Séance 7 - MP+ - 28/03/25

Exercice 1 (***)

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

$$\mathrm{G}\times\mathrm{E}\to\mathrm{E},\ (g,x)\mapsto g\cdot x$$

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

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

$$\mathrm{O}_x=\{g\cdot x, g\in\mathrm{G}\}$$

le *stabilisateur* de x noté G_x par

$$\mathrm{G}_x=\{g\in\mathrm{G}\mid g\cdot x=x\}$$

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

$$x\mathcal{R}y \iff y\in\mathrm{O}_x$$

1. Vérifier que le groupe G agit sur lui-même par translation à gauche $\mathrm{G}^2\to\mathrm{G},(g,x)\mapsto gx$ et par conjugaison $\mathrm{G}^2\to\mathrm{G},(g,x)\mapsto gxg^{-1}$.
2. Établir que la relation $\mathcal{R}$ est une relation d'équivalence dont les classes d'équivalence sont les orbites.
3. Soit $x\in\mathrm{E}$. Établir que G_x est sous-groupe de G puis vérifier que la relation binaire $\mathcal{R}_x$ définie pour $(a,b)\in\mathrm{G}^2$ 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 $\qquad \forall x\in\mathrm{E} \qquad \mathrm{Card}\,\mathrm{G}=\mathrm{Card}\,\mathrm{O}_x\times\mathrm{Card}\,\mathrm{G}_x$
5. Conclure en montrant *l'équation aux classes*

   $$\mathrm{Card}\,\mathrm{E}=\sum_{i=1}^{n}\frac{\mathrm{Card}\,\mathrm{G}}{\mathrm{Card}\,\mathrm{G}_{x_i}}$$

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

Exercice 2 (***)

On définit les *polynômes cyclotomiques* par

$$\forall n \in \mathbb{N}^* \qquad \Phi_n = \prod_{k \in [\![1\,;\,n]\!],\ k \wedge n = 1} \left(\mathrm{X} - \mathrm{e}^{\frac{2\mathrm{i}k\pi}{n}} \right)$$

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

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

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

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

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

   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
   $$\mathrm{Card}\ \mathrm{O}_x = \frac{\mathrm{Card}\ \mathbb{K}^*}{\mathrm{Card}\ {\mathbb{K}^*}_x}$$

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

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 $$\forall n \in \mathbb{N} \qquad \sum_{k=1}^{n} \tau(k) = \sum_{d=1}^{n} \left\lfloor \frac{n}{d} \right\rfloor$$

2. En déduire $$\sum_{k=1}^{n} \tau(k) \underset{n \to +\infty}{\sim} n \ln n$$

3. Établir l'égalité $$\forall n \in \mathbb{N} \qquad \sum_{k=1}^{n} \sigma(k) = \sum_{j=1}^{n} \frac{1}{2} \left\lfloor \frac{n}{j} \right\rfloor \left(\left\lfloor \frac{n}{j} \right\rfloor + 1 \right)$$

4. En déduire $$\sum_{k=1}^{n} \sigma(k) \underset{n \to +\infty}{\sim} \frac{\zeta(2)}{2} n^2 \quad \text{où} \quad \zeta(2) = \sum_{n=1}^{+\infty} \frac{1}{n^2}$$

Exercice 5 (****)

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

Exercice 6 (****)

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

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

Exercice 7 (****)

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

1. Montrer que $$a^{2^{n-2}} \equiv 1 \ [2^n]$$
2. Le groupe $\mathrm{U}(\mathbb{Z}/2^n\mathbb{Z})$ est-il cyclique ?
3. Trouver le plus petit entier nul k tel que $3^k \equiv 1 \ [2^n]$.
4. Montrer que $\mathrm{U}(\mathbb{Z}/2^n\mathbb{Z})$ 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 $\mathscr{A}$ 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 $x \neq \dfrac{p}{q}$, on a
$$\left| x - \frac{p}{q} \right| \geqslant \frac{c}{q}$$
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
$$\left| x - \frac{p}{q} \right| \geqslant \frac{a}{q^b}$$
4. Montrer que $\sum\limits_{n=0}^{+\infty} 10^{-n!}$ n'est pas algébrique.

Exercice 9 (***)

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

1. Montrer $\qquad \forall n \geqslant 2 \qquad \pi(n) \geqslant \dfrac{\ln d_n}{\ln n} \quad$ avec $\quad d_n = \mathrm{ppcm}(1, 2, \ldots, n)$
2. On pose $\mathrm{J}_n = \displaystyle\int_0^1 t^n (1-t)^n \, \mathrm{d}t$. Montrer
$$\forall n \in \mathbb{N} \qquad 1 \leqslant d_{2n+1} \times \mathrm{J}_n \leqslant \frac{d_{2n+1}}{4^n}$$
3. Conclure que $$\frac{n}{\ln n} = \mathrm{O}(\pi(n))$$

Exercice 10 (***)

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

1. Établir $\qquad n \not\equiv 1\ [p] \qquad n^2 \not\equiv 1\ [p] \qquad n^3 \equiv 1\ [p]$
2. En déduire $\qquad 3 | p - 1 \quad$ puis $\quad 6 | p - 1$
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 $a\mathrm{G}_x$ avec $a \in \mathrm{G}$. 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

$$[\![1\,;n]\!] = \bigsqcup_{d|n} \{k \in [\![1\,;n]\!] \mid k \wedge n = d\}$$

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

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

Exercice 3 (****)

Indications : 1. Observer que $\mathbb{K}$ est un 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 Z puis établir que pour d entier non nul, si $q^d - 1 | q^n - 1$, alors $d|n$.
5. Déduire de ce qui précède que $\Phi_n(q) | q - 1$ et aboutir à une contradiction.

Exercice 4 (**)

Indications : 1. Écrire $\sum\limits_{k=1}^{n} \tau(k) = \sum\limits_{k=1}^{n} \left(\sum\limits_{d|k} 1 \right)$ puis changer l'ordre de sommation.
2. Encadrer la partie entière et utiliser un résultat de comparaison série/intégrale.
3. Écrire $\sum\limits_{k=1}^{n} \sigma(k) = \sum\limits_{k=1}^{n} \left(\sum\limits_{(i,j)\in[\![1\,;n]\!]^2 \ \mid \ i\times j=k} i \right)$ 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 $\{k \in \mathbb{N}^* \mid \forall x \in \mathrm{G} \quad x^k = 1\}$ 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 $x_i \in \mathrm{G}$ tel que $p_i^{\alpha_i} | o(x_i)$ et construire un élément y_i d'ordre $p_i^{\alpha_i}$.
5. Comparer $\quad \mathrm{G} \quad$ et $\quad \{x \in \mathbb{K}^* \mid x^\ell = 1\}$

puis exploiter les résultats précédents ainsi que le fait qu'un polynôme de $\mathbb{K}[\mathrm{X}]$ 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 $(\mathrm{X}+1)(\mathrm{X}-1)$.
2. Comparer l'ordre de $\mathrm{U}(\mathbb{Z}/2^n\mathbb{Z})$ avec l'ordre d'un de ses éléments.
3. Montrer que $o(\overline{3})$ dans $\mathrm{U}(\mathbb{Z}/2^n\mathbb{Z})$ est une puissance de 2 qu'on note 2^p puis factoriser $3^{2^p} - 1$ et déterminer p.

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

On pourra s'intéresser aux congruences de 3 modulo 8 pour en déduire un résultat modulo 2^n et déterminer le noyau Ker φ.

Exercice 8 (****)

Indications : 1. Avec l'égalité $\mathbb{Q}[\mathrm{X}] = \bigcup_{n\in\mathbb{N}} \mathbb{Q}_n[\mathrm{X}]$, établir que $\mathbb{Q}[\mathrm{X}]$ est dénombrable puis décrire $\mathscr{A}$ à l'aide de $\mathbb{Q}[\mathrm{X}]$.
2. Écrire x sous forme de fraction et mettre au même dénominateur dans l'expression $x - \dfrac{p}{q}$.
3. Considérer $\mathrm{P} \in \mathbb{Q}[\mathrm{X}]$ irréductible de degré $d \geqslant 2$ tel que $\mathrm{P}(x) = 0$ puis invoquer le théorème des accroissements finis sur $\mathrm{P}\left(\dfrac{p}{q}\right) = \mathrm{P}\left(\dfrac{p}{q}\right) - \mathrm{P}(x)$. Observer qu'il existe A entier non nul tel que $\mathrm{AP} \in \mathbb{Z}[\mathrm{X}]$. Majorer $|\mathrm{P}'|$ sur $[\,x-1\,; x+1\,]$ puis généraliser le résultat obtenu.
4. Utiliser les critères précédemment établis et l'inégalité

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

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 $\pi(2n+2) \geqslant \pi(2n+1)$ pour conclure.

Exercice 10 (***)

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