

Feuille 5 : caractères

Soit m un entier positif. On appelle un *caractère additif* (resp. *multiplicatif*) de l'anneau $\mathbb{Z}/m\mathbb{Z}$ un caractère du groupe additif $\mathbb{Z}/m\mathbb{Z}$ (resp., du groupe multiplicatif $(\mathbb{Z}/m\mathbb{Z})^\times$). Sauf indication contraire, ψ signifie un caractère additif et χ signifie un caractère multiplicatif de $\mathbb{Z}/m\mathbb{Z}$. L'écriture $\psi \neq 1$ ou $\chi \neq 1$ signifie que le caractère n'est pas principal. On étend la définition d'un caractère multiplicatif χ sur $\mathbb{Z}/m\mathbb{Z}$ en posant $\chi(a) = 0$ pour tout élément non inversible de $\mathbb{Z}/m\mathbb{Z}$.

À toute fonction f sur $\mathbb{Z}/m\mathbb{Z}$ on associe son « relèvement » $f \circ \pi_m$ sur \mathbb{Z} , où $\pi_m : \mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ est la réduction modulo m . Par abus de notation ce relèvement est aussi noté par f . En particulier, à tout caractère (additif ou multiplicatif) de $\mathbb{Z}/m\mathbb{Z}$ on associe son relèvement sur \mathbb{Z} , qui est appelé un *caractère de Dirichlet* (additif ou multiplicatif) modulo m .

1. (a) Montrer que le groupe de caractères additifs modulo m est cyclique. Montrer que le groupe de caractères multiplicatifs modulo m est cyclique si $m = p^k$ est une puissance d'un premier $p > 2$. (Utiliser le fait que le groupe $(\mathbb{Z}/m\mathbb{Z})^\times$ est cyclique si $m = p^k$ avec $p > 2$.)
- (b) Soit χ un caractère multiplicatif modulo m . Montrer que $\chi(-1) \in \{1, -1\}$.
- (c) Déterminer s'il existe un caractère multiplicatif χ modulo 7 vérifiant la condition indiquée ; si la réponse est positive, déterminer si un tel χ est unique :

$$\chi(3) = -1; \quad \chi(3) = \frac{1 + i\sqrt{3}}{2}; \quad \chi(2) = -1; \quad \chi(2) = \frac{1 + i\sqrt{3}}{2}; \quad \chi(2) = \frac{-1 + i\sqrt{3}}{2}.$$

- (d) Déterminer s'il existe un caractère multiplicatif χ modulo 15 vérifiant la condition indiquée ; si la réponse est positive, déterminer si un tel χ est unique :

$$\chi(-2) = -1; \quad \chi(4) = i; \quad \chi(2) = i \text{ et } \chi(7) = -1; \quad \chi(-4) = \chi(7) = -1.$$

- (e) Supposons qu'il existe un caractère multiplicatif χ modulo m et un $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ tels que $\chi(a) = i$. Montrer que m admet un diviseur premier $p \equiv 1 \pmod{4}$. Est-ce que la réciproque est vraie ?

Dans la suite on suppose que $m = p$ est un nombre premier, et on note par $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps fini de p éléments.

2. (sommes des Gauss) La somme de Gauss est

$$g(\psi, \chi) = \sum_{x \in \mathbb{F}_p} \psi(x)\chi(x),$$

où ψ est un caractère additif de \mathbb{F}_p non principal et χ est un caractère multiplicatif (principal ou non). Le but de cet exercice est de montrer que

$$|g(\psi, \chi)| = \sqrt{p}. \tag{1}$$

si χ n'est pas principal.

- (a) Considérons l'espace vectoriel des fonctions $f : \mathbb{F}_p \rightarrow \mathbb{C}$ muni du produit scalaire défini par

$$(f, g) = \frac{1}{p} \sum_{x \in \mathbb{F}_p} f(x)\overline{g(x)}.$$

Montrer que les caractères additifs forment une base orthonormée de cet espace. En déduire la « formule de Parseval »

$$(f, f) = \sum_{\psi} |(f, \psi)|^2,$$

pour toute $f : \mathbb{F}_p \rightarrow \mathbb{C}$. (Le symbole \sum_{ψ} signifie une somme sur tous caractères additifs de \mathbb{F}_p .)

(b) Montrer que pour $b \in \mathbb{Z}$, non divisible par p , on a

$$(\chi \cdot \psi^b) = \overline{\chi(b)}(\chi \cdot \psi).$$

(c) Montrer que $|(\chi \cdot \psi_1)| = |(\chi \cdot \psi_2)|$ où les caractères additifs ψ_1 et ψ_2 ne sont pas principaux.

(d) Déterminer $(\chi \cdot \psi)$ avec ψ principal.

(e) Déterminer $(\chi \cdot \chi)$.

(f) Déterminer $|(\chi \cdot \psi)|$ avec χ et ψ non principaux. (Indication : utiliser la formule de Parseval.)
En déduire (1).

3. (**sommes exponentielles**) Le but de cet exercice est de majorer la somme

$$\sum_{x \in \mathbb{F}_p} \psi(ax^r),$$

où $r \in \mathbb{N}^*$, $a \in \mathbb{F}_p^\times$ et ψ est un caractère additif non principal. (Ceci est équivalent à la majoration de la somme

$$\sum_{x=0}^{p-1} e^{\frac{2\pi i ax^r}{p}},$$

avec $a \in \mathbb{Z}$ non divisible par p ; une telle somme s'appelle la *somme exponentielle*.)

(a) Considérons l'espace vectoriel des fonctions $f : \mathbb{F}_p^\times \rightarrow \mathbb{C}$ muni du produit scalaire défini par

$$(f \cdot g) = \frac{1}{p-1} \sum_{x \in \mathbb{F}_p^\times} f(x) \overline{g(x)}.$$

Montrer que les caractères multiplicatifs forment une base orthonormée de cet espace.

(b) Exprimer les coordonnées de $\psi|_{\mathbb{F}_p^\times}$ dans cette base en terme de sommes de Gauss. En déduire que

$$\psi(x) = \frac{1}{p-1} \sum_{\chi} g(\psi, \bar{\chi}) \chi(x) \quad (x \in \mathbb{F}_p^\times).$$

(c) Montrer que

$$\sum_{x \in \mathbb{F}_p} \psi(ax^r) = \frac{1}{p-1} \sum_{\chi \neq 1} g(\psi, \bar{\chi}) \chi(a) \sum_{x \in \mathbb{F}_p^\times} \chi^r(x).$$

(d) Montrer que le nombre des caractères multiplicatifs vérifiant $\chi^r = 1$ est $d = \text{pgcd}(r, p-1)$.

(e) Montrer que

$$\left| \sum_{x \in \mathbb{F}_p} \psi(ax^r) \right| \leq (d-1) \sqrt{p}.$$

(f) Supposons que $p > 2$. Montrer que

$$\left| \sum_{x \in \mathbb{F}_p} \psi(ax^2) \right| = \sqrt{p}.$$

4. (**théorème de Weil-Lang pour les polynômes diagonaux**) Soit $\Phi(\mathbf{x}) \in \mathbb{F}_p[\mathbf{x}]$ un polynôme de n variables $\mathbf{x} = (x_1, \dots, x_n)$ sur \mathbb{F}_p . Soit $N(\Phi)$ le nombre des solutions de l'équation $\Phi(\mathbf{x}) = 0$ en $\mathbf{x} \in \mathbb{F}_p^n$. Le *théorème* célèbre de *Weil-Lang* affirme que pour Φ absolument irréductible¹ on a

$$|N(\Phi) - p^{n-1}| \leq Cp^{n-1-1/2},$$

où la constante C ne dépend que du degré de Φ et du nombre des variables n . Le but de cet exercice est de démontrer ce théorème (en forme raffinée) pour les *polynômes diagonaux*

$$\Phi(\mathbf{x}) = a_1 x_1^{r_1} + \dots + a_n x_n^{r_n} \quad (2)$$

(où $a_1, \dots, a_n \in \mathbb{F}_p^\times$) en $n \geq 3$ variables.

1. c'est-à-dire, irréductible sur la clôture algébrique $\overline{\mathbb{F}_p}$

(a) Montrer que pour tout $\Phi \in \mathbb{F}_p[\mathbf{x}]$ on a

$$N(\Phi) = \frac{1}{p} \sum_{\psi} \sum_{\mathbf{x} \in \mathbb{F}_p^n} \psi(\Phi(\mathbf{x})).$$

En déduire que

$$N(\Phi) = p^{n-1} + \frac{1}{p} \sum_{\psi \neq 1} \sum_{\mathbf{x} \in \mathbb{F}_p^n} \psi(\Phi(\mathbf{x})).$$

(b) Montrer que pour Φ diagonal, comme dans (2), on a

$$\sum_{\mathbf{x} \in \mathbb{F}_p^n} \psi(\Phi(\mathbf{x})) = \prod_{i=1}^n \sum_{x \in \mathbb{F}_p} \psi(a_i x^{r_i}).$$

(c) En déduire que pour Φ diagonal on a

$$|N(\Phi) - p^{n-1}| \leq Cp^{n/2}, \quad (3)$$

où $C = (d_1 - 1) \cdots (d_n - 1)$ avec $d_i = \text{pgcd}(r_i, p - 1)$.

(d) L'inégalité (3) implique que $N(\Phi) = p^{n-1}$ si l'un des d_i est 1. Démontrer cette affirmation sans utiliser (3).

5. Soient $a_1, \dots, a_n \in \mathbb{Z}$, $a_1 \cdots a_n \neq 0$ et $n \geq 3$. Montrer que pour tout premier p suffisamment grand, la congruence

$$a_1 x_1^{r_1} + \cdots + a_n x_n^{r_n} \equiv 0 \pmod{p}$$

admet une *solution primitive* (c'est-à-dire, avec $x_1 \cdots x_n \not\equiv 0 \pmod{p}$). (En particulier, pour a, b, c entiers non nuls les congruences $ax^2 + by^2 + cz^2 \equiv 0 \pmod{p}$ et $ax^3 + by^3 + cz^3 \equiv 0 \pmod{p}$ admettent des solutions primitives pour p suffisamment grand.)

6. (**inégalité de Pólya-Vinogradov**) Le but de cet exercice est de démontrer l'*inégalité de Pólya-Vinogradov*

$$\left| \sum_{A \leq n \leq B} \chi(n) \right| \leq \sqrt{p}(1 + \log p), \quad (4)$$

où χ est un caractère de Dirichlet non principal modulo p et A, B sont des entiers, $A \leq B$.

(a) Pour $a \in \mathbb{Z}$ on définit la fonction $\psi_a : \mathbb{Z} \rightarrow \mathbb{C}$ par $\psi_a(x) = e^{\frac{2\pi i ax}{p}}$. Expliquer le lien entre les fonctions ψ_a et les caractères additifs de \mathbb{F}_p . Montrer que pour a non divisible par p et pour tous entiers A, B on a

$$\left| \sum_{A \leq n \leq B} \psi_a(n) \right| \leq \frac{1}{\sin(\pi a/p)}$$

(b) On note par $\|x\|$ la distance entre $x \in \mathbb{R}$ et son plus proche entier :

$$\|x\| = \min\{|x - n| : n \in \mathbb{Z}\}.$$

Montrer que $|\sin(\pi x)| \geq 2\|x\|$.

(c) Montrer que

$$\sum_{a=1}^{p-1} \frac{1}{\|a/p\|} \leq 2p(1 + \log p).$$

(d) Considérons l'espace vectoriel des fonctions p -périodiques $f : \mathbb{Z} \rightarrow \mathbb{C}$ muni du produit scalaire défini par

$$(f.g) = \frac{1}{p} \sum_{n=0}^{p-1} f(n) \overline{g(n)}.$$

Montrer que les fonctions $\psi_0, \dots, \psi_{p-1}$ forment une base orthonormée de cet espace. Pour un caractère de Dirichlet non principal χ , montrer que

$$|(\chi, \psi_a)| = \begin{cases} 0 & \text{si } p \mid a, \\ \frac{1}{\sqrt{p}} & \text{si } p \nmid a. \end{cases}$$

(e) En déduire que

$$\left| \sum_{A \leq n \leq B} \chi(n) \right| \leq \frac{1}{\sqrt{p}} \sum_{a=1}^{p-1} \left| \sum_{A \leq n \leq B} \psi_a(n) \right|.$$

Conclure.