HX3 Mathématiques

Devoir surveillé N^{o}2

Samedi 12 octobre 2002

- Durée : 4 heures -

Les deux exercices et les deux problèmes sont totalement indépendants. Il est demandé de rédiger les deux exercices et le premier problème sur un premier ensemble de copies relevé au bout de trois heures trente minutes. Le second ensemble de copie relevé au bout des quatre heures portera la rédaction du second problème.

On prendra bien soin de préciser toute notation non donnée dans l'énoncé. Toute affirmation devra être justifiée. Les récurrences ne sauraient être commencées sans une formulation claire de l'hypothèse de récurrence.

Il n'est pas interdit d'admettre certains éléments de démonstration (voire des questions entières) afin de ne pas rester bloqué. Mais ils doivent absolument être mentionnés.

On laissera une marge à gauche.

Il est demandé de ne pas recopier l'énoncé, on mettra seulement en évidence les numéros des questions traitées. Il est recommandé par contre d'annoncer ce qui va être démontré et éventuellement par quel type de raisonnement (récurrence, absurde, contraposée...). Seules les conclusions et les résultats mis en valeur seront pris en compte.

Enfin, les solutions doivent être rédigées et le formalisme utilisé avec parcimonie. La présentation et la rédaction pourront représenter jusqu'à 15% *de la note obtenue.*

Exercice 1 : Morphismes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$

1) Soient G, H deux groupes finis, $a \in G$, $f : G \longrightarrow H$ un morphisme de groupes. Montrer que l'ordre de $f(a)$ dans H divise celui de a dans G.

2) On considère $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$ muni de leur structure de groupes ($n, m \geqslant 2$) et $f : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ un morphisme de groupes. On note d l'ordre de $x = f(\bar{1})$.

a. Montrer que d divise n et m.

b. Que peut-on dire de f lorsque n et m sont premiers entre eux (i.e. sans autre diviseur positif commun que 1) ?

c. Exhiber un élément d'ordre d de $\mathbb{Z}/m\mathbb{Z}$.

3) Soit d un diviseur positif commun à n et m, x un élément d'ordre d dans $\mathbb{Z}/m\mathbb{Z}$. Construire un morphisme de groupes $f : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ tel que $f(\bar{1}) = x$.

Exercice 2 : Inversion binômiale

On admet dans cet exercice qu'étant données deux familles de $\mathbb{Q}$, $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ à support fini pour $+$, le fait que

$$\sum_{n\in\mathbb{N}} a_n x^n = \sum_{n\in\mathbb{N}} b_n x^n,$$

pour tout $x \in \mathbb{Q}$, entraine que $a_n = b_n$ pour tout $n \in \mathbb{N}$.

1) Soit $x \in \mathbb{Q}$. En factorisant l'expression $\sum_{k=0}^{n} C_n^k (x-1)^k$, puis en la développant, démontrer que

$$\sum_{k=l}^{n} (-1)^{k-l} C_n^k C_k^l = \begin{cases} 0 \text{ si } k < n \\ 1 \text{ si } k = n \end{cases}$$

2) Soit $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ deux suites de $\mathbb{Q}$. Démontrer l'équivalence des propositions suivantes

(i) pour tout $n \in \mathbb{N}$, $v_n = \sum_{k=0}^{n} C_n^k u_k$;

(ii) pour tout $n \in \mathbb{N}$, $u_n = \sum_{k=0}^{n} (-1)^{n-k} C_n^k v_k$.

Problème : Le théorème de Frobénius

Soient G un groupe fini de cardinal n, H un sous-groupe de G. On suppose que $\dfrac{\mathrm{Card}G}{\mathrm{Card}H} = p$ où p est le plus petit nombre premier divisant $\mathrm{Card}G$ (en particulier, si $k \geqslant 0$ divise $\mathrm{Card}G$, $k = 1$ ou $k \geqslant p$).

On note G/H l'ensemble des parties de G qui s'écrivent $xH = \{xh, h \in H\}$ avec $x \in G$.

1) Soit $x, y \in G$. Démontrer que si xH et yH ont un élément en commun, $xH = yH$.

2) Démontrer que G/H constitue une partition de G.

Pour $a, b \in G/H$ avec $a = xH$ ($x \in G$), on note $a \sim b$ lorsqu'il existe $g \in H$ tel que $b = (gx)H$.

3) Démontrer que $\sim$ est une relation d'équivalence.

On note $\Omega_1, \dots, \Omega_r$ les classes déquivalences de G/H pour $\sim$. On choisit pour $1 \leqslant i \leqslant r$, $x_i \in G$ tel que $x_i H \in \Omega_i$.

4) On suppose que Ω_1 est la classe de $1H = H$. Quel est le cardinal de Ω_1 ?

5) Soit $1 \leqslant i \leqslant r$. On considère $f : H \longrightarrow \Omega_i$ qui à $g \in H$ associe gx_iH.

a. Démontrer que $K = f^{<-1>}(\{x_iH\}) = \{g \in H, gx_iH = x_iH\}$ est un sous-groupe de H.

b. Soit $g_0 \in H$. Démontrer que $f^{<-1>}(\{g_0x_iH\}) = g_0K$.

c. En déduire que $\mathrm{Card}\Omega_i = \dfrac{\mathrm{Card}H}{\mathrm{Card}K}$.

6) Démontrer que toutes les parties Ω_i sont de cardinal 1.

7) Conclure que H est un sous-groupe distingué i.e. pour tout $x \in G$,

$$xHx^{-1} \subset H.$$

Problème : Loi sur les parties finies de $\mathbb{Z}$

Une suite arithmétique de raison r est une suite $(x_n)_{n\in\mathbb{N}}$ de $\mathbb{Z}$ telle que $x_{k+1} = x_k + r$ pour tout $k \geqslant 0$.

Une suite arithmétique finie de raison r est une suite $(x_0, \dots, x_n)$ de $\mathbb{Z}$ telle que $x_{k+1} = x_k + r$ pour tout $0 \leqslant k \leqslant n$.

On note $\mathcal{S}$ l'ensemble des parties finies de $\mathbb{Z}$.

Si S_1 et S_2 sont deux parties finies de $\mathbb{Z}$, on note

$$S_1 + S_2 = \{x_1 + x_2, x_1 \in S_1, x_2 \in S_2\}.$$

Étant donnée une partie finie de S, on note

$$n * S = \underbrace{S + S + \cdots + S}_{n \text{ termes}}.$$

Par contre, nS désigne la partie $\{nx, x \in S\}$.

Enfin, pour $a \in \mathbb{Z}$, on pose $a + S = \{a\} + S$.

I. Questions préliminaires.

1) Montrer que la loi $+$ définie plus haut confère à $\mathcal{S}$ la structure de monoïde commutatif.

2) Est-il vrai que toute partie finie de $\mathbb{Z}$ est régulière ? (A est dite régulière si pour tout B et C dans $\mathcal{S}$, $A + B = A + C$ entraine $B = C$)

3) a. On se donne deux suites finies arithmétiques $(x_0, \ldots, x_n)$ et $(y_0, \ldots, y_m)$ de $\mathbb{Z}$ de même raison r. On note $A = \{x_0, \ldots, x_n\}$ et $B = \{y_0, \ldots, y_m\}$ les supports de ces suites. Calculer $\text{Card}(A + B)$ en fonction de $\text{Card}A + \text{Card}B$.

b. On note $A_1, A_2, \ldots, A_n$ le support de n suites arithmétiques finies de même raison r. Calculer le cardinal de $A_1 + \cdots + A_n$ en fonction de $\text{Card}A_1 + \cdots + \text{Card}A_n$.

II. Cardinal de $2 * S$.

Dans cette partie, S désigne une partie finie non vide de $\mathbb{Z}$ de cardinal q. On note $a_1 < a_2 < \ldots < a_q$ les éléments de S.

1) En considérant l'ensemble

$$\{2a_1, a_1 + a_2, 2a_2, a_2 + a_3, 2a_3, \ldots, a_{q-1} + a_q, 2a_q\},$$

établir que $\text{Card}(2 * S) \geqslant 2\text{Card}S - 1$.

2) On suppose réalisée l'égalité $\text{Card}(2 * S) = 2\text{Card}S - 1$. Montrer en considérant les nombres $a_{i-1} + a_{i+1}$ que S est une progression arithmétique (i.e. l'ensemble des termes d'une suite arithmétique finie).

III. Cardinal de $S + T$

Soient S et T deux parties finies non vides de $\mathbb{Z}$, $p = \text{Card}S$, $q = \text{Card}T$. On supposera $p \leqslant q$ et on notera $a_1 < a_2 < \ldots < a_p$ les éléments de S et $b_1 < b_2 < \ldots < b_q$ ceux de T.

1) En considérant l'ensemble

$$\{a_1 + b_1, a_2 + b_1, a_2 + b_2, a_3 + b_2, \ldots, a_p + b_{p-1}, a_p + b_p, a_p + b_{p+1}, \ldots, a_p + b_q\},$$

établir l'inégalité $\text{Card}(S + T) \geqslant \text{Card}S + \text{Card}T - 1$.

2) On suppose $\text{Card}(S + T) = \text{Card}S + \text{Card}T - 1$.

a. Établir que

$$\begin{aligned}
a_1 + b_2 &= a_2 + b_1 \\
a_2 + b_3 &= a_3 + b_2 \\
&\vdots \\
a_{p-1} + b_p &= a_p + b_{p-1} \\
a_{p-1} + b_{p+1} &= a_p + b_p \\
a_{p-1} + b_{p+2} &= a_p + b_{p+1} \\
&\vdots \\
a_{p-1} + b_q &= a_p + b_{q-1}.
\end{aligned}$$

b. Soit $T' = \{b_1, b_2, \dots, b_p\}$. Montrer que $T' = (b_1 - a_1) + S$. En déduire que $\mathrm{Card}(2 * S) = 2p - 1$.

c. Montrer que S et T sont des progressions arithmétiques de même raison.

IV. Cardinal de $S_1 + \cdots + S_p$

Soient $S_1, \dots, S_p$ des parties finies non vides de $\mathbb{Z}$.

1) En faisant une récurrence sur p, établir l'inégalité

$$\mathrm{Card}(S_1 + \cdots + S_p) \geqslant \mathrm{Card} S_1 + \cdots + \mathrm{Card} S_p - (p - 1).$$

2) On suppose $p \geqslant 2$. Montrer que si

$$\mathrm{Card}(S_1 + \cdots + S_p) = \mathrm{Card} S_1 + \cdots + \mathrm{Card} S_p - (p - 1),$$

alors les S_i sont des progressions arithmétiques.