Colle semaine 5 MP*

Pierre Le Scornet

17 octobre 2020

Cours 1

Énoncer et démontrer la propriété universelle sur les morphismes de $(\mathbb{Z}, +)$ vers un groupe G.

Cours 2

Énoncer et démontrer un isomorphisme entre un groupe monogène infini et $(\mathbb{Z}, +)$ et entre un groupe cyclique et $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}^*$.

Cours 3

Énoncer et démontrer la relation entre l'ordre d'un groupe et l'ordre de chacun de ses éléments.

Exercice 1 - *

Soient $A, B \in \mathcal{M}_n(\mathbb{R})$.
1) On suppose que $tr({}^tAA) = 0$. Que peut-on dire de la matrice A ?
2) On suppose que pour tout $X \in \mathcal{M}_n(\mathbb{R})$, on a $tr(AX) = tr(BX)$. Montrer que $A = B$.

Exercice 2 - *

1) Soit G un groupe et $x \in G$ d'ordre n. Quel est l'ordre de x^2 ?
2) Soit G un groupe dont tous les éléments (sauf l'élément neutre) sont d'ordre 2. Montrer que G est abélien.

Exercice 3 - *

On note $\mathcal{GL}_n(\mathbb{Z})$ l'ensemble des matrices inversibles à coefficients entiers de $\mathcal{M}_n(\mathbb{R})$ dont l'inverse est aussi à coefficients entiers.
1) Montrer que si M est à coefficients dans $\mathbb{Z}$, alors $M \in \mathcal{GL}_n(\mathbb{Z})$ ssi $detM = \pm 1$.
2) En déduire que $\mathcal{GL}_n(\mathbb{Z})$ est un sous-groupe de $\mathcal{GL}_n(\mathbb{R})$.

Exercice 4 - **

Montrer que G est fini si et seulement si il possède un nombre fini de sous-groupe.

Exercice 5 - **

Pour $n \in \mathbb{N}^*$ à quoi est congru $(n-1)!$ modulo n ?

Exercice 6 - **

1) Soit G un groupe, H et K deux sous-groupes de G d'ordres premiers. Montrer que $H = K \vee H \cap K = \{e\}$.
2) En déduire que dans un groupe d'ordre 35, il existe un élément d'ordre 5 et un d'ordre 7.

Exercice 7 - Bonus

Montrer que si deux matrices réelles sont semblables dans $\mathcal{M}_n(\mathbb{C})$, elles le sont dans $\mathcal{M}_n(\mathbb{R})$.
Le rang caractérise exactement les classes d'équivalences des matrices de $\mathcal{M}_{m,n}(\mathbb{K})$.

Solution 1

1) On peut calculer les coefficients diagonaux de $C = {}^tAA$: cela nous donne $c_{ii} = \sum_{j=1}^{n} a_{ij}.a_{ij} = \sum_{j=1}^{n} a_{ij}^2$. On a donc $tr({}^tAA) = \sum_{i=0}^{n}\sum_{j=0}^{n} a_{ij}^2$. On a donc une somme de termes positifs : si elle est nulle, alors tous ces termes sont nuls. Ainsi, $A = 0$.
2) On va appliquer cette égalité aux matrices E^{kl} de la base canonique de $\mathcal{M}_n(\mathbb{R})$. On a alors $tr(AE^{kl}) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}e_{ji}^{kl} = a_{lk} = b_{lk} = tr(BE^{kl})$ pour tous $k, l \in [\![1; n]\!]$, donc $A = B$.

Solution 2

1) D'une part, $(x^2)^n = (x^n)^2 = e$, donc $o(x^2)|n$.
   — Si n est pair, alors $(x^2)^{\frac{n}{2}} = e$ et donc $o(x^2)|\frac{n}{2}$. De plus, $(x^2)^{o(x^2)} = x^{2o(x^2)} = e$ donc $2o(x^2) \equiv 0$ mod n. On a donc $\frac{n}{2}|o(x^2)$ et donc $o(x^2) = \frac{n}{2}$.
   — Si n est impair, alors on a aussi $x^{2o(x^2)} = e$. On a donc $n|2o(x^2)$, et puisque $pgcd(2, n) = 1$, on a $n|o(x^2)$ par le lemme de Gauss et donc $n = o(x^2)$.
2) Pour tous $x, y \in G$, x, y, et xy sont d'ordres 1 ou 2. On a donc $x^2y^2 = e = (xy)^2$. En simplifiant par x d'un côté et y de l'autre, on a donc $xy = yx$, et G est donc abélien.

Solution 3

1) Montrons le sens direct. M est inversible dans $\mathcal{GL}_n(\mathbb{R})$ ssi $detM \neq 0$. Or le déterminant est un polynôme en les coefficients des matrices (avec des coefficients 1 devant les termes), donc $detM \in \mathbb{Z}$. Enfin, son inverse est aussi à coefficients entiers donc $det(M^{-1}) \in \mathbb{Z}$, et on a $det(MM^{-1}) = det(M)det(M^{-1}) = 1$, donc $det(M) = \pm 1$.

Montrons le sens réciproque. On a directement que $det(M) \neq 0$ donc M est inversible et à coefficients entiers. On a aussi $det(M^{-1}) = det(M)^{-1} \in \mathbb{Z}$. Or $M^{-1} = \frac{1}{det(M)}{}^t com(M)$, et $\frac{1}{det(M)} \in \mathbb{Z}$ et les coefficients de la comatrice sont des déterminants de sous-matrices de M, donc sont entiers. Ainsi, M^{-1} est à coefficients entiers, et $M \in \mathcal{GL}(\mathbb{Z})$.
2) D'abord, $I_n \in \mathcal{GL}_n(\mathbb{Z})$. Ensuite, pour $M \in \mathcal{GL}_n(\mathbb{Z})$, on a par définition que $M^{-1} \in \mathcal{GL}_n(\mathbb{Z})$. Enfin, pour $M, N \in \mathcal{GL}_n(\mathbb{Z})$, MN matrice inversible à coefficients entiers et de déterminant $det(MN) = det(M)det(N) = \pm 1. \pm 1 = \pm 1$, donc $MN \in \mathcal{GL}_n(\mathbb{Z})$. On peut donc conclure que $\mathcal{GL}_n(\mathbb{Z})$ est un sous-groupe de $\mathcal{GL}_n(\mathbb{R})$.

Solution 4

Le sens direct est trivial (car les sous groupes de G sont inclus dans les sous-ensembles de G, qui sont en nombre fini). Pour la réciproque, on va le montrer en deux étapes. D'une part, pour $x \in G$, le groupe engendré par x est soit fini ($n.x = 0$ pour un certain $n \in \mathbb{N}^*$), soit infini et isomorphe à $(\mathbb{Z}, +)$. S'il est isomorphe à $\mathbb{Z}$, alors il a une infinité de sous-groupes ce qui est impossible car G a un nombre fini de sous-groupes, donc $\langle x \rangle$ est isomorphe à $\mathbb{Z}/_{n\mathbb{Z}}, n \in \mathbb{N}^*$. D'autre part, puisque $G = \cup_{x \in G} \langle x \rangle$, et qu'on a un nombre fini de sous-groupes de la forme $\langle x \rangle$ (qui sont finis), G est fini.

Solution 5

On va distinguer des cas :

- Si n n'est pas premier : on a tous les diviseurs positifs non triviaux de n qui sont dans le produit $(n-1)!$.
  - Si n s'écrit $n = ab$, $a \neq b$, alors on a $ab|(n-1)!$ et donc $(n-1)! \equiv 0 \mod n$.
  - S'il ne peut pas s'écrire de cette façon, alors il est égal au carré d'un nombre premier $n = p^2$. On a alors ou $p = 2$ et $n = 4$, alors $(n-1)! \equiv 2[n]$, ou $p > 2$ et $2p < n$. On a donc $n = p^2 | 2p.p | (n-1)!$ et on a $(n-1)! \equiv 0 \mod n$.
- Si n est premier, alors on se place dans le groupe des inversibles de $\mathbb{Z}/_{n\mathbb{Z}}$. Puisque n est premier, ce groupe contient tous les éléments non nuls de $\mathbb{Z}/_{n\mathbb{Z}}$. Dans ce groupe, on peut réarranger le produit $(n-1)!$ en regroupant par deux les éléments et leurs inverses, et en laissant de côté ceux qui sont leurs propres inverses. Ainsi, $(n-1)!$ est égal dans $\mathbb{Z}/_{n\mathbb{Z}}{}^*$ aux produits des éléments qui sont leurs propres inverses, c'est à dire 1 et -1 (il ne peut pas y en avoir plus, car ils sont racines du polynôme $X^2 - 1$ qui ne peut pas avoir plus de deux racines à un polynôme de degré 2 dans un corps). On a donc si $n = 2$, $(n-1)! \equiv 1 \equiv -1 \mod n$, et si $n > 2$, $(n-1)! \equiv 1. - 1 \equiv -1 \mod n$.

On a donc $(n-1)! \equiv -1 \mod n \iff n$ premier.

Solution 6

1) D'une part, $H \cap K$ est un sous-groupe de G d'ordre fini. Pour tout élément $x \in H \cap K$, on a donc H d'ordre divisant p et q : son ordre est donc soit 1 (alors $x = e$) soit $p = q$ et donc il engendre H et K. Ainsi, tout élément de $H \cap K$ qui n'est pas l'élément neutre engendre entièrement H et K, et donc soit $H \cap K = \{e\}$, soit il existe un tel x et puisqu'il engendre H et K entièrement on a

$H = \langle x \rangle = K$.

2) Soit G un tel groupe. Ses éléments sont d'ordre divisant 35, ils sont donc d'ordre 1, 5, 7 ou 35.
   - S'il existe un élément $a \in G$ d'ordre 35, alors l'ordre de a^5 est 7 et l'ordre de a^7 est 5.
   - S'il n'en existe pas, raisonnons par l'absurde : supposons qu'il n'existe pas d'élément d'ordre 7. Alors ils sont tous d'ordre 5 (sauf e) et G s'écrit comme la réunion de sous-groupes d'ordres 5 (la réunion de tous les sous-groupes engendrés par un élément non trivial). D'après la première question, les intersections de deux de ces sous-groupes distincts sont donc réduites à e, et notons les $G_1 \dots G_n$. Alors si l'on note $H_i = G_i \setminus \{e\}$, on a les H_i qui sont disjoints deux à deux et $G = \{e\} \cup H_1 \cup \dots \cup H_n$. En passant au cardinal, on a donc $35 = 1 + 4n$, ce qui est impossible pour $n \in \mathbb{N}$.
   - De même si l'on suppose qu'il n'y a pas d'éléments d'ordre 5, le même raisonnement nous donne $m \in \mathbb{N}$ tel que $35 = 1 + 6m$, ce qui est impossible.

On en déduit donc qu'il existe au moins un élément d'ordre 5 et un élément d'ordre 7.

Solution 7

Pour la première question, on peut remarquer que si $A = PBP^{-1}$ avec $P \in \mathcal{M}_n(\mathbb{C})$. On passe le P^{-1} de l'autre côté, et on obtient $AP = PB$. Or si l'on pose $Re = Re(P), Im = Im(P)$, on a donc en décomposant en partie réelle et partie imaginaire notre égalité $ReP = PRe$ et $ImP = PIm$. On ne sait pas si l'une de ces deux matrices est inversible (sinon on a gagné). Si les deux ne le sont pas, on a quand même $(Re + xIm)P = P(Re + xIm)$ pour tout $x \in \mathbb{R}$. Si l'on note $Q(x) = det(Re + xIm)$, Q est un polynôme à coefficient réels en x et on sait que Q est non nul puisque $Q(i) = detP \neq 0$. Ainsi, Q admet une infinité de valeurs x telles que $Q(x) \neq 0$, et alors $Re + xIm$ est inversible et l'on a gagné.

Pour la deuxième, voici une idée de la preuve : on va montrer que toute matrice de rang r est équivalente à une matrice de même taille avec r 1 sur la diagonale en haut à gauche (et des 0 partout ailleurs). Pour cela, il suffit de prendre comme base de départ une famille dont les $(n - r)$ derniers vecteurs forment une base du noyau de A (qui existe avec le théorème de la base incomplète) et comme base d'arrivée une famille avec les r images des r premiers vecteurs de la bases, complétée à droite.