Corrigés RMS 2019

Exercice 228 :

Soit G un groupe fini. Pour $x \in G$, on note $\overline{x} = \{gxg^{-1}/g \in G\}$ la classe de conjugaison de x. On dit que x est ambivalent si $x^{-1} \in \overline{x}$.
a) Montrer que si une classe de conjugaison contient un élément ambivalent alors tous ses éléments le sont.
b) Pour $x \in G$, soit $\rho(x)$ le nombre de $g \in G$ tel que $g^2 = x$. Montrer que $\dfrac{1}{|G|}\displaystyle\sum_{x\in G}\rho(x)^2$ est le nombre de classes de conjugaison ambivalentes de G.

a) Soit C une classe de conjugaison et $x \in C$ ambivalent. On a $x^{-1} \in \overline{x} = C$ donc $C = \overline{x^{-1}}$. Soit $y \in \overline{x}$. Il existe $g \in G$ tel que $y = gxg^{-1}$. Alors $y^{-1} = gx^{-1}g^{-1} \in \overline{x^{-1}} = C$. Or on a aussi $C = \overline{y}$ donc $y^{-1} \in \overline{y}$, ce qui conclut.

b) Notons Γ l'ensemble des classes ambivalentes. Par le calcul, on a :

$$\begin{aligned}
\frac{1}{|G|}\sum_{x\in G}\rho(x)^2 &= \frac{1}{|G|}\sum_{x\in G}\left(\sum_{l\in G}\delta(l^2=x)\right)^2\\
&= \frac{1}{|G|}\sum_{x\in G}\left(\sum_{(l,h)\in G^2}\delta(l^2=x)\delta(h^2=x)\right)\\
&= \frac{1}{|G|}\sum_{(l,h)\in G^2}\delta(l^2=h^2)\\
&= \frac{1}{|G|}\sum_{(u,h)\in G^2}\delta(huhu=h^2) \text{ car } u\to hu \text{ est une bijection}\\
&= \frac{1}{|G|}\sum_{\gamma\in\Gamma}\sum_{u\in\gamma}\sum_{h\in G}\delta(u=hu^{-1}h^{-1})
\end{aligned}$$

Or $\forall u \in \gamma$ considérons la fonction $\Phi_u : h \in G \to hu^{-1}h^{-1} \in \gamma = \overline{u}$. Elle est surjective.
On a alors:

$$\sum_{u\in\gamma}\sum_{h\in G}\delta(u=hu^{-1}h^{-1}) = \sum_{u\in\gamma}|\Phi_u^{-1}(\{u\})|$$

Cependant, $\Phi_u^{-1}(\{u\})$ et $\Phi_x^{-1}(\{u\})$ sont en bijection pour tout $x \in \gamma$.
En effet, si $x \in \gamma$ alors il existe $g \in G$ tel que $x = gu^{-1}g^{-1}$ et comme u est ambivalent il existe $h \in G$ tel que $u = hu^{-1}h^{-1}$.
x est aussi ambivalent donc il existe $k \in G$ tel que $x^{-1} = kxk^{-1}$.
On a alors en regroupant $u = (hg^{-1}k^{-1})x^{-1}(hg^{-1}k^{-1})^{-1}$.
On peut donc définir $f : h \in \Phi_u^{-1}(\{u\}) \to hg^{-1}k^{-1} \in \Phi_x^{-1}(\{u\})$. C'est alors clairement une bijection.
Finalement, on a :

$$\sum_{u\in\gamma}|\Phi_u^{-1}(\{u\})| = \sum_{r\in\gamma}|\Phi_u^{-1}(\{r\})| = |G|$$

(La dernière somme est le cardinal de l'ensemble des antécédents des images qui est G.)

$$\text{D'où } \frac{1}{|G|}\sum_{x\in G}\rho(x)^2 \text{ est le nombre de classes de conjugaison de } G.$$

Exercice 237 :

Soient $\lambda_1, \ldots, \lambda_d$ des nombres complexes de module au plus 1, $P = \prod_{i=1}^{d}(X - \lambda_i)$.

Pour $n \in \mathbb{N}$, soit $f(n) = \sum_{i=1}^{d} \lambda_i^n$. On suppose que $P \in \mathbb{Z}[X]$.

a) Montrer que $f(\mathbb{N}) \subset \mathbb{Z}$

b) Montrer que f est périodique à partir d'un certain rang.

c) Montrer que, pour tout $i \in \{1, \ldots, d\}$, λ_i est nul ou racine de l'unité.

a) On procède par récurrence sur $n \in \mathbb{N}$.

Initialisation : $n = 0$

$\sum_{i=1}^{d} \lambda_i^0 = d \in \mathbb{Z}$

Hérédité : On suppose, pour un certain $n \in \mathbb{N}^*$, que $\forall k < n \in \mathbb{N}^*, \sum_{i=1}^{d} \lambda_i^k \in \mathbb{Z}$

On a :

$$\begin{aligned}
\sum_{i=1}^{d} \lambda_i^n &= \left(\sum_{i=1}^{d} \lambda_i\right)\left(\sum_{i=1}^{d} \lambda_i^{n-1}\right) - \sum_{1 \leqslant i \neq j \leqslant d} \lambda_i \lambda_j^{n-1} \\
&= \left(\sum_{i=1}^{d} \lambda_i\right)\left(\sum_{i=1}^{d} \lambda_i^{n-1}\right) - \frac{1}{2}\left(\sum_{1 \leqslant i \neq j \leqslant d} \lambda_i \lambda_j\right)\left(\sum_{k=1}^{d} \lambda_k^{n-2}\right) + \frac{1}{2} \sum_{1 \leqslant i \neq j \neq k \leqslant d} \lambda_i \lambda_j \lambda_k^{n-2} \\
&= \cdots \\
&= \sum_{k=1}^{n}\left((-1)^{k+1}\left(\sum_{i=1}^{d} \lambda_i^{n-k}\right)\left(\sum_{1 \leqslant i_1 < \cdots < i_k \leqslant d} \prod_{j=1}^{k} \lambda_{i_j}\right)\right)
\end{aligned}$$

Or, par hypothèse de récurrence, $\forall k \in [\![1, n]\!], \sum_{i=1}^{d} \lambda_i^{n-k} \in \mathbb{Z}$

De plus, pour tout $k \in [\![1, n]\!]$, $(-1)^k \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant d} \prod_{j=1}^{k} \lambda_{i_j}$ est le coefficient de degré $n - k$ du polynôme P donc appartient à $\mathbb{Z}$.

Finalement,

$$\sum_{i=1}^{d} \lambda_i^n \in \mathbb{Z}$$

Cela conclut la récurrence.

b) Pour $n \geqslant d$, on a :

$$f(n) = \sum_{k=1}^{d}\left((-1)^{k+1} f(n-k)\left(\sum_{1 \leqslant i_1 < \cdots < i_k \leqslant d} \prod_{j=1}^{k} \lambda_{i_j}\right)\right)$$

Or, $\forall n \in \mathbb{N}, f(n) \in [\![-d, d]\!]$.

Comme $[\![-d, d]\!]^d$ est fini, il existe $n < n' \in \mathbb{N}$ tels que $n' - n > d$ et $\forall k \in [\![0, d-1]\!], f(n+k) = f(n'+k)$.

Et comme $f(n)$ dépend des d termes précédents,

la suite $(f(n))_{n \in \mathbb{N}}$ est $(n' - n)$-périodique

c) f est périodique à partir d'un certain rang donc $\exists r \in \mathbb{N}, \forall n \in \mathbb{N}^*, f(mr) = f(r)$

On pose $S(x) = \sum_0^{+\infty} f(nr)x^n$. Alors :

$$\begin{aligned}
S(x) &= d + f(r)\frac{x}{1-x} \\
&= d + \sum_{n=1}^{+\infty}\sum_{i=1}^{d} \lambda_i^{rn} x^n \\
&= \sum_{n=0}^{+\infty}\sum_{i=1}^{d} (\lambda_i^r x)^n \\
&= \sum_{i=1}^{d}\sum_{n=0}^{+\infty} (\lambda_i^r x)^n \\
&= \sum_{i=1}^{d} \frac{1}{1-\lambda_i^r x}
\end{aligned}$$

Donc $d - f(r) + \dfrac{f(r)}{1-x} = \sum_{i=1}^{d} \dfrac{1}{1-\lambda_i^r x}$

$$\text{Par unicité de la DES, tous les } \lambda_i \text{ sont nuls ou tels que } \lambda_i^{-r} = 1$$

Exercice 251 :

Soit $A \in \mathcal{M}_n[\mathbb{R}]$. Comparer ses polynômes minimaux dans $\mathcal{M}_n(\mathbb{R})$ et dans $\mathcal{M}_n(\mathbb{C})$.

Soient $R \in \mathbb{R}[X]$ et $C \in \mathbb{C}[X]$ les polynômes minimaux de A dans $\mathcal{M}_n(\mathbb{R})$ et $\mathcal{M}_n(\mathbb{C})$ respectivement.

On a bien sur $C|R$.

$C(A) = 0$ donc $iC(A) = 0$ donc $\mathrm{Re}(iC(A)) = 0$ donc $\mathrm{Re}(iC)(A) = 0$
Or C est unitaire donc $\mathrm{Re}(iC)$ est de degré strictement inférieur à C (le coefficient de plus haut degré est imaginaire pur).
Ainsi, si C n'est pas à coefficients réels, $\mathrm{Re}(iC)$ est un polynôme non-nul, annulant A et de degré strictement inférieur à celui de C, ce qui est absurde.
Ainsi, C est réel et $R|C$.

Finalement,

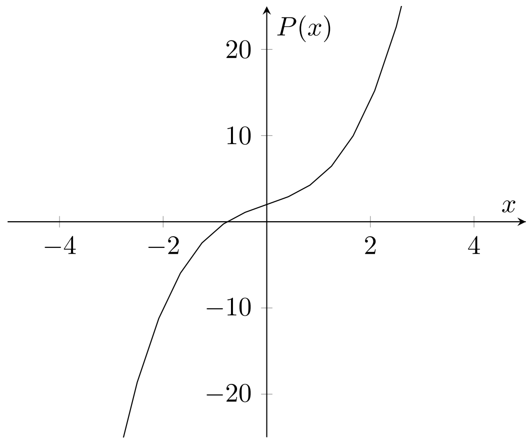
$$R = C$$

Exercice 254 :

Déterminer les $n \in \mathbb{N}$ tel qu'existe $A \in \mathcal{M}_n(\mathbb{R})$ de polynôme minimal $X^3 + 2X + 2$.
Même question dans $\mathcal{M}_n(\mathbb{Q})$.

Dans $\mathcal{M}_n(\mathbb{R})$: On note $P = X^3 + 2X + 2$. On obtient $P' = 3X^2 + 2$.

x	$-\infty$	α	$+\infty$
$P'(x)$		$+$	
$P(x)$	$-\infty$	0	$+\infty$



Ainsi, par théorème de la bijection, P n'admet qu'une seule racine réel α. On note β et $\overline{\beta}$ ses racines complexes conjuguées.
Pour $n \leqslant 3$, il n'existe pas de matrice de $\mathcal{M}_n(\mathbb{R})$ admettant P comme polynôme minimal (Théorème de Caley-Hamilton).
Pour $n = 3$, la matrice $A = \begin{pmatrix} 0 & 0 & 2 \\ -1 & 0 & 2 \\ 0 & -1 & 0 \end{pmatrix}$ admet comme polynôme caractéristique $\chi_A = P$.
P est un polynôme annulateur de A (théorème de Caley-Hamilton), et P est scindé à racines simples donc P est le polynôme minimal de A.
Pour $n \geqslant 3$, la matrice $B = \begin{pmatrix} \alpha I_{n-3} & \\ & A \end{pmatrix}$ admet comme polynôme caractéristique $\chi_B = (X - \alpha)^{n-3} P$.
P est un polynôme annulateur de B et tout polynôme annulateur de B divise P donc P est le polynôme minimal de B.

Dans $\mathcal{M}_n(\mathbb{Q})$: On suppose par l'absurde que $\alpha \in \mathbb{Q}$, donc il existe $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ t.q. $p \wedge q = 1$.
$P(\alpha) = 0 \implies \left(\dfrac{p}{q}\right)^3 + 2 \cdot \dfrac{p}{q} + 2 = 0 \implies p^3 + 2pq^2 + 2q^3 = 0$ donc par théorème de Gauss, $p|2$ et $q|2$ donc $\alpha \in \left\{\dfrac{1}{2}, 1, 2, -\dfrac{1}{2}, -1, -2,\right\}$ Absurde. Donc $\alpha \notin \mathbb{Q}$ et P, de degré 3 , est irréductible dans $\mathbb{Q}[X]$.

Pour $n \in 3\mathbb{N}$, la matrice $C = \begin{pmatrix} A & & \\ & \ddots & \\ & & A \end{pmatrix} \in \mathcal{M}_n(\mathbb{Q})$ admet bien comme polynôme minimal P.

Pour $n \notin 3\mathbb{N}$, par l'absurde on suppose qu'il existe $C \in \mathcal{M}_n(\mathbb{Q})$ ayant P comme polynôme minimal.
χ_C et P ont même racines, donc $\chi_C = (X - \alpha)^p \left((X - \beta)(X - \overline{\beta})\right)^q$ avec $p + 2q = n$ donc $p \neq q$ car $n \notin 3\mathbb{N}$.

- Si $p > q$, $\chi_C = (X - \alpha)^{p-q} P^q$ donc $(X - \alpha)^{p-q} \in \mathbb{Q}[X]$. Or le coefficient de degré $p - q - 1$ de $(X - \alpha)^{p-q}$ est $\alpha \notin \mathbb{Q}$. Absurde.
- Si $q > p$, $\chi_C = \left((X - \beta)(X - \overline{\beta})\right)^{q-p} P^p$ donc $\left((X - \beta)(X - \overline{\beta})\right)^{q-p} \in \mathbb{Q}[X]$. Or le coefficient de degré $q - p - 1$ de $\left((X - \beta)(X - \overline{\beta})\right)^{q-p}$ est $2\mathrm{Re}(\beta)$. Par relation coefficient racines sur P, $\alpha + 2\mathrm{Re}(\beta) = 0$ donc $2\mathrm{Re}(\beta) \notin \mathbb{Q}$. Absurde.