

Feuille 4 : le groupe multiplicatif

Exercice 1. (*Groupes multiplicatifs cycliques*) Le but de cet exercice est de déterminer tous les n tels que le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique.

(a) Soient G et H des groupes finis cycliques. Montrer que $G \times H$ est cyclique si et seulement si $\text{pgcd}(|G|, |H|) = 1$.

(b) Soit $0 \xrightarrow{i} K \rightarrow G \xrightarrow{\pi} H \rightarrow 0$ une suite exacte des groupes abéliens. On suppose que $\text{pgcd}(|K|, |H|) = 1$. Montrer que la suite est *scindée* ; c'est-à-dire, il existe un sous-groupe $\tilde{H} \leq G$ tel que $\pi|_{\tilde{H}}$ est un isomorphisme. (*Indication* : pour tout $x \in H$ choisir un $\tilde{x} \in \pi^{-1}(x)$ et considérer l'ensemble

$$\tilde{H} = \{K\tilde{x} : x \in H\}.$$

En déduire que $G \cong K \times H$.

(c) Soit p un premier et $m, k \in \mathbb{N}^*$. On suppose que $p^m \neq 2$. Montrer que pour tout $a \in \mathbb{Z}$

$$(1 + p^m a)^{p^k} \equiv 1 + p^{m+k} a \pmod{p^{m+k+1}}.$$

(Indication : utiliser la formule binomiale et la récurrence par k .)

(d) Soit p un premier impair et $k \in \mathbb{N}^*$. Montrer que

$$\{x \in \mathbb{Z}/p^k\mathbb{Z} : x \equiv 1 \pmod{p}\}$$

est un groupe multiplicatif cyclique engendré par $1 + p$. En déduire que le groupe $(\mathbb{Z}/p^k\mathbb{Z})^\times$ est cyclique.

(e) Montrer que

$$\{x \in \mathbb{Z}/2^k\mathbb{Z} : x \equiv 1 \pmod{4}\}$$

est un groupe multiplicatif cyclique engendré par 5. En déduire que le groupe $(\mathbb{Z}/2^k\mathbb{Z})^\times$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$.

(f) Montrer que le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si n est l'un des nombres suivants :

$$1, \quad 2, \quad 4, \quad p^k, \quad 2p^k,$$

où p est un premier impair et $k \in \mathbb{N}^*$.

Exercice 2. (*Réciprocité quadratique*) Le but de cet exercice est de démontrer la *loi de la réciprocité quadratique* :

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod{4}, \\ -1 & \text{si } p \equiv -1 \pmod{4}, \end{cases} \quad (1)$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv \pm 1 \pmod{8}, \\ -1 & \text{si } p \equiv \pm 3 \pmod{8}, \end{cases} \quad (2)$$

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{si } p \text{ ou } q \equiv 1 \pmod{4} \\ -\left(\frac{p}{q}\right) & \text{si } p, q \equiv -1 \pmod{4}, \end{cases} \quad (3)$$

où p et q sont des premiers impairs et $\left(\frac{*}{p}\right)$ est le symbole de Legendre. Plus brièvement :

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}, \quad \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}.$$

(a) Soit G un groupe cyclique d'ordre n , et soit m entier naturel. Montrer que $a \in G$ est un m -ième puissance si et seulement si $a^{n/d} = 1$, où $d = \text{pgcd}(m, n)$.

(b) Montrer que $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. En déduire (1).

(c) Soit ψ un caractère additif non principal. Considérons la somme de Gauss $g = g\left(\psi, \left(\frac{*}{p}\right)\right)$ avec le symbole de Legendre comme le caractère multiplicatif. Montrer que $g^2 = \left(\frac{-1}{p}\right)p$.

(d) Montrer que l'anneau \mathbb{Z} est intégralement clos. C'est-à-dire, si $\alpha \in \mathbb{Q}$ est entier sur \mathbb{Z} , alors $\alpha \in \mathbb{Z}$. En déduire l'affirmation suivante : si la congruence $a \equiv b \pmod{m}$ (où $a, b, m \in \mathbb{Z}$ et $m \neq 0$) est vérifiée dans un certain anneau des entiers algébriques, alors elle est vérifiée dans \mathbb{Z} .

(e) Utiliser la congruence $(a+b)^q \equiv a^q + b^q$ pour montrer que $g^q \equiv \left(\frac{a}{p}\right)g \pmod{q}$ dans l'anneau $\mathbb{Z}[e^{2\pi i/p}]$.

En déduire que $g^{q-1} \equiv \left(\frac{q}{p}\right) \pmod{q}$ dans \mathbb{Z} .

(f) Démontrer (3).

(g) Utiliser l'identité $\sqrt{2} = e^{\pi i/4} + e^{-\pi i/4}$ et la congruence $(a+b)^p \equiv a^p + b^p$ pour montrer que

$$2^{(p-1)/2} = \begin{cases} 1 & \text{si } p \equiv \pm 1 \pmod{8}, \\ -1 & \text{si } p \equiv \pm 3 \pmod{8}. \end{cases}$$

En déduire (2).

(h) Déterminer $\left(\frac{534}{997}\right)$.

Exercice 3. (*Symbole de Jacobi*) Soit b un entier positif impaire. Écrivons $b = p_1 \cdots p_m$ où les premiers p_1, \dots, p_m ne sont pas forcément distincts. Pour $a \in \mathbb{Z}$ définissons le *symbole de Jacobi* par

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_m}\right).$$

(a) Vérifier la « bi-multiplicativité » du symbole de Jacobi :

$$\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right) \left(\frac{a_2}{b}\right); \quad \left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right) \left(\frac{a}{b_2}\right).$$

(b) Montrer que a n'est pas un carré mod b si $\left(\frac{a}{b}\right) = -1$. Est-ce que la réciproque est vraie ?

(c) Soient a_1, \dots, a_m des entiers impairs. Montrer que

$$\sum_{k=1}^m \frac{a_k - 1}{2} \equiv \frac{a_1 \cdots a_m - 1}{2} \pmod{2},$$

$$\sum_{k=1}^m \frac{a_k^2 - 1}{8} \equiv \frac{a_1^2 \cdots a_m^2 - 1}{8} \pmod{2}.$$

(d) Démontrer la loi de réciprocité pour le symbole de Jacobi :

$$\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}, \quad \left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$$

et pour a et b impairs positifs

$$\left(\frac{a}{b}\right) \left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}.$$

(e) Déterminer $\left(\frac{534}{997}\right)$ en utilisant le symbole de Jacobi.

(f) Soit b impair positif. Utiliser le théorème de Dirichlet pour montrer qu'il existe un infinié des premiers p vérifiant $p \equiv 1 \pmod{8}$ et $\left(\frac{p}{b}\right) = -1$.

(g) Soit $a \in \mathbb{Z}$. Montrer que les affirmations suivantes sont équivalentes.

1. Le nombre a est carré mod p pour tout premier p sauf un nombre fini.
2. Le nombre a est positif et il est carré mod n pour tout entier n non nul.
3. Le nombre a est un carré dans \mathbb{Z} .