

# Devoir Maison 1 - Structures algébriques

L'objectif de ce devoir est de démontrer le théorème suivant :

**Théorème 1.** Soit  $\mathbb{F}_q$  un corps fini. On a l'isomorphisme de groupes :

$$(\mathbb{F}_q^\times, \times) \simeq (\mathbb{Z}/(q-1)\mathbb{Z}, +).$$

**Question 1 :** Rappeler la définition de  $\mathbb{F}_q^\times$  et justifier que son cardinal vaut  $q-1$ .

Regardons un exemple :

**Question 2 - a :** Justifier que  $\mathbb{Z}/7\mathbb{Z}$  est un corps fini.

**Question 2 - b :** Calculer les ordres de tous les éléments du groupe  $(\mathbb{Z}/7\mathbb{Z})^\times, \times$ , puis en déduire qu'on a bien un isomorphisme de groupes :

$$(\mathbb{Z}/7\mathbb{Z}^\times, \times) \simeq (\mathbb{Z}/6\mathbb{Z}, +).$$

**Question 2 - c :** Sachant que 1021 est premier, le groupe  $((\mathbb{Z}/1021\mathbb{Z})^\times, \times)$  admet-il un élément d'ordre 56 ?

On attaque maintenant la démonstration du théorème général. On commence par prouver un lemme.

**Lemme 2.** On note  $\varphi : \mathbb{N}^* \rightarrow \mathbb{N}^*$  l'indicatrice d'Euler, c'est-à-dire la fonction définie par

$$\varphi(n) = |\{k \in \llbracket 1, n \rrbracket, k \wedge n = 1\}|.$$

Alors pour tout entier  $n \in \mathbb{N}^*$ , on a

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

Pour  $n \in \mathbb{N}^*$  et  $d$  un diviseur de  $n$ , on note

$$Z_d := \{k \in \mathbb{Z}/n\mathbb{Z}, o(k) = d\}.$$

Soit  $G_d$  le sous-groupe de  $\mathbb{Z}/n\mathbb{Z}$  engendré par l'élément  $\frac{n}{d}$ .

**Question 3 - a :** Montrer que  $Z_d \subset G_d$ .

**Question 3 - b :** En déduire que le cardinal de  $Z_d$  vaut  $\varphi(d)$ .

**Question 3 - c :** En déduire le lemme.

**Question 3 :** Soit  $\mathbb{F}_q$  un corps fini et  $d$  un diviseur de  $q-1$ . Soit  $x \in (\mathbb{F}_q^\times, \times)$  un élément d'ordre  $d$ . On note  $H = \langle x \rangle$  le sous-groupe de  $(\mathbb{F}_q^\times, \times)$  engendré par  $x$ . Justifier soigneusement que tout élément d'ordre  $d$  appartient à  $H$ , puis que le groupe  $\mathbb{F}_q^\times$  admet exactement  $\varphi(d)$  éléments d'ordre  $d$ .

**Question 4 :** Démontrer le théorème à l'aide des questions précédentes.