, P_2 \,|\, \cdots |P_s$, tels que dans une base $e$ convenable de $V$ on ait*

$$\mathrm{Mat}_e u = \begin{bmatrix} \mathrm{C}(P_1) & & & \\ & \mathrm{C}(P_2) & & \\ & & \ddots & \\ & & & \mathrm{C}(P_s) \end{bmatrix}.$$

Les polynômes $P_1, \dots, P_s$ sont appelés *invariants de similitude* de $u$.

*(ii) Deux endomorphismes de $V$ sont conjugués si, et seulement si, ils ont même invariants de similitudes.*

DÉMONSTRATION — Pour $u \in \mathrm{End}_k(V)$, on considère le $k[X]$-module $V_u$. Il est de dimension finie comme $k$-espace vectoriel, donc *a fortiori* de type fini comme $k[X]$-module. On peut donc lui appliquer le Théorème 3.3. Il est de rang nul car il ne possède aucun sous-module isomorphe à $k[X]$ (de dimension infinie comme $k$-espace vectoriel). Le (i) et (ii) se déduisent alors de ce théorème et des Exemples 1.10 et 1.14. □

REMARQUE 3.5. (i) Comme la matrice compagnon $\mathrm{C}(P)$ a pour polynôme caractéristique $P$, on constate que le produit $P_1 \dots P_s$ des invariants de similitudes de $u$ est le polynôme caractéristique de $u$. De plus, le polynôme $P_s$ est le polynôme minimal de $u$.

(ii) Cet énoncé contient la *décomposition de Jordan*. En effet, dans le cas particulier où $u$ est nilpotent, les $P_i$ sont de la forme $X^{p_i}$, et $\mathrm{C}(P_i)$ est alors un *bloc de Jordan*.

(iii) Soit $u$ un endomorphisme d'un $k$-espace vectoriel $V$ de dimension $n$, et soit $M \in \mathrm{M}_n(k)$ la matrice de $u$ dans une certaine base de $V$. On peut montrer que les invariants de similitude de $u$ sont les facteurs invariants non inversibles de la matrice $M - X1_n$ de $\mathrm{M}_n(k[X])$ (voir l'Exercice 8.18). Comme $k[X]$ est euclidien, cela fournit un procédé algorithmique pour déterminer les invariants de similitude de $u$.

(iv) Si on a $u \in \mathrm{M}_n(k)$ et si $K$ est un surcorps de $k$, l'assertion d'unicité montre que les invariants de similitude de $u$ sont les même que ceux de $u$ vu dans $\mathrm{M}_n(K)$. On en déduit que si $u$ et $u'$ sont dans $\mathrm{M}_n(k)$, et s'ils sont conjugués dans $\mathrm{M}_n(K)$, alors ils sont conjugués dans $\mathrm{M}_n(k)$. (Un énoncé pas si facile à démontrer directement, notamment si $k$ est fini).