Matrices circulantes

Marc Lorenzi

10 avril 2021

Dans cet article, n désigne un entier naturel non nul. On note (en caractères gras) $\mathbf{n} = [\![0, n-1]\!]$.

Les indices de ligne et de colonne des matrices seront, contrairement à l'usage hélas répandu, numérotés à partir de 0. Toutes les matrices considérées appartiendront à $\mathcal{M}_n(\mathbb{C})$, leurs indices seront donc des éléments de $\mathbf{n}$.

1 Une algèbre de matrices

1.1 Opérations modulaires

Pour tous entiers $i, j \in \mathbf{n}$, nous noterons $i \oplus j$ l'unique entier $k \in \mathbf{n}$ tel que $i + j \equiv k \bmod n$. De même $i \ominus j$ est l'unique entier $k \in \mathbf{n}$ tel que $i - j \equiv k \bmod n$.

On vérifie aisément que $(\mathbf{n}, \oplus)$ est un groupe abélien, isomorphe au groupe $(\mathbb{Z}/n\mathbb{Z}, +)$. L'opération $\ominus$ correspond à la soustraction dans $\mathbb{Z}/n\mathbb{Z}$. Les deux opérations $\oplus$ et $\ominus$ vérifient ainsi toutes les propriétés souhaitables. Nous utiliserons par exemple un peu plus loin

$$(i \ominus j) \ominus k = i \ominus (j \oplus k)$$

Nous aurons à faire fréquemment des changements d'indices du type « $k = i \ominus j$ », où $i, j \in \mathbf{n}$ et i est fixé. Lorsque j décrit $\mathbf{n}$, k décrit aussi $\mathbf{n}$. Ainsi, via ce changement d'indice,

$$\sum_{j=0}^{n-1} a_{i \ominus j} = \sum_{k=0}^{n-1} a_k$$

Il en serait de même pour des changements d'indices du type $k = j \ominus i$ ou $k = i \oplus j$.

1.2 Matrices circulantes

Pour tout $a = (a_0, \ldots, a_{n-1}) \in \mathbb{C}^n$, soit

$$\Gamma(a) = \begin{pmatrix} a_0 & a_1 & a_2 & \ldots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \ldots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \ldots & a_{n-3} \\ \ldots & & & & \\ a_1 & a_2 & a_3 & \ldots & a_0 \end{pmatrix} = (a_{j \ominus i})_{i,j \in \mathbf{n}}$$

On note

$$E = \{\Gamma(a), a \in \mathbb{C}^n\}$$

Les matrices $\Gamma(a)$ sont appelées les *matrices circulantes d'ordre n.*

Proposition 1. *E est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{C})$ de dimension n. L'application $\Gamma : \mathbb{C}^n \to \mathcal{M}_n(\mathbb{C})$ qui à tout vecteur $a \in \mathbb{C}^n$ associe $\Gamma(a)$ est un isomorphisme d'espaces vectoriels de $\mathbb{C}^n$ sur E.*

Démonstration. Il est clair que pour tous $a, b \in \mathbb{C}^n$ et tout $\lambda \in \mathbb{C}$, $\Gamma(a + b) = \Gamma(a) + \Gamma(b)$ et $\Gamma(\lambda a) = \lambda\Gamma(a)$.

Ainsi, Γ est linéaire et donc, $E = \operatorname{Im}\Gamma$ est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{C})$.

Γ est injectif. En effet, si $a \in \mathbb{C}^n$ vérifie $\Gamma(a) = 0$, alors la première ligne de la matrice $\Gamma(a)$ est nulle, donc $a = 0$. En tant qu'injection linéaire, Γ conserve les dimensions, donc

$$\dim E = \dim \Gamma(\mathbb{C}^n) = \dim \mathbb{C}^n = n$$

□

Proposition 2. *E est une sous-algèbre commutative de $\mathcal{M}_n(\mathbb{C})$ de dimension n.*

Démonstration. Il reste à montrer les propriétés relatives à la multiplication.

Remarquons que $I = \Gamma(1, 0, \ldots, 0) \in E$.

Montrons maintenant que E est stable pour la multiplication. Soient $A = \Gamma(a)$ et $B = \Gamma(b)$ deux éléments de E. On a pour tous $i, j \in \mathbf{n}$,

$$(AB)_{ij} = \sum_{k=0}^{n-1} A_{ik} B_{kj} = \sum_{k=0}^{n-1} a_{k \ominus i} b_{j \ominus k}$$

En particulier, notons

$$c_j = (AB)_{0j} = \sum_{k=0}^{n-1} a_k b_{j\ominus k}$$

Nous avons

$$\begin{aligned} c_{j\ominus i} &= \sum_{k=0}^{n-1} a_k b_{(j\ominus i)\ominus k} \\ &= \sum_{k=0}^{n-1} a_k b_{j\ominus(i\oplus k)} \end{aligned}$$

Par la remarque faite au début de l'article au sujet des opérations modulo n, le changement d'indice $k' = i \oplus k$ donne

$$\sum_{k=0}^{n-1} a_k b_{j\ominus(i\oplus k)} = \sum_{k'=0}^{n-1} a_{k'\ominus i} b_{j\ominus k'} = (AB)_{ij}$$

Ainsi,

$$AB = \Gamma(c_0, \ldots, c_{n-1}) \in E$$

Il reste à voir que la multiplication dans E est commutative. Reprenons l'égalité

$$c_j = \sum_{k=0}^{n-1} a_k b_{j\ominus k}$$

et faisons le changement d'indice $k' = j \ominus k$. Il vient

$$c_j = \sum_{k'=0}^{n-1} b_{k'} a_{j\ominus k'}$$

Ainsi, $BA = \Gamma(c_0, \ldots, c_{n-1}) = AB$ $\square$

1.3 Une matrice de Vandermonde

Posons $\omega = e^{2i\pi/n}$ et

$$\Omega = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \omega & \omega^2 & \ldots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \ldots & \omega^{(n-1)2} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \ldots & \omega^{(n-1)(n-1)} \end{pmatrix} = (\omega^{ij})_{i,j\in\mathbf{n}}$$

La matrice Ω est une matrice de Vandermonde. Son déterminant est donc

$$\det \Omega = \prod_{0 \leq i < j < n} (\omega^j - \omega^i) \neq 0$$

Livrons nous à un petit calcul. Calculons le produit $\Omega\overline{\Omega}$. On a pour tous $i, j \in \mathbf{n}$

$$\begin{aligned}(\Omega\overline{\Omega})_{ij} &= \sum_{k=0}^{n-1} \Omega_{ik}\overline{\Omega}_{kj} \\ &= \sum_{k=0}^{n-1} \omega^{ik}\omega^{-kj} \\ &= \sum_{k=0}^{n-1} \omega^{(i-j)k}\end{aligned}$$

Si $i \neq j$, $\omega^{i-j} \neq 1$ et donc

$$(\Omega\overline{\Omega})_{ij} = \frac{\omega^{n(i-j)} - 1}{\omega^{i-j} - 1} = 0$$

car ω^{i-j} est une racine $n$ième de l'unité.

Si $i = j$, $\omega^{i-j} = 1$ et donc

$$(\Omega\overline{\Omega})_{ij} = n$$

Ainsi,

$$\Omega\overline{\Omega} = nI$$

On retrouve le fait que Ω est inversible. De plus, l'inverse de Ω est

$$\Omega^{-1} = \frac{1}{n}\overline{\Omega}$$

Remarquons pour finir que l'on obtient par ce calcul un renseignement sur $\det \Omega$. En effet

$$\det(\Omega\overline{\Omega}) = \det \Omega \ \overline{\det \Omega} = |\det \Omega|^2 = \det(nI) = n^n$$

d'où

$$|\det \Omega| = \sqrt{n^n}$$

Ainsi, $\det \Omega = z\sqrt{n^n}$ où z est un nombre complexe de module 1. On peut montrer que $z \in \{\pm 1, \pm i\}$ et même obtenir la valeur précise de z selon les valeurs de n, mais ceci est une autre histoire ...

La matrice Ω intervient dans de nombreux domaines, en particulier en théorie du signal, dans ce que l'on appelle la Transformation de Fourier Discrète (DFT).

1.4 Le déterminant des matrices circulantes

Soit $A = \Gamma(a_0, \ldots, a_{n-1}) \in E$. Calculons $A\Omega$. Pour $i, j \in \mathbf{n}$,

$$\begin{aligned}(A\Omega)_{ij} &= \sum_{k=0}^{n-1} A_{ik}\Omega_{kj} \\ &= \sum_{k=0}^{n-1} a_{k\ominus i}\omega^{kj} \\ &= \omega^{ij}\sum_{k=0}^{n-1} a_{k\ominus i}\omega^{(k\ominus i)j}\end{aligned}$$

La dernière ligne résulte du fait que ω est une racine $n$ième de l'unité, et donc

$$\omega^{kj} = \omega^{(k\ominus i)j\oplus ij} = \omega^{(k\ominus i)j+ij}$$

Revenons à la somme. Par le changement d'indice $k' = k \ominus i$,

$$(A\Omega)_{ij} = \omega^{ij}\sum_{k'=0}^{n-1} a_{k'}\omega^{k'j} = \omega^{ij}\varphi_j(A)$$

où l'on a posé

$$\varphi_j(A) = \sum_{k=0}^{n-1} a_k\omega^{kj}$$

On constate ainsi qu'en appelant C'_j la $j$ième colonne de $A\Omega$ et C_j la $j$ième colonne de Ω,

$$C'_j = \varphi_j(A)C_j$$

Ainsi, par n-linéarité du déterminant,

$$\det(A\Omega) = \det(C'_1, \ldots, C'_n) = \left(\prod_{j=0}^{n-1}\varphi_j(A)\right)\det(C_1, \ldots, C_n) = \left(\prod_{j=0}^{n-1}\varphi_j(A)\right)\det\Omega$$

De plus, $\det(A\Omega) = \det A \det\Omega$, donc

$$\det A \det\Omega = \left(\prod_{j=0}^{n-1}\varphi_j(A)\right)\det\Omega$$

Comme $\det\Omega \neq 0$, il vient finalement

$$\det A = \prod_{j=0}^{n-1}\varphi_j(A)$$

2 Une base de formes linéaires

2.1 Rappel

Pour tout $j \in \mathbf{n}$, nous disposons de l'application $\varphi_j : E \to \mathbb{C}$ définie par

$$\varphi_j(A) = \sum_{k=0}^{n-1} a_k \omega^{kj}$$

où $A = \Gamma(a_0, \ldots, a_{n-1})$. Les applications φ_j sont clairement des formes linéaires sur E.

2.2 Des matrices circulantes « orthogonales »

Pour $i \in \mathbf{n}$, considérons la matrice

$$U_i = \frac{1}{n}\Gamma(1, \omega^{-i}, \omega^{-2i}, \ldots, \omega^{-(n-1)i})$$

Que vaut $\varphi_j(U_i)$? On a

$$\begin{aligned} n\varphi_j(U_i) &= \sum_{k=0}^{n-1} \omega^{-ik}\omega^{kj} \\ &= \sum_{k=0}^{n-1} (\omega^{j-i})^k \end{aligned}$$

Si $j \neq i$, alors $\omega^{j-i} \neq 1$ et donc

$$n\varphi_j(U_i) = \frac{(\omega^{j-i})^n - 1}{\omega^{j-i} - 1} = 0$$

car ω^{j-i} est une racine $n$ième de l'unité.

Si, en revanche, $j = i$, alors clairement $\varphi_j(U_i) = 1$.

Ainsi, pour tous $i, j \in \mathbf{n}$,

$$\varphi_j(U_i) = \delta_{ij}$$

où δ_{ij} est le symbole de Kronecker. Remarquons en particulier que $\varphi_j(U_j) \neq 0$ et donc, ce qui n'était pas clair a priori, que φ_j est une forme linéaire non nulle sur E.

2.3 Une base du dual des matrices circulantes

Posons $\mathcal{B}^* = (\varphi_j)_{j\in\mathbf{n}}$. Nous allons montrer que $\mathcal{B}^*$ est une base du dual E^* de E. Comme card $B^* = n$, il suffit de prouver que $\mathcal{B}^*$ est libre. Pour cela, soient $\alpha_0, \ldots, \alpha_{n-1} \in \mathbb{C}$. Supposons que

$$\sum_{j=0}^{n-1} \alpha_j \varphi_j = 0$$

Soit $i \in \mathbf{n}$. Appliquons l'égalité ci-dessus en U_i. Il vient

$$0 = \sum_{j=0}^{n-1} \alpha_j \varphi_j(U_i) = \sum_{j=0}^{n-1} \alpha_j \delta_{ij} = \alpha_i$$

Ainsi, $\alpha_i = 0$.

Nous noterons dorénavant

$$H_j = \ker \varphi_j$$

Proposition 3. *Les H_j sont n hyperplans de E.*

Démonstration. Ce sont les noyaux de formes linéaires non nulles. □

2.4 Morphismes d'algèbres

Proposition 4. *Les $\varphi_j : E \to \mathbb{C}$ sont des morphismes d'algèbres.*

Démonstration. Nous avons déjà vu que les φ_j sont des formes linéaires.

Montrons que $\varphi_j(I) = 1$. On a $I = \Gamma(1, 0, \ldots, 0)$. Ainsi,

$$\varphi_j(I) = \sum_{k=0}^{n-1} \delta_{k0} \omega^{kj} = \omega^0 = 1$$

Soient deux éléments A, B de E. Montrons que $\varphi_j(AB) = \varphi_j(A)\varphi_j(B)$. On a

$$\begin{aligned} \varphi_j(A)\varphi_j(B) &= \sum_{p=0}^{n-1} a_p \omega^{pj} \sum_{q=0}^{n-1} b_q \omega^{qj} \\ &= \sum_{p=0}^{n-1} \sum_{q=0}^{n-1} a_p b_q \omega^{(p+q)j} \end{aligned}$$

Par ailleurs, en notant $AB = \Gamma(c_0, \dots, c_{n-1})$,

$$\varphi_j(AB) = \sum_{k=0}^{n-1} c_k \omega^{kj} = \sum_{k=0}^{n-1} \sum_{p=0}^{n-1} a_p b_{k \ominus p} \omega^{kj}$$

Faisons le changement d'indice $q = k \ominus p$ pour obtenir

$$\varphi_j(AB) = \sum_{q=0}^{n-1} \sum_{p=0}^{n-1} a_p b_q \omega^{(p \oplus q)j}$$

Il reste à remarquer que, comme ω est une racine $n$ième de l'unité,

$$\omega^{(p \oplus q)j} = \omega^{(p+q)j}$$

□

2.5 Retour sur les matrices « orthogonales »

Posons $\mathcal{B} = (U_0, \dots, U_{n-1})$.

Proposition 5. *$\mathcal{B}$ est une base de E. La base duale de $\mathcal{B}$ est précisément la base $\mathcal{B}^*$ des formes φ_j.*

Démonstration. Une fois que nous aurons montré que $\mathcal{B}$ est une base, il sera clair que $\mathcal{B}^*$ en est la base duale, puisque $\varphi_j(U_i) = \delta_{ij}$.

Comme le cardinal de $\mathcal{B}$ est n, il suffit de montrer que $\mathcal{B}$ est libre. Pour cela, soient $\alpha_0, \dots, \alpha_{n-1} \in \mathbb{C}$. Supposons que

$$\sum_{i=0}^{n-1} \alpha_i U_i = 0$$

Soit $j \in \mathbf{n}$. Appliquons φ_j à l'égalité ci-dessus. Il vient

$$0 = \sum_{i=0}^{n-1} \alpha_i \varphi_j(U_i) = \sum_{i=0}^{n-1} \alpha_i \delta_{ij} = \alpha_j$$

Ainsi, $\alpha_j = 0$. □

Proposition 6. *Soit $k \in [\![0, n]\!]$. Soit S une partie de $\mathbf{n}$ de cardinal k. Soit*

$$F = \bigcap_{j \in S} H_j$$

Alors F est un sous-espace vectoriel de E de dimension $n - k$. Précisément, F est le sous-espace vectoriel de E engendré par la famille $(U_i)_{i \notin S}$.

Démonstration. Soit $A = \sum_{i=0}^{n-1} \alpha_i U_i \in E$. Alors $A \in F$ si et seulement si pour tout $j \in S$, $A \in H_j$, c'est à dire $\varphi_j(A) = 0$. Or,

$$\varphi_j(A) = \sum_{i=0}^{n-1} \alpha_j \varphi_j(U_i) = \alpha_j$$

Ainsi, $A \in F$ si et seulement si

$$A = \sum_{i \notin S} \alpha_i U_i$$

où les α_i appartiennent à $\mathbb{C}$. On a donc

$$F = \mathrm{Vect}(U_i)_{i \notin S}$$

□

2.6 Produits

Soient $i, j \in \mathbf{n}$. Calculons $U_i U_j$. Pour tout $k \in \mathbf{n}$, on a

$$\varphi_k(U_i U_j) = \varphi_k(U_i)\varphi_k(U_j) = \delta_{ki}\delta_{kj}$$

Si $k \neq i$ ou $k \neq j$, cette quantité est donc nulle.

Supposons d'abord $i \neq j$. Tout entier k est alors différent de i ou de j, donc $\varphi_k(U_i U_j) = 0$. On a donc

$$U_i U_j \in \bigcap_{k \in \mathbf{n}} H_k$$

Par la proposition 6, cette intersection est un sous-espace vectoriel de E de dimension $n - n = 0$. Ainsi, $U_i U_j = 0$.

Supposons maintenant $i = j$. Cette fois,

$$U_i^2 \in D = \bigcap_{k \neq i} H_k$$

Par la proposition 6, D est la droite engendrée par U_i. Il existe donc $\lambda \in \mathbb{C}$ tel que $U_i^2 = \lambda U_i$. Que vaut λ ? Appliquons φ_i à cette égalité. Il vient

$$\varphi_i(U_i^2) = \varphi_i(U_i)^2 = \lambda \varphi_i(U_i)$$

Mais $\varphi_i(U_i) = 1$, donc $\lambda = 1$. Ainsi,

$$U_i U_j = \delta_{ij} U_i$$

Tous les calculs dans la base $\mathcal{B} = (U_0, \ldots, U_{n-1})$ se font de façon très simple :

Proposition 7. *Soient* $A = \sum_{i=0}^{n-1} \alpha_i U_i$, $B = \sum_{i=0}^{n-1} \beta_i U_i$ *et* $\lambda \in \mathbb{C}$. *alors*

$$A + B = \sum_{i=0}^{n-1} (\alpha_i + \beta_i) U_i$$

$$\lambda A = \sum_{i=0}^{n-1} (\lambda \alpha_i) U_i$$

$$AB = \sum_{i=0}^{n-1} (\alpha_i \beta_i) U_i$$

De plus, $\alpha_i = \varphi_i(A)$.

Démonstration. Les égalités concernant la somme et le produit par λ sont évidentes. On a

$$\begin{aligned} AB &= \sum_{i=0}^{n-1} \alpha_i U_i \sum_{j=0}^{n-1} \beta_j U_j = \sum_{i,j \in \mathbf{n}} \alpha_i \beta_j U_i U_j \\ &= \sum_{i,j \in \mathbf{n}} \alpha_i \beta_j \delta_{ij} U_i = \sum_{i \in \mathbf{n}} \alpha_i \beta_i U_i \end{aligned}$$

Enfin,

$$\varphi_j(A) = \sum_{i=0}^{n-1} \alpha_i \varphi_j(U_i) = \sum_{i=0}^{n-1} \alpha_i \delta_{ij} = \alpha_j$$

□

3 Les matrices circulantes inversibles

3.1 Caractérisation

Soit $A \in E$. Il faut a priori faire la distinction entre le fait que A soit une matrice inversible, c'est à dire qu'il existe $B \in \mathrm{GL}_n(\mathbb{C})$ telle que $AB = I$, et le fait que A soit un élément inversible de E, c'est à dire qu'il existe $B \in E$ telle que $AB = I$. Bien évidemment, si A est un élément inversible de E, alors A est une matrice inversible. Nous allons voir que la réciproque est vraie.

Lemme 8. *On a*

$$\sum_{j=0}^{n-1} U_j = I$$

Démonstration. On a

$$I = \sum_{j=0}^{n-1} \varphi_j(I) U_j$$

Or, comme $I = \Gamma(1, 0, \ldots, 0)$,

$$\varphi_j(I) = \sum_{k=0}^{n-1} \delta_{k0} \omega^{kj} = 1$$

□

Proposition 9. *Soit $A \in E$. A est inversible en tant qu'élément de E si et seulement si $A \in GL_n(\mathbb{C})$.*

Démonstration. Nous avons déjà une des deux implications. Supposons que $A \in \mathrm{GL}_n(\mathbb{C})$. Écrivons

$$A = \sum_{i=0}^{n-1} \alpha_i U_i$$

où les $\alpha_i \in \mathbb{C}$. La matrice A est inversible, on a donc pour tout $i \in \mathbf{n}$, $\varphi_i(A) \neq 0$. Or, $\varphi_i(A) = \alpha_i$. Ainsi, tous les α_i sont différents de 0. Considérons l'élément de E

$$B = \sum_{i=0}^{n-1} \frac{1}{\alpha_i} U_i$$

On a

$$AB = \sum_{i=0}^{n-1} \alpha_i \frac{1}{\alpha_i} U_i = \sum_{i=0}^{n-1} U_i = I$$

Ainsi, l'inverse de A est $B \in E$. □

3.2 Calcul efficace de l'inverse

Soit $A = \sum_{i=0}^{n-1} \alpha_i U_i$. Supposons A inversible c'est à dire, comme nous l'avons vu, les α_i non nuls. L'inverse de A est immédiat si l'on sait calculer les α_i. Or, $AU_i = \alpha_i U_i$. De plus, $(U_i)_{00} = 1$, donc $\alpha_i = (AU_i)_{00}$. On a donc

$$\begin{aligned}
\alpha_i &= \sum_{k=0}^{n-1} A_{0k} (U_i)_{k0} = \frac{1}{n} \sum_{k=0}^{n-1} A_{0k} (\omega^{-i})^{0 \ominus k} = \frac{1}{n} \sum_{k=0}^{n-1} A_{0k} \omega^{ki} \\
&= \frac{1}{n} \sum_{k=0}^{n-1} A_{0k} \Omega_{ki} \\
&= \frac{1}{n} (A\Omega)_{0i}
\end{aligned}$$

Ainsi, on obtient tous les α_i en calculant la ligne zéro du produit matriciel $A\Omega$, ce qui se fait de façon naïve en $O(n^2)$ opérations arithmétiques.

Une fois les α_i connus, appelons $\beta_i = \frac{1}{\alpha_i}$. L'inverse de A est la matrice $B = \sum_{i=0}^{n-1} \beta_i U_i$. Ici encore, la matrice Ω va nous être utile. En effet, B étant une matrice circulante, il suffit de déterminer sa première ligne. Pour tout $j \in \mathbf{n}$, $B_{0j} = b_j$, et donc

$$\begin{aligned} b_j &= \sum_{i=0}^{n-1} \beta_i (U_i)_{0j} = \frac{1}{n} \sum_{i=0}^{n-1} \beta_i (\omega^{-i})^{j \ominus 0} \\ &= \frac{1}{n} \sum_{i=0}^{n-1} \beta_i \omega^{-ij} \end{aligned}$$

Appelons $\hat{B} = \Gamma(\beta_0, \ldots, \beta_{n-1})$. On a

$$\begin{aligned} b_j &= \frac{1}{n} \sum_{i=0}^{n-1} \hat{B}_{0i} \overline{\Omega}_{ij} \\ &= \frac{1}{n} (\hat{B}\overline{\Omega})_{0j} \end{aligned}$$

Il suffit donc de déterminer la première ligne du produit $\hat{B}\overline{\Omega}$, ce qui, ici encore, s'effectue naïvement en $O(n^2)$ opérations arithmétiques.

Il s'avère qu'il existe un algorithme appelé la transformée de Fourier rapide (Fast Fourier Transform, ou encore FFT), permet d'effectuer ces calculs en $O(n \log n)$ opérations arithmétiques. Nous n'entrerons pas ici dans les détails de cet algorithme. Retenons qu'il est possible d'inverser une matrice circulante de taille n en $O(n \log n)$ opérations.

4 Intermède

Faisons une pause et examinons les objets que nous avons défini depuis le début de l'article dans les cas particuliers $n = 2, 3, 4$. Ce qui suit se passe de commentaires.

4.1 Le cas $n = 2$

Une matrice circulante quelconque de taille 2 :

$$A = \Gamma(a,b) = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$$

La racine primitive carrée de l'unité : $\omega = -1$.

Les formes linéaires φ_j :

$$\begin{cases} \varphi_0(A) &= a+b \\ \varphi_1(A) &= a-b \end{cases}$$

La matrice de Vandermonde Ω :

$$\Omega = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Les matrices U_i :

$$\begin{cases} U_0 &= \frac{1}{1}\Gamma(1,1) &= \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \\ U_1 &= \frac{1}{2}\Gamma(1,-1) &= \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \end{cases}$$

4.2 Le cas $n = 3$

Une matrice circulante quelconque de taille 3 :

$$A = \Gamma(a,b,c) = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix}$$

La racine primitive cubique de l'unité : $\omega = e^{2i\pi/3}$.

Les formes linéaires φ_j :

$$\begin{cases} \varphi_0(A) &= a+b+c \\ \varphi_1(A) &= a+\omega b+\omega^2 c \\ \varphi_2(A) &= a+\omega^2 b+\omega c \end{cases}$$

La matrice de Vandermonde Ω :

$$\Omega = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$$

Les matrices U_i :

$$\begin{cases} U_0 &= \frac{1}{3}\Gamma(1,1,1) &= \frac{1}{3}\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \\ U_1 &= \frac{1}{3}\Gamma(1,\omega^2,\omega) &= \frac{1}{3}\begin{pmatrix} 1 & \omega^2 & \omega \\ \omega & 1 & \omega^2 \\ \omega^2 & \omega & 1 \end{pmatrix} \\ U_2 &= \frac{1}{3}\Gamma(1,\omega,\omega^2) &= \frac{1}{3}\begin{pmatrix} 1 & \omega & \omega^2 \\ \omega^2 & 1 & \omega \\ \omega & \omega^2 & 1 \end{pmatrix} \end{cases}$$

4.3 Le cas $n = 4$

Une matrice circulante quelconque de taille 4 :

$$A = \Gamma(a,b,c,d) = \begin{pmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{pmatrix}$$

La racine primitive quatrième de l'unité : $\omega = i$.

Les formes linéaires φ_j :

$$\begin{cases} \varphi_0(A) &= a+b+c+d \\ \varphi_1(A) &= a+ib-c-id \\ \varphi_2(A) &= a-b+c-d \\ \varphi_3(A) &= a-ib-c+id \end{cases}$$

La matrice de Vandermonde Ω :

$$\Omega = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

Les matrices U_i :

$$\begin{cases} U_0 = \frac{1}{4}\Gamma(1,1,1,1) = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \\ U_1 = \frac{1}{4}\Gamma(1,-i,-1,i) = \frac{1}{4}\begin{pmatrix} 1 & -i & -1 & i \\ i & 1 & -i & -1 \\ -1 & i & 1 & -i \\ -i & -1 & i & 1 \end{pmatrix} \\ U_2 = \frac{1}{4}\Gamma(1,-1,1,-1) = \frac{1}{4}\begin{pmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \end{pmatrix} \\ U_3 = \frac{1}{4}\Gamma(1,i,-1,-i) = \frac{1}{4}\begin{pmatrix} 1 & i & -1 & -i \\ -i & 1 & i & -1 \\ -1 & -i & 1 & i \\ i & -1 & -i & 1 \end{pmatrix} \end{cases}$$

5 Idéaux

5.1 Introduction

Un *idéal* de l'algèbre E est un sous-espace vectoriel F de E vérifiant, de plus,

$$\forall A \in F, \forall B \in E, AB \in F$$

Proposition 10. *Soit F un idéal de E différent de E. Alors F ne contient aucune matrice inversible.*

Démonstration. Supposons que F contient un élément A qui est une matrice inversible. Par la proposition 9, A est inversible dans E. Il existe donc $B \in E$ telle que $AB = I$. Ainsi, comme F est un idéal de E, $I \in F$. De là, pour tout élément C de E, $C = IC \in F$ (toujours par la propriété d'idéal) et finalement $F = E$. □

5.2 Hyperplans

Proposition 11. *Les hyperplans H_j sont des idéaux de E.*

Démonstration. Soient $A \in H_j$ et $B \in E$. On a

$$\varphi_j(AB) = \varphi_j(A)\varphi_j(B) = 0\varphi_j(B) = 0$$

Ainsi, $AB \in H_j$. □

Nous allons maintenant prouver que les H_j sont les seuls idéaux de E de dimension $n-1$. Cela demande un peu de travail.

Lemme 12. *Soit F un idéal de E différent de E. Soient $A_0, \dots, A_{N-1}$ N éléments de F. Alors il existe un entier $j \in \mathbf{n}$ tel que pour tout $k \in [\![0, N-1]\!]$, $\varphi_j(A_k) = 0$.*

Démonstration. Pour tout $\lambda \in \mathbb{C}$, considérons la matrice

$$A(\lambda) = \sum_{k=0}^{N-1} \lambda^k A_k$$

On a $A(\lambda) \in F$, donc, comme $F \neq E$, $\det A(\lambda) = 0$. Mais

$$\det A(\lambda) = \prod_{j=0}^{n-1} \varphi_j(A(\lambda)) = \prod_{j=0}^{n-1} \sum_{k=0}^{N-1} \lambda^k \varphi_j(A_k)$$

Considérons le polynôme

$$P = \prod_{j=0}^{n-1} \left(\sum_{k=0}^{N-1} \varphi_j(A_k) X^k \right)$$

Ce polynôme P est le polynôme nul. Par intégrité de l'anneau $\mathbb{C}[X]$, il existe donc un entier $j \in \mathbf{n}$ tel que

$$\sum_{k=0}^{N-1} \varphi_j(A_k) X^k = 0$$

Ce polynôme est nul donc tous ses coefficients sont nuls : pour tout k entre 0 et $N-1$, $\varphi_j(A_k) = 0$. □

Lemme 13. *Tout idéal de E différent de E est inclus dans l'un des H_j.*

Démonstration. Soit F un idéal de E différent de E. Comme $F \neq E$, tout élément A de F est non inversible, ce qui entraîne

$$\det A = \prod_{j=0}^{n-1} \varphi_j(A) = 0$$

L'un des facteurs du produit est donc nul, d'où

$$F \subset \bigcup_{j=0}^{n-1} H_j$$

Supposons maintenant que F ne soit inclus dans aucun des H_j. Pour tout $j \in \mathbf{n}$, il existe $A_j \in F$ telle que $A_j \notin H_j$, c'est à dire telle que $\varphi_j(A_j) \neq$

0. Quitte à diviser A_j par le nombre complexe $\varphi_j(A_j)$, on peut supposer $\varphi_j(A_j) = 1$. Soit $i \in \mathbf{n}$. Comme les A_j, $j \neq i$, sont dans F, par le lemme 12 il existe $k \in \mathbf{n}$ tel que pour tout $j \neq i$, $\varphi_k(A_j) = 0$. Ce k ne peut être aucun des j, c'est donc i. Ainsi, pour tous i, j distincts, $\varphi_i(A_j) = 0$. Pour résumer,

$$\forall i, j \in \mathbf{n}, \phi_j(A_i) = \delta_{ij}$$

Considérons maintenant

$$A = \sum_{j=0}^{n-1} A_j$$

On a pour tout $j \in \mathbf{n}$,

$$\varphi_j(A) = \sum_{k=0}^{n-1} \varphi_j(A_k) = \sum_{k=0}^{n-1} \delta_{jk} = 1$$

Comme $A \in F$, on a $\det A = 0$. Or

$$\det A = \prod_{j=0}^{n-1} \varphi_j(A) = 1 \neq 0$$

Contradiction. □

Proposition 14. *Les idéaux de E de dimension $n-1$ sont les H_j.*

Démonstration. Les H_j sont, comme on l'a vu, des hyperplans de E qui sont aussi des idéaux de E.

Inversement, soit F un idéal de E de dimension $n-1$. Par la proposition précédente, F est inclus dans l'un des H_j. Par l'égalité de leurs dimensions F et H_j sont donc égaux. □

5.3 Des idéaux

Proposition 15. *Soit $k \in [\![0, n]\!]$. Pour toute partie S de $\mathbf{n}$ de cardinal k, $\bigcap_{j \in S} H_j$ est un idéal de E de dimension $n-k$.*

Démonstration. En tant qu'intersection d'idéaux, c'est un idéal. De plus, par la proposition 6, c'est un sous-espace vectoriel de E de dimension $n-k$. □

Corollaire 16. *Pour tout $k \in [\![0, n]\!]$, E possède au moins $\binom{n}{k}$ idéaux de dimension $n-k$.*

Démonstration. $\binom{n}{k}$ est le nombre de parties S de $\mathbf{n}$ de cardinal k. Pour chacune de ces parties, l'intersection $\bigcap_{j \in S} H_j$ est un idéal de E de dimension $n-k$, et tous ces idéaux sont clairement distincts. □

Nous noterons dorénavant, pour tout ensemble $S \subset \mathbf{n}$,

$$F_S = \bigcap_{j \in S} H_j$$

et

$$F'_S = \mathrm{Vect}(U_i)_{i \in S}$$

Rappelons que, par la proposition 6, $F_S = F'_{\mathbf{n} \setminus S}$. Les F_S sont par ce que nous venons de voir des idéaux de E de dimension $n - \mathrm{card}\ S$ et les F'_S sont des idéaux de E de dimension card S. Nous allons montrer que les F'_S sont les seuls idéaux de E.

5.4 Tous les idéaux

Proposition 17. *Soit $k \in \mathbf{n}$. Tout idéal de E de dimension k est de la forme F'_S où $S \subset \mathbf{n}$.*

Démonstration. Nous allons montrer par récurrence sur k que pour tout entier $k \in \mathbf{n}$, si F est un idéal de E de dimension k, alors il existe $S \subset \mathbf{n}$ de cardinal k telle que $F = F'_S$.

Supposons tout d'abord $k = 0$. Soit F un idéal de E de dimension 0. Alors $F = \{0\}$, donc $F = F'_\emptyset$.

Soit maintenant $k \in [\![1, n]\!]$. Supposons la propriété vraie pour tout $k' < k$.

Soit F un idéal de E de dimension k. Soit

$$A = \sum_{j=0}^{n-1} \alpha_j U_j \in F \setminus \{0\}$$

Pour tout i, $AU_i \in F$ car F est un idéal de E. De plus $AU_i = \alpha_i U_i$. Donc, $\alpha_i = 0$ ou alors $U_i = \frac{1}{\alpha} AU_i \in F$. Comme l'un des α_i est non nul, il en résulte que l'un des U_i, disons U_{i_0}, est dans F. Soit

$$G = \{A \in F, AU_{i_0} = 0\}$$

G est clairement un sous-espace vectoriel de F. De plus, si $A \in G$ et $B \in E$, alors $AB \in F$ car F est un idéal de E, et

$$(AB)U_{i_0} = B(AU_{i_0}) = 0$$

Donc $AB \in G$. Ainsi, G est un idéal de E. Comme G est strictement inclus dans F (il ne contient pas U_{i_0}), sa dimension est un entier $k' < k$. Par l'hypothèse de récurrence, il existe une partie S' de $\mathbf{n}$ de cardinal k' telle que $G = F'_{S'}$. Comme $U_{i_0} \notin G$, $S' \subset \mathbf{n} \setminus \{i_0\}$.

Soit $S = S' \cup \{i_0\}$, de sorte que

$$F'_S = G \oplus < U_{i_0} >$$

Montrons que $F = F'_S$.

Comme $G \subset F$ et $U_{i_0} \in F$, par linéarité, $F'_S \subset F$.

Inversement, soit $A \in F$. On a $AU_{i_0} = \alpha U_{i_0}$ où $\alpha \in \mathbb{C}$. De là,

$$(A - \alpha U_{i_0})U_{i_0} = AU_{i_0} - \alpha U_{i_0}^2 = AU_{i_0} - \alpha U_{i_0} = 0$$

et donc $A - \alpha U_{i_0} \in G$. Ainsi,

$$A = (A - \alpha U_{i_0}) + \alpha U_{i_0} \in G \oplus < U_{i_0} >= F'_S$$

□

Corollaire 18. *Pour tout entier $k \in \mathbf{n}$, les idéaux de E de dimension k sont les F'_S où S est une partie de $\mathbf{n}$ de cardinal k.*

Corollaire 19. *Pour tout entier $k \in \mathbf{n}$, E possède $\binom{n}{k}$ idéaux de dimension k.*

Corollaire 20. *E possède 2^n idéaux.*

Démonstration. En effet,

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

□