UNIVERSITÉ GRENOBLE-ALPES Prépa Agreg

Enseignant : Rémi Molinier remi.molinier@univ-grenoble-alpes.fr

Les carrés de $\mathbb{F}_q$ et le symbole de Legendre

L'étude des carrés dans $\mathbb{F}_q$ est un classique de l'agrégation. En particulier la Loi de réciprocité quadratique est un développement classique. De bonnes références sur le sujet sont [Ser70, Per81].

Soit p un nombre premier et soit $q = p^\alpha$ une puissance de p.

1 L'ensemble des carrés de $\mathbb{F}_q$

On note $\mathbb{F}_q^2$ l'ensemble des carrés de $\mathbb{F}_q$ et $\mathbb{F}_q^{*2}$ l'ensemble des carrés non nul.

Exercice 1 – L'ensemble des carrés de $\mathbb{F}_q$

1) Montrer que si $p = 2$ alors tout élément de $\mathbb{F}_q$ est un carré.

2) Montrer que si $p \neq 2$ alors les carrés de $\mathbb{F}_q^*$ forment un sous-groupe d'indice 2 de $\mathbb{F}_q^*$. [1].

3) Montrer que $\mathbb{F}_q^{*2}$ est l'ensemble des racines de $X^{(q-1)/2} - 1$ dans $\mathbb{F}_q$.

4) En déduire que dans $\mathbb{F}_q$, si $x \in \mathbb{F}_q$ et $y \in \mathbb{F}_q$ ne sont pas des carrés alors, xy est un carré de $\mathbb{F}_q$ [2].

Exercice 2 – Application à la classification des formes quadratiques sur $\mathbb{F}_q$

Supposons que $p \neq 2$.

Soit $Q \colon \mathbb{F}_q^2 \to \mathbb{F}_q$ une forme quadratique non dégénérée.

1) Montrer qu'il existe une base de $\mathbb{F}_q^2$ dans laquelle Q prend la forme $Q(x, y) = ax^2 + by^2$ avec $a, b \in \mathbb{F}_q$.

2) Montrer que Q est surjective.

3) Montrer qu'il existe une base de $\mathbb{F}_q^2$ dans laquelle Q prend l'un des deux formes suivantes :

(a) $Q(x, y) = x^2 + y^2$, ou

(b) $Q(x, y) = x^2 + \lambda y^2$ avec $\lambda \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{*2}$.

4) Généraliser ce dernier résultat aux formes quadratiques non-dégénérées sur $\mathbb{F}_q^n$.

2 Symbole de Legendre

On suppose maintenant que p est un nombre premier impair.

Définition 1. Soit $a \in \mathbb{Z}$.

Le *symbole de Legendre* de a modulo p est l'entier

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \mid a, \\ 1 & \text{si } p \nmid a \text{ et } a \text{ est un carré modulo } p, \\ -1 & \text{sinon.} \end{cases}$$

On dit que a est un *résidu quadratique modulo* p si $\left(\frac{a}{p}\right) = 0$ ou 1.

1. Indice : on pourra considérer l'application $x \mapsto x^2$.
2. Indice : on pourra considérer l'application $x \mapsto x^{(q-1)/2}$.

Remarque. $\left(\frac{a}{p}\right)$ ne dépend que de la classe de a modulo p. Ainsi, on s'autorisera à utiliser ce symbole pour $a \in \mathbb{F}_p$.

Exercice 3 – Propriétés élémentaires du symbole de Legendre
Soit $a, b \in \mathbb{Z}$.

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

2) Montrer que $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

Exercice 4 – Premiers calculs

1) Monter que $\left(\frac{1}{p}\right) = 1$.

2) Montrer que $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

Calcul de $\left(\frac{2}{p}\right)$:

3) Montrer que $8 \mid p^2 - 1$.

4) Montrer qu'il existe $\zeta \in \mathbb{F}_{p^2}$ tel que $\zeta^8 = 1$ et $\zeta^4 \neq 1$.

5) Vérifier que $y = \zeta + \zeta^{-1}$ est une racine de 2 dans $\mathbb{F}_{p^2}$. [3]

6) Montrer que si $p \equiv \pm 1 \pmod{8}$ alors $y^p = y$ et que si $p \equiv \pm 5 \pmod{8}$ alors $y^p = -y$.

7) En déduire que $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

3 La loi de réciprocité quadratique

Ici nous voulons démontrer le résultat suivant.

Théorème 1 (Loi de réciprocité quadratique)**.** *Soit p et l deux nombres premiers impairs distincts. On a l'égalité*

$$\left(\frac{p}{l}\right)\left(\frac{l}{p}\right) = (-1)^{\frac{(p-1)(l-1)}{4}}.$$

Il existe plusieurs preuves de ce résultat et celles-ci donnent des développements possibles pour l'oral de l'agrégation (en particulier, beaucoup sont disponibles en ligne et bien détaillées). Nous présentons ici une preuve classique que l'on peut retrouver dans [Ser70].

Soient p et l deux nombres premiers impairs distincts. Soit $\mathbb{F}$ un corps de décomposition de $X^l - 1 \in \mathbb{F}_p[X]$. En particulier $\mathbb{F}$ contient les racines $l^{\text{ième}}$ de l'unité et on fixe ω une racine primitive $l^{\text{ième}}$ de l'unité.

Comme $\omega^n = \omega^m$ si et seulement si $n \equiv m \pmod{l}$, pour $x \in \mathbb{F}_l$ donné, on écrira ω^x à la place de ω^n losque $\overline{n} = x$ dans $\mathbb{F}_l$.

On considère alors la *somme de Gauss*

$$S = \sum_{x \in \mathbb{F}_l} \left(\frac{x}{l}\right) \omega^x.$$

3. Indice : $0 = \zeta^{-2} + \zeta^2$ et que $\zeta^4 = -1$ on pourra vérifier que.

Exercice 5 – Un premier lemme

1) Montrer que

$$S^2 = \sum_{u \in \mathbb{F}_l} \omega^u \left(\sum_{t \in \mathbb{F}_l} \left(\frac{t(u-t)}{l} \right) \right).$$

2) Montrer que si $t \neq 0$, alors

$$\left(\frac{t(u-t)}{l} \right) = -1^{(l-1)/2} \left(\frac{1-ut^{-1}}{l} \right).$$

3) Montrer que

$$\sum_{t \in \mathbb{F}_l^*} \left(\frac{1-ut^{-1}}{l} \right) = \begin{cases} l-1 & \text{si } u = 0, \\ -1 & \text{si } u \neq 0. \end{cases}$$

4) En déduire que $S^2 = (-1)^{(l-1)/2} l$ (en notant, par abus de notation, l l'image de l dans $\mathbb{F}_p$).

Exercice 6 – Un deuxième lemme

1) Montrer que $S^p = \sum_{x \in \mathbb{F}_l} \left(\frac{x}{l} \right) \omega^{xp}$.

2) En déduire que $S^p = \left(\frac{p}{l} \right) S$. [4]

Exercice 7 – Conclusion
En calculant $\left(\frac{S^2}{p} \right)$ de deux façons différentes démontrer le Théorème 1.

4 Exemples de calculs et applications

Exercice 8
Calculer les symboles de Legendre suivants.

1) $\left(\frac{-1}{17} \right)$.

2) $\left(\frac{2}{29} \right)$.

3) $\left(\frac{13}{17} \right)$.

4) $\left(\frac{7}{19} \right)$.

5) $\left(\frac{38}{71} \right)$.

6) $\left(\frac{-8}{23} \right)$.

Exercice 9
Pour quel nombre premier p le nombre 3 est-il un résidu quadratique modulo p ?

Exercice 10
Montrer qu'il existe une infinité de nombres premiers congrus à 1 modulo 4. [5]

4. Indice : on pourra de nouveau faire un changement de variable dans l'égalité précédente.
5. Indice : on pourra considérer un facteur premier de $(n!)^2 + 1$.

L'exercice suivant est un autre développement possible. Il est tiré de [BMP05, Exercice 5.4].

Exercice 11 – Théorème de Frobenius-Zolotarev

1) soient k un corps et M un groupe abélien. Montrer que si $k \neq \mathbb{F}_2$ ou $n \neq 2$ alors tout morphisme de groupe $f\colon \mathrm{GL}_n(k) \to M$ se factorise de façon unique à travers le determinant, i.e. il existe un unique morphisme $\delta\colon k^* \to M$ tel que $f = \delta \circ \det$. [6]

2) Soit p un nombre premier impair. Montrer que le symbole de Legendre est l'unique morphisme non trivial de $\mathbb{F}_p^*$ dans $\{\pm 1\}$.

3) En déduire le théorème de Frobenius-Zolotarev : soit p un nombre premier impair et V un $\mathbb{F}_p$-espace vectoriel de dimension fini, alors pour tout $u \in \mathrm{GL}(V)$,

$$\epsilon(u) = \left(\frac{\det(u)}{p}\right)$$

où ϵ est la signature de u vu comme un permutation de l'ensemble fini V. [7]

4) *Application :* pour p impair, la signature de l'automorphisme de Frobenius $F\colon x \mapsto x^p$ sur $\mathbb{F}_p^n$, est

$$\epsilon(F) = (-1)^{\frac{(p-1)(n-1)}{2}}.$$

5 Calcul des racines carrés dans $\mathbb{F}_q$

L'exercice suivant est un résultat classique à connaitre.

Exercice 12 – Tout sous-groupe du groupe multiplicatif d'un corps est cyclique
Soit k un corps (fini ou infini) et soit G un sous-groupe fini de k^*. On note n le cardinal de G.

1) Montrer que $n = \sum_{d|n} \varphi(d)$ (où φ est l'indicatrice d'Euler).

2) Montre que si x est d'ordre d alors $< x >$ est l'ensemble des racine de $X^d - 1$.

Pour $d \mid n$, on note A_d l'ensemble des éléments d'ordre d de G et a_d le cardinal de A_d.

3) Montrer que $n = \sum_{d|n} a_d$.

4) On suppose $A_d \neq \emptyset$ et on fixe $x \in A_d$. Montrer que $A_d \subseteq < x >$.

5) En déduire que $a_d = 0$ ou $a_d = \varphi(d)$.

6) En conclure que G est cyclique.

Exercice 13 – Un décomposition utile de $\mathbb{F}_q^*$
Soit q un nombre premier impair.
Montrer que, en tant que groupe, $\mathbb{F}_q^* \cong G_1 \times G_2$ avec G_1 un 2-groupe cyclique et G_2 un groupe cyclique d'ordre impair. On prendra soin d'expliciter un isomorphisme.

Exercice 14 – Calcul de racine carrée dans un groupe d'ordre impair
Soit G un groupe fini d'ordre n impair. Montrer que tout élément x de G est un carré et donner la racine carrée de x dans G.

6. Indice : on pourra utiliser le fait que, sous les hypothèses de la question, $\mathrm{D}(\mathrm{GL}_n(k)) = \mathrm{SL}_n(k)$ (voir [Per81, Théorème IV.3.1]).
7. Indice : on pourra considérer l'endomorphisme donné par la multiplication par un générateur de $\mathbb{F}_{p^n}$.

Il ne reste donc plus qu'à étudier les racines carrées dans un 2-groupe cyclique.

Exercice 15 – Carrés et racines carrées dans un 2-groupe cyclique
Soit G un 2-groupe cyclique et soient $x, y \in G$.

1) Montrer que si x et y ont le même ordre, alors xy est d'ordre strictement plus petit.

2) Montrer que les carrés de G sont exactement les éléments d'ordre strictement inférieur à l'ordre de G.

Notons 2^α l'ordre de G et soit g un générateur de G. On fixe $x \in G$ qui est un carré et soit $\beta \in \{0, 1, \dots, 2^\alpha - 1\}$ tel que $x = g^\beta$. Comme x est un carré, β est pair et $g^\beta/2$ est une racine carré de x. Ainsi, pour determiner une racine carré de x il nous faut déterminer β.
Écrivons $\beta = \beta_0 + 2\beta_1 + 4\beta_2 + \cdots + \beta_{\alpha-1}2^{\alpha-1}$ en base 2.

3) Montrer que, si i est le plus petit entier tel que $\beta_i \neq 0$ alors x est d'ordre $2^{\alpha-i}$.

4) En déduire un algorithme pour déterminer β.

En pratique, la dernière difficulté est de trouver le générateur du 2-Sylow de $\mathbb{F}_q^*$. Pour cela, on peut tirer au hasard des éléments de $\mathbb{F}_q^*$ jusqu'à tomber sur un élément qui n'est pas un carré. En effet, si $q - 1 = 2^\alpha r$ avec r impair et si $x \in \mathbb{F}_q^*$ n'est pas un carré, alors x^r non plus et est d'ordre une une puissance de 2, c'est donc un générateur du 2-Sylow de $\mathbb{F}_q$.

Références

[BMP05] Vincent Beck, Jerôme Malick, and Gabriel Peyré. *Objectif agrégation.* H&K, 2005.

[Per81] Daniel Perrin. *Cours d'algèbre.* Ecole Normale Supérieure de jeunes filles, 1981.

[Ser70] Jean-Pierre Serre. *Cours d'arithmétique.* Presses Universitaires de France, 1970.