Lycée Louis-Le-Grand, Paris
MP2I – Mathématiques
A. Troesch

Pour le 23/04/2024

DM n° 21 : Polynômes, groupes symétriques

Suggestion de travail supplémentaire (à ne pas me rendre) : Le problème 16 de la sélection : Le DS 8 de l'année dernière, et le problème 3 ci-dessous (qui n'est pas à rendre).

Exercices à revoir pendant les vacances :

- Chapitre 20 : 2, 5, 6, 9, 14, 15, 16, 20, 23, 24, 28
- Chapitre 21 : 3, 6, 9, 10, 12, 13, 15, 16, 20, 22, 23, 24, 26, 28, 31, 33, 36, 38, 39, 40
- Chapitre 15 : 1, 4, 6, 7, 9, 10, 12, 15, 19, 22
- Chapitre 22 : 1, 3, 4, 5, 6, 8, 9, 10, 13, 15, 16, 18, 23, 28, 32, 35, 36, 37, 39, 40, 43, 48, 50

Exercices à préparer pendant les vacances :

- Chapitre 22 : la fin des exercices du chapitre 22, s'il en reste
- Chapitre 25 : 1 à 9.

Problème 1 – Simplicité de $\mathfrak{A}_n$

Le but du problème est de prouver la simplicité de $\mathfrak{A}_n$ lorsque $n \geqslant 5$, ce qui signifie que $\mathfrak{A}_n$ n'a pas d'autre sous-groupe distingué que $\{\mathrm{id}\}$ et lui-même. Ce résultat est à la base de la preuve de Galois de la non-résolubilité des équations de degré $n \geqslant 5$ par radicaux. Soit $n \geqslant 5$.

Préliminaire

1. Montrer que le produit de deux transpositions (non nécessairement à supports disjoints) de $\mathfrak{S}_n$ est soit un 3-cycle, soit la composée de deux 3-cycles.
2. En déduire que les 3-cycles engendrent $\mathfrak{A}_n$, c'est-à-dire que tout élément de $\mathfrak{A}_n$ s'écrit comme produit de 3-cycles.

Partie I – Conjugaison

On dit que deux permutations τ_1 et τ_2 de $\mathfrak{S}_n$ sont conjuguées s'il existe $\sigma \in \mathfrak{S}_n$ tel que $\tau_2 = \sigma \circ \tau_1 \circ \sigma^{-1}$.

1. Montrer que la relation de conjugaison est une relation d'équivalence.
2. Soit, avec les notations précédentes, $\tau_1 = (i_1\ i_2\ \cdots\ i_k)$ un cycle, et τ_2 conjugué (par s) à τ_1. Montrer que τ_2 est égal au cycle :
$$\tau_2 = (\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_k)).$$
3. Montrer que deux permutations sont conjuguées dans $\mathfrak{S}_n$ si et seulement si elles ont même type cyclique.

Partie II – Simplicité de $\mathfrak{A}_5$

1. Soit $a_1, \ldots, a_{n-2}$ des éléments 2 à 2 distincts de $[\![1, n]\!]$, et a_{n-1}, a_n les deux éléments de $[\![1, n]\!]$ n'étant pas dans cette liste. On se donne de même $b_1, \ldots, b_{n-2}$ des éléments distincts de $[\![1, n]\!]$, complétés par les 2 éléments manquant b_{n-1} et b_n. Montrer qu'il existe une permutation paire σ telle que
$$\forall i \in [\![1, n-2]\!], \quad \sigma(a_i) = b_i.$$
On pourra éventuellement utiliser une composition par une certaine transposition pour obtenir la bonne parité.

2. En déduire que les 3-cycles (a_1, a_2, a_3) sont conjugués dans $\mathfrak{A}_5$, c'est-à-dire que si c_1 et c_2 sont deux 3-cycles, il existe $\sigma \in \mathfrak{A}_5$ tel que $c_2 = \sigma c_2 \sigma^{-1}$.
3. Montrer de même que les composées de deux transpositions à supports disjoints sont conjuguées dans $\mathfrak{A}_5$.
4. Soit $c_0 = (1\ 2\ 3\ 4\ 5)$, et $c = (a_1\ a_2\ a_3\ a_4\ a_5)$ un 5-cycle, et $\sigma \in \mathfrak{S}_5$ définie par $\sigma(k) = a_k$. Expliciter un élément τ de $\mathfrak{S}_5$ tel que $c^2 = (\sigma \circ \tau) \circ c_0 \circ (\sigma \circ \tau)^{-1}$.
5. En déduire que pour tout 5-cycle c, soit c, soit c^2 est conjugué dans $\mathfrak{A}_5$ au cycle c_0.
6. Soit H un sous-groupe distingué de $\mathfrak{A}_5$ (donc stable par conjugaison). Montrer que si H contient un 3-cycle, il les contient tous, et de même pour les produits de 2 transpositions à supports disjoints, ainsi que pour les 5-cycles.
7. En comptant le nombre de 3-cycles, le nombre de 5-cycles et le nombre de produits de 2 transpositions à supports disjoints, en déduire que $H = \{\mathrm{id}\}$ ou $H = \mathfrak{A}_5$. Conclure.

Partie III – Simplicité de $\mathfrak{A}_n$, $n > 5$

Soit $n > 5$, et soit H un sous-groupe distingué de $\mathfrak{A}_n$, différent de $\{\mathrm{id}\}$. Soit $\sigma \neq \mathrm{id}$ dans H

1. Soit a tel que $\sigma(a) \neq a$. On pose $b = \sigma(a)$, et on considère c différent de a, b et $\sigma(b)$. Soit τ le 3-cycle $(a\ b\ c)$. Quel est le type cyclique de $\sigma\tau^{-1}\sigma^{-1}$? Montrer que $\tau\sigma\tau^{-1}\sigma^{-1}$ admet au moins $n-5$ points fixes.
2. Soit F un sous-ensemble de $[\![1, n]\!]$ de cardinal 5, contenant l'ensemble des points non fixes de $\tau\sigma\tau^{-1}\sigma^{-1}$. Soit $\mathfrak{A}(F)$ l'ensemble des permutations de $\mathfrak{A}_n$ laissant tous les points extérieurs à F fixes. Montrer que $\mathfrak{A}(F)$ est isomorphe, en tant que groupe, à $\mathfrak{A}_5$, et en déduire que $\mathfrak{A}(F)$ est simple.
3. Montrer que $H \cap \mathfrak{A}(F)$ est distingué dans $\mathfrak{A}(F)$, et en déduire que H contient au moins un 3-cycle.
4. En déduire que $\mathfrak{A}_n$ est simple.

Problème 2 – (Autour de la conjecture d'Ilieff-Sendov, d'après ENS 1989)

Le but de ce problème est de prouver, dans certains cas particuliers, la conjecture explicitée ci-après, souvent nommée conjecture d'Ilieff-Sendov.
Soit $S \in \mathbb{C}[X]$ un polynôme à coefficients complexes, de degré au moins égal à 2. On désigne par $\mathrm{rac}(S)$ l'ensemble des racines (complexes) de S. Soit $z \in \mathrm{rac}(S)$. On dit que :

- *S vérifie $\mathcal{IS}(z)$ s'il existe $\zeta \in \mathrm{rac}(S')$ vérifiant $|z - \zeta| \leqslant 1$, où S' désigne le polynôme dérivé de S ;*
- *S vérifie $\mathcal{IS}$ si pour tout $z \in \mathrm{rac}(S)$, S vérifie $\mathcal{IS}(z)$.*

La conjecture d'Ilieff-Sendov stipule que tout polynôme de $\mathbb{C}[X]$ de degré au moins égal à 2 et dont les racines sont de module au plus 1 vérifie $\mathcal{IS}$.
Le but de ce problème est de montrer que tout polynôme de degré au moins 2 n'ayant pas plus de 4 racines complexes distinctes vérifie $\mathcal{IS}$.

La conjecture reste à ce jour non démontrée dans le cas général. Certains autres cas sont démontrés, par exemple le cas des polynômes de degré au plus 5, et le cas des polynômes ayant au plus 4 coefficients non nuls.

Dans tout le problème, on fixe un entier $n \geqslant 2$ et un polynôme $P = a_n X^n + \cdots + a_0$ de $\mathbb{C}[X]$, de degré n. On note $z_0, z_1, \ldots, z_m$ les racines distinctes de P, et pour tout $i \in [\![0, m]\!]$, on désigne par n_i la multiplicité de la racine z_i de P. On suppose que les z_i vérifient $|z_i| \leqslant 1$.

On rappelle qu'un polynôme est dit unitaire s'il est non nul et si son coefficient dominant est égal à 1. On rappelle également que $\mathbb{U}$ désigne le sous-ensemble de $\mathbb{C}$ constitué des nombres complexes de module 1.

Questions préliminaires

1. Que vaut $\displaystyle\sum_{i=0}^{m} n_i$?
2. Exprimer la décomposition en facteurs irréductibles dans $\mathbb{C}[X]$ du polynôme P en fonction des z_i, n_i et de a_n.

Partie I – Quelques cas simples de la conjecture

1. **Cas des polynômes de degré 2**

   On suppose ici que $n = 2$.

   (a) Exprimer l'unique racine ζ de P' en fonction des racines de P.

   (b) En déduire que P vérifie $\mathcal{IS}$.

2. **Cas d'une racine multiple**

   Montrer que si $n_0 \geqslant 2$, alors P vérifie $\mathcal{IS}(z_0)$.

3. **Cas d'un polynôme ayant peu de racines distinctes**

   (a) Montrer qu'il existe des nombres complexes (non nécessairement distincts) $w_1, \ldots, w_m$, non racines de P, tels que

   $$P' = na_n \prod_{i=0}^{m} (X - z_i)^{n_i - 1} \prod_{j=1}^{m} (X - w_j).$$

   (b) On suppose que $n_0 = 1$. En exprimant de deux manières différentes $P'(z_0)$, montrer que :

   $$\prod_{j=1}^{m} (z_0 - w_j) = \frac{1}{n} \prod_{i=1}^{m} (z_0 - z_i).$$

   En déduire que si $n \geqslant 2^m$, alors P vérifie $\mathcal{IS}(z_0)$.

   (c) Montrer que si $n \geqslant 2^m$, P vérifie $\mathcal{IS}$.

Partie II – Étude du cas de certaines racines

1. **Cas de la racine nulle**

   On suppose dans cette question que $z_0 = 0$.

   (a) Exprimer la décomposition en éléments simples de $\dfrac{P'}{P}$.

   (b) Soit $j \in [\![1, m]\!]$. En considérant $\dfrac{P'}{P}(w_j)$, montrer que w_j est un barycentre à coefficients strictement positifs des z_i, et que l'on a $|w_j| \leqslant 1$.

   (c) En déduire que P vérifie $\mathcal{IS}(z_0)$, c'est-à-dire $\mathcal{IS}(0)$.

2. **Cas d'une racine de module** 1

   On note $t_1, \ldots, t_{n-1}$ les racines complexes non nécessairement distinctes de P'. Ainsi,

   $$P' = na_n \prod_{i=1}^{n-1} (X - t_i).$$

   On suppose que $n_0 = 1$.

   (a) Prouver que si $\left| \dfrac{P''}{P'}(z_0) \right| \geqslant n - 1$, alors P vérifie $\mathcal{IS}(z_0)$.

   (b) Montrer que

   $$\frac{P''}{P'}(z_0) = 2 \sum_{i=1}^{m} \frac{n_i}{z_0 - z_i}.$$

   On pourra utiliser le polynôme Q tel que $P = (X - z_0)Q$.

   (c) Montrer que si $z \in \mathbb{C}$ vérifie $|z| \leqslant 1$ et $z \neq 1$, alors $\operatorname{Re}\left(\dfrac{1}{1-z}\right) \geqslant \dfrac{1}{2}$.

   (d) On suppose $z_0 = 1$. Montrer qu'il existe $i \in [\![1, n-1]\!]$ tel que $\operatorname{Re}\left(\dfrac{1}{1-t_i}\right) \geqslant 1$. Montrer qu'alors $|t_i - 1| \leqslant 1$, et conclure.

   (e) On suppose maintenant que $|z_0| = 1$. En composant P par une transformation géométrique simple de $\mathbb{C}$, montrer que P vérifie $\mathcal{IS}(z_0)$.

Partie III – Cas des polynômes de degrés 3 et 4

Dans cette partie, on suppose que $n_0 = 1$ et que z_0 est un réel vérifiant $0 < z_0 < 1$. Pour simplifier les notations, on pose $a = z_0$. On définit l'application T sur $\mathbb{C}\backslash\{\frac{1}{a}\}$ par

$$T(w) = \frac{w-a}{aw-1}.$$

On note $\tilde{P}$ la fraction rationnelle $\tilde{P}(X) = (aX-1)^n P\left(\dfrac{X-a}{aX-1}\right)$.
L'hypothèse $n \leqslant 4$ n'intervient qu'en fin de partie ; auparavant, n est considéré quelconque.

1. **Étude de T**
   (a) Montrer que $T \circ T = \mathrm{id}_{\mathbb{C}\backslash\{\frac{1}{a}\}}$
   (b) Montrer que si $|w| = 1$, alors $|T(w)| = 1$.
   (c) En déduire que $T(\mathbb{U}) = \mathbb{U}$, puis que pour tout w de $\mathbb{C}\backslash\{\frac{1}{a}\}$ tel que $|w| \neq 1$, $|T(w)| \neq 1$.
   (d) Montrer que si $|w| < 1$, alors $|T(w)| < 1$ (on pourra considérer la fonction continue sur $[0,1]$ définie par $f(t) = |T(tw)|$)
   (e) Montrer que si $|w| > 1$ et $w \neq \frac{1}{a}$, alors $|T(w)| > 1$.
2. (a) Montrer que $\tilde{P}$ est un polynôme de $\mathbb{C}[X]$. On écrit $\tilde{P}(X) = b_n X^n + \cdots + b_1 X + b_0$.
   (b) Justifier que les racines de $\tilde{P}$ sont de module inférieur ou égal à 1.
   (c) Prouver que $|b_1| \leqslant |b_n|$ et $|b_{n-1}| \leqslant (n-1)|b_n|$.
   Indication : *On pourra remarquer que 0 est racine de $\tilde{P}$.*

On pose

$$R(X) = \sum_{i=1}^{n} \left((n-i) b_i X^i + \frac{i b_i}{a} X^{i-1} \right),$$

et on écrit

$$R(X) = A \prod_{k=1}^{n-1} (X - \gamma_k),$$

où les γ_k sont numérotés de sorte à avoir :

$$|\gamma_1| \leqslant |\gamma_2| \leqslant \cdots \leqslant |\gamma_{n-1}|.$$

3. (a) Montrer que $\displaystyle\prod_{k=1}^{n-1} |\gamma_k| \leqslant \frac{1}{n - a(n-1)}$.
   (b) Montrer que $aR(X) = na\tilde{P}(X) - (aX-1)\tilde{P}'(X)$.
   (c) Montrer que pour tout $w \in \mathbb{C}\backslash\{\frac{1}{a}\}$,

$$P'(T(w)) = \frac{a}{(1-a^2)(aw-1)^{n-1}} \cdot R(w).$$

   (d) Soit μ un nombre réel tel que $|\gamma_1| \leqslant \mu < \frac{1}{a}$. Montrer que P' a une racine ζ vérifiant

$$|\zeta - a| \leqslant \frac{\mu(1-a^2)}{1-a\mu}.$$

   (e) Montrer que si μ vérifie de plus $\mu \leqslant \dfrac{1}{1+a-a^2}$, alors P' a une racine ζ vérifiant $|\zeta - a| \leqslant 1$.
4. Montrer que si $n \leqslant 4$, alors P vérifie $\mathcal{IS}(a)$.
   Indication : *On pourra se ramener à l'étude de la fonction $x \mapsto (n-1)\ln(1+x-x^2) - \ln(n-(n-1)x)$, et étudier séparément les cas $n = 3$ et $n = 4$.*
5. On ne suppose plus z_0 réel. On rappelle que toutes les racines de P sont de module inférieur ou égal à 1. Montrer que si $n \leqslant 4$, P vérifie $\mathcal{IS}$.

Partie IV – Cas des polynômes de degré 5, 6, 7 avec une racine double de module 1

1. Adapter la méthode de la partie précédente pour montrer que si $n = 5, 6$ ou 7, et si P admet un zéro réel $z_0 = a \in]0, 1[$, et un zéro au moins double de module 1, alors P vérifie $\mathcal{IS}(a)$.
   Indication : *On pourra montrer que si w est racine double de P, alors $T(w)$ est racine de R, et justifier qu'on peut alors se ramener à l'étude de la fonction $x \mapsto (n-2)\ln(1+x-x^2) - \ln(n-(n-1)x)$.*
2. Montrer que tout polynôme de degré 5, 6 ou 7 ayant une racine de module 1 au moins double et toutes ses racines de module au plus 1 vérifie $\mathcal{IS}$.

Partie V – Continuité des racines d'un polynôme

On rappelle que $\mathbb{C}_n[X]$ désigne l'espace vectoriel des polynômes de $\mathbb{C}[X]$ de degré au plus n. Pour $S = \sum_{i=0}^{n} s_i X^i \in \mathbb{C}_n[X]$, on pose :

$$\|S\| = \sum_{i=0}^{n} |s_i|.$$

On dit qu'une suite $(S_k)_{k\in\mathbb{N}}$ de polynômes converge vers S si $\|S_k - S\| \underset{k\to+\infty}{\longrightarrow} 0$.

1. Soit S tel que ci-dessus, et $S_k = \sum_{i=0}^{n} s_{i,k} X^i \in \mathbb{C}_n[X]$. Montrer que (S_k) converge vers S si et seulement si pour tout $i \in [\![0, n]\!]$, $s_{i,k} \underset{k\to+\infty}{\longrightarrow} s_i$.
2. Montrer que si $(S_k)_{k\in\mathbb{N}}$ converge vers S, alors pour tout $z \in \mathbb{C}$, $S_k(z) \to S(z)$.
3. Montrer que si S est de degré n, toute racine z de S dans $\mathbb{C}$ vérifie $|z| \leqslant \frac{\|S\|}{|s_n|}$.
   Indication : *on pourra distinguer les cas $|z| \leqslant 1$ et $|z| > 1$.*
4. Soit $(S_k)_{k\in\mathbb{N}}$ une suite de polynômes de degré n convergeant vers S de degré n. On note $S_k = \alpha_k \prod_{i=1}^{n} (X - x_{i,k})$.
   (a) Montrer que pour tout $i \in [\![1, n]\!]$, la suite $(x_{i,k})_{k\in\mathbb{N}}$ est bornée.
   (b) En déduire qu'on peut extraire de $(S_k)_{k\in\mathbb{N}}$ une suite $(S_{\varphi(k)})_{k\in\mathbb{N}}$ telle que les suites de racines $(x_{i,\varphi(k)})_{k\in\mathbb{N}}$ soient convergentes pour tout $i \in [\![1, n]\!]$.
   (c) En déduire que pour tout $\varepsilon > 0$, et toute racine ζ de S de multiplicité β, il existe K tel que pour tout $k \geqslant K$, la boule $B(\zeta, \varepsilon)$ contienne au moins β racines (non nécessairement distinctes) de S_k.
   Indication : *on pourra raisonner par l'absurde, et faire une première extraction d'une suite de polynômes qui possèdent moins de β racines dans une boule $B(\zeta, \varepsilon)$ donnée, puis exploiter la question précédente pour obtenir une contradiction.*
   (d) Justifier que sous les mêmes conditions, si ε est suffisamment petit (dans un sens qu'on explicitera), il existe K tel que pour tout $k \geqslant K$ et toute racine ζ de S de multiplicité β, $B(\zeta, \varepsilon)$ contienne exactement β racines de S_k.

Partie VI – Polynômes extrémaux

Soit k un entier vérifiant $n \geqslant k \geqslant 2$. On note $P_n(k)$ la partie de $\mathbb{C}_n[X]$ formée des polynômes unitaires de degré n ayant au plus $k+1$ racines distinctes, toutes de module au plus 1.
Pour $S \in P_n(k)$, et pour z une racine de S, on note :

$$I_S(z) = \min_{\zeta \in \mathrm{rac}(P')} |z - \zeta| \qquad \text{et} \qquad I(S) = \max_{z \in \mathrm{rac}(P)} I_S(z).$$

1. (a) Montrer qu'on a $I(S) \leqslant 2$ pour $S \in P_n(k)$, et qu'il existe un polynôme S de $P_n(n-1)$ tel que $I(S) = 1$.
   On note $I(P_k(n))$ la borne supérieure des $I(S)$ lorsque S parcourt $P_n(k)$.
   (b) Prouver que si on a $I(P_n(k)) \leqslant 1$, alors tout polynôme de $P_n(k)$ vérifie $\mathcal{IS}$.

(c) Prouver que $P_n(k)$ est une partie compacte de $\mathbb{C}_n[X]$, donc que de toute suite d'éléments de $P_n(k)$, on peut extraire une suite convergente (au sens défini dans la partie précédente), de limite dans $P_n(k)$.

Indication : *étant donnée une suite d'éléments de $P_n(k)$, construire une extraction de sorte à assurer la convergence coefficient par coefficient.*

(d) Prouver que $I : S \mapsto I(S)$ est une application continue de $P_n(k)$ dans $\mathbb{R}$ et qu'il existe un polynôme S de $P_n(k)$ vérifiant $I(S) = I(P_n(k))$.

2. On appelle polynôme extrémal de $P_n(k)$ un polynôme S de $P_n(k)$ vérifiant $I(S) = I(P_n(k))$.

(a) Prouver qu'un polynôme extrémal de $P_n(k)$ a une racine de module 1 (on pourra utiliser une transformation géométrique simple de $\mathbb{C}$)

(b) Prouver que pour tout nombre réel θ, un polynôme extrémal de $P_n(k)$ a au moins une racine de la forme $\mathrm{e}^{\mathrm{i}\,\alpha}$, où $\alpha \in [\theta, \theta + \pi[$.

(c) On suppose $n = 5, 6$ ou 7 et $k = 3$. On note S un polynôme extrémal de $P_n(k)$. On suppose que S a une racine a réelle vérifiant $0 < a < 1$. Prouver que S vérifie $\mathcal{IS}(a)$.

Indication : *dans le cas où S a exactement 2 zéros distincts u et v de module 1, on pourra prouver que leur somme est nulle, et établir la formule $|a - \zeta|^k \leqslant 2^{k-2}|a - u| \cdot |a - v|/n$, où ζ est la racine de S' la plus proche de a.*

(d) On suppose $n = 5, 6$ ou 7. Prouver qu'on a $I(P_n(3)) \leqslant 1$.

3. Prouver que tout polynôme de $\mathbb{C}[X]$ ayant au plus 4 racines distinctes, ces racines étant toutes de module au plus 1, vérifie $\mathcal{IS}$.