HX3 Mathématiques

Devoir en temps libre N^{o}3

A remettre le vendredi 5 novembre 2004

Il est demandé de ne pas recopier l'énoncé. Il n'est pas nécessaire de rédiger les questions 1) à 3) de la première partie du premier problème. Il en va de même de la partie V du second problème.

On prendra bien soin de préciser toute notation non donnée dans l'énoncé. Toute affirmation devra être justifiée et on hésitera pas à faire référence aux propriétés utilisées.

On laissera une marge à gauche.

Enfin, les solutions doivent être rédigées et le formalisme utilisé avec parcimonie.

Problème 1 : indicatrice d'Euler

Pour tout $n \in \mathbb{N}^*$, on note $\varphi(n)$ le nombre d'entiers $k \in [\![1, n]\!]$ tel que $\text{pgcd}(k, n) = 1$ (c'est aussi le nombre de $k \in [\![0, n-1]\!]$ tel que $\text{pgcd}(k, n) = 1$).

I. Première partie.

Soit G un groupe dont la loi est notée multiplicativement. On suppose G cyclique d'ordre $n \geqslant 1$ engendré par a.

1) Soit $1 \leqslant k \leqslant n$. Montrer l'équivalence des deux conditions suivantes :

(i) a^k engendre G.

(ii) k et n sont premiers entre eux.

En déduire que tout groupe cyclique d'ordre n admet $\varphi(n)$ générateurs.

2) Soit d un diviseur de n. Montrer que $a^{\frac{n}{d}}$ est d'ordre d.

3) Soit $p \in \mathbb{Z}$. Montrer que l'ordre de a^p est $\dfrac{n}{\text{pgcd}(n,p)}$.

Si d est un diviseur de n, on note H_d le sous-groupe engendré par $a^{\frac{n}{d}}$.

4) Soit H' un sous-groupe de G d'ordre d. Montrer que $H' = H_d$. En déduire que pour tout diviseur d de n, G possède un unique sous-groupe d'ordre d.

5) Soit $b \in G$, $d \in \mathbb{N}$. Montrer que b engendre H_d si et seulement si b est d'ordre d. Combien H_d a t-il de générateurs?

6) Conclure que

$$n = \sum_{d|n} \varphi(d)$$

II. Deuxième partie.

1) Soit m et n deux entiers premiers entre eux. Soit $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ muni de la

structure de groupe produit : si $(a,b,c,d) \in \mathbb{Z}^4$,

$$(\overline{a},\dot{b}) + (\overline{c},\dot{d}) = (\overline{a+b}, \dot{c+d}),$$

la classe de $x \in \mathbb{Z}$ modulo m (resp. n) étant noté $\overline{x}$ (resp. $\dot{x}$).

a. Quel est l'ordre de $a = (\overline{1},\dot{1})$ dans le groupe $(G,+)$. En déduire que a engendre G. À quel groupe simple est isomorphe G ?

b. Soit $(k,l) \in \mathbb{Z}^2$. On suppose que k est premier avec m, l premier avec n. Montrer que $(\overline{k},\dot{l})$ est d'ordre mn.

c. Soit $(k,l) \in \mathbb{Z}^2$. On suppose que k n'est pas premier avec m. Montrer que $(\overline{k},\dot{l})$ a un ordre strictement inférieur à mn.

On montrerait qu'il en va de même si l n'est pas premier avec n.

d. Conclure que $\varphi(mn) = \varphi(m)\varphi(n)$.

2) Soit p un nombre premier.

a. Calculer $\varphi(p)$.

b. Soit $\alpha \in \mathbb{N}^*$. Dénombrer les multiples de p dans $[\![\, 1, p^\alpha]\!]$. En déduire $\varphi(p^\alpha)$.

3) Soit $n \in \mathbb{N}^*$, $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ sa décomposition en facteurs premiers (les p_i sont premiers deux à deux distincts). Montrer que

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_r}\right)$$

Problème 2 : sous-groupes de $\mathbb{R}$

Dans ce problème, U désigne l'ensemble des complexes de module 1 et si $n \in \mathbb{N}^*$,

$$U_n = \{z \in U,\ \ z^n = 1\}$$

On admettra que π est irrationnel.

I. Soient H un sous-groupe de $(\mathbb{R},+)$ distinct de $\{0\}$ et $H_+ = H \cap \mathbb{R}_+^*$.

1) Montrer que H_+ est non vide.

2) On suppose que H_+ possède un plus petit élément a. Montrer que $H = a\mathbb{Z}$

3) On suppose que H_+ ne possède pas de plus petit élément. Montrer que $\inf H_+ = 0$ et en déduire que H est dense dans $\mathbb{R}$.

4) Donner un exemple de sous-groupe de $\mathbb{R}$ dense dans $\mathbb{R}$ et distinct de $\mathbb{R}$.

II. Soient $a > 0$ et $b > 0$. On pose $H = a\mathbb{Z} + b\mathbb{Z}$.

1) On suppose que $\dfrac{a}{b} = \dfrac{n}{p}$ avec $(n,p) \in \mathbb{N}^{*2}$ et $\operatorname{pgcd}(n,p) = 1$. Montrer que $H = \dfrac{a}{n}\mathbb{Z} = \dfrac{b}{p}\mathbb{Z}$.

2) On suppose que $\dfrac{a}{b} \notin \mathbb{Q}$. Montrer alors que H est dense dans $\mathbb{R}$.

III. Une partie B du cercle trigonométrique U est dite dense dans U si : pour tout $z \in U$ et tout $\varepsilon > 0$, il existe $b \in B$ tel que $|z-b| \leqslant \varepsilon$. On admettra que pour tout $\alpha \in \mathbb{R}$, $|\sin\alpha| \leqslant |\alpha|$.

1) Montrer que pour tout $(x,y) \in \mathbb{R}^2$, on a $|e^{ix} - e^{iy}| \leqslant |x-y|$.

2) Soit A une partie dense de $\mathbb{R}$. Montrer que e^{iA} est dense dans U.

3) Montrer que $e^{i\pi\mathbb{Q}} = \{e^{i\pi q} \in U, q \in \mathbb{Q}\}$ est un sous-groupe dense de U de cardinal infini tel que tout élément est d'ordre fini.

IV. Soient $a > 0$, $G = e^{ia\mathbb{Z}}$.

1) On suppose que $\frac{a}{\pi} \in \mathbb{Q}$ et on prend $(n,p) \in \mathbb{N}^{*2}$ tel que $\frac{a}{2\pi} = \frac{n}{p}$ et $\text{pgcd}(n,p) = 1$. Montrer que $G = U_p$.

2) On suppose que $\frac{a}{\pi} \notin \mathbb{Q}$. Montrer que G est dense dans U.

3) Montrer que $(\cos n)_{n\in\mathbb{Z}}$ est dense dans $[-1.1]$ (i.e. pour tout $x \in [-1,1]$ et tout $\varepsilon > 0$, il existe $n \in \mathbb{Z}$ tel que $|\cos n - x| \leqslant \varepsilon$). Même question avec $(\sin n)_{n\in\mathbb{Z}}$.

4) Démontrer que si $A \subset [-1,1]$ est dense dans $[-1,1]$, pour toute partie F finie, $A\backslash F$ est encore dense dans $[-1,1]$.

5) Déduire de la question précédente que la suite $(\sin n)_{n\in\mathbb{N}}$ est dense dans $[-1,1]$.

V. Soient G un sous-groupe de $\mathbb{C}^*$ de cardinal n. Prouver que $G = U_n$.

Problème 3 : théorème de Wilson

1) Soit K un corps fini commutatif. Montrer que $\prod_{x\in K^*} x = -1$.

2) Soit p un nombre premier. Montrer que $(p-1)! \equiv -1 \pmod{p}$.

3) Soit $p \geqslant 5$ un nombre premier et $N \in \mathbb{N}$ défini par :

$$\sum_{k=1}^{p-1} \frac{1}{k^2} = \frac{N}{(p-1)!^2}$$

Montrer que p divise N.