Agrégation Interne

Les corps $\mathbb{Z}/p\mathbb{Z}$

1 Énoncé

Pour tout entier naturel $n \geq 2$, $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est l'anneau des classes résiduelles modulo n.

On note $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^* = \left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right) \setminus \{\overline{0}\}$ et $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$ est le groupe multiplicatif des éléments inversibles de l'anneau $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

Si k est un entier relatif, on note $\overline{k} = k + n\mathbb{Z}$ la classe de k dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$.

Pour tout couple (a, b) d'entiers relatifs, on note $a \wedge b$ le pgcd de a et b et $a \vee b$ leur ppcm.

– I – Les corps $\mathbb{Z}/p\mathbb{Z}$

1. Soit a un entier relatif. Montrer que les propriétés suivantes sont équivalentes :
   (a) $\overline{a}$ est inversible dans $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$;
   (b) a est premier avec n ;
   (c) $\overline{a}$ est un générateur de $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}, +\right)$.

   On note $\varphi(n)$ le cardinal de $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$ (fonction indicatrice d'Euler).
2. Montrer que pour tout entier relatif a premier avec n, on a $a^{\varphi(n)} \equiv 1 \ (n)$ (théorème d'Euler).
3. Montrer que, pour tout entier $n \geq 2$, les assertions suivantes sont équivalentes :
   (a) n est premier ;
   (b) pour tout entier naturel non nul α, on a $\varphi(n^\alpha) = (n-1)\, n^{\alpha-1}$;
   (c) $\varphi(n) = n - 1$;
   (d) $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est un corps ;
   (e) $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est un intègre ;
   (f) $(n-1)! \equiv -1 \ (n)$ (théorème de Wilson) ;
   (g) pour tout entier k compris entre 1 et $n-1$, on a $\dbinom{n}{k} \equiv 0 \pmod{n}$.

– II – Ordre d'un élément dans un groupe

On rappelle que si $(G, \cdot)$ est un groupe, en notant $\langle g \rangle = \left\{g^k \mid k \in \mathbb{Z}\right\}$ le sous-groupe de G engendré par un élément g de G et $\theta(g)$ le cardinal de ce groupe, on a les équivalences :

$$\begin{aligned}(\theta(g) = n) &\Leftrightarrow (\langle g \rangle = \{g^r \mid 0 \leq r \leq n-1\}) \\ &\Leftrightarrow \left(k \in \mathbb{Z} \text{ et } g^k = 1 \text{ équivaut à } k \equiv 0 \bmod (n)\right) \\ &\Leftrightarrow \left(g^n = 1 \text{ et } g^k \neq 1 \text{ pour } 1 \leq k \leq n-1\right) \ (\text{si } n \geq 2) \\ &\Leftrightarrow (n \text{ est le plus petit entier naturel non nul tel que } g^n = 1)\end{aligned}$$

$\theta(g)$ est l'ordre de g dans le groupe G.

1. Soit $(G, \cdot)$ un groupe commutatif fini.

   (a) Montrer que si g_1, g_2 sont deux éléments de G d'ordres respectifs m_1, m_2 premiers entre eux, alors $g_0 = g_1 g_2$ est d'ordre $m_1 m_2$.

   (b) Montrer que si $g_1, \cdots, g_r$ sont $r \geq 2$ éléments de G d'ordres respectifs $m_1, \cdots, m_r$ deux à deux premiers entre eux, alors $g_0 = g_1 \cdots g_r$ est d'ordre $m_1 \cdots m_r$.

   (c) Soient g_1, g_2 deux éléments de G d'ordres respectifs m_1, m_2.
   En écrivant les décompositions en facteurs premiers de m_1 et m_2 sous la forme :

$$m_1 = \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=k+1}^{r} p_i^{\alpha_i} = n_1 q_1,\ m_2 = \prod_{i=1}^{k} p_i^{\beta_i} \prod_{i=k+1}^{r} p_i^{\beta_i} = n_2 q_2$$

   où les facteurs premiers p_i ont été regroupés de sorte que $\alpha_i > \beta_i$ pour $1 \leq i \leq k$ et $\alpha_i \leq \beta_i$ pour $k+1 \leq i \leq r$, les exposants α_i, β_i étant positifs ou nuls, montrer que $g_1^{n_1}$ et $g_2^{n_2}$ sont d'ordres respectifs q_1 et q_2 et en déduire que $g_1^{n_1} g_2^{n_2}$ est d'ordre $\text{ppcm}\,(m_1, m_2)$.

   (d) Montrer que :

$$\max_{g \in G} \theta(g) = \text{ppcm}\,\{\theta(g) \mid g \in G\}$$

2. Montrer que tout sous-groupe fini du groupe multiplicatif $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ d'un corps commutatif $\mathbb{K}$ est cyclique.

– III – Carrés dans $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$

Pour ce qui suit, $p \geq 3$ est un nombre premier impair et on note $\mathbb{F}_p$ le corps $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$.

1. Montrer que :

   (a) il y a exactement $\dfrac{p-1}{2}$ carrés et $\dfrac{p-1}{2}$ non carrés dans $\mathbb{F}_p^*$;

   (b) les carrés de $\mathbb{F}_p^*$ sont les racines de $X^{\frac{p-1}{2}} - 1$ et les non carrés sont les racines de $X^{\frac{p-1}{2}} + 1$;

   (c) le produit de deux carrés ou de deux non carrés de $\mathbb{F}_p^*$ est un carré, le produit d'un carré et d'un non carré est un non carré.

   Pour tout $\lambda \in \mathbb{F}_p^*$, on définit le symbole de Legendre $\left(\dfrac{\lambda}{p}\right)$ par :

$$\left(\frac{\lambda}{p}\right) = \begin{cases} 1 \text{ si } \lambda \text{ est un carré dans } \mathbb{F}_p^* \\ -1 \text{ sinon} \end{cases}$$

2. Montrer que :

   (a) pour tout $\lambda \in \mathbb{F}_p^*$, le nombre de solutions de l'équation $\lambda x^2 = 1$ dans $\mathbb{F}_p^*$ est $\left(\dfrac{\lambda}{p}\right) + 1$;

   (b) pour tout $\lambda \in \mathbb{F}_p^*$, on a $\lambda^{\frac{p-1}{2}} = \overline{\left(\dfrac{\lambda}{p}\right)}$ dans $\mathbb{F}_p^*$;

   (c) l'application :

$$\begin{array}{ccc} \mathbb{F}_p^* & \to & \{-1, 1\} \\ \lambda & \mapsto & \left(\dfrac{\lambda}{p}\right) \end{array}$$

   est l'unique morphisme de groupes non trivial de $\mathbb{F}_p^*$ sur $\{-1, 1\}$.

3.

(a) Calculer $\left(\dfrac{\overline{1}}{p}\right)$ et $\left(\dfrac{-\overline{1}}{p}\right)$.

(b) Calculer $\displaystyle\sum_{k=1}^{p-1}\left(\dfrac{\overline{k}}{p}\right)$ et $\displaystyle\sum_{k=1}^{p-2}\left(\dfrac{\overline{k\left(k+1\right)}}{p}\right)$.

– IV – Générateurs de $GL_n\left(\mathbb{K}\right)$

$\mathbb{K}$ est un corps commutatif et $n \geq 2$ un entier naturel.

Pour i, j entiers compris entre 1 et n, on note E_{ij} la matrice dont tous les coefficients sont nuls sauf celui d'indice (i, j) qui vaut 1. La famille $\left\{E_{i,j} \mid 1 \leq i, j \leq n\right\}$ est alors une base de $\mathcal{M}_n\left(\mathbb{K}\right)$.

On appelle matrice de transvection toute matrice de la forme :

$$T_{ij}\left(\lambda\right) = I_n + \lambda E_{ij}$$

avec $1 \leq i \neq j \leq n$ et $\lambda \in \mathbb{K}$ et matrice de dilatation toute matrice de la forme :

$$D_i\left(\lambda\right) = I_n + \left(\lambda - 1\right) E_{ii}$$

avec $1 \leq i \leq n$ et $\lambda \in \mathbb{K}^*$.

1. Montrer que les matrices de transvection et de dilatations sont inversibles.
2. Soit $A \in \mathcal{M}_n\left(\mathbb{K}\right)$.
   (a) Montrer que, pour $1 \leq i \leq n$ et $\lambda \in \mathbb{K}^*$, la matrice $D_i\left(\lambda\right) A$ est déduite de A en multipliant sa ligne numéro i par λ.
   (b) Montrer que, pour $1 \leq j \leq n$ et $\lambda \in \mathbb{K}^*$, la matrice $AD_j\left(\lambda\right)$ est déduite de A en multipliant sa colonne numéro j par λ
   (c) Montrer que, $1 \leq i \neq j \leq n$ et $\lambda \in \mathbb{K}$, la matrice $T_{ij}\left(\lambda\right) A$ est déduite de A en ajoutant à la ligne numéro i la ligne numéro j multipliée par λ.
   (d) Montrer que, $1 \leq i \neq j \leq n$ et $\lambda \in \mathbb{K}$, la matrice $AT_{ij}\left(\lambda\right)$ est déduite de A en ajoutant à la colonne numéro j la colonne numéro i multipliée par λ.
3. Montrer que, pour toute matrice $A \in GL_n\left(\mathbb{K}\right)$ il existe des matrices de transvection $P_1, \cdots, P_r$ et $Q_1, \cdots, Q_s$ telles que :

   $$A = P_1 \cdots P_r D_n\left(\det\left(A\right)\right) Q_1 \cdots Q_s$$

   Ce résultat se traduit en disant que l'ensemble des matrices de dilatation ou de transvection forme un système générateur du groupe multiplicatif $GL_n\left(\mathbb{K}\right)$.

– V – Le théorème de Frobenius-Zolotarev

1.

(a) Montrer que l'application $A \in GL_n\left(\mathbb{F}_p\right) \mapsto \left(\dfrac{\det\left(A\right)}{p}\right) \in \left\{-1, 1\right\}$ est un morphisme de groupes non trivial.

(b) Soit $\gamma : GL_n\left(\mathbb{F}_p\right) \to \left\{-1, 1\right\}$ un morphisme de groupes non trivial.

i. Montrer que $\gamma\left(A\right) = 1$ pour toute matrice de transvection A.

ii. Montrer que $\gamma(A) = \left(\dfrac{\det(A)}{p}\right)$ pour toute matrice de dilatation A.

iii. Montrer que $\gamma(A) = \left(\dfrac{\det(A)}{p}\right)$ pour toute matrice $A \in GL_n(\mathbb{F}_p)$.

On rappelle que, si E est un un ensemble fini, la signature est l'unique morphisme de groupes non trivial du groupe symétrique $\mathcal{S}(E)$ sur $\{-1, 1\}$.

Si E est un $\mathbb{F}_p$-espace vectoriel E de dimension n, le choix d'une base de E permet d'identifier toute matrice $A \in GL_n(\mathbb{F}_p)$ à un automorphisme de E qui est une permutation particulière de l'ensemble fini E, donc la restriction de la signature à $GL(E)$ permet de définir une morphisme de groupes ε de $GL_n(\mathbb{F}_p)$ dans $\{-1, 1\}$.

On admettra que, pour tout entier naturel non nul n, il existe dans l'anneau $\mathbb{F}_p[X]$ un polynôme irréductible de degré n.

2. Soit P un polynôme unitaire et irréductible de degré n dans $\mathbb{F}_p[X]$.

   (a) Montrer que l'anneau quotient $\dfrac{\mathbb{F}_p[X]}{(P)}$ est un $\mathbb{F}_p$-espace vectoriel de dimension n et un corps à p^n éléments.

   On notera $\mathbb{F}_{p^n}$ ce corps.

   (b) En désignant par ω un générateur du groupe cyclique $\mathbb{F}_{p^n}^*$, montrer que l'application $\sigma : x \mapsto \omega x$ est une permutation de de signature -1 de $\mathbb{F}_{p^n}^*$.

   (c) Montrer que :

$$\forall A \in GL_n(\mathbb{F}_p),\ \varepsilon(A) = \left(\frac{\det(A)}{p}\right)$$

   (théorème de Frobenius-Zolotarev).

3. En utilisant le théorème de Frobenius-Zolotarev, calculer $\left(\dfrac{2}{p}\right)$.