Epreuve du 3 décembre 2024

Durée: 1 h 30

Les documents et écrans divers ne sont pas autorisés.

Exercice 1 Répondre par A ou B aux assertions suivantes. Justifier toute réponse à l'aide d'un argument, d'un énoncé de cours ou d'un contre-exemple.

Assertion 1 Tout groupe d'ordre p premier est cyclique.

A. *Vrai* B. *Faux*

réponse: A.
Soit K un groupe d'ordre p. Par Lagrange, tout $x \in K$ est d'ordre un diviseur de p, i.e. ord $(x) = 1$ ou ord $(x) = p$. Le neutre $e \in K$ est l'unique élément d'ordre 1; tout $x \neq e$ est d'ordre p et $K = \langle x \rangle$.

Assertion 2 Soit $(U_n, \cdot)$ le groupe des racines $n-$ièmes de l'unité de $\mathbf{C}$. Pour tout $n, m \in \mathbf{N}^\star$,

A. $U_m \cap U_n = U_{\text{ppcm}(m,n)}$ B. $U_m \cap U_n = U_{\text{pgcd}(m,n)}$.

réponse: B.
On peut exclure A par un contre-exemple: pour $m = 2, n = 3$, $U_2 = \{1, -1\}$ $U_3 = \{1, j, j^2\}$ $(j = e^{\frac{2\pi i}{3}})$, $U_2 \cap U_3 = \{1\}$ et ppcm $(2, 3) = 6$.

On peut aussi montrer B en se servant de la propriété: pour $z \in (\mathbf{C}^\times, \cdot)$ et $l \in \mathbf{N}^\star$, $z^l = 1$ ssi ord $(z) \mid l$.
Ici, $z \in U_m \cap U_n$ ssi ord(z) divise m et n ssi ord (z) divise pgcd (m, n) ssi $z^{\text{pgcd}(m,n)} = 1$.

Assertion 3 Le groupe cyclique $(\mathbf{Z}/100\mathbf{Z}, +)$ a 20 éléments d'ordre 100.

A. *Vrai* B. *Faux*

réponse: B.
Tout groupe cyclique d'ordre n a $\varphi(n)$ éléments d'ordre n (φ est l'indicatrice d'Euler) et $\varphi(100) = \varphi(4 \times 25) = \varphi(4)\varphi(25) = 2 \times 20 = 40$.
[*Une remarque à ce propos: le calcul de $\varphi(n)$ utilise i) si a et b sont premiers entre eux, $\varphi(ab) = \varphi(a)\varphi(b)$ et ii) pour p premier et $l \in \mathbf{N}^\star$, $\varphi(p^l) = p^l - p^{l-1}$. Ici pgcd $(4, 25) = 1$ et $\varphi(25) = \varphi(5^2) = 5^2 - 5 = 20$.*]

Assertion 4 Soit p un nombre premier. Dans le groupe produit direct $U_p \times U_{p^2}$ des racines $p-$ièmes et p^2-ièmes de l'unité de $\mathbf{C}$, la liste L des ordres des éléments est

A. $L = (1, p, p^2)$ B. $L = (1, p, p^2, p^3)$

réponse: A.
Tout couple (z, z') est d'ordre un diviseur de $|U_p \times U_{p^2}| = p^3$. Cet ordre est au plus p^2 car

$$(z, z')^{p^2} = (z^{p^2}, (z')^{p^2}) = ((z^p)^p, (z')^{p^2}) = (1, 1).$$

Les trois autres diviseurs $1, p$ et p^2 figurent dans la liste L car $(1, 1)$ est d'ordre 1, $(e^{\frac{2i\pi}{p}}, 1)$ est d'ordre p et $(1, e^{\frac{2i\pi}{p^2}})$ est d'ordre p^2.

[*Cf aussi le cours:* dans le groupe produit $H \times K$, ord$(h, k) =$ ppcm(ord(h), ord(k)).]

Exercice 2
Soit K un groupe cyclique. On rappelle que pour tout diviseur d de l'ordre $|K|$, K contient un unique sous - groupe d'ordre d.

On désigne par $((\mathbf{Z}/n\mathbf{Z})^\times, \cdot)$ le groupe des inversibles multiplicatifs de l'anneau $(\mathbf{Z}/n\mathbf{Z}, +, \cdot)$.

On se propose ici de montrer par un calcul d'ordre que pour $n = 175 = 7\times 25$, le groupe $((\mathbf{Z}/n\mathbf{Z})^\times, \cdot)$ n'est pas cyclique.

1. Résoudre pour r et s dans $\mathbf{Z}$ les deux systèmes de congruences

$$\begin{cases} r \equiv 6 \mod 7 \\ r \equiv 1 \mod 25 \end{cases}, \qquad \begin{cases} s \equiv 1 \mod 7 \\ s \equiv 24 \mod 25 \end{cases}$$

2. Montrer que la classe $\overline{r}$ est d'ordre 2 dans le groupe $((\mathbf{Z}/175\mathbf{Z})^\times, \cdot)$. Quel est l'ordre de la classe $\overline{s}$?

3. En vous servant du rappel, conclure que $((\mathbf{Z}/175\mathbf{Z})^\times, \cdot)$ n'est pas un groupe cyclique.

Solution:
1. Il y a plusieurs manières de faire:
- en voici une: par la deuxième congruence r s'écrit $r = 1 + 25k$ pour un certain $k \in \mathbf{Z}$ et par la première $\overline{r} = \overline{6}$ dans $\mathbf{Z}/7\mathbf{Z}$. On a, dans le corps $\mathbf{Z}/7\mathbf{Z}$,

$$\overline{6} = \overline{r} = \overline{1} + \overline{25}\overline{k} = \overline{1} + \overline{4}\overline{k},$$

dont la solution est

$$\overline{k} = (\overline{4})^{-1}(\overline{6} - \overline{1}) = \overline{2} \cdot \overline{5} = \overline{3}$$

($(\overline{4})^{-1} = \overline{2}$ car $\overline{2} \cdot \overline{4} = \overline{8} = \overline{1}$), i.e.

$$k = 3 + 7l, \quad r = 1 + 25k = 1 + 25(3 + 7l) = 76 + 175l, \quad l \in \mathbf{Z}.$$

Des manipulations analogues pour s donne $s = -76 + 175l$, $l \in \mathbf{Z}$.

- en voici une autre: supposons pgcd $(p_1, p_2) = 1$, une solution du système $x \equiv a_1 \mod p_1$, $x \equiv a_2 \mod p_2$ s'obtient comme suit: si $up_1 + vp_2 = 1$, alors $x_0 = a_1 vp_2 + a_2 up_1$ est solution.

Pour r, ceci s'écrit $-7 \times 7 + 2 \times 25 = 1$ et $r = 6 \times 2 \times 25 - 1 \times 7 \times 7 = 300 - 49 = 251 \equiv 76 \mod 175$. Idem pour s.

2. Une réponse: la première congruence donne $r^2 \equiv 36 \mod 7 = 1 \mod 7$ et la deuxième donne $r^2 \equiv 1 \mod 25$.

On a donc $7|r^2 - 1$, $25|r^2 - 1$ et pgcd $(7, 25) = 1$. Par le lemme de Gauss, $7 \times 25 = 175 \mid r^2 - 1$, i.e. $\overline{r}^2 = \overline{1}$ dans $(\mathbf{Z}/175\mathbf{Z})^\times$.

Comme $\overline{r} = -\overline{s}$, on a aussi $\overline{s}^2 = \overline{1}$.

Une autre réponse: $76^2 = 5776$ et $5776 = 33 \times 175 + 1$, i.e. dans $(\mathbf{Z}/175\mathbf{Z})^\times$, $\overline{r}^2 = \overline{76}^2 = \overline{1}$.

3. Par le rappel, un groupe cyclique d'ordre pair a un unique sous-groupe d'ordre 2 donc un unique élément d'ordre 2. Comme $\overline{r}$ et $\overline{s}$ sont d'ordre 2 et distincts, $(\mathbf{Z}/175\mathbf{Z})^\times$ n'est pas cyclique.

Exercice 3 On note $\mathbf{N}^\star = \mathbf{N} \setminus \{0\}$. Soit

$$\sigma : \mathbf{N}^\star \to \mathbf{N}^\star : n \mapsto \sigma(n) = \sum_{d|n} d$$

l'application qui à tout entier $n > 0$ associe la somme de ses diviseurs. On admettra ici que pour tout $(a, b) \in (\mathbf{N}^\star)^2$ avec pgcd $(a, b) = 1$, on a

$$\sigma(ab) = \sigma(a)\sigma(b).$$

1. Soit p un nombre premier et $d \in \mathbf{N}^\star$. Faire la liste des diviseurs de p^d. En déduire que

$$\sigma(p^d) = \frac{p^{d+1} - 1}{p - 1}.$$

On dit que l'entier $N \in \mathbf{N}^\star$ est *parfait* si $\sigma(N) = 2N$. On se propose ici de caractériser les entiers parfaits pairs.

2. Montrer que 6 et 28 sont des nombres parfaits.

3. On suppose que p et $2^p - 1$ sont premiers. Montrer que $2^{p-1}(2^p - 1)$ est parfait. [*On pourra par exemple relire les premières lignes de cet exercice.*]

4. Soit $N \in \mathbf{N}^\star$ pair.

i) Justifier l'existence d'un entier $n \geq 2$ et d'un entier impair q tels que $N = 2^{n-1}q$.

ii) On suppose N parfait. Montrer qu'il existe $t \in \mathbf{N}^\star$ tel que $q = (2^n - 1)t$ et $\sigma(q) = 2^n t$.

iii) En déduire que l'entier q est premier et $t = 1$. [*Se servir de l'égalité* $2^n t = (2^n - 1)t + t$.]

iv) En conclusion, montrer que tout nombre parfait pair N s'écrit $N = 2^{p-1}(2^p - 1)$ avec p un nombre premier tel que $2^p - 1$ est premier.

Solution:
Deux rappels utiles:
- si $N = p_1^{s_1} \cdots p_r^{s_r}, s_j > 0$, est la factorisation primaire de l'entier $N \geq 2$, les diviseurs de N sont les entiers

$$p_1^{a_1} \cdots p_r^{a_r}, \quad 0 \leq a_j \leq s_j \text{ pour tout } j.$$

- pour $z \in \mathbf{C}$ et $n \in \mathbf{N}^\star$, $(z^n - 1) = (z - 1)(1 + z + \cdots + z^{n-1})$.

1. Voici la liste des diviseurs de p^d: $1, p, p^2, \ldots, p^d$ et leur somme $\sigma(p^d)$ s'écrit

$$\sigma(p^d) = 1 + p + p^2 + \cdots + p^d = \frac{p^{d+1} - 1}{p - 1}.$$

2. $6 = 2 \times 3$ a quatre diviseurs 1, 2, 3 et 6 et $\sigma(6) = 1 + 2 + 3 + 6 = 2 \times 6$.
$28 = 4 \times 7 = 2^2 \times 7$ a six diviseurs 1, 2, 4, 7, $2 \times 7 = 14$ et 28 et $\sigma(28) = 2 \times 28$.

3. pgcd $(2^{p-1}, 2^p - 1) = 1$ car 2^{p-1} a 2 pour seul facteur premier et $2^p - 1$ est impair. Par la propriété admise,

$$\sigma(2^{p-1}(2^p - 1)) = \sigma(2^{p-1})\sigma(2^p - 1).$$

Par la question 1, $\sigma(2^{p-1}) = \frac{2^p - 1}{2 - 1} = 2^p - 1$.
D'autre part, $2^p - 1$ étant supposé premier, ses diviseurs sont 1 et $2^p - 1$, donc $\sigma(2^p - 1) = (2^p - 1) + 1 = 2^p$ et on obtient

$$\sigma(2^{p-1}(2^p - 1)) = (2^p - 1)2^p = 2\,(2^{p-1}(2^p - 1)).$$

Observer que les exemples de la question 2 sont les deux premiers nombres parfaits de ce type : $6 = 2^{2-1}(2^2 - 1)$ et $28 = 2^{3-1}(2^3 - 1)$.

4.

i) soit $N = p_1^{s_1} \cdots p_r^{s_r}$, $s_j > 0$, la factorisation primaire de N. N étant pair, $p_1 = 2$, les autres p_j sont impairs, donc $q = p_2^{s_2} \cdots p_s^{s_r}$ est impair. En posant $s_1 = n - 1$, on a $N = 2^{n-1}q$.

ii) En se servant de pgcd $(2^{n-1}, q) = 1$, la condition $2N = \sigma(N)$ s'écrit

$$2^n q = 2N = \sigma(N) = \sigma(2^{n-1}q) = \sigma(2^{n-1})\sigma(q) = (2^n - 1)\sigma(q).$$

Ceci montre que $2^n - 1$ divise $2^n q$. Comme pgcd $(2^n - 1, 2^n) = 1$, par Gauss, $2^n - 1$ divise q, i.e. il existe $t \in \mathbf{N}^\star$ tel que $q = (2^n - 1)t$.

Ensuite, l'égalité $2^n q = (2^n - 1)\sigma(q)$ s'écrit $2^n(2^n - 1)t = (2^n - 1)\sigma(q)$, i.e. $2^n t = \sigma(q)$.

iii) On a deux informations: $q = (2^n - 1)t$ et $\sigma(q) = 2^n t = (2^n - 1)t + t = q + t$.

Puisque q et t divise q et $\sigma(q) = \sum_{d|q} d = q + t$, l'entier $q > 1$ a exactement deux diviseurs t et q, i.e. q est premier. Enfin, $t = 1$ car les diviseurs de q premier sont 1 et q.

iv) Par ce qui précède, tout entier N pair et parfait s'écrit $N = 2^{n-1}(2^n - 1)$ avec $n \geq 2$ et $2^n - 1$ premier.

Pour conclure, il nous reste à montrer que si $2^n - 1$ est premier, alors n l'est aussi. Ceci se fait (comme au premier partiel) en contraposant, i.e. en observant que si $n = ab$ avec $a > 1, b > 1$, alors $2^n - 1$ est composé:
$(2^{ab} - 1) = ((2^a)^b - 1) = (2^a - 1)(1 + 2^a + \cdots + (2^a)^{b-1})$ et ces deux facteurs sont > 1.