

# Devoir maison N°1

## Notations et rappels

- Soit  $n$  un entier  $\geq 2$ . On note  $\mathbb{Z}/n\mathbb{Z}$  l'anneau des classes d'entiers modulo  $n$ , et  $\mathbb{U}(\mathbb{Z}/n\mathbb{Z})$  le groupe multiplicatif des éléments inversibles de  $\mathbb{Z}/n\mathbb{Z}$ .
- Si  $a \in \mathbb{Z}$  est un entier quelconque, on note  $\bar{a}$  la classe de  $a$  dans l'anneau  $\mathbb{Z}/n\mathbb{Z}$ .
- On rappelle que, si  $p$  est un nombre premier, l'anneau  $\mathbb{Z}/p\mathbb{Z}$  est un corps et  $\text{Card}(\mathbb{U}(\mathbb{Z}/p\mathbb{Z})) = p - 1$ .
- On rappelle le **lemme des bergers** que l'on pourra utiliser librement :

Soient  $X, Y$  deux ensembles finis, et  $f : X \rightarrow Y$  une application surjective telle que tout élément de  $Y$  a exactement  $n$  antécédents dans  $X$ . Alors  $\text{Card}(X) = n \text{Card}(Y)$ .

- Dans tout le problème,  $p$  un nombre **premier impair** :  $p = 2p' + 1$ .

## Partie I : Groupe $\mathbb{U}(\mathbb{Z}/p\mathbb{Z})$ .

L'objectif de cette partie est de montrer que le groupe  $\mathbb{U}(\mathbb{Z}/p\mathbb{Z})$  est cyclique.

1. Soit  $K$  un corps et  $P \in K[X]$  un polynôme non nul à coefficients dans  $K$ .
  - a. Soit  $\alpha \in K$  une racine de  $P$ . Montrer qu'il existe  $Q \in K[X]$  tel que  $P = (X - \alpha)Q$ .
  - b. Montrer que  $P$  a au plus  $\deg P$  racines dans  $K$ .
2. Soit  $d$  un diviseur de  $p - 1$ .
  - a. Justifier que le polynôme  $X^{p-1} - 1$  admet exactement  $p - 1$  racines dans  $\mathbb{Z}/p\mathbb{Z}$ .
  - b. Montrer que le polynôme  $X^d - 1$  admet exactement  $d$  racines dans  $\mathbb{Z}/p\mathbb{Z}$ .
3.
  - a. Soit  $a, b$  dans  $\mathbb{U}(\mathbb{Z}/n\mathbb{Z})$  d'ordres respectivement  $r$  et  $s$ . On suppose que  $r \wedge s = 1$ . Montrer que  $ab$  est d'ordre  $rs$ .
  - b. Plus généralement, montrer que, si  $a_1, \dots, a_k$  dans  $\mathbb{U}(\mathbb{Z}/n\mathbb{Z})$  d'ordres respectivement  $r_1, \dots, r_k$  tels que, pour tout  $i \neq j$ ,  $r_i \wedge r_j = 1$ , alors  $\prod_{i=1}^k a_i$  est d'ordre  $\prod_{i=1}^k r_i$ .
4. Soit  $p - 1 = \prod_{j=1}^m p_j^{\alpha_j}$  la décomposition en nombres premiers de  $p - 1$ . Fixons  $j \in \llbracket 1, m \rrbracket$ .
  - a. Montrer l'existence d'un élément  $x_j$  dans  $\mathbb{Z}/p\mathbb{Z}$  tel que  $x_j^{p_j^{\alpha_j}} = 1$  et  $x_j^{p_j^{\alpha_j-1}} \neq 1$ .
  - b. Montrer que  $x_j$  est d'ordre  $p_j^{\alpha_j}$  dans  $\mathbb{U}(\mathbb{Z}/p\mathbb{Z})$ .
  - c. On pose  $x = \prod_{j=1}^m x_j$ . Montrer que  $x$  est d'ordre  $p - 1$ .
5. Conclure.

## Partie II : Carrés modulo $n$ .

6. Soit  $a \in \mathbb{Z}$ .
  - a. Montrer l'équivalence :  $\bar{a} \in \mathbb{U}(\mathbb{Z}/n\mathbb{Z}) \iff a \wedge n = 1$ .
  - b. Montrer que  $\overline{-1}$  et  $\bar{1}$  sont distincts dans  $\mathbb{Z}/p\mathbb{Z}$ .
7. Pour tout  $\alpha \in \mathbb{U}(\mathbb{Z}/p\mathbb{Z})$ , on pose  $\sigma(\alpha) = \alpha^2$ .
  - a. Démontrer que l'application  $\sigma$  de  $\mathbb{U}(\mathbb{Z}/p\mathbb{Z})$  dans lui-même ainsi définie est un morphisme de groupes.

- b.** Déterminer  $\ker(\sigma)$ , le noyau de  $\sigma$ .
- c.** En déduire que  $\text{Card}(\text{Im}(\sigma)) = p'$ . **Indication.** utiliser le lemme des bergers.
- d.** On note  $T$  le complémentaire de  $\text{Im}(\sigma)$  dans  $\mathbb{U}(\mathbb{Z}/p\mathbb{Z})$ .
  - i.** Déterminer le cardinal de  $T$ .
  - ii.** Démontrer que, si on fixe un élément  $\theta$  de  $T$ , on a  $T = \{\theta s, s \in \text{Im}(\sigma)\}$ .
- e.** Pour tout  $\alpha \in \mathbb{U}(\mathbb{Z}/p\mathbb{Z})$ , on pose

$$\chi_p(\alpha) = \begin{cases} 1 & \text{si } \alpha \in \text{Im}(\sigma) \\ -1 & \text{si } \alpha \in T \end{cases}$$

Démontrer que l'application  $\chi_p$  de  $\mathbb{U}(\mathbb{Z}/p\mathbb{Z})$  dans le groupe multiplicatif  $\{-1, 1\}$  ainsi définie est un morphisme de groupes surjectif.

- f.** Démontrer que l'application  $\chi_p$  est le seul morphisme surjectif du groupe  $\mathbb{U}(\mathbb{Z}/p\mathbb{Z})$  dans le groupe multiplicatif  $\{-1, 1\}$ .
- 8.** Pour tout entier  $a \in \mathbb{Z}$ , non divisible par  $p$ , on pose

$$\left(\frac{a}{p}\right) = \chi_p(a).$$

Le nombre  $\left(\frac{a}{p}\right)$  est appelé *symbole de Legendre*.

Calculer le nombre  $\left(\frac{a}{11}\right)$  pour tout entier  $a$  tel que  $1 \leq a \leq 10$ .

### Partie III : Symbole de Legendre.

On rappelle que  $p$  est un nombre premier impair :  $p = 2p' + 1$ . On se propose de calculer, en fonction des valeurs de  $p$ , le symbole de Legendre  $\left(\frac{-1}{p}\right)$ .

- 9.** Soit  $\alpha \in \mathbb{U}(\mathbb{Z}/p\mathbb{Z})$ . Démontrer que l'on a  $\alpha^{2p'} = \bar{1}$ , et en déduire que  $\alpha^{p'}$  est égal à  $\bar{1}$  ou  $-\bar{1}$ .  
**Indication.** utiliser les résultats de la question 7.

- 10.** Pour tout  $\alpha \in \mathbb{U}(\mathbb{Z}/p\mathbb{Z})$ , on pose

$$\varphi(\alpha) = \begin{cases} 1 & \text{si } \alpha^{p'} = \bar{1} \\ -1 & \text{si } \alpha^{p'} = -\bar{1} \end{cases}$$

- a.** Démontrer que l'on définit ainsi un morphisme  $\varphi$  du groupe  $\mathbb{U}(\mathbb{Z}/p\mathbb{Z})$  dans le groupe multiplicatif  $\{-1, 1\}$ . Démontrer que le morphisme  $\varphi$  est surjectif.  
**Indication.** utiliser les résultats de la première partie.

- b.** En déduire que, pour tout nombre entier  $a$  premier avec  $p$ , on a

$$a^{p'} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

- 11.** Démontrer les équivalences suivantes :

$$\begin{aligned} \left(\frac{-1}{p}\right) = 1 & \iff p \equiv 1 \pmod{4}, \\ \left(\frac{-1}{p}\right) = -1 & \iff p \equiv 3 \pmod{4}. \end{aligned}$$

D'après : Agrégation interne 2000 (extrait).