

DS 3 : *Arithmétiques.*
Groupes cycliques.
Suites numériques.

MPSI-Maths.

Mr Mamouni & El Hassani : myismail1@menara.ma

Source disponible sur :

©<http://www.chez.com/myismail>

Lundi 10 Décembre 2007.

Durée: 3 heures 30mn.

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ
وَقُلْ إِعْمَلُوا فَمَا يَرَى اللَّهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ
صَدَقَ اللَّهُ الْعَظِيمِ

Conseils pour la rédaction et la présentation des copies. (4 points)

- Chaque variable utilisée dans une démonstration doit être définie.
- L'énoncé ne doit pas être recopié sur les copies.
- Chaque résultat annoncé doit être justifié en citant précisément le théorème du cours avec ses hypothèses exactes utilisé ou en

citant le numéro de la question précédente utilisée.

- Les résultats importants doivent être simplifiés et encadrés.
- Les calculs doivent être détaillés et expliqués à l'aide de phrases simples.
- Laisser une marge à gauche de chaque feuille, en tirant un trait vertical, et un horizontal de la 1ère double feuille pour la note et les remarques du correcteur.
- Numérotter les double feuille de la façon suivante : 1/n, 2/n, ..., n/n où n est le nombre total de double feuille.
- Les questions doivent être traités dans l'ordre de l'énoncé.
- Tirer deux traits diagonaux pour rayer une partie du raisonnement que vous considérez fausse.

Problème 1. (Fonction indicatrice d'Euler.)

Pour tout $n \in \mathbb{N}^*$, on pose

$$\varphi(n) = \text{card}\{k \in [1, n] \text{ tel que } k \wedge n = 1\}$$

- 1) Montrer que n est premier $\iff \varphi(n) = 1$.
- 2) Montrer que dans $\mathbb{Z}/n\mathbb{Z}$, on a :
 \bar{k} est inversible $\iff k \wedge n = 1$
- 3) En déduire que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps $\iff n$ est premier.
- 4) On notera $U(\mathbb{Z}/n\mathbb{Z})$ l'ensemble des éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$, que vaut $\text{card}U(\mathbb{Z}/n\mathbb{Z})$
- 5) Soit $(m, n) \in \mathbb{N}^*$ tel que $n \wedge m = 1$.

a) Montrer que l'application

$$\theta : ((\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}), \times) \longrightarrow (\mathbb{Z}/nm\mathbb{Z}, \times)$$

$$(\bar{x}, \bar{y}) \longmapsto \overline{xy}$$

est un isomorphisme.

b) Montrer que :

$$\begin{aligned} & \bar{x} \text{ inversible dans } \mathbb{Z}/n\mathbb{Z}, \bar{y} \text{ inversible dans } \mathbb{Z}/m\mathbb{Z} \\ \iff & (\bar{x}, \bar{y}) \text{ inversible dans } \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ \iff & \overline{xy} \text{ inversible dans } \mathbb{Z}/nm\mathbb{Z} \end{aligned}$$

c) Conclure que

$$\varphi(nm) = \varphi(n)\varphi(m)$$

- 6) Montrer que si $(n_i)_{1 \leq i \leq r}$ sont des entiers naturels premiers entre eux deux à deux, alors

$$\varphi\left(\prod_{i=1}^r n_i\right) = \prod_{i=1}^r \varphi(n_i)$$

- 7) Soit p premier, $\alpha \in \mathbb{N}^*$, montrer que

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$$

- 8) *Application :*

- a) Déterminer les entiers naturels $n \geq 2$ tel que $\varphi(n)$ divise n .

Indication : Ecrire n sous la forme $n = \prod_{i=1}^r p_i^{\alpha_i}$ avec p_i premier et $\alpha_i \in \mathbb{N}^*$.

- b) Soit d un diviseur de n , parmi les fractions $\frac{k}{n}$, tel que $1 \leq k \leq n$, combien peut-on mettre sous la forme $\frac{a}{d}$, avec $a \wedge d = 1$. En déduire que

$$\sum_{d \text{ divise } n} \varphi(d) = n$$

Problème 2. (Groupes cycliques)

Dans tout le problème, G est un groupe de cardinal n , d'élément neutre e , cyclique engendré par a . On notera par \mathcal{D}_n l'ensemble des diviseurs de n dans \mathbb{N} et par \mathcal{H} celui des sous groupes de G . on pose $\varphi(n) = \text{card}\{k \in [1, n] \text{ tel que } k \wedge n = 1\}$.

- 1) Montrer que $(G, .)$ est abélien.
- 2) Montrer que si q divise p , alors $\langle a^p \rangle \subset \langle a^q \rangle$.
- 3) a) Montrer que $o(a^k) = \frac{n}{n \wedge k}$
 b) En déduire que $G = \langle a^k \rangle \iff k \wedge n = 1$.
 c) Combien G a-t-il de générateurs exactement ?
- 4) On pose $U_n = \{z \in \mathbb{C} \text{ tel que } z^n = 1\}$. Montrer que U_n est sous-groupe de (\mathbb{C}^*, \times) , cyclique. Ses générateurs s'appellent racines $n^{\text{ème}}$ primitives de l'unité. Combien y'en a-t-il exactement. Donner ceux de U_3 et U_4 .
- 5) Pour tout $d \in \mathcal{D}_n$, on pose $H_d = \{x \in G \text{ tel que } x^d = e\}$.
 a) Montrer que H_d est un sous-groupe de G , puis que

$$H_d = \langle a^{\frac{n}{d}} \rangle$$

b) Inversement, soit H un sous groupe de (G, \cdot) .

i. Montrer que $\exists p \in \mathbb{N}$ tel que $H = \langle a^p \rangle$.

Indication : On pourra utiliser l'application :

$$f: (\mathbb{Z}, +) \longrightarrow (G, \cdot) \\ m \longmapsto a^m$$

ii. Montrer que $\langle a^p \rangle = \langle a^{p^n} \rangle$.

6) En déduire que l'application : $\Phi: \mathcal{D}_n \longrightarrow \mathcal{H}$ est bijective.
$$d \longmapsto H_d$$

7) Combien y-a-t exactement de sous groupes dans G , si $n = p^\alpha$, où p est un nombre premier.

Exercice. (Groupe symétrique.)

Soit $(n, p) \in \mathbb{N}^*$ tel que $p \leq n$ et $\sigma = (i_1, \dots, i_p)$ un p -cycle.

1) Montrer que : $\forall \alpha \in \mathcal{S}_n, \alpha \sigma \alpha^{-1} = (\alpha(i_1), \dots, \alpha(i_p))$.

2) En déduire : $(1 \ 3 \ 2)(1 \ 2 \ 3 \ 4)(1 \ 2 \ 3)$.

3) Calculer $(1 \ 2 \ 3 \ 4)^k$, pour $k = 2, k = 3$.

Problème 3. (Étude d'une suite récurrente)