Polynômes minimaux

Cours d'Agnès David,
notes de Clémentine Laurens

Octobre 2019

Soient K un corps et $n \in \mathbb{N}^*$. On considère L une extension de K, finie de degré n. On fixe α dans L et on note $\mu_{L/K,\alpha}$ son polynôme minimal. On considère également une matrice $M \in \mathcal{M}_n(K)$, et on note $\mu_{K,M}$ son polynôme minimal. Dans toute la suite, μ désigne respectivement $\mu_{L/K,\alpha}$ ou $\mu_{K,M}$ (en fonction du contexte), d désigne le degré de μ, et R l'ensemble correspondant $K[\alpha] = \{P(\alpha) | P \in K[X]\}$ ou $K[M] = \{P(M) | P \in K[X]\}$.

	Valable pour $\alpha \in L/K$	Valable pour $\alpha \in L/K$ **et** $M \in \mathcal{M}_n(K)$ (notation générique $x = \alpha$ ou M)	Valable pour $M \in \mathcal{M}_n(K)$
Définition du polynôme minimal, justification de son existence	*Cf. ci-contre.*	Considérons l'application Φ_x de $K[X]$ dans $\mathcal{M}_n(K)$ *ou* L, qui à P associe $P(x)$. C'est un morphisme de K-algèbres. Donc $Ker(\Phi_x)$ est un idéal non nul (car L et $\mathcal{M}_n(K)$ sont de dimension finie) de $K[X]$, qui est principal. Donc $\exists! \mu \in K[X]$ unitaire tel que $Ker(\Phi_x) = (\mu)$. μ est le polynôme minimal de x.	*Cf. ci-contre.*
Description de R	*Cf. ci-contre.*	$R \simeq K[X]/(\mu)$	*Cf. ci-contre.*
μ est-il irréductible sur K ?	**OUI** Par l'absurde : si on avait $(P, Q) \in K[X]$ non constants tels que $\mu = PQ$, alors on aurait (par intégrité du corps K) $P(\alpha) = 0$ ou $Q(\alpha) = 0$. Comme $P, Q \mid \mu$, ceci contredirait la minimalité de μ comme polynôme annulateur de α.	/	**NON** Pour $M = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, on a $\mu_M(X) = X^2$ réductible (M matrice nilpotente) .

μ est-il irréductible sur L ?	Par définition, $\mu(\alpha) = 0$. Donc $(X - \alpha)\|\mu$ dans $L[X]$. Donc μ est irréductible sur L **ssi** $\mu(X) = (X - \alpha)$. Or, $\mu \in K[X]$. On obtient donc que μ **est irréductible sur** L **ssi** $\alpha \in K$.	/	**NON** Pour $\theta \notin \pi\mathbb{Z}$ et $M = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & cos(\theta) \end{pmatrix}$ on a $\mu_M(X) = (X - e^{i\theta})(X - e^{-i\theta})$ qui est irréductible sur $\mathbb{R}$ mais réductible sur $\mathbb{C}$.
μ est-il à racines simples sur son corps de décomposition ?	**Si** K **est parfait** (i.e. si K est de caractéristique nulle ou si K est de caractéristique première p et tel que le morphisme de Frobenius $\Phi : x \mapsto x^p$ est surjectif), alors μ **est à racines simples sur son corps de décomposition**. En effet, si K est de caractéristique nulle, alors μ est scindé à racines simples sur L **ssi** μ est premier avec μ', ce qui est le cas car μ est irréductible sur K. Si K est de caractéristique p première, alors cette propriété est vraie si le morphisme de Frobenius est surjectif. Sinon, ce résultat est **faux en général**.	/	**NON** Pour $M = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, on a $\mu_{K,M}(X) = \mu_{L,M}(X) = X^2$, qui n'est pas à racines simples.
R est-il un espace vectoriel sur K de dimension finie ?	*Cf. ci-contre.*	**OUI** R est un espace vectoriel de degré d, dont une base est donnée par $\mathcal{B} = \left(\overline{1}, \cdots, \overline{X^{d-1}}\right)$. En effet, soit $P \in K[X]$ et notons $P = Q\mu + S$ sa division euclidienne dans $K[X]$. On a alors $deg(S) < d$. Or, par définition de μ, on a $P(x) = S(x)$, ce qui permet de conclure.	*Cf. ci-contre.*

R est-il un sous-anneau de L resp. $\mathcal{M}_n(K)$?	*Cf. ci-contre.*	**OUI** R est l'image d'un morphisme d'algèbres.	*Cf. ci-contre.*
R est-il une K-algèbre ?	*Cf. ci-contre.*	**OUI** R est l'image d'un morphisme d'algèbres.	*Cf. ci-contre.*
R est-il commutatif ?	*Cf. ci-contre.*	**OUI** K est commutatif, et R est un quotient de $K[X]$ commutatif.	*Cf. ci-contre.*
A-t-on $\{R$ intègre $\Rightarrow R$ corps $\}$?	*Cf. ci-contre.*	**OUI (et c'est un résultat important !)** R intègre $\Leftrightarrow \mu$ est irréductible $\Leftrightarrow (\mu)$ est maximal (car $K[X]$ est principal) $\Leftrightarrow R \simeq K[X]/(\mu)$ est un corps.	*Cf. ci-contre.*
R est-il intègre ?	**OUI** R est un sous-anneau de L, qui est un corps. En particulier, R est donc toujours un corps, donc intègre.	/	$R \simeq K[X]/(\mu)$ est intègre **ssi** (μ) est premier **ssi μ est irréductible** (car $K[X]$ est principal).
R est-il le plus petit sous-anneau de L (resp. de $\mathcal{M}_n(K)$) contenant K et α (resp. K et M) ?	*Cf. ci-contre.*	**OUI** Tout anneau contenant K et x contient également $K[x]$. Donc $R = K[x]$ est le plus petit sous-anneau de L vérifiant cette propriété.	*Cf. ci-contre.*
R est-il le plus petit sous-corps de L (resp. de $\mathcal{M}_n(K)$) contenant K et α (resp. K et M) ?	**OUI** Cf. ci-dessus, R est intègre et est le plus petit sous-anneau de L contenant à K et α.	/	C'est le cas **ssi R est un corps commutatif.**

Si K' est une extension de K, a-t-on $\mu_{K',M} = \mu_{K,M}$?	/	/	**OUI** Soit K' une extension de K. Alors $\mu_{K',M} \vert \mu_{K,M}$. Par ailleurs, $deg(\mu_{K',M}) = dim\left(Vect_{K'}\left((M^k)_{k\in\mathbb{N}}\right)\right) = rg_{K'}\left((M^k)_{k\in\mathbb{N}}\right)$. Or, le rang d'une famille de vecteurs est invariant par extension de corps (cf. pivot de Gauss). Donc $deg(\mu_{K',M}) = rg_{K'}\left((M^k)_{k\in\mathbb{N}}\right) = rg_K\left((M^k)_{k\in\mathbb{N}}\right) = deg(\mu_{K,M})$. Etant donné que $\mu_{K,M}$ et $\mu_{K',M}$ sont tous deux unitaires, la relation de divisibilité et l'égalité des degrés donnent bien $\mu_{K',M} = \mu_{K,M}$.
Si K' est une extension de K et si K' est également un sous-corps de L contenant α, a-t-on $\mu_{K'/K,\alpha} = \mu_{L/K,\alpha}$ et/ou $\mu_{L/K,\alpha} = \mu_{L/K',\alpha}$?	$\alpha \in K'$, donc **on a bien** $\mu_{K'/K,\alpha} = \mu_{L/K,\alpha}$. En revanche, **on n'a pas** $\mu_{L/K,\alpha} = \mu_{L/K',\alpha}$ **!** En effet, si $\alpha \in K' \backslash K$, alors $\mu_{L/K',\alpha} = (X - \alpha)$, mais comme $\alpha \notin K$ on ne peut pas avoir $\mu_{L/K,\alpha}$ de degré 1.	/	/