Leçon 144-Racines d'un polynôme-Polynômes symétriques

Introduction :

C'est une leçon qui a beaucoup en commun avec la leçon 125 sur les extensions de corps, sauf qu'il ne faut jamais s'éloigner du thème de la racine d'un polynôme. On peut commencer par définir rapidement la notion de polynômes et de racines. Noter que l'ensemble des racines arrive sans ordre prédéterminé ; par exemple, l'ensemble des racines d'un polynôme de degré n sur K dans une clôture algébrique $\overline{K}$ peut être vu comme un élément de $\overline{K}^n/\mathfrak{S}_n$. Ceci débouche naturellement sur la notion de polynômes symétriques à n indéterminées puisque les fonctions polynomiales sur $\overline{K}^n/\mathfrak{S}_n$ correspondent, via un passage au quotient, aux fonctions polynomiales sur $\overline{K}^n$ constantes sur les orbites pour l'action de $\mathfrak{S}_n$, c'est-à-dire les polynômes symétriques sur $\overline{K}^n$.

Il faut insister sur l'importance des polynômes dans la réduction (polynômes caractéristiques d'un endomorphisme, en particulier, car ses racines sont les valeurs propres de l'endomorphisme en question) et inversement, sur l'importance actuelle de la réduction dans la recherche d'approximation de racines ainsi que pour la borne de Cauchy.

Peaux de bananes classiques et pièges à mammouths :

1. Attention aux conditions sur le corps de base ou sur l'anneau de base. Par exemple :
   (a) Si l'anneau n'est pas intègre, on n'a pas l'additivité des degrés $\deg(PQ) = \deg(P) + \deg(Q)$ et donc, le degré n'est plus une borne pour le nombre de racines.
   (b) Si A n'est pas un corps, alors $A[X]$ n'est pas principal, et donc non euclidien. Toutefois, on peut toujours diviser par un polynôme unitaire. Parfois, l'identité

$$X^n - a^n = (X - a)(X^{n-1} + aX^{n-2} + \cdots + a^{n-1})$$

peut s'avérer très utile.

(c) Pour pouvoir identifier polynômes et fonctions polynômes, il faut que le corps soit infini. Si le corps est fini, de cardinal q, le polynôme $X^q - X$ est non nul comme polynôme mais nul comme fonction. C'est même le générateur de l'idéal des polynômes vérifiant cette propriété.

(d) La formule de Taylor polynomiale, et donc le critère qui en découle sur les racines multiples, est valable sur un corps de caractéristique nulle.

2. Les fonctions symétriques élémentaires sont des générateurs de l'algèbre $\mathbb{K}[X_1, \cdots, X_n]^{\mathfrak{S}_n}$. Cela marche aussi en remplaçant $\mathbb{K}$ par $\mathbb{Z}$. Les sommes de Newton engendrent aussi l'algèbre mais en caractéristique nulle. Observer les formules $s_2 = e_1^2 - 2e_2$ et $e_2 = \frac{1}{2}(s_1^2 - s_2)$ et méditez !
3. Attention, la notion d'irréductibilité dépend dramatiquement du corps sur lequel on se trouve. On dit « irréductible sur le corps $\mathbb{K}$ ».
4. Attention aux corps finis. Le piège le plus énorme est de croire que $\mathbb{F}_4$ est égal à $\mathbb{Z}/4\mathbb{Z}$. Il faut savoir répondre à la question « Pourquoi ne sont-ils pas isomorphes ? ».

I. Les fondamentaux

1. La division euclidienne, le degré qui est à valeurs dans $\mathbb{N}$ (et donc, on ne peut pas le diminuer indéfiniment), on ne peut donc pas diviser indéfiniment par $(X-a)$ et, sur un anneau intègre, le nombre de racines est limité par le degré. Contre-exemple : le lemme chinois permet de voir que, dans $\mathbb{Z}/pq\mathbb{Z}$, p, q premiers impairs distincts, l'équation $x^2 = 1$ possède $2^2 = 4$ racines.
2. Bien comprendre le lien entre polynômes et fonctions polynômes. On a un morphisme de $\mathbb{K}$-algèbres qui envoie $\mathbb{K}[X]$ sur la $\mathbb{K}$-algèbre des fonctions polynômes à une variable. Il est surjectif par définition, et injectif si et seulement si le corps est infini ; on a alors, dans ce cas, une identification canonique entre polynômes et fonctions polynômes. On peut remplacer dans ce résultat le corps $\mathbb{K}$ par le corps des fractions de $k[X_1, \cdots, X_{n-1}]$, ce qui permet de généraliser facilement cette identification quand le corps k est infini.
3. La multiplicité d'une racine a du polynôme $P \in \mathbb{K}[X]$ est égale au nombre m maximal tel que $P^{(m-1)}(a) = 0$ et $P^{(m)}(a) \neq 0$. Attention, quitte à se répéter ce critère demande $\mathbb{K}$ de caractéristique nulle pour pouvoir utiliser Taylor. Contre-exemple : X^2 en caractéristique 2, dont 0 est racine d'ordre 2 alors que toutes les dérivées s'annulent.

4. Le corps $\mathbb{C}$ est algébriquement clos. Voir le développement dans [1, 1.3.21].
5. Sur un corps fini, pour l'existence de racines en degré 2, on utilise le symbole de Legendre (qui vient remplacer la notion de signe du discriminant dans $\mathbb{R}$).
6. On va chercher des racines dans des extensions. Soit P un polynôme irréductible sur $\mathbb{K}$, alors $\mathbb{L} := \mathbb{K}[X]/(P)$ est un corps de rupture pour P, c'est-à-dire une extension de $\mathbb{K}$ dans laquelle P possède une racine, nommément $\alpha := \overline{X}$, la classe de X. On a alors $\mathbb{L} = \mathbb{K}[\alpha]$ et le degré de $\mathbb{L}$ sur $\mathbb{K}$ est égal au degré du polynôme.
7. Réciproquement, si α est dans une extension finie de $\mathbb{K}$, alors, il existe un unique polynôme μ_α de $\mathbb{K}[X]$ qui annule α. Ce polynôme est irréductible, son degré est égal au degré de $\mathbb{L}$ sur $\mathbb{K}$ et tous les polynômes qui annulent α sont multiples de μ_α. Du coup, cela donne un joli critère d'irréductibilité : si P dans $\mathbb{K}[X]$ annule α et si son degré vaut le degré de l'extension $[\mathbb{K}[\alpha] : \mathbb{K}]$, alors P est irréductible.
8. Maintenant, à quelle condition une racine, que l'on est allé chercher dans une extension appartient-elle au corps de base ? La théorie de Galois répond à cette question. Dans la pratique, on utilise souvent des extensions cycliques et il suffit que la racine soit invariante par un seul élément (le générateur du groupe cyclique). Par exemple, a) la racine α de $\mathbb{C}$ est réelle si et seulement si $\bar{\alpha} = \alpha$, b) la racine α de $\mathbb{F}_{p^n}$ est dans $\mathbb{F}_p$ si et seulement si $\alpha^p = \alpha$, et c) on a un a une propriété analogue dans les extensions cyclotomiques, voir [2, 13-E.33].
9. (Sympa mais pas indispensable) On met une topologie quotient sur l'ensemble $\mathbb{C}^n/\mathfrak{S}_n$. On a alors un homéomorphisme de $\mathbb{C}^n/\mathfrak{S}_n$ sur $\mathbb{C}^n$ qui envoie la classe de
$$(\lambda_1, \cdots, \lambda_n)$$
sur
$$(e_1(\lambda_1, \cdots, \lambda_n), e_2(\lambda_1, \cdots, \lambda_n), e_n(\lambda_1, \cdots, \lambda_n)),$$
où les e_i sont les polynômes symétriques élémentaires. Voir [3, Exercice II-F.33] ou [1, 1.3.42].

II. Questions classiques du jury

1. Trouver le polynôme unitaire de degré 3 ayant pour racines a^2, b^2, c^2, où a, b, c sont les racines de $X^3 + X + 1$.

   Tout l'art consiste à ne pas calculer les racines. Il faut écrire les relations entre les polynômes symétriques élémentaires en les a^2, b^2, c^2 (qui

sont des polynômes symétriques en a, b, c) en fonction des polynômes symétriques élémentaires en a, b, c.

2. Résoudre le système

$$\begin{cases} x+y+z & = 1 \\ x^2+y^2+z^2 & = 21 \\ 1/x+1/y+1/z & = 1 \end{cases}$$

On trouve alors la valeur des trois fonctions symétriques élémentaires en x, y, z. On trouve donc le polynôme P de degré 3 dont x, y, z sont racines et on trouve ensuite les racines de P...

3. Montrer que le polynôme $X^5 - X - 1$ est irréductible sur $\mathbb{Q}$.
Il suffit de le montrer sur $\mathbb{Z}$ car $\mathbb{Z}$ est factoriel, et pour ce faire, on montre qu'il est irréductible sur $\mathbb{F}_5$. Faire agir le Frobenius sur l'ensemble des racines du polynôme s'avère utile.

4. Pouvez-vous déterminer le corps $\mathbb{F}_3(\alpha)$, où α est une racine primitive 7-ième de 3 ?
Pareil, on fait agir le Frobenius. L'orbite de α est $\{\alpha, \alpha^3, \alpha^2, \alpha^6, \alpha^4, \alpha^5\}$. Donc, le polynôme ϕ_7 reste irréductible modulo 5 et $\mathbb{F}_3(\alpha) = \mathbb{F}_{3^6}$.

5. Soit α une racine du polynôme P sur $\mathbb{K}[X]$. On suppose $[\mathbb{K}(\alpha) : \mathbb{K}] > \deg P/2$. Montrer que P est irréductible.
Il n'y a plus d'extension intermédiaire une fois passé le degré $\deg P/2$. Donc, le degré est bien $\deg P$, d'où l'irréductibilité du polynôme.

6. Soient P, Q dans $\mathbb{Z}[X]$ sans racine commune dans $\mathbb{C}$. Quels sont les nombres premiers tels que P et Q ont une racine dans $\mathbb{F}_p$?
Les p premiers qui divisent le résultant de P et Q.

III. Pour enjoliver la leçon. Les extensions du domaine.

1. Incontournable : Des polynômes (et leurs racines !) vers la réduction :
   (a) On connaît l'application qui envoie une matrices carrée A vers son polynôme caractéristique χ_A. Comme inverse à droite de cette application, on peut associer à $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$, unitaire de degré n, sa matrice compagnon C_P. a) On a $\chi_{C_P} = P$ et donc les racines de P sont les valeurs propres de C_P. b) Pour ce qui est du polynôme minimal : $\mu_{C_P} = P$. Donc, C_P est diagonalisable si et seulement si P est à racines simples. c) Sur le corps $\mathbb{C}$ des complexes. On a les disques de Gershgorin (ou borne de Cauchy) : on voit en prenant un vecteur propre $v := (v_i)$ de $\mathbb{C}^n$ pour la

valeur propre λ de C_P (et donc la racine λ de P), avec v_i tel que $|v_k|$ soit maximum, que $\lambda \leq 1 + |a_i|$ et même $|a_0|$ pour $i = 0$. Voir [3, III-D8], ou [1, 1.3.11,1.3.43].

On en déduit une localisation des racines : elles se trouvent dans un disque de centre 0 et de rayon

$$R = \max\{|a_0|, 1 + |a_1|, \cdots, 1 + |a_{n-1}|\}.$$

On peut voir que c'est optimal.

(b) Si $\mathbb{L}$ est une extension du corps $\mathbb{K}$, alors pour deux matrices de $\mathcal{M}_n(\mathbb{K})$, $\mathrm{GL}_n(\mathbb{L})$-semblables implique $\mathrm{GL}_n(\mathbb{K})$-semblables.

(c) Un peu de topologie : on met une topologie quotient sur $\mathbb{C}^n/\mathfrak{S}_n$. On a alors un homéomorphisme de $\mathbb{C}^n/\mathfrak{S}_n$ sur $\mathbb{C}^n$ qui envoie la classe de

$$(\lambda_1, \cdots, \lambda_n)$$

sur

$$(e_1(\lambda_1, \cdots, \lambda_n), e_2(\lambda_1, \cdots, \lambda_n), e_n(\lambda_1, \cdots, \lambda_n)).$$

On voit facilement qu'il s'agit d'une application continue (après passage au quotient), bijective. Pour la bicontinuité, c'est la borne de Cauchy qui l'assure.

En fait, on peut faire beaucoup plus simple, et obtenir un résultat de continuité des racines sans se servir de la topologie quotient, voir annexe.

Comme applications, on a les résultats suivants :

• L'adhérence de l'ensemble des matrices diagonalisables réelles est égal à l'ensemble des matrices trigonalisables sur $\mathbb{R}$. En effet,

Soit $P \in \mathbb{R}[X]$, P unitaire de degré n. Alors les conditions suivantes sont équivalentes :

i. P est scindé sur $\mathbb{R}$, *phi. e. toutes les racines de P sont réelles,*

ii. $|\mathrm{Im}(z)|^n \leq |P(z)|$, *pour tout* $z \in \mathbb{C}$.

Il est clair que (ii) implique (i) puisque dans ce cas une racine (complexe) z de P vérifie $0 \leq |\mathrm{Im}(z)|^n \leq |P(z)| = 0$, et donc $\mathrm{Im}(z) = 0$, ce qui implique que z est réel. Réciproquement, si P est scindé sur $\mathbb{R}$, alors

$$|P(z)|^2 = \prod_{k-1}^{n} |z - x_k|^2,$$

avec x_k réels, et donc $|z - x_k|^2 = |(\mathrm{Re}(z) - x_k) + i\,\mathrm{Im}(z)|^2 \geq |\mathrm{Im}(z)|^2$, ce qui prouve bien que $|\mathrm{Im}(z)|^n \leq |P(z)|$.

Cette condition est *fermée*, dans le sens où elle est stable par passage à la limite. Donc, si $(P_m)_m$ est une suite de polynômes unitaires de degré n, scindés sur $\mathbb{R}$, qui tendent vers un polynôme P, alors P est encore scindé sur $\mathbb{R}$. Comme l'application qui à une matrice A de $\mathcal{M}_n(\mathbb{R})$, associe son polynôme caractéristique, est continue, et qu'une matrice est trigonalisable si, et seulement si, son polynôme caractéristique est scindé sur $\mathbb{R}$, on en déduit qu'une suite de matrices trigonalisables réelles qui converge tend vers une matrice trigonalisable réelle. La réciproque se fait comme dans le cas complexe.

• Trouver l'adhérence de l'ensemble des matrices symétriques réelles de signature donnée. Voir [3, V-D9]

(d) Le passage de l'anneau (intègre) A à son corps de fraction $\mathbb{K}$. On passe de résultats sur $A[X]$ à des résultats sur $\mathbb{K}[X]$.

• C'est ce qui va permettre de passer de une à plusieurs variables, en posant $A := k[X_1, \cdots, X_{n-1}]$.

• Si A est factoriel, le lemme de Gauss permet de voir que si p/q, p, q premiers entre eux dans A, est racine de $a_n X^n + \cdots a_0$, alors q divise a_n et p divise a_0. Dans la pratique, cela permet souvent de chercher les racines rationnelles parmi un nombre fini d'entiers. Dans la théorie cela dit qu'un anneau factoriel est intégralement clos : toute racine de $\mathrm{Frac}(A)$ d'un polynôme unitaire de $A[X]$ est en fait dans A.

(e) Théorème de Gauss-Wantzel : un nombre complexe est constructible à la règle et au compas si et seulement s'il appartient à une tour d'extensions quadratiques.

(f) Payback time ! Les applications de la réduction à l'approximation de racines.

• La méthode QR. Si A est une matrice carrée, on peut la décomposer en une matrice Q orthogonale et une matrice R triangulaire supérieure. C'est disons du "Gram-Schmidt" version matricielle. Ensuite, on pose $A_0 = A$, $A_1 = RQ$, qui est semblable à A. On décompose $A_1 := Q_1 R_1$, on pose $A_2 := R_1 Q_1$ et ainsi de suite. On obtient une suite A_k de matrices toutes semblables entre elles et, avec des hypothéses raisonnables (les valeurs propres de A doivent être de modules distincts, A est donc diagonalisable mais on veut ajouter que la matrice de passage assurant la diagonalisation vé-

rifie la condition LU !) A_k tend vers une matrice triangulaire supérieure. Bref, on voit appraître les valeurs propres (approchées) sur la diagonale des A_k.

Donc, si l'on part d'un polynôme P dans $\mathbb{R}[X]$, on applique la méthode à C_P pour voir apparaître ses racines. Voir [4]

• La méthode des puissances. Soit A est une matrice carrée de $\mathbb{C}$ et $(\lambda_1, \cdots, \lambda_n)$ ses valeur propres. Si l'on suppose l'hypothèse que λ_1 est l'unique valeur propre de module maximal, alors en partant d'un vecteur w générique (il faut le prendre dans le complémentaire de la somme des sous-espace caractéristiques associées aux λ_i, $i > 1$), on peut calculer λ_1. On pose $w_0 := w$, puis on normalise Aw_0 et on réitère. On tend alors vers un vecteur propre pour la valeur propre λ_1. Voir [Carnet de Voyage en Analystan, Ex. 81].

IV. Les développements

1. Le théorème de Kronecker : si un polynôme unitaire de $\mathbb{Z}[X]$ a toutes ses racines dans le disque unité, alors ses racines sont des racines de l'unité. Voir [3, III-D10]. Niveau : 4/5 Originalité : 3/5
2. Les formes de Hankel. Trouver le nombre de racines distinctes et le nombre de racines réelles d'un polynôme réel à partir du rang et de la signature d'une forme quadratique associée. Voir [1, 2.3.4]. Niveau : 4/5 Originalité : 4/5
3. L'adhérence de l'ensemble des matrices réelles diagonalisables est égal à l'ensemble des matrices réelles trigonalisables, voir [1, 1.3.45].
4. Un petit théorème de Harish-Chandra. Trouver toutes les fonctions polynomiales sur $\mathcal{M}_n(\mathbb{C})$ invariantes par l'action par conjugaison de $\mathrm{GL}_n(\mathbb{C})$ (il y a le déterminant et la trace, mais à part ça ?). Voir [3, III-D29] Niveau : 4/5 Originalité : 5/5
5. Nombre de polynômes unitaires irréductibles de degré n sur $\mathbb{F}_q$ [Francinou-Gianella, Algèbre, p. 189]. Niveau : 4/5 Originalité : 3/5
6. Irréductibilité (ou pas) des polynômes cyclotomiques, [1, 4.2.24]. Niveau : 3/5 Originalité : 3/5

Références

[1] Philippe Caldero et Marie Péronnier. *Carnet de Voyage en Algébrie.* Calvage et Mounet, 2019.

[2] Philippe Caldero et Jérôme Germoni. *Nouvelles Histoires Hédonistes de Groupes et de Géométries, tome second.* Calvage et Mounet, 2018.

[3] Philippe Caldero et Jérôme Germoni. *Nouvelles Histoires Hédonistes de Groupes et de Géométries*. Calvage et Mounet, 2017.

[4] Denis Serre. *Matrices, volume 216 of Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.