

Compléments et errata à

Algèbre et géométrie

81 thèmes pour l'Agrégation de mathématiques

Jean Fresnel Michel Matignon

p. 44, ligne 8, remplacer cette ligne par la suivante.

sance du stabilisateur de $DQ(\sigma)$ dans les cas de la décomposition $LDQ(\sigma)U$ que le stabilisa-

p. 80, à propos du paragraphe I.8.

1. Actualité des résultats sur $\mathbb{R}$

Si V est un sous-espace vectoriel de $M_n(\mathbb{R})$ tel que $V - \{0\} \subset Gl_n(\mathbb{R})$, alors on sait que le maximum possible pour la dimension de V est le nombre de Hurwitz-Radon défini comme il suit.

Si $n = 2^{4a+b}(2m+1)$ avec a, b, m entiers $a \geq 0$, $0 \leq b \leq 3$, alors
$$\rho(n) := 8a + 2^b.$$

L'existence de sous-espaces vectoriels V de $M_n(\mathbb{R})$ tels que $V - \{0\} \subset Gl_n(\mathbb{R})$, est associé à l'existence d'algèbres de Clifford qui sont des algèbres d'endomorphismes d'espaces vectoriels sur $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, i.e. les réels, les complexes, les quaternions. Si bien qu'on obtient des dimensions un peu supérieures à celles obtenues en 4. à 11. ([P] p. 272 à 273).

Le problème de la borne maximum de la dimension des espaces vectoriels V a été résolu en 1962 par un article de **J. F. Adams** concernant les champs de vecteurs tangents à la sphère ([A]).

[A] **Adams J. F.** *Vector fields on spheres* Annals of Math. 75 (1962) 603-632

[P] **Porteous I. R.** *Topological Geometry* 1969 Van Nostrand Reinhold company

2. Une question plus générale

Soient K un corps commutatif, $n \geq 1$, $1 \leq k \leq n$, V est un sous-espace vectoriel de $M_n(K)$ tel que tout élément de $V - \{0\}$ est de rang supérieur ou égal à k . Alors que peut-on dire de la dimension de V ?

Facilement, on a $\dim V \leq n(n-k+1)$.

En effet, soit $\rho: V \rightarrow M_{n-k+1,n}(K)$ définie par

$$\rho([m_{i,j}]) := \begin{bmatrix} m_{1,1} & m_{1,2} & \cdots & m_{1,n} \\ m_{2,1} & m_{2,2} & \cdots & m_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n-k+1,1} & \vdots & \cdots & m_{n-k+1,n} \end{bmatrix}. \text{ Si on avait}$$

$\dim V > n(n-k+1)$, on aurait alors $\ker \rho \neq \{0\}$; cela veut dire que V contiendrait une matrice non nulle de rang strictement plus petit que k , ce qui est une contradiction.

Remarque 1. On peut considérer le même type de questions en remplaçant sous-espace vectoriel V de $M_n(K)$ par sous-espace vectoriel V de $M_{n,p}(K)$.

Remarque 2. On peut considérer le même type de questions en remplaçant sous-espace vectoriel V par sous-espace affine E de $M_n(K)$.

Dans ce cas les résultats sont plus simples parce qu'ils ne dépendent pas essentiellement de la nature du corps commutatif K (voir [S]).

[S] de Seguin Pazzis C. *Large affine spaces of matrices with rank bounded below* Linear Algebra Appl. 437 (2012) 499-512

Page 145, complément

Famille de transpositions génératrice de $\mathfrak{S}_n$ et connexité du graphe associé

Définition du graphe associé à une famille finie de transpositions

Soit $n \geq 2$, $\mathfrak{S}_n$ le groupe des permutations de l'ensemble $\{1, 2, \dots, n\}$. Soit $\Lambda \neq \emptyset$ une famille finie de transpositions de $\mathfrak{S}_n$. Alors le graphe $G(\Lambda)$ associé à Λ est le graphe dont l'ensemble des *sommets* est $S := \bigcup_{t \in \Lambda} \text{support}(t)$, sachant que si t est la transposition $t = (a, b)$, alors $\text{support}(t) = \{a, b\}$.

Par ailleurs les *arêtes du graphe* $G(\Lambda)$ sont définies comme il suit : si $x, y \in S$, il y a une arête qui relie x et y si et seulement si $x \neq y$ et si la transposition (x, y) est élément de Λ . Ainsi donc l'ensemble des arêtes du graphe $G(\Lambda)$ s'identifie aux parties $\{x, y\}$ à deux éléments de S telles que la transposition (x, y) est un élément de Λ .

Soit $x, y \in S$, un *chemin qui relie* x à y est une suite finie $(a_1, a_2, \dots, a_r)$ d'éléments de S telle que $a_1 = x$, $a_r = y$ et $\{a_k, a_{k+1}\}$ est une arête pour $1 \leq k < r$.

Soit $x \in S$, on appelle *composante connexe de* x l'ensemble des $y \in S$ pour lesquels il existe un chemin qui relie x à y . En particulier, on dit que le graphe $G(\Lambda)$ est *connexe*, s'il existe un point $x \in S$ tel que la composante connexe de x soit S ; c'est équivalent de dire que pour tout $x, y \in S$, $x \neq y$, il existe un chemin qui relie x à y .

Théorème Soient $n \geq 2$, $\mathfrak{S}_n$ le groupe des permutations de l'ensemble $\{1, 2, \dots, n\}$, Λ une famille finie, non vide de transpositions de $\mathfrak{S}_n$ et $G(\Lambda)$ le graphe associé à Λ selon la définition ci-dessus.

Alors les propriétés suivantes sont équivalentes.

- i) La famille Λ engendre le groupe $\mathfrak{S}_n$,
- ii) le graphe $G(\Lambda)$ a pour ensemble de sommets $\{1, 2, \dots, n\}$ et le graphe $G(\Lambda)$ est connexe selon la définition ci-dessus.

Démonstration

1) Montrons i) implique ii).

1.1) Montrons que 1 est un sommet du graphe $G(\Lambda)$.

Sinon $1 \notin \text{support}(t)$ pour tout $t \in \Lambda$, ainsi $t(1) = 1$ pour tout $t \in \Lambda$. Comme Λ engendre $\mathfrak{S}_n$, il suit que $\sigma(1) = 1$ pour tout $\sigma \in \mathfrak{S}_n$; ce qui est une contradiction, en particulier pour le cycle $\sigma = (1, 2, \dots, n)$.

De la même façon k est un sommet si $1 \leq k \leq n$.

1.2) Montrons que $G(\Lambda)$ est connexe.

Soit A la composante connexe de 1, selon la définition ci-dessus. Il s'agit de montrer que $A = \{1, 2, \dots, n\}$. Supposons le contraire, on a donc $\{1, 2, \dots, n\} = A \cup B$ avec $B \neq \emptyset$. Il suit de la définition de la composante connexe de 1 que pour tout $t \in \Lambda$, on a $\text{support}(t) \subset A$ ou $\text{support}(t) \subset B$. Il suit de cela que pour tout $t \in \Lambda$, on a $t(A) = A$ et $t(B) = B$. Comme Λ engendre $\mathfrak{S}_n$, on a aussi pour tout $\sigma \in \mathfrak{S}_n$, $\sigma(A) = A$ et $\sigma(B) = B$. Cela donne une contradiction en considérant $\sigma = (1, 2, \dots, n)$ et $\sigma^k(1)$ pour $1 \leq k \leq n$.

2) Montrons ii) implique i).

Soit H le sous-groupe de $\mathfrak{S}_n$ engendré par Λ . Il suffit de montrer que $(1, k) \in H$ pour $2 \leq k \leq n$ puisque l'on sait que la

famille $\{(1, k) \mid 2 \leq k \leq n\}$ engendre $\mathfrak{S}_n$ (Fr.E. corollaire 2.2.1.3.4.).

Il suit du lemme ci-après qu'il existe un chemin $(b_1, b_2, \dots, b_s)$ qui relie 1 à k avec $1 = b_1$, $k = b_s$, $b_1 \notin \{b_2, b_3, \dots, b_s\}$ et $(b_i, b_{i+1}) \in \Lambda$ pour $1 \leq i < s$. On a donc $(b_1, b_2) \in H$, et sachant que b_1 est invariant par (b_2, b_3) , on a

$$(b_2, b_3)(b_1, b_2)(b_2, b_3)^{-1} = (b_1, b_3) \in H.$$

De même $(b_3, b_4)(b_1, b_3)(b_3, b_4)^{-1} = (b_1, b_4) \in H$. Ainsi par récurrence, on a $(b_1, b_s) \in H$, i.e. $(1, k) \in H$.

Lemme Soient x, y deux sommets de $G(\Lambda)$ avec $x \neq y$. On suppose en plus qu'il existe un chemin qui relie x à y . Alors il existe un chemin $(b_1, b_2, \dots, b_s)$ avec $b_1 = x$, $b_s = y$ et $b_1 \notin \{b_2, b_3, \dots, b_s\}$.

Démonstration Soit $(a_1, a_2, \dots, a_r)$ un chemin qui relie x à y , i.e. $x = a_1$, $y = a_r$ et $(a_i, a_{i+1}) \in \Lambda$ pour $1 \leq i < r$. Comme $a_1 \neq a_r$, il existe un plus grand entier $j < r$ tel que $a_j = a_1$. Ainsi $a_j \notin \{a_{j+1}, a_{j+2}, \dots, a_r\}$ et $(a_{j+1}, a_{j+2}, \dots, a_r)$ est un chemin qui relie $a_1 = a_j = x$ à $a_r = y$ avec les propriétés du lemme.

Remarque Les propriétés suivantes sont équivalentes.

- i) L'ensemble des sommets du graphe $G(\Lambda)$ est $\{1, 2, \dots, n\}$,
- ii) $\{k \in \{1, 2, \dots, n\} \mid t(k) = k \text{ pour tout } t \in \Lambda\} = \emptyset$.

[Fr. E.] Fresnel J. *Groupes* (Hermann 2001)

p. 302 paragraphe V.2.1.

La démonstration de 2) de la ligne -4 p. 302 à la ligne 16 p. 303.

On peut avantageusement remplacer cette démonstration (qui est juste) par la suivante.

Par ([Fr. F] théorème 7.7.1.7. p. 268) on sait que

$$R(X) = F(X, Y) U(X, Y) + G(X, Y) V(X, Y)$$

avec $(U(X, Y), V(X, Y)) \neq (0, 0)$ et $\deg_Y U(X, Y) < m$,
 $\deg_Y V(X, Y) < n$.

Supposons $R(X) = 0$, on a donc

$$(1) \quad F(X, Y) U(X, Y) = -G(X, Y) V(X, Y).$$

Sachant que $\mathbb{C}[X, Y]$ est intègre, on a donc $U(X, Y) \neq 0$ et $V(X, Y) \neq 0$. Et de plus

$$(2) \quad \deg_Y F(X, Y) + \deg_Y U(X, Y) = \deg_Y G(X, Y) + \deg_Y V(X, Y).$$

Sachant de plus que $\mathbb{C}[X, Y]$ est factoriel, et que $F(X, Y)$ et $G(X, Y)$ n'ont pas de facteur irréductible en commun, il suit de (1) que $G(X, Y)$ divise $U(X, Y)$ dans $\mathbb{C}[X, Y]$.

Sachant que $U(X, Y) \neq 0$, cela veut dire que

$$\deg_Y G(X, Y) \leq \deg_Y U(X, Y),$$

ce qui est une contradiction.

Ainsi l'hypothèse $R = 0$ est à rejeter.

[Fr. F.] Fresnel J. *Anneaux* (Hermann 2001)

.

p. 306 paragraphe V.2.2.

La démonstration de 3) de la ligne 3 p. 306 à la ligne -2 p. 306.

On peut avantageusement remplacer cette démonstration (qui est juste) par la suivante.

3) Soit $R(X, Y, Z)$ le résultant de $\tilde{F}$, $\tilde{G}$ en degré n et m considérés comme polynômes de la variable T à coefficients dans $\mathbb{C}[X, Y, Z]$.

Montrons que $R(X, Y, Z) \neq 0$ et que $\deg R(X, Y, Z) = nm$. En

Par ([Fr. F] théorème 7.7.1.7. p. 268) on sait que

$$R(X, Y, Z) = \tilde{F}(X, Y, Z, T) U(X, Y, Z, T) + \tilde{G}(X, Y, Z, T) V(X, Y, Z, T)$$

avec $(U(X, Y, Z, T), V(X, Y, Z, T)) \neq (0, 0)$ et

$$\deg_T U(X, Y, Z, T) < m, \deg_T V(X, Y, Z, T) < n.$$

Supposons $R(X, Y, Z) = 0$, on a donc

$$(1) \quad \tilde{F}(X, Y, Z, T) U(X, Y, Z, T) = -\tilde{G}(X, Y, Z, T) V(X, Y, Z, T).$$

Sachant que $\mathbb{C}[X, Y, Z, T]$ est intègre, on a donc

$$U(X, Y, Z, T) \neq 0 \text{ et } V(X, Y, Z, T) \neq 0. \text{ Et de plus}$$

$$(2) \quad \deg_T \tilde{F}(X, Y, Z, T) + \deg_T U(X, Y, Z, T) = \deg_T \tilde{G}(X, Y, Z, T) + \deg_{YT} V(X, Y, Z, T).$$

Sachant de plus que $\mathbb{C}[X, Y, Z, T]$ est factoriel, et par 2) que

$\tilde{F}(X, Y, Z, T)$ et $\tilde{G}(X, Y, Z, T)$ n'ont pas de facteur irréductible en commun, il suit de (1) que $\tilde{G}(X, Y, Z, T)$ divise $U(X, Y, Z, T)$ dans $\mathbb{C}[X, Y, Z, T]$.

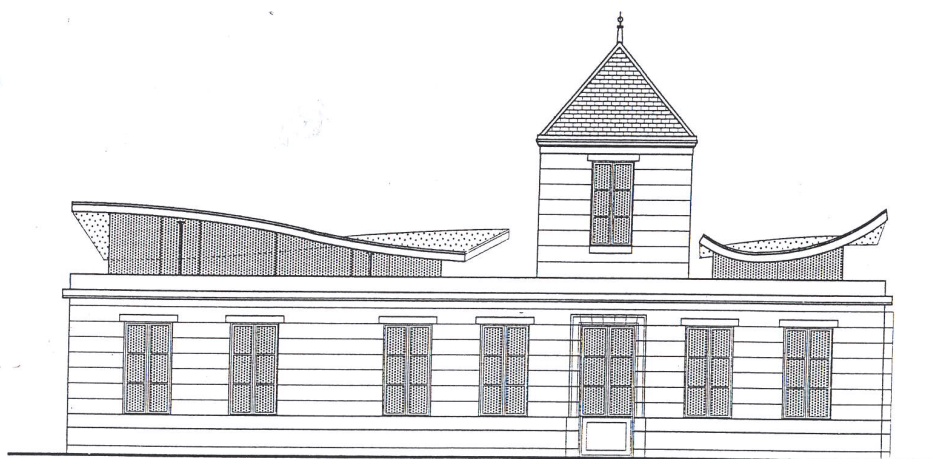
Sachant que $U(X, Y, Z, T) \neq 0$, cela veut dire que

$$\deg_T \tilde{G}(X, Y, Z, T) \leq \deg_T U(X, Y, Z, T),$$

ce qui est une contradiction.

Ainsi l'hypothèse $R=0$ est à rejeter.

[Fr. F.] Fresnel J. *Anneaux* (Hermann 2001)



*Bibliothèque Diophante d'Alexandrie
de l'Ecole mathématique et informatique de l'Université de Bordeaux*