

Fiche d'exercices n° 2

Groupes et géométrie

Groupes monogènes

Exercice 1. *Théorème de Gauss.*

Montrer que, a, b, c étant trois éléments non nuls de $\mathbb{Z}$, si a et b sont premiers entre eux et si a divise bc , alors a divise c .

Exercice 2.

m et n sont des entiers strictement positifs.

- a.* Démontrer que $m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z} \Leftrightarrow (m, n) = 1$
- b.* En déduire alors une démonstration du théorème 11, chapitre 3.

Exercice 3.

Soit $n \geq 1$ un entier naturel.

- a.* Soit d un diviseur de n . Combien y a-t-il d'éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$?
Démontrer la relation : $\forall n \geq 1, \sum_{d|n} \phi(d) = n$
- b.* Soit G un sous-groupe fini du groupe multiplicatif d'un corps commutatif, et n son ordre. Pour chaque diviseur d de n , on note $\psi(d)$ le nombre d'éléments de G qui sont d'ordre d . Montrer que $\psi(d)$ vaut 0 ou $\phi(d)$
- c.* Montrer que l'on a $\sum_{d|n} \psi(d) = n$
- d.* Déduire de ce qui précède que tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique.

Exercice 4.

Soit $n \geq 1$ un entier naturel.

- a.* Soit $k \in \mathbb{Z}$ un entier. Quel est le cardinal du sous groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par la classe de k modulo n ?
- b.* Si $m \geq 1$, combien y a-t-il de morphismes de $\mathbb{Z}/m\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$?
- c.* Montrer que $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$

Exercice 5. *Deux classiques.*

- a.* Théorème d'Euler
Soit $n \in \mathbb{N}^*$, soit $a \in \mathbb{Z}^*$, premier avec n .
 φ désignant la fonction d'Euler, démontrer que : $a^{\varphi(n)} \equiv 1 \pmod{n}$
- b.* Théorème de Fermat
Soient p un nombre premier, et $a \in \mathbb{Z}$.
Démontrer que $a^p \equiv a \pmod{p}$

Exercice 6.

Soit G un groupe commutatif, et x, y deux éléments de G d'ordre respectif m et n .

- a.* Montrer que si m et n sont premiers entre eux, xy est d'ordre mn .
- b.* Montrer que, dans le cas général, il existe un diviseur m' de m et un diviseur n' de n tels que m' et n' soient premiers entre eux et $m'n' = \text{ppcm}(m, n)$.
- c.* Montrer qu'il existe dans G un élément d'ordre $\text{ppcm}(m, n)$.
- d.* Montrer que si G est d'exposant N , (c'est à dire $\forall g \in G, g^N = 1$ et N est le plus petit entier non nul jouissant de cette propriété), G admet un élément d'ordre N .
Montrer que ce n'est pas forcément le cas si G n'est pas commutatif.
- e.* En déduire une autre démonstration du fait que tout sous-groupe fini du groupe multiplicatif d'un corps (commutatif) est cyclique.

Exercice 7. Théorème de Wilson.

Soit $p \geq 2$ un nombre premier.

- a.* Quels sont les éléments de $\mathbb{Z}/p\mathbb{Z}$ égaux à leur inverse ?
- b.* En déduire que p divise $(p-1)! + 1$.
- c.* Réciproquement, montrer que si $n \geq 2$ divise $(n-1)! + 1$, alors n est premier.

Exercice 8.

Soit p un entier premier.

Montrer que pour tout $k \in \mathbb{N}$, on a $\sum_{x \in \mathbb{Z}/p\mathbb{Z}} x^k$ est égal à 0 ou -1.

Exercice 9. (Théorème 12 du cours).

- a.* Montrer le lemme suivant :

Si p est un nombre premier, pour tout $\alpha \geq 1 \in \mathbb{N}$, on a :

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

- b.* En déduire que :

Soit $n > 1$ un entier.

Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ est la décomposition en facteurs premiers de n , alors :

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

- c.* Application : Que vaut $\varphi(3960)$

Exercice 10.

- a.** Montrer que si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ est la décomposition en facteurs premiers de n , alors :

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^k (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$$

- b.** Soit $p \geq 3$ un nombre premier.

- a.** Montrer qu'il existe un élément d'ordre $(p-1)$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$ et aussi dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ si $\alpha \geq 1$.
- b.** Montrer que l'ordre de la classe de $1+p$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est $p^{\alpha-1}$.
- c.** En déduire que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.

- c.** Cas $p = 2$.

- a.** Expliciter la structure de $(\mathbb{Z}/2\mathbb{Z})^\times, (\mathbb{Z}/4\mathbb{Z})^\times$ et $(\mathbb{Z}/8\mathbb{Z})^\times$
- b.** Montrer que pour $\alpha \geq 2$, l'ordre de la classe de 5 dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ est $2^{\alpha-2}$.
- c.** Montrer que, dans ce cas,

$$(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$$

Exercice 11.

Déterminer la structure des quelques groupes suivant :

- a.** $(\mathbb{Z}/15\mathbb{Z})^\times$
- b.** $(\mathbb{Z}/55\mathbb{Z})^\times$
- c.** $(\mathbb{Z}/27\mathbb{Z})^\times$
- d.** $(\mathbb{Z}/16\mathbb{Z})^\times$