

exercice 43 de réduction (avec une jolie erreur d'énoncé)

Léane Parent

29 novembre 2025

Exercice 43 : (Mines-Ponts 2019)

Déterminer les matrices $A \in M_n(\mathbb{R})$ telles que $A^5 - 2A^4 - 2A^3 + A^2 + 4A + I_n = 0$, $\text{tr}(A) = 0$ et $\det(A) = \pm 1$.

Dans tout l'exercice, on note P le polynôme annulateur décrit dans l'énoncé.

Cette correction se repose sur Introduction à la théorie de Galois¹, par Yves Laszlo, et d'un théorème très puissant qui résout l'exercice tout seul, trouvé sur [wikipedia.org](https://en.wikipedia.org) (on fait avec les sources qu'on trouve, et avec la flemme qu'on a).

0.1 Suggestion de correction

L'énoncé original utilisait probablement le polynôme $P(X) = X^5 - 2X^4 - 2X^3 + X^2 + 4X + 4$, qui se factorise aisément en $(X + 1)(X - 2)^2(X^2 + X + 1)$. Or, toutes ses racines sont de module supérieurs ou égaux à 1. Ainsi, pour avoir un déterminant égal à ± 1 , les valeurs propres de A ne peuvent être que $-1, j, j^2$.

En trigonalisant dans $M_n(\mathbb{C})$, on remarque que la trace est alors strictement négative (de valeur $-m_1 - m_j$), ce qui est absurde : l'ensemble des matrices convenant est \emptyset .

1 Irréductibilité de P dans $\mathbb{Q}[X]$

P est unitaire, donc, d'après le lemme de Gauss, si celui-ci est réductible dans $\mathbb{Q}[X]$, alors il est réductible dans $\mathbb{Z}[X]$.

De plus, si P est réductible, alors il l'est modulo 2. Supposons P réductible, et notons $P(X) = (X^3 + aX^2 + bX + c)(X^2 + dX + e)$. Il en découle, dans $\mathbb{F}_2[X]$ (en assimilant les entiers à leur congruence modulo 2 par la surjection canonique) :

$$X^5 + X^2 + 1 = (X^3 + aX^2 + bX + c)(X^2 + dX + e)$$

1. <https://www.cmls.polytechnique.fr/perso/laszlo/galois/galois.pdf>

On en déduit :

$$0 = a + c \quad (1)$$

$$0 = d + ac + b \quad (2)$$

$$1 = e + da + cb \quad (3)$$

$$0 = db + ea \quad (4)$$

$$1 = eb \quad (5)$$

(5) nous donne $e = b = 1$. On déduit de (4) que $a = e = 1$, d'où, d'après (1), $c = 1$. On a alors $d = 1$ d'après (3).

(2) n'est alors plus vérifiée, ce qui est absurde : P n'est pas réductible modulo 2, donc pas réductible.

2 Calcul du groupe de Galois

On vérifie aisément par une étude de P qu'il admet exactement trois racines réelles distinctes, donc deux complexes non réelles conjuguées.

Or, P est de degré premier. Il vérifie ainsi les hypothèses d'un théorème, trouvé sur l'article Galois group de wikipedia² (voir "symmetric group of prime order") : Si un polynôme irréductible de degré premier p admet exactement $p - 2$ racines réelles, alors son groupe de Galois est S_p tout entier.

(Je n'ai pas trop de doutes sur le fait que ça se calcule plus explicitement, mais vous avez envie de le faire, vous?)

3 \mathbb{Q} -indépendance linéaire des racines de P

lemme : Si $V \subset \mathbb{Q}^5$ est un \mathbb{Q} -espace vectoriel stable par permutation, alors $V = \{0\}$, $\text{Vect}_{\mathbb{Q}}(1, \dots, 1)$, ou contient $W = \{(q_1, \dots, q_5) \mid q_1 + \dots + q_5 = 0\}$.

démonstration : Supposons qu'il existe un élément $(q_1, \dots, q_5) \in V$ admettant deux éléments distincts. Quitte à permuter, supposons $q_1 \neq q_2$.

Par stabilité par permutation, $(q_2, q_1, q_3, q_4, q_5) \in V$. Par différence, $(q_2 - q_1, q_1 - q_2, 0, 0, 0) \in V$, donc $(1, -1, 0, 0, 0)$ également.

On en déduit par permutation que $(1, 0, -1, 0, 0), \dots, (1, 0, 0, 0, -1) \in V$. Or, ces éléments forment une base de W , donc $W \subset V$.

On note r_1, r_2, r_3, r_4 et r_5 les racines de P , avec $r_4, r_5 \notin \mathbb{R}$, et $L = \mathbb{Q}(r_1, \dots, r_5)$. Soit $V = \{(q_1, \dots, q_5) \in \mathbb{Q}^5 \mid q_1 r_1 + \dots + q_5 r_5 = 0\}$, ie l'ensemble des coefficients de combinaisons linéaires rationnelles annulant les racines de P . On montre aisément que V est un \mathbb{Q} -espace vectoriel

Soit $(q_1, \dots, q_5) \in V$. Soit $\sigma \in \text{Gal}(L/\mathbb{Q})$.

On a $q_1 r_1 + \dots + q_5 r_5 = 0$, d'où, par composition par $\sigma : q_1 \sigma(r_1) + \dots + q_5 \sigma(r_5) = \sigma(0) = 0$.

2. https://en.wikipedia.org/wiki/Galois_group, source : Lang, Serge. Algebra (Revised Third ed.). pp. 263, 273.

(En effet, σ est un automorphisme laissant invariant les rationnels.)

Or, en assimilant σ à une permutation, on a $\sigma(r_i) = r_{\sigma(i)}$.

On en déduit que $\sigma^{-1}(q_1, \dots, q_5) \in V$: V est stable par permutation (car $\text{Gal}(L/\mathbb{Q}) \cong S_5$, donc σ^{-1} décrit S_5).

D'après le lemme ci-dessus, on a $V = \{0\}$, $\mathbb{Q}(1, \dots, 1)$, ou contient W .

En observant le coefficient en X^4 de P , on obtient $r_1 + \dots + r_5 = 2$, d'où $V \neq \text{Vect}_{\mathbb{Q}}(1, \dots, 1)$.

De plus, $r_1 - r_4 \notin \mathbb{R}$, donc $r_1 - r_4 \neq 0$. On en déduit que $(1, 0, 0, -1, 0) \notin V$, donc $W \not\subset V$.

Ainsi, $V = \{0\}$, ie r_1, \dots, r_5 sont linéairement indépendants.

4 Conclusion

Soit A convenant. En trigonalisant (dans $M_n(\mathbb{C})$), on obtient une matrice dont la trace est combinaison linéaire (à coefficients naturels) des racines de P .

Or, par hypothèse, la trace de A est nulle, ce qui est absurde car les racines de P sont libres.

L'ensemble des matrices convenant est \emptyset .