Leçon 144 - Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications

Extrait du rapport de jury

Dans cette leçon, il est indispensable de bien définir l'ordre de multiplicité d'une racine (définition algébrique et analytique, quand c'est possible). Les fonctions symétriques élémentaires et les relations entre coefficients et racines doivent être maîtrisées et pouvoir être mises en oeuvre. Des méthodes, même élémentaires, de localisation des racines ont toute leur place et peuvent déboucher sur des résultats de topologie à propos de la continuité des racines.
Il peut être pertinent d'introduire la notion de polynôme scindé et de citer le théorème de d'Alembert-Gauss. Il est apprécié de faire apparaître le lien entre la recherche des racines d'un polynôme et la réduction des matrices. Les candidats peuvent également s'intéresser aux racines des polynômes orthogonaux, ou aux règles des signes de Descartes et de Sturm. L'étude des propriétés des nombres algébriques peuvent trouver leur place dans cette leçon. La théorie des corps et le cas particulier des corps finis peuvent aussi être évoqués de façon pertinente.
Les candidates et candidats peuvent s'intéresser à des problèmes de localisation des valeurs propres, comme les disques de Gershgorin ou au calcul effectif d'expressions polynomiales symétriques des racines d'un polynôme.
Il ne s'agit par contre en aucun cas d'adapter le plan de la leçon 141 : l'irréductibilité des polynômes peut être évoquée mais ne doit pas être l'élément central de la leçon.

Présentation de la leçon

Je vais vous présenter la leçon 144 intitulée : "Racines d'un polynôme. Fonctions symétriques élémentaires. Exemples et applications.". Le but de cette leçon sera de donner des généralités sur les racines de polynômes, de chercher des racines dans des extensions de corps lorsqu'un polynôme n'en possède pas (assez) sur un corps de base, parler des polynômes symétriques élémentaires et enfin de donner une application des racines de polynômes à la réduction.
Dans une première partie, on s'intéresse aux généralités concernant les racines d'un polynôme. Dans un premier point on introduit ce qu'est une racine d'un polynôme en rappelant la définition ainsi qu'une caractérisation. Cette caractérisation nous permet de borner le nombre de racines d'un polynôme et d'en donner une factorisation. On se rend également compte qu'il existe des polynômes comme $(X-1)^2$ qui sont de degré 2 mais n'ont "qu'une seule racine", il vient alors naturellement la question de multiplicité d'une racine : c'est ce dont nous parlons dans le deuxième point. On introduit ainsi ce qu'est la multiplicité d'une racine ainsi qu'un exemple et on ré-énonce les corollaires 3 et 4 avec cette notion supplémentaire. On termine ce point par rappeler ce qu'est le polynôme dérivé ainsi que la formule de Taylor en vue d'énoncer le corollaire 14 qui donne une caractérisation de la multiplicité d'une racine. On termine cette première partie avec l'étude du cas réel et complexe où l'on commence par énoncer le théorème de D'Alembert-Gauss puis l'écriture d'un polynôme en produit d'irréductibles dans le cas complexe puis réel.
On remarque cependant qu'un polynôme n'admet pas forcément de racines dans un corps donné. Il est donc nécessaire d'aller dans des sur-corps du corps considéré pour trouver des racines d'un polynôme. C'est donc pour cela que dans une deuxième partie, on s'intéresse aux extensions de corps. On commence dans une première sous-partie à parler d'élément algébrique en en donnant la définition ainsi qu'un premier exemple, puis en donnant une caractérisation très utile en pratique des éléments algébriques. On conclut cette première sous-partie par la définition d'une extension finie et algébrique ainsi que d'un corps algébriquement clos qui nous seront utiles dans la suite de cette leçon. Dans un deuxième point, on s'intéresse aux corps de rupture et de décomposition (c'est eux qui nous donnerons de nouvelles racines d'un polynôme). On commence par donner la définition d'un corps de rupture puis on énonce une close d'existence et d'unicité à isomorphisme près d'un corps de rupture d'un polynôme irréductible. On fait ensuite de même avec le corps de décomposition et l'on termine cette sous-partie avec l'existence d'un corps fini à p^n éléments en tant que corps de décomposition du polynôme $X^{p^n}-X$ sur $\mathbb{F}_p$. Dans une troisième sous-partie on va s'intéresser à l'irréductibilité de polynômes grâce à ses racines. On commence par donner la définition d'un polynôme irréductible avant de passer à des critères d'irréductibilité ainsi que des exemples. On énonce notamment les propositions 35 et 37 qui donnent l'irréductibilité d'un polynôme en fonction de son degré ou de ses racines et on donne des exemples de ces propositions. On termine cette partie avec un dernier point consacré aux racines de l'unité et polynômes cyclotomiques. On donne notamment la définition d'un polynôme

cyclotomique et on montre qu'ils sont dans $\mathbb{Z}[X]$ et irréductibles dans $\mathbb{Q}[X]$.
Dans une troisième partie on s'intéresse aux polynômes symétriques élémentaires avec tout d'abord les premières définitions ainsi que les relations coefficients/racines. On donne ainsi la définition d'un polynôme symétrique et d'un polynôme symétrique élémentaire et on termine par les relations coefficients/racines ainsi que quelques exemples. Dans une deuxième sous-partie, on parle du théorème en structure en donnant son énoncé ainsi qu'un exemple et le théorème de Kronecker.
Enfin, on consacre une dernière partie aux liens entre cette leçon et la réduction. Tout d'abord on regarde tout particulièrement le lien avec la diagonalisation et la trigonalisation en montrant tout d'abord que les valeurs propres sont exactement les racines du polynôme caractéristique puis on donne des critères de diagonalisation et de trigonalisation en fonction du polynôme minimal et caractéristique ainsi qu'une application avec les matrices circulantes. On conclut finalement cette partie et cette leçon avec la localisation des valeurs propres d'une matrice et des racines d'un polynôme grâce aux disques de Gerschgorin qui permettent d'énoncer le théorème de Gerschgorin puis on conclut avec un encadrement du module d'une racine d'un polynôme complexe.

Plan général

Cours détaillé

I Généralités

Dans toute cette partie, on considère un corps commutatif $\mathbb{K}$ quelconque.

I.1 Racine d'un polynôme

Définition 1 : Racine d'un polynôme [Deschamps, p.897] :
On considère un polynôme $P \in \mathbb{K}[X]$.
On dit qu'un élément $\alpha \in \mathbb{K}$ est une **racine de** P (dans $\mathbb{K}$) lorsque $P(x) = 0_{\mathbb{K}}$.

Proposition 2 : [Deschamps, p.897]
Soit $P \in \mathbb{K}[X]$.
Un élément $\alpha \in \mathbb{K}$ est racine de P si, et seulement si, $(X - \alpha)$ divise P.

Corollaire 3 : [Deschamps, p.898]
Soit $n \in \mathbb{N}$.
Un polynôme de $\mathbb{K}[X]$ degré n admet au plus n racines distinctes.
En particulier, un polynôme de $\mathbb{K}_n[X]$ admettant au moins $n+1$ racines deux à deux distinctes est le polynôme nul.

Corollaire 4 : [Deschamps, p.899]
Soient $n \in \mathbb{N}$ et $P \in \mathbb{K}[X]$.
Si P est de degré n et admet n racines deux à deux distinctes notées $\alpha_1, ..., \alpha_n$, alors on a :

$$P(X) = \lambda \prod_{i=1}^{n} (X - \alpha_i)$$

avec λ le coefficient dominant de P.

Exemple 5 : [Deschamps, p.899]
Pour $n \in \mathbb{N}^*$, le polynôme unitaire $X^n - 1 \in \mathbb{C}[X]$ possède n racines distinctes qui sont les racines n-ièmes de l'unité. On a donc :

$$X^n - 1 = \prod_{k=0}^{n-1} \left(X - e^{\frac{2ik\pi}{n}} \right)$$

I.2 Multiplicité d'une racine

Définition 6 : Ordre de multiplicité d'une racine [Deschamps, p.902] :
On considère $P \in \mathbb{K}[X]$ un polynôme non nul et $\alpha \in \mathbb{K}$ une racine de P.
On appelle **ordre de multiplicité** de α le plus grand entier naturel p tel que $(X-a)^p$ divise P. On dit alors que α est une racine d'ordre p de P.

Remarque 7 : [Deschamps, p.903]
Si α est racine d'ordre p d'un polynôme non nul $P \in \mathbb{K}[X]$, alors $(X-a)^p$ divise P et $(X-a)^{p+1}$ ne divise pas P.

Exemple 8 : [Deschamps, p.904]
Le polynôme $(X-1)(X+1)^2(X-2)^3$ possède 3 racines distinctes (-1,1 et 2) et 6 racines comptées avec multiplicité (-1,1,1,2,2 et 2).

Proposition 9 : [Deschamps, p.904]
Soit $n \in \mathbb{N}$.
Un polynôme de degré n admet au plus n racines distinctes comptées avec multiplicité.

Exemple 10 :
$*$ Le polynôme X^3+2X+1 admet au plus 3 racines dans $\mathbb{C}[X]$.
$*$ La proposition précédente devient fausse dans le cas d'un anneau non intègre. En effet, le polynôme $P(X) = 4X \in \mathbb{Z}/8\mathbb{Z}[X]$ admet trois racines $(\overline{0}, \overline{2}, \overline{4})$ mais n'est que de degré 1.

Corollaire 11 : [Deschamps, p.904]
Soit P un polynôme non nul de $\mathbb{K}[X]$.
Si $\alpha_1, ..., \alpha_p$ sont p racines deux à deux distinctes de P et d'ordre respectivement égal à $r_1, ..., r_p$ et si $\deg(P) = \sum_{i=1}^{p} r_i$, alors :

$$P(X) = \lambda \prod_{i=1}^{n} (X-\alpha_i)^{r_i}$$

avec λ le coefficient dominant de P.

Définition 12 : Polynôme dérivé [Deschamps, p.906] :
On considère $P(X) = \sum_{k=0}^{n} a_k X^k$.
On appelle **polynôme dérivé de** P le polynôme $P'(X) = \sum_{k=1}^{n} k a_k X^{k-1}$.

Proposition 13 : Formule de Taylor [Deschamps, p.908] :
Soient $P \in \mathbb{K}[X]$ et $\alpha \in \mathbb{K}$.
Si $\mathrm{car}(\mathbb{K}) = 0$, alors on a $P(X) = \sum_{k=0}^{+\infty} \frac{P^{(k)}(\alpha)}{k!}(X-\alpha)^k$.

Corollaire 14 : [Deschamps, p.909]
Soient $P \in \mathbb{K}[X]$, $\alpha \in \mathbb{K}$ et $r \in \mathbb{N}^*$.
Si $\mathrm{car}(\mathbb{K}) = 0$, alors α est racine de P d'ordre r si, et seulement si, on a :

$$P(\alpha) = P'(\alpha) = ... = P^{(r-1)}(\alpha) = 0 \text{ et } P^{(r)}(\alpha) \neq 0_{\mathbb{K}}$$

Remarque 15 :
En caractéristique non nulle, le corollaire précédent devient faux. En effet, dans $\mathbb{Z}/3\mathbb{Z}$, $\overline{0}$ est racine d'ordre 3 de X^3 mais $P^{(3)}\left(\overline{0}\right) = \overline{0}$.

I.3 Cas réel et complexe

Théorème 16 : Théorème de D'Alembert-Gauss [Deschamps, p.910] :
Tout polynôme non constant de $\mathbb{C}[X]$ admet au moins une racine dans $\mathbb{C}$ (autrement dit, $\mathbb{C}$ est algébriquement clos (cf. df. 25)).

Proposition 17 : [Deschamps, p.910]
Soit P un polynôme non nul à coefficients complexes.
Si $\alpha_1, ..., \alpha_p$ sont les racines complexes deux à deux distinctes de P et $r_1, ..., r_p$ leurs ordres de multiplicité respectifs, alors on a :

$$P(X) = \lambda \prod_{k=1}^{p} (X-\alpha_k)^{r_k}$$

avec λ le coefficient dominant de P.

Exemple 18 : [Deschamps, p.911]
Le polynôme X^2+X+1 divise le polynôme X^8+X^4+1.

Proposition 19 : [Deschamps, p.911]
Tout polynôme non nul P de $\mathbb{R}[X]$ peut s'écrire sous la forme :

$$P(X) = \lambda \prod_{j=1}^{p} (X-\alpha_j)^{r_j} \prod_{k=1}^{q} (X^2+\beta_k X+\gamma_k)^{s_k}$$

où p et q sont deux entiers naturels, λ un réel, les r_j et s_k sont des entiers naturels non nuls et les α_j, β_k et γ_k sont des réels avec $\beta_k^2 - 4\gamma_k < 0$.

Exemple 20 : [Deschamps, p.911]
Dans $\mathbb{R}[X]$, on a :

$$X^4+1 = \left(X^2+\sqrt{2}X+1\right)\left(X^2-\sqrt{2}X+1\right)$$

II Extension de corps

II.1 Élément algébrique

Définition 21 : Élément algébrique/transcendant [Perrin, p.66] :
On considère une extension de corps $\mathbb{L}/\mathbb{K}$, $\alpha \in \mathbb{L}$ ainsi que le morphisme φ : $\mathbb{K}[T] \longrightarrow \mathbb{L}$ tel que $\varphi|_{\mathbb{K}} = \mathrm{Id}_{\mathbb{K}}$ et $\varphi(T) = \alpha$.
$*$ Lorsque φ est injectif, il n'y a que le polynôme nul qui s'annule en α. On dit alors que α est **transcendant sur** $\mathbb{K}$.
$*$ Lorsque φ n'est pas injectif, il existe $\mu_\alpha \in \mathbb{K}[T]$ non nul unitaire tel que $\mathrm{Ker}(\varphi) = (\mu_\alpha)$. On dit alors que α est **algébrique sur** $\mathbb{K}$ et que μ_α est le **polynôme minimal de** α **sur** $\mathbb{K}$.

Exemple 22 : [Perrin, p.66]
$*$ Les nombres $\sqrt{2}$, i et $\sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$ de polynômes minimaux respectifs X^2-2, X^2+1 et X^3-2.
$*$ Les nombres π et e sont transcendants sur $\mathbb{Q}$ (mais pas sur $\mathbb{R}$) [ADMIS].

Proposition 23 : Caractérisation des éléments algébriques [Perrin, p.66] :
Soient $\mathbb{L}/\mathbb{K}$ une extension de corps et $\alpha \in \mathbb{L}$.
Les assertions suivantes sont équivalentes :
$*$ α est algébrique sur $\mathbb{K}$. $*$ On a $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$.
$*$ On a $\dim_{\mathbb{K}} \mathbb{K}[\alpha] < +\infty$ (plus précisément, $\dim_{\mathbb{K}} \mathbb{K}[\alpha] = \deg(\mu_\alpha)$).
$*$ Il existe un unique polynôme $\mu_\alpha \in \mathbb{K}[X]$ unitaire et irréductible dans $\mathbb{K}[X]$ tel que $\mu_\alpha(\alpha) = 0_{\mathbb{K}}$.
$*$ $\mathbb{K}(\alpha) = \mathrm{Vect}_{\mathbb{K}}(1_{\mathbb{K}}, \alpha, \alpha^2, ..., \alpha^{\deg(\mu_\alpha)-1})$.

Définition 24 : Extension finie/algébrique [Perrin, p.67] :
On considère une extension de corps $\mathbb{L}/\mathbb{K}$.
On dit que $\mathbb{L}/\mathbb{K}$ est une **extension algébrique** lorsque tout élément de $\mathbb{L}$ est algébrique sur $\mathbb{K}$.

Définition 25 : Corps algébriquement clos [Perrin, p.67] :
On considère un corps $\mathbb{K}$ commutatif quelconque.
On dit que $\mathbb{K}$ est un **corps algébriquement clos** lorsqu'il vérifie l'une des propriétés équivalentes suivantes :
$*$ Tout polynôme $P \in \mathbb{K}[X]$ de degré strictement positif admet une racine dans $\mathbb{K}$.
$*$ Tout polynôme $P \in \mathbb{K}[X]$ est produit de polynômes de degré 1.
$*$ Les éléments irréductibles de $\mathbb{K}[X]$ sont exactement les $X - a$ avec $a \in \mathbb{K}$.
$*$ Si une extension $\mathbb{L}/\mathbb{K}$ est algébrique, alors $\mathbb{L} = \mathbb{K}$.

II.2 Corps de rupture et de décomposition

Dans toute cette sous-partie, on considère un corps commutatif $\mathbb{K}$ quelconque.

Définition 26 : Corps de rupture [Perrin, p.70] :
On considère $P \in \mathbb{K}[X]$ un polynôme irréductible dans $\mathbb{K}[X]$.
Une extension de corps $\mathbb{L}/\mathbb{K}$ est appelée **corps de rupture de** P **sur** $\mathbb{K}$ lorsque $\mathbb{L}$ est monogène $\mathbb{L} = \mathbb{K}(\alpha)$, avec $P(\alpha) = 0$.

Théorème 27 : [Perrin, p.70]
Soit $P \in \mathbb{K}[X]$ irréductible.
Il existe un corps de rupture de P sur $\mathbb{K}$, unique à isomorphisme près.
De plus, $\mathbb{K}[X]/(P)$ est un corps de rupture de P (si on note α la classe de X dans $\mathbb{K}[X]/(P)$, on a $P(X)$ congru à 0 modulo $P(X)$, c'est-à-dire $P(\alpha) = 0$. Ainsi, α est une racine de P dans $\mathbb{K}[X]/(P)$).

Définition 28 : Corps de décomposition [Perrin, p.71] :
On considère $P \in \mathbb{K}[X]$.
Une extension de corps $\mathbb{L}/\mathbb{K}$ est appelée **corps de décomposition de** P **sur** $\mathbb{K}$ lorsque dans $\mathbb{L}[X]$, P est produit de facteurs de degrés 1 et que le corps $\mathbb{L}$ est minimal pour cette propriété.

Exemple 29 :
$*$ Pour $\mathbb{K} = \mathbb{Q}$, $P(X) = X^3 - 2$ a pour corps de décomposition $\mathbb{Q}\left(\sqrt[3]{2}, j\right)$.
$*$ Pour $\mathbb{K} = \mathbb{Q}$, $P(X) = X^4 - 2$ a pour corps de décomposition $\mathbb{Q}\left(\sqrt[4]{2}, i\right)$.

Théorème 30 : [Perrin, p.71]
Pour tout $P \in \mathbb{K}[X]$, il existe un corps de décomposition de P sur $\mathbb{K}$ et il est unique à isomorphisme près.

Théorème 31 : [Perrin, p.73]
Soient p un nombre premier et $n \in \mathbb{N}^*$.
Si l'on pose $q = p^n$, alors il existe un corps $\mathbb{K}$ à q éléments (c'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$).
En particulier, $\mathbb{K}$ est unique à isomorphisme près et on le note $\mathbb{F}_q$.

II.3 Irréductibilité de polynômes et racines

Dans toute cette sous-partie, on considère A un anneau factoriel et commutatif.

Définition 32 : Polynôme irréductible [Perrin, p.46] :
Un polynôme $P \in A[X]$ est un **polynôme irréductible** lorsque $P \notin A^\times$ et ses seuls diviseurs dans $A[X]$ sont les éléments inversibles de $A[X]$ et les associés du polynôme P.

Proposition 33 : Critère de réduction [Perrin, p.77] :
Soient I un idéal premier de A et $P \in A[X]$ unitaire.
Si $\overline{a}_n \neq 0$ dans A/I et si $\overline{P}$ est irréductible sur A/I ou $\mathrm{Frac}(A/I)$, alors le polynôme P est irréductible sur $\mathrm{Frac}(A)$.

Exemple 34 : [Perrin, p.77]
Le polynôme $X^3+462X^2+2433X-67691$ est irréductible dans $\mathbb{Q}[X]$ par le critère de réduction.

Proposition 35 : [Perrin, p.78]
Soit $P \in \mathbb{K}[X]$ de degré $n > 0$.
P est irréductible sur $\mathbb{K}$ si, et seulement si, P n'a pas de racines dans toute extension $\mathbb{L}$ de $\mathbb{K}$ qui vérifie $[\mathbb{L} : \mathbb{K}] \leq \frac{n}{2}$.

Exemple 36 : [Perrin, p.78]
Le polynôme $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$.

Proposition 37 : [Deschamps, p.14]
Soient $\mathbb{K}$ un corps commutatif et $P \in \mathbb{K}[X]$.
* Si $\deg(P) = 1$, alors P est irréductible.
* Si $\deg(P) > 1$ et P est irréductible, alors P n'a pas de racines dans $\mathbb{K}$.
* Si $\deg(P) \in \{2; 3\}$, alors P est irréductible dans $\mathbb{K}[X]$ si, et seulement si, P n'a pas de racines dans $\mathbb{K}$.

Exemple 38 : [Deschamps, p.15]
* Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
* Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatifs.
* Le polynôme $(X^2+1)^2 \in \mathbb{Q}[X]$ n'a pas de racines dans $\mathbb{Q}$ mais n'est pas irréductible.
* Le polynôme $2X$ n'est pas irréductible dans $\mathbb{Z}[X]$.

II.4 Racines de l'unité et polynômes cyclotomiques

Dans toute cette sous-partie, on suppose que $\mathbb{K}$ est un corps commutatif de caractéristique p, on note $\mu_n(\mathbb{K}) = \{\zeta \in \mathbb{K} \text{ tq } \zeta^n = 1\}$ l'ensemble des racines n-ièmes de l'unité dans $\mathbb{K}$ et on suppose que $\mathrm{PGCD}(p, n) = 1$.

Définition 39 : Racine primitive n-ième de l'unité [Perrin, p.80] :
On considère $P(X) = X^n - 1$ et $\mathbb{K}_n$ un corps de décomposition de P.
On appelle **racine primitive n-ième de l'unité**, tout élément $\zeta \in \mathbb{K}_n$ tel que $\zeta^n = 1$ et pour tout $d \in [\![1; n-1]\!]$, $\zeta^d \neq 1$ (et on note $\mu_n^*(\mathbb{K})$ cet ensemble).

Définition 40 : n-ième polynôme cyclotomique [Perrin, p.80] :
On appelle **n-ième polynôme cyclotomique sur** $\mathbb{K}$ le polynôme :
$$\Phi_{n,\mathbb{K}}(X) = \prod_{\zeta \in \mu_n^*(\mathbb{K})} (X - \zeta)$$

Exemple 41 : [Perrin, p.81]
Sur $\mathbb{Q}$, on a :
$\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$ et $\Phi_4(X) = X^2 + 1$.

Proposition 42 : [Perrin, p.80]
On a la formule :
$$X^n - 1 = \prod_{d|n} \Phi_{d,\mathbb{Q}}(X)$$

Développement 1 : [cf. PERRIN]

Théorème 43 : [Perrin, p.82]
Le polynôme $\Phi_n(X)$ est irréductible dans $\mathbb{Q}[X]$.

Corollaire 44 : [Perrin, p.83]
Si ζ est une racine primitive n-ième de l'unité dans un corps commutatif de caractéristique nulle, alors son polynôme minimal sur $\mathbb{Q}$ est $\Phi_{n,\mathbb{Q}}$ et $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

III Polynômes symétriques élémentaires

Dans toute cette partie, on considère A un anneau commutatif.

III.1 Définitions et relation coefficients/racines

Définition 45 : Polynôme symétrique [Berhuy, p.433] :
On considère $P \in A[X_1, ..., X_n]$.
On dit que P est un **polynôme symétrique** lorsque pour tout $\sigma \in \mathfrak{S}_n$, on a $P(X_{\sigma(1)}, ..., X_{\sigma(n)}) = P(X_1, ..., X_n)$.

Exemple 46 : [Berhuy, p.433]
* Si $n = 3$, alors $X_1 + X_2 + X_3$ est symétrique.
* Si $n = 4$, alors $X_1 + X_2 + X_3$ n'est pas symétrique à cause par exemple de la transposition $(1\ 4)$.
* Si $n = 3$, alors $X_1X_2X_3$ est symétrique.

Définition 47 : Somme de Newton :
On considère $k \in \mathbb{N}$.
On appelle **somme de Newton de degré** k **en** n **variables**, le polynôme $\sum_k^{(n)} (X_1, ..., X_n) = \sum_{i=1}^{n} X_i^k$.

Définition 48 : Polynômes symétriques élémentaires [Berhuy, p.434] :
On considère $k \in \mathbb{N}$.
On définit le k**-ième polynôme symétrique** (en n variables) par :

$$\sigma_k(X_1, ..., X_n) = \sum_{\substack{I \subseteq [\![1;n]\!] \\ \mathrm{Card}(I)=k}} \prod_{i \in I} X_i = \sum_{1 \leq i_1 < ... < i_k \leq n} X_{i_1} ... X_{i_k}$$

Théorème 49 : Relations coefficients/racines [Deschamps, p.906] :
Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$.
Si P est scindé de racines $x_1, ..., x_n$ (comptées avec multiplicité), alors on a pour tout $p \in [\![1;n]\!]$, on a $\sigma_p(x_1, ..., x_n) = (-1)^p \frac{a_{n-p}}{a_n}$.

Exemple 50 : [Deschamps, p.906]
Pour $n = 2$, on a :

$$\begin{aligned} P(X) &= a_0(X - x_1)(X - x_2) = a_0(X^2 - (x_1 + x_2)X + x_1 x_2) \\ &= a_0(X^2 - \sigma_1(x_1, x_2)X + \sigma_2(x_1, x_2)) \end{aligned}$$

Exemple 51 : [Deschamps, p.906]
Les solutions du système :

$$\begin{cases} x + y = 3 \\ x^2 + y^2 = 5 \end{cases}$$

sont les couples $(1, 2)$ et $(2, 1)$.

III.2 Théorème de structure

Théorème 52 : Théorème de structure [ADMIS] [Berhuy, p.435] :
Pour tout polynôme symétrique $P \in A[X_1, ..., X_n]$, il existe un unique polynôme $Q \in A[T_1, ..., T_n]$ tel que $P(X) = Q(\sigma_1, ..., \sigma_n)$.
De plus, si P est de degré partiel égal à d, alors Q est de degré d.

Exemple 53 : [Berhuy, p.441 + 442]
∗ Si $P = X_1^2 X_3 + X_1^2 X_2 + X_2^2 X_1 + X_2^2 X_3 + X_3^2 X_1 + X_3^2 X_2$, alors on a $P = \sigma_1\sigma_2 - 3\sigma_3$ et $Q(T_1, T_2, T_3) = T_1 T_2 - 3T_3$.
∗ Si $P = X_1^2 + X_2^2 + X_3^2$, alors $P = \sigma_1^2 - 2\sigma_2$ et $Q = T_1^2 - 2T_2$.

Théorème 54 : Théorème de Kronecker [Francinou, p.257] :
Soit $P \in \mathbb{Z}[X]$ unitaire dont les racines complexes sont de module inférieur ou égal à 1.
Si $P(0) \neq 0$, alors toutes les racines de P sont des racines de l'unité.

Corollaire 55 :
Soit $P \in \mathbb{Z}[X]$ unitaire et irréductible.
Si toutes les racines complexes sont de module inférieur ou égal à 1, alors $P(X) = X$ ou $P(X) = \Phi_k(X)$ pour un certain $k \in \mathbb{N}^*$.

IV Application à la réduction

Dans toute cette partie, on considère $\mathbb{K}$ un corps commutatif, E un $\mathbb{K}$-espace vectoriel de dimension finie notée $n \in \mathbb{N}^*$, $u \in \mathcal{L}(E)$ et $M \in \mathcal{M}_n(\mathbb{K})$ la matrice de u dans une base $\mathcal{B}$ de E.

IV.1 Lien avec la diagonalisation et la trigonalisation

Définition 56 : Polynôme caractéristique [Berhuy, p.946] :
On appelle **polynôme caractéristique de** M le polynôme $\chi_M \in \mathbb{K}[X]$ défini par $\chi_M = \det(XI_n - M)$.

Théorème 57 : [Deschamps, p.78]
Un scalaire λ est une valeur propre de M si, et seulement si, c'est une racine du polynôme caractéristique de M.

Définition 58 : Polynôme minimal [Berhuy, p.945] :
On appelle **polynôme minimal de** u (noté π_u) l'unique polynôme unitaire de $\mathbb{K}[X]$ tel que :

$$(\forall P \in \mathbb{K}[X],\ P(u) = 0) \iff (\pi_u | P)$$

Théorème 59 : Théorème de Cayley-Hamilton [Deschamps, p.99] :
Le polynôme caractéristique de u annule u, c'est-à-dire $\chi_u(u) = 0$.
En particulier, π_u divise χ_u.

Proposition 60 : [Deschamps, p.88 + 102]
Si $\mathrm{Sp}_{\mathbb{K}}(u) = \{\lambda_1, ..., \lambda_p\}$ où les $\lambda_1, ..., \lambda_p$ sont distincts deux à deux, alors les assertions suivantes sont équivalentes :
∗ u est diagonalisable.
∗ u possède un polynôme annulateur scindé à racines simples.
∗ π_u est scindé à racines simples.

Exemple 61 : [Deschamps, p.98]

Soient $P = X^n + \sum_{k=0}^{n-1} a_k X^k$ et la matrice :

$$\mathcal{C}_P = \begin{pmatrix} 0 & 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & \cdots & 0 & -a_1 \\ 0 & 1 & \ddots & & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & -a_{p-2} \\ 0 & 0 & \cdots & 0 & 1 & -a_{p-1} \end{pmatrix}$$

On a alors $\chi_{\mathcal{C}_P} = \pi_{\mathcal{C}_P} = P$.

Définition 62 : Matrice circulante [Gourdon, p.190] :

On appelle **matrice circulante** toute matrice carrée telle que l'on passe d'une ligne à la suivante par décalage à droite des coefficients de façon circulaire. Une matrice circulante C de taille n s'écrit donc :

$$C = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_n & a_1 & \cdots & a_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix}$$

où $a_1, a_2, ..., a_n$ sont des nombres complexes.

Développement 2 : [cf. GOURDON + CALDERO]

Proposition 63 : [Gourdon, p.153]

Si l'on note $P = \sum_{k=0}^{n-1} a_k X^k$ et $\omega = e^{\frac{2i\pi}{n}}$, alors $\det(C) = \prod_{i=0}^{n-1} P\left(\omega^i\right)$.

Proposition 64 : [Caldero, p.45]

Soient P un polygone du plan complexe dont les sommets sont notés $z_1, ..., z_n$ et $a, b \in]0;1[$ tels que $a+b=1$.
Si l'on définit par récurrence la suite $(P_k)_{k\in\mathbb{N}}$ par $P_0 = P$ et $P_{k+1} = \mathcal{B}_{a,b}(P)$ le polygone $(z_i')_{i\in[\![1;n]\!]}$ avec $z_i' = az_i + bz_{i+1}$, alors la suite $(P_k)_{k\in\mathbb{N}}$ converge vers l'isobarycentre de P.

Théorème 65 : [Deschamps, p.93 + 103]

Les assertions suivantes sont équivalentes :
* u est trigonalisable. * u possède un polynôme annulateur scindé.
* Le polynôme minimal de u est scindé.

Corollaire 66 : [Rombaldi, p.676]

Si u est trigonalisable, alors la trace de u est égale à la somme des valeurs propres de u et le déterminant de u est égal au produit des valeurs propres de u.

IV.2 Localisation de valeurs propres et racines

Dans toute cette sous-partie, on écrit $M = (m_{i,j})_{1\leq i,j\leq n} \in \mathcal{M}_n(\mathbb{C})$.

Définition 67 : Disques de Gerschgorin d'une matrice [Rombaldi, p.650] :

On appelle **disques de Gerschgorin de** M les disques fermés $D_i(M)$ définis par :

$$\forall i \in [\![1;n]\!],\ D_i(M) = \mathcal{D}\left(m_{i,i}, R_i(M)\right),\ \text{avec } R_i(M) = \sum_{\substack{j=1\\ j\neq i}}^{n} |m_{i,j}|$$

Définition 68 : Matrice à diagonale strictement dominante [Rombaldi, p.651] :

La matrice M est une **matrice à diagonale strictement dominante** lorsque :

$$\forall i \in [\![1;n]\!],\ |a_{i,i}| > \sum_{\substack{j=1\\ j\neq i}}^{n} |a_{i,j}|$$

Théorème 69 : Théorème de Gerschgorin [Rombaldi, p.651] :

L'ensemble des valeurs propres d'une matrice carrée complexe est inclus dans la réunion de ses disques de Gerschgorin.

Proposition 70 : [Rombaldi, p.651]

Si l'on pose $L = \max_{i\in[\![1;n]\!]} \{R_i(M) + m_{i,i}\}$ et $C = \max_{j\in[\![1;n]\!]} \{R_j(M^\intercal) + m_{j,j}\}$, alors pour toute valeur propre complexe λ de M, on a $|\lambda| \leq \min(L, C)$.

Lemme 71 : Lemme d'Hadamard [Rombaldi, p.651] :

Si M est une matrice complexe à diagonale strictement dominante, alors M est inversible.

Exemple 72 :

La matrice $A = \begin{pmatrix} 3+i & -1,5 & 0 & 1,5i \\ 0,5 & 4 & i & 0,5i \\ \sqrt{2} & \sqrt{2}i & 2+3i & 0 \\ i & 1 & i & 4i \end{pmatrix} \in \mathcal{M}_4(\mathbb{C})$ est inversible.

Proposition 73 :

Soient $P := \sum_{k=0}^{n} a_k X^k$ de degré $n \in \mathbb{N}^*$ et $z \in \mathbb{C}$.
Si z est racine de P, alors on a l'encadrement :

$$\frac{|a_0|}{\max\left(|a_1| + |a_0|, ..., |a_{n-1}| + |a_0|, |a_n|\right)} \leq |z| \leq \frac{\max\left(|a_0|, |a_1| + |a_n|, ..., |a_{n-1}| + |a_n|\right)}{|a_n|}$$

Remarques sur la leçon

— Il est bon de connaître l'algorithme de Waring concernant les polynômes symétriques élémentaires ainsi que l'utilisation concrète du théorème de structure.

— On peut parler du résultant de manière générale (matrice de Sylvester, résultant comme polynôme sur $\mathbb{Z}$, résultant de deux polynômes, etc.) ainsi que du discriminant.

— On peut aussi énoncer d'autres propriétés concernant la localisation de racines comme le théorème de Gauss-Lucas et le théorème de Kronecker.

Liste des développements possibles

— Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}[X]$.

— Matrice circulante.

Bibliographie

— Claude Deschamps, *Tout-en-un MPSI*.

— Daniel Perrin, *Cours d'algèbre*.

— Grégory Berhuy, *Algèbre : le grand combat*.

— Serge Francinou, *Exercices de mathématiques, Oraux X-ENS, Algèbre 1*.

— Xavier Gourdon, *Les maths en tête, Algèbre et Probabilités*.

— Philippe Caldero, *Carnet de voyage en Algébrie*.

— Jean-Étienne Rombaldi, *Mathématiques pour l'agrégation, Algèbre et géométrie*.