

Séance 7 - MP+ - 27/03/26

Exercice 1 (***)

Étant donné un ensemble E et un groupe $(G, \times)$ de neutre e , une *action* de G sur E est une application

$$G \times E \rightarrow E, (g, x) \mapsto g \cdot x$$

$$\text{vérifiant} \quad \forall x \in E \quad e \cdot x = x \quad \text{et} \quad \forall (g, g', x) \in G^2 \times E \quad g' \cdot (g \cdot x) = (g'g) \cdot x$$

On dit que le groupe G *agit* ou *opère* sur l'ensemble E . Pour $x \in E$, on définit *l'orbite* de x notée O_x par

$$O_x = \{g \cdot x, g \in G\}$$

le *stabilisateur* de x noté G_x par

$$G_x = \{g \in G \mid g \cdot x = x\}$$

et la relation binaire $\mathcal{R}$ pour $(x, y) \in E^2$ par

$$x\mathcal{R}y \iff y \in O_x$$

1. Vérifier que le groupe G agit sur lui-même par translation à gauche $G^2 \rightarrow G, (g, x) \mapsto gx$ et par conjugaison $G^2 \rightarrow G, (g, x) \mapsto gxg^{-1}$.
2. Établir que la relation $\mathcal{R}$ est une relation d'équivalence dont les classes d'équivalence sont les orbites.
3. Soit $x \in E$. Établir que G_x est sous-groupe de G puis vérifier que la relation binaire $\mathcal{R}_x$ définie pour $(a, b) \in G^2$ par

$$a\mathcal{R}_x b \iff a \cdot x = b \cdot x$$

est une relation d'équivalence.

Dans ce qui suit, les ensembles E et G sont supposés finis.

4. En déduire $\forall x \in E \quad \text{Card } G = \text{Card } O_x \times \text{Card } G_x$
5. Conclure en montrant *l'équation aux classes*

$$\text{Card } E = \sum_{i=1}^n \frac{\text{Card } G}{\text{Card } G_{x_i}}$$

où $x_1, \dots, x_n$ sont des représentants des classes d'équivalence de $\mathcal{R}$.

Exercice 2 (***)

On définit les *polynômes cyclotomiques* par

$$\forall n \in \mathbb{N}^* \quad \Phi_n = \prod_{k \in [1; n], k \wedge n = 1} (X - e^{\frac{2ik\pi}{n}})$$

1. Montrer $\forall n \in \mathbb{N}^* \quad \prod_{d|n} \Phi_d = X^n - 1$

2. Montrer $\forall n \in \mathbb{N}^* \quad \Phi_n \in \mathbb{Z}[X]$

Exercice 3 (****)

La définition générale d'un corps est la suivante :

Définition 1. On appelle corps un anneau $(\mathbb{K}, +, \times)$ non réduit à $\{0\}$ et tel que tous les éléments de $\mathbb{K} \setminus \{0\}$ sont inversibles.

Notations : On note $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

L'objectif de ce problème est d'établir le *théorème de Wedderburn* : tout corps fini est commutatif.

Soit $\mathbb{K}$ un corps fini. On définit son *centre* noté Z par

$$Z = \{x \in \mathbb{K} \mid \forall y \in \mathbb{K} \quad xy = yx\}$$

1. Montrer que le centre Z est un sous-corps commutatif de $\mathbb{K}$ de cardinal $q \geq 2$.
En déduire qu'il existe n entier non nul tel que $\text{Card } \mathbb{K} = q^n$.

On suppose le corps $\mathbb{K}$ non commutatif.

2. En considérant que $\mathbb{K}^*$ opère sur lui-même par conjugaison, pour $x \in \mathbb{K}^*$, établir

$$\text{Card } O_x = \frac{\text{Card } \mathbb{K}^*}{\text{Card } \mathbb{K}_x^*}$$

3. Pour d entier non nul diviseur strict de n , montrer que $\Phi_n(q)$ divise $\frac{q^n - 1}{q^d - 1}$.

4. Établir
$$q^n - 1 = q - 1 + \sum \frac{q^n - 1}{q^d - 1}$$

la somme portant sur un certain nombre de diviseurs stricts de n .

5. Conclure.

Exercice 4 (**)

Pour n entier, on note $\tau(n)$ le nombre de diviseurs de n et $\sigma(n)$ la somme des diviseurs de n .

1. Établir l'égalité $\forall n \in \mathbb{N} \quad \sum_{k=1}^n \tau(k) = \sum_{d=1}^n \left\lfloor \frac{n}{d} \right\rfloor$
 2. En déduire $\sum_{k=1}^n \tau(k) \underset{n \rightarrow +\infty}{\sim} n \ln(n)$
 3. Établir l'égalité $\forall n \in \mathbb{N} \quad \sum_{k=1}^n \sigma(k) = \sum_{j=1}^n \frac{1}{2} \left\lfloor \frac{n}{j} \right\rfloor \left(\left\lfloor \frac{n}{j} \right\rfloor + 1 \right)$
 4. En déduire $\sum_{k=1}^n \sigma(k) \underset{n \rightarrow +\infty}{\sim} \frac{\zeta(2)}{2} n^2$ où $\zeta(2) = \sum_{n=1}^{+\infty} \frac{1}{n^2}$
-

Exercice 5 (****)

Soit $(G, +)$ un groupe abélien fini d'ordre pq avec p et q deux nombres premiers distincts. Montrer que G est cyclique.

Exercice 6 (****)

Soit $(G, \times)$ un groupe abélien fini.

1. Montrer qu'il existe ℓ entier non nul minimal tel que $x^\ell = 1$ pour tout $x \in G$.
 2. Soit $x \in G$ et $k \in \mathbb{Z}$. Établir
$$o(x^k) = \frac{o(x)}{o(x) \wedge k}$$
 3. Soit $(x, y) \in G^2$. Si $o(x) \wedge o(y) = 1$, déterminer $o(xy)$.
 4. Établir
$$\exists g \in G \quad | \quad o(g) = \ell$$
 5. Soit $\mathbb{K}$ un corps et G un sous-groupe fini de $\mathbb{K}^*$. Montrer que G est cyclique.
-

Exercice 7 (****)

Soit $n \geq 3$ et a entier impair.

1. Montrer que
$$a^{2^{n-2}} \equiv 1 \pmod{2^n}$$
2. Le groupe $U(\mathbb{Z}/2^n\mathbb{Z})$ est-il cyclique ?
3. Trouver le plus petit entier nul k tel que $3^k \equiv 1 \pmod{2^n}$.
4. Montrer que $U(\mathbb{Z}/2^n\mathbb{Z})$ est isomorphe au groupe produit $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}, +)$.

Exercice 8 (****)

Un nombre complexe est dit *algébrique* s'il est racine d'un polynôme à coefficients rationnels. Un nombre complexe qui n'est pas algébrique est dit *transcendant*.

1. Montrer que l'ensemble $\mathcal{A}$ des nombres algébriques est dénombrable.
2. Soit x un rationnel. Montrer qu'il existe $c > 0$ tel que, pour tout $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ avec $x \neq \frac{p}{q}$, on a

$$\left| x - \frac{p}{q} \right| \geq \frac{c}{q}$$

3. Soit x un réel irrationnel algébrique. Montrer qu'il existe $(a, b) \in (\mathbb{R}_+^*)^2$ tel que, pour tout $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$, on a

$$\left| x - \frac{p}{q} \right| \geq \frac{a}{q^b}$$

4. Montrer que $\sum_{n=0}^{+\infty} 10^{-n!}$ n'est pas algébrique.

Exercice 9 (***)

Pour n entier, on note $\pi(n)$ le nombre de nombres premiers dans $\llbracket 1; n \rrbracket$.

1. Montrer $\forall n \geq 2 \quad \pi(n) \geq \frac{\ln(d_n)}{\ln(n)}$ avec $d_n = \text{ppcm}(1, 2, \dots, n)$

2. On pose $J_n = \int_0^1 t^n (1-t)^n dt$. Montrer

$$\forall n \in \mathbb{N} \quad 1 \leq d_{2n+1} \times J_n \leq \frac{d_{2n+1}}{4^n}$$

3. Conclure que $\frac{n}{\ln(n)} = O(\pi(n))$

Exercice 10 (***)

Soit n entier non nul et p un nombre premier avec $p \geq 5$ tels que $p \mid 1 + n + n^2$.

1. Établir $n \not\equiv 1 \pmod{p} \quad n^2 \not\equiv 1 \pmod{p} \quad n^3 \equiv 1 \pmod{p}$
2. En déduire $3 \mid p-1$ puis $6 \mid p-1$
3. Conclure en montrant qu'il existe une infinité de nombres premiers de la forme $6k+1$ avec k entier non nul.

Indications

Exercice 1 (***)

Indications : 4. Établir que les classes d'équivalence pour la relation $\mathcal{R}_x$ sont de la forme aG_x avec $a \in G$. En déduire que ces classes ont même cardinal.

5. Utiliser le fait que les classes d'équivalence pour la relation $\mathcal{R}$ forment une partition de l'ensemble E .

Exercice 2 (***)

Indications : 1. Utiliser le fait que

$$\llbracket 1; n \rrbracket = \bigsqcup_{d|n} \{k \in \llbracket 1; n \rrbracket \mid k \wedge n = d\}$$

2. Procéder par récurrence. Établir et utiliser le lemme suivant :

Lemme 1. Soit $B \in \mathbb{Z}[X]$ non nul unitaire. Pour $A \in \mathbb{Z}[X]$, le quotient et reste de la division euclidienne de A par B dans $\mathbb{R}[X]$ sont dans $\mathbb{Z}[X]$.

Exercice 3 (****)

Indications : 1. Observer que $\mathbb{K}$ est un $\mathbb{Z}$ -ev.

3. Utiliser les résultats établis sur les polynômes cyclotomiques.

4. Observer que pour $x \in \mathbb{K}^*$, l'ensemble $\mathbb{K}_x^* \cup \{0\}$ est un corps contenant $\mathbb{Z}$ puis établir que pour d entier non nul, si $q^d - 1 \mid q^n - 1$, alors $d \mid n$.

5. Dédire de ce qui précède que $\Phi_n(q) \mid q - 1$ et aboutir à une contradiction.

Exercice 4 (**)

Indications : 1. Écrire $\sum_{k=1}^n \tau(k) = \sum_{k=1}^n \left(\sum_{d|k} 1 \right)$ puis changer l'ordre de sommation.

2. Encadrer la partie entière et utiliser un résultat de comparaison série/intégrale.

3. Écrire $\sum_{k=1}^n \sigma(k) = \sum_{k=1}^n \left(\sum_{(i,j) \in \llbracket 1; n \rrbracket^2 \mid i \times j = k} i \right)$ puis changer l'ordre de sommation.

Exercice 5 (****)

Indications : Si G possède un élément d'ordre p et un d'ordre q , montrer que G cyclique. Puis supposer G non cyclique avec, par exemple, tous ses éléments autres que 0 d'ordre p . Pour z d'ordre p , considérer la relation d'équivalence $\mathcal{R}$ définie par $x \mathcal{R} y$ où $y = x + kz$ avec $k \in \mathbb{Z}$ puis montrer que l'ensemble des classes d'équivalence possède une structure de groupe et établir une contradiction.

Exercice 6 (****)

Indications : 1. Justifier que $\{k \in \mathbb{N}^* \mid \forall x \in G \quad x^k = 1\}$ est non vide.

2. Notant $d = o(x)$, $\delta = d \wedge k$, $d = \delta d'$ et $k = \delta k'$ avec $d' \wedge k' = 1$, établir que d' et $o(x^k)$ sont associés.

3. Pour k entier tel que $(xy)^k = 1$, passer à la puissance $o(x)$ et utiliser le théorème de Gauss. Exploiter ensuite la symétrie des rôles.

4. Relier ℓ avec les ordres des éléments de x . Puis, notant $\ell = \prod_{i=1}^r p_i^{\alpha_i}$ avec les p_i premiers deux à deux distincts et les α_i entiers non nuls, observer qu'il existe $x_i \in G$ tel que $p_i^{\alpha_i} \mid o(x_i)$ et construire un élément y_i d'ordre $p_i^{\alpha_i}$.

5. Comparer G et $\{x \in \mathbb{K}^* \mid x^\ell = 1\}$

puis exploiter les résultats précédents ainsi que le fait qu'un polynôme de $\mathbb{K}[X]$ de degré n admet au plus n racines distinctes.

Exercice 7 (****)

Indications : 1. Considérer $a^{2^{n-2}} - 1$ puis considérer une factorisation du type $(X+1)(X-1)$.

2. Comparer l'ordre de $U(\mathbb{Z}/2^n\mathbb{Z})$ avec l'ordre d'un de ses éléments.

3. Montrer que $o(\bar{3})$ dans $U(\mathbb{Z}/2^n\mathbb{Z})$ est une puissance de 2 qu'on note 2^p puis factoriser $3^{2^p} - 1$ et déterminer p .

4. Considérer
$$\varphi: \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z} \longrightarrow U(\mathbb{Z}/2^n\mathbb{Z}) \\ (\widehat{k}, \ell) \longmapsto \overline{(-1)^k 3^\ell} \end{cases}$$

On pourra s'intéresser aux congruences de 3 modulo 8 pour en déduire un résultat modulo 2^n et déterminer le noyau $\text{Ker } \varphi$.

Exercice 8 (****)

Indications : 1. Avec l'égalité $\mathbb{Q}[X] = \bigcup_{n \in \mathbb{N}} \mathbb{Q}_n[X]$, établir que $\mathbb{Q}[X]$ est dénombrable puis décrire $\mathcal{A}$ à l'aide de $\mathbb{Q}[X]$.

2. Écrire x sous forme de fraction et mettre au même dénominateur dans l'expression $x - \frac{p}{q}$.

3. Considérer $P \in \mathbb{Q}[X]$ irréductible de degré $d \geq 2$ tel que $P(x) = 0$ puis invoquer le théorème des accroissements finis sur $P\left(\frac{p}{q}\right) = P\left(\frac{p}{q}\right) - P(x)$. Observer qu'il existe A entier non nul tel que $AP \in \mathbb{Z}[X]$. Majorer $|P'|$ sur $[x-1; x+1]$ puis généraliser le résultat obtenu.

4. Utiliser les critères précédemment établis et l'inégalité

$$\forall N \in \mathbb{N} \quad \sum_{n=N+1}^{+\infty} \frac{1}{10^{n!}} \leq \sum_{n=(N+1)!}^{+\infty} \frac{1}{10^n}$$

Exercice 9 (***)

- Indications :** 1. Utiliser la décomposition de d_n en facteurs premiers.
2. Étudier $t \mapsto t(1 - t)$ sur $[0; 1]$ et développer J_n à l'aide du binôme de Newton.
3. Minorer $\pi(2n + 1)$ puis utiliser $\pi(2n + 2) \geq \pi(2n + 1)$ pour conclure.
-

Exercice 10 (***)

- Indications :** 1. Procéder par l'absurde pour les deux premières relations.
2. Observer que $\bar{n} \in U(\mathbb{Z}/p\mathbb{Z})$ puis considérer $o(\bar{n})$.
3. Suivre une idée semblable à celle de la preuve de l'infinité des nombres premiers.