

I Questions de cours

- 1 - Énoncer et démontrer la caractérisation de l'ordre d'un élément par cardinal.
- 2 - Donner le lien entre l'ordre d'un élément et le cardinal d'un groupe fini puis faire la preuve dans le cas commutatif.
- 3 - Donner les générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$ puis démontrer ce résultat.

II Exercices

Exercice 1 :

Soient p un nombre premier supérieur à 3 et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (on rappelle que \mathbb{F}_p est un corps).

- 1 - Montrer que $f : x \mapsto x^2$ est un morphisme de groupes de (\mathbb{F}_p^*, \times) dans lui-même.
- 2 - Montrer que $\ker(f) = \{\overline{-1}; \overline{1}\}$.
- 3 - Montrer que pour tout $x \in \mathbb{F}_p^*$, on a $x^{\frac{p-1}{2}} = \overline{-1}$ ou $\overline{1}$.
- 4 - Montrer qu'il y a $\frac{p-1}{2}$ carrés dans \mathbb{F}_p^* .

Exercice 2 :

- 1 - Est-ce que $\overline{18}$ est inversible dans $\mathbb{Z}/19\mathbb{Z}$? Si oui, quel est son inverse?
- 2 - Quel est l'ordre de $\overline{6}$ dans $(\mathbb{Z}/24\mathbb{Z}, +, \times)$? Cet anneau est-il intègre?

Exercice 3 :

- 1 - Résoudre l'équation $\overline{7}x = \overline{2}$ dans $\mathbb{Z}/37\mathbb{Z}$.
- 2 - Résoudre l'équation $x^2 + \overline{2}x = \overline{0}$ dans $\mathbb{Z}/8\mathbb{Z}$.

Exercice 4 :

- 1 - Résoudre l'équation $\overline{10}x = \overline{6}$ dans $\mathbb{Z}/34\mathbb{Z}$.
- 2 - Résoudre l'équation $x^3 + \overline{2}x^2 - x + \overline{1} = \overline{0}$ dans $\mathbb{Z}/5\mathbb{Z}$.

Exercice 5 :

Déterminer les inversibles de $\mathbb{Z}/8\mathbb{Z}$. Le groupe des inversibles $(\mathbb{Z}/8\mathbb{Z})$ est-il cyclique?

Exercice 6 :

Soient a et b deux entiers naturels supérieurs ou égaux à 2 dont on note m leur ppcm et d leur pgcd.
Démontrer que $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$.

Exercice 7 :

Résoudre le système suivant :

$$\begin{cases} x \equiv 1 [5] \\ x \equiv 2 [11] \end{cases}$$

Exercice 8 :

Résoudre le système suivant :

$$\begin{cases} x \equiv 1 [2] \\ x \equiv 2 [3] \\ x \equiv 3 [5] \end{cases}$$

Exercice 9 :

- 1 - Soit $n \in \mathbb{N}$.

Montrer que $n+1$ divise $\binom{2n}{n}$.

- 2 - Soient p un nombre premier et $k \in \llbracket 1; p-1 \rrbracket$.

Montrer que p divise $\binom{p}{k}$.

- 3 - En déduire une preuve du petit théorème de Fermat : si $n \in \mathbb{N}^*$ et p est un nombre premier, alors $n^p \equiv n [p]$.