Polynôme minimal

www.h-k.fr/publications/objectif-agregation

Soient k un corps et A une k-algèbre de dimension finie. On sait que tout élément $x \in \mathrm{A}$ admet un polynôme minimal π_x sur k. Il est défini comme l'unique polynôme unitaire qui engendre l'idéal des polynômes annulateurs de x [BPM, application 4.2 p.149]. Cette note l'occasion d'étudier au travers d'exercices quelques propriétés du polynôme minimal. Elle apporte des éléments de réponses aux trois questions suivantes.

Q1. Peut-on le caractériser autrement ?

Q2. Étant donné une k-algèbre A, quels polynômes sont des polynômes minimaux d'éléments de A ?

Q3. Tout polynôme unitaire à coefficients dans k est-il un polynôme minimal ?

Exercice 1 – Polynôme minimal et irréductibilité. Soient A une k-algèbre de dimension finie et $x \in \mathrm{A}$. On note

$$\mathrm{I}_x = \{\mathrm{P} \in k[\mathrm{X}], \quad \mathrm{P}(x) = 0\}$$

l'idéal annulateur de x et π_x le polynôme minimal de x.

a) On suppose que I_x contient un polynôme irréductible Q. Montrer que le polynôme unitaire P associé à Q est le polynôme minimal de x et que la k-algèbre $k[x]$ est un corps.

b) On suppose que A est un corps que l'on note K. Montrer que π_x est un polynôme irréductible sur k.

c) Déduire des questions précédentes une caractérisation du polynôme minimal lorsque A est un corps.

Commentaires. Ce premier exercice répond en partie à la question Q1 de caractérisation des polynômes minimaux. Il traite le cas particulier où l'algèbre $\mathrm{A} = \mathrm{K}$ est un corps. Dans ce cas, le polynôme minimal de x est l'unique polynôme irréductible unitaire appartenant à I_x. Dès que l'on a trouvé un polynôme irréductible qui annule x, on a en fait le polynôme minimal de x à un coefficient multiplicatif près.

Dans la question **b**, on suppose que A est un corps alors que seule l'intégrité de A sert. Mais, comme A est une k-algèbre de dimension finie, elle est intègre si et seulement si c'est un corps (voir [BPM, application 4.16]).

Corrigé.

a) Par hypothèse, P annule x, donc π_x divise P. Comme P est irréductible et π_x non constant, on en déduit que π_x et P sont associés. Or π_x et P sont unitaires, donc $\mathrm{P} = \pi_x$. De plus,

$$k[x] \overset{k\text{-alg.}}{\simeq} k[\mathrm{X}]/\langle \pi_x \rangle = k[\mathrm{X}]/\langle \mathrm{P} \rangle$$

est un corps puisque P est irréductible.

b) Supposons que $\pi_x = \mathrm{PQ}$ avec $\mathrm{P}, \mathrm{Q} \in k[\mathrm{X}]$. On a alors

$$0 = \pi_x(x) = \mathrm{P}(x)\mathrm{Q}(x).$$

Comme K est un anneau intègre, on a $\mathrm{P}(x) = 0$ ou $\mathrm{Q}(x) = 0$. Ainsi π_x divise P ou Q. Comme par hypothèse P et Q divisent π_x, on en déduit que P et π_x sont associés, ou que Q et π_x sont associés. Ainsi Q ou P est inversible et donc π_x est irréductible.

c) Le polynôme minimal de x est l'unique polynôme irréductible unitaire appartenant à I_x. En effet, d'après la question **b**, π_x est un polynôme irréductible unitaire. Par ailleurs, si P est un polynôme irréductible annulateur de x alors, d'après la question **a**, P est associé au polynôme minimal de x. De plus, si P est unitaire, alors P et π_x sont associés avec le même coefficient dominant et donc $\mathrm{P} = \pi_x$. ■

Intéressons-nous à présent à la question Q2 qui est délicate. La question **b** de l'exercice 1 peut amener à penser qu'un polynôme minimal est nécessairement irréductible. L'exemple de l'algèbre des endomorphismes d'un espace vectoriel montre qu'il n'en est rien. En effet,

(i) le polynôme minimal d'un projecteur distinct de 0 et id est $\mathrm{X}^2 - \mathrm{X}$ [BPM, exemple 4.42] ;

(ii) celui d'une symétrie distincte de id et $-$id est $\mathrm{X}^2 - 1 = (\mathrm{X}-1)(\mathrm{X}+1)$ [BPM, exemple 4.43] ;

(iii) il peut aussi avoir des facteurs multiples : si u est nilpotent non nul, son polynôme minimal est $\pi_u = \mathrm{X}^p$ avec $p \geqslant 2$ [BPM, proposition 4.56].

En fait, l'exercice suivant donne une réponse à cette deuxième question Q2 lorsque A est l'algèbre des endomorphismes d'un espace vectoriel.

Exercice 2 — Polynôme minimal d'endomorphisme. Soient k un corps, V un k-espace vectoriel de dimension finie n et $\mathrm{P} \in k[\mathrm{X}]$. À quelle condition P est-il le polynôme minimal d'un endomorphisme de V ?

Commentaires. Si P est le polynôme minimal de $u \in \mathscr{L}(\mathrm{V})$, alors d'après le théorème de Cayley-Hamilton (voir [RDO1, 12.3.3]), P divise χ_u le polynôme caractéristique de u et ainsi, $\deg \mathrm{P} \leqslant n$. Cependant, cette condition n'est pas suffisante. Par exemple, si $k = \mathbb{R}$ et n est impair alors le polynôme $\mathrm{P} = \mathrm{X}^2 + 1$ n'est pas le polynôme minimal d'un endomorphisme de V car $u^2 = -\mathrm{id}$ et $(\det u)^2 = (-1)^n = -1$. Il est nécessaire de mener un raisonnement plus précis sur les degrés et de considérer la décomposition de P en facteurs irréductibles

$$\mathrm{P} = \prod_{i=1}^{\ell} \mathrm{P}_i{}^{m_i}$$

où les P_i sont irréductibles unitaires deux à deux distincts et $m_i \in \mathbb{N}^*$.

Corrigé. Supposons que P soit le polynôme minimal de $u \in \mathscr{L}(\mathrm{V})$. D'après l'application 6.100 et le théorème de Cayley-Hamilton, on a

$$\chi_u = \prod_{i=1}^{\ell} \mathrm{P}_i{}^{n_i} \qquad \text{avec} \qquad n_i \geqslant m_i.$$

L'équation

$$\sum_{i=1}^{\ell} x_i \deg \mathrm{P}_i = n \tag{$*$}$$

d'inconnues $(x_i)_{1 \leqslant i \leqslant \ell}$ a alors pour solution $(n_i)_{1 \leqslant i \leqslant \ell}$.

Réciproquement, supposons que l'équation $(*)$ admet une solution $(y_i)_{1 \leqslant i \leqslant \ell} \in \mathbb{N}^\ell$ telle que $y_i \geqslant m_i$ pour tout $i \in [\![1 , \ell]\!]$. Construisons une matrice M diagonale par blocs vérifiant $\pi_{\mathrm{M}} = \mathrm{P}$. La diagonale est constituée d'un bloc compagnon $\mathcal{C}_{\mathrm{P}}$ suivi de $n_i - m_i$ blocs $\mathcal{C}_{\mathrm{P}_i}$ pour tout $i \in [\![1 , \ell]\!]$. La matrice M est une matrice carrée de taille n et d'après la remarque 4.34, son polynôme minimal est P. ■

Le lemme 4 de la note « Signature et corps finis » donne la réponse à la question Q2 dans le cas où $k = \mathbb{F}_q$ et $\mathrm{A} = \mathbb{F}_{q^n}$. L'exercice suivant traite le cas où $\mathrm{A} = \overline{k}$ est la clôture algébrique de k.

Exercice 3 — Polynôme minimal et clôture algébrique. Soient k un corps, $\overline{k}$ la clôture algébrique de k et P un élément de $k[\mathrm{X}]$. On suppose que $\overline{k}$ est de dimension finie sur k. À quelle condition P est-il le polynôme minimal d'un élément de $\overline{k}$?

Commentaires. Le résultat s'applique en particulier si $k = \mathbb{R}$ et donc $\overline{k} = \mathbb{C}$. Les polynômes minimaux sur $\mathbb{R}$ des éléments de $\mathbb{C}$ sont les éléments irréductibles unitaires de $\mathbb{R}[\mathrm{X}]$ c'est-à-dire les $\mathrm{X} - a$ pour $a \in \mathbb{R}$ et les $\mathrm{X}^2 + s\mathrm{X} + t$ avec $s^2 - 4t < 0$. Par ailleurs, l'hypothèse $\overline{k}$ est de dimension finie sur k est présente uniquement pour appliquer l'exercice 1. En fait, le résultat reste vrai même lorsque cette hypothèse n'est pas vérifiée.

Corrigé. D'après la question **b** de l'exercice 1, P est irréductible et unitaire. Réciproquement, on suppose que P est irréductible sur k et unitaire. Comme $\overline{k}$ est algébriquement clos, P admet une racine $x \in \overline{k}$. Le polynôme P est donc irréductible unitaire et annule x, la question **a** de l'exercice 1 montre que $\mathrm{P} = \pi_x$. En conclusion, les polynômes minimaux des éléments de $\overline{k}$ sont les polynômes unitaires et irréductibles sur k. ■

Remarque 1 — Dimension et degré. Une dernière remarque à propos de la question Q2. On a $\deg \pi_x \leqslant \dim_k \mathrm{A}$, pour tout $x \in \mathrm{A}$.

Remarque 2 — « Tout polynôme est un polynôme minimal ». À propos de la question Q3, on dispose du résultat suivant. Pour tout polynôme P unitaire non constant à coefficients dans k, il existe une k-algèbre A et $x \in \mathrm{A}$ tel que le polynôme minimal de x soit P. En effet, considérons la k-algèbre $k[\mathrm{X}]/\langle \mathrm{P} \rangle$ et $\pi : k[\mathrm{X}] \to k[\mathrm{X}]/\langle \mathrm{P} \rangle$ la surjection canonique. Alors $x = \pi(\mathrm{X})$ admet pour polynôme minimal P. En effet, comme π est un morphisme de k-algèbre, on a

$$\mathrm{Q}(x) = 0 \iff \mathrm{Q}(\pi(\mathrm{X})) = 0 \iff \pi(\mathrm{Q}(\mathrm{X})) = 0 \iff \mathrm{Q} \in \langle \mathrm{P} \rangle.$$

Ainsi l'idéal des polynômes annulateurs de x est l'idéal $\langle \mathrm{P} \rangle$ et P est bien le polynôme minimal de x.

Références

[BPM] V. Beck, J. Malick, et G.Peyré. *Objectif Agrégation.* H & K, 2004.

[RDO1] E. Ramis, C. Deschamps, et J. Odoux. *Cours de Mathématiques 1, Algèbre.* Dunod, 1998.