

# Le groupe multiplicatif d'un corps fini est cyclique.

2013 – 2014

Référence : Daniel Perrin, *Cours d'algèbre*, Ellipses, 1996, p.74.

## **Théorème.**

Le groupe multiplicatif  $\mathbb{F}_q^*$  est un groupe cyclique, isomorphe à  $\mathbb{Z}/(q-1)\mathbb{Z}$ .

## **Lemme.**

Soit  $n \in \mathbb{N}^*$ , on a

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

*Démonstration.* Tout élément de  $\mathbb{Z}/n\mathbb{Z}$  a pour ordre un diviseur  $d$  de  $n$  et il y a exactement  $\varphi(d)$  éléments d'ordre  $d$  car ils engendrent l'unique sous-groupe cyclique d'ordre  $d$  de  $\mathbb{Z}/n\mathbb{Z}$ .  $\square$

*Démonstration du théorème.* Posons  $n := q - 1$ , soit  $d$  un diviseur de  $n$ . S'il existe  $x \in \mathbb{F}_q^*$  d'ordre  $d$ , on considère le sous-groupe  $H := \langle x \rangle \simeq \mathbb{Z}/d\mathbb{Z}$  de  $\mathbb{F}_q^*$ . On a  $|H| = d$  et pour tout  $y \in H$ ,  $y^d = 1$ . De plus, le polynôme  $Y^d - 1$  a au plus  $d$  racines dans  $\mathbb{F}_q$  donc tout élément d'ordre  $d$  de  $\mathbb{F}_q^*$  est dans  $H$ . Par conséquent, le nombre  $N(d)$  d'éléments d'ordre  $d$  de  $\mathbb{F}_q^*$  vaut 0 ou  $\varphi(d)$  (nombre de générateurs de  $\mathbb{Z}/d\mathbb{Z}$ ), donc  $N(d) \leq \varphi(d)$ . Or tout élément de  $\mathbb{F}_q^*$  a pour ordre un diviseur de  $n$  donc

$$n = |\mathbb{F}_q^*| = \sum_{d|n} N(d).$$

Par le lemme, on en déduit  $N(d) = \varphi(d)$  pour tout  $d$ , d'où  $N(n) = \varphi(n) > 0$  donc  $\mathbb{F}_q^*$  contient un élément d'ordre  $n$  donc est cyclique.  $\square$

*Remarque.* Cette démonstration permet aussi de montrer que tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique, ce qui permet par exemple de montrer que tout sous-groupe fini de  $SO(2)$  est cyclique.