

Lemme de Zolotarev et réciprocity quadratique

Merci d'indiquer sur la première page de votre copie le temps passé sur le devoir.

Étant donné un élément a d'un groupe G , on dira que a est un **carré** ssi il existe un élément $x \in G$ tel que $a = x^2$. Dans la suite, on considérera particulièrement le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$ pour un nombre premier p . On note alors

$$K_p = \{x^2, x \in (\mathbb{Z}/p\mathbb{Z})^\times\}$$

l'ensemble des carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$.

On définit le symbole de Legendre pour $a \in \mathbb{Z}/p\mathbb{Z}$ par

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a = 0 \\ 1 & \text{si } a \in K_p \\ -1 & \text{si } a \in (\mathbb{Z}/p\mathbb{Z})^\times \setminus K_p \end{cases}$$

Plus généralement, étant donné $a \in \mathbb{Z}$ premier avec p , on dit que a est un carré modulo p ssi $[a]_p$ est un carré dans $(\mathbb{Z}/p\mathbb{Z})^\times$, ce qui revient donc à l'existence de $b \in \mathbb{Z}$ premier avec p tel que $a \equiv b^2 \pmod{p}$.

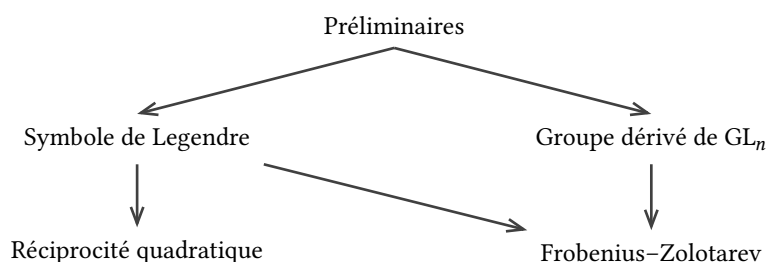
On définit de même pour $a \in \mathbb{Z}$ et p un nombre premier le symbole de Legendre

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \text{ divise } a \\ 1 & \text{si } p \text{ ne divise pas } a \text{ et } a \text{ est un carré modulo } p \\ -1 & \text{si } p \text{ ne divise pas } a \text{ et } a \text{ n'est pas un carré modulo } p. \end{cases}$$

L'objectif de ce sujet est d'étudier le lien entre symbole de Legendre et signature des applications affines sur $\mathbb{Z}/p\mathbb{Z}$, ainsi que de démontrer la célèbre **loi de réciprocity quadratique**, pour p, q premiers impairs distincts

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

Le graphe de dépendance des parties est le suivant :



A. Préliminaires

On pourra aussi utiliser les résultats suivants dans tout le sujet :

- pour tout nombre premier p , le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique,
- pour K un corps et $n \geq 2$ un entier, toute matrice de $SL_n(K)$ est un produit de transvections élémentaires, c'est-à-dire de matrices de la forme $I_n + \lambda E_{i,j}$ avec $\lambda \in K$ et $i \neq j$.

Les questions suivantes sont indépendantes entre elles et pourront être utilisées dans tout le sujet.

Q1. Soient G, H des groupes, G fini et $\varphi : G \rightarrow H$ un morphisme de groupes.

Montrer que

$$|\text{Im}(\varphi)| \times |\text{Ker}(\varphi)| = |G|.$$

Q2. Soit G un groupe fini et H un sous-groupe de G .

On suppose

$$\frac{|G|}{|H|} = 2.$$

Soit $\alpha \in G \setminus H$.

Montrer que $(H, \alpha H)$ est une partition de G .

Q3. Soit $(E, \leq)$ un ensemble fini totalement ordonné et $\sigma \in S(E)$.

On note

$$d_\sigma = |\{(x, y) \in E^2 \mid x < y \text{ et } \sigma(x) > \sigma(y)\}|.$$

Montrer que

$$\varepsilon(\sigma) = (-1)^{d_\sigma}.$$

B. Propriétés du symbole de Legendre

Q4. Soit $a \in \mathbb{Z}$. Que dire de $\left(\frac{a}{2}\right)$?

Dans la suite, on fixe p un nombre premier **impair**.

Q5. Montrer que K_p est un sous-groupe de $(\mathbb{Z}/p\mathbb{Z})^\times$ et que

$$|K_p| = \frac{p-1}{2}$$

Q6. En déduire que

$$K_p = \left\{ a \in (\mathbb{Z}/p\mathbb{Z})^\times \mid a^{\frac{p-1}{2}} - 1 = 0 \right\}.$$

Q7. En déduire que pour tout $a \in \mathbb{Z}$,

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

Q8. Montrer que

$$\left(\frac{\cdot}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow \{-1, +1\}$$

$$a \mapsto \left(\frac{a}{p}\right)$$

est un morphisme de groupes.

Q9. Soit

$$\psi : (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow \{-1, +1\}$$

$$a \mapsto \psi(a)$$

un morphisme de groupes.

Montrer que $\psi = 1$ (l'application constante égale à 1) ou $\psi = \left(\frac{\cdot}{p}\right)$.

Remarque : $\left(\frac{\cdot}{p}\right)$ est donc l'unique morphisme non trivial de $(\mathbb{Z}/p\mathbb{Z})^\times$ vers $\{1, -1\}$.

Pour $(a, b) \in (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/p\mathbb{Z}$ on note

$$f_{a,b} : \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$$

$$x \mapsto ax + b$$

et on note

$$\text{GA}_1(\mathbb{Z}/p\mathbb{Z}) = \{f_{a,b}, (a, b) \in (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/p\mathbb{Z}\}.$$

Q10. Montrer que $\text{GA}_1(\mathbb{Z}/p\mathbb{Z})$ est un sous-groupe de $S(\mathbb{Z}/p\mathbb{Z})$.

Q11. À l'aide des questions précédentes démontrer le **lemme de Zolotarev** : pour tout $(a, b) \in (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/p\mathbb{Z}$,

$$\varepsilon(f_{a,b}) = \left(\frac{a}{p}\right).$$

C. Groupe dérivé de GL_n

Étant donné un groupe G , on définit le **groupe dérivé** de G par

$$D(G) = \langle \{xyx^{-1}y^{-1}, (x, y) \in G^2\} \rangle$$

c'est-à-dire le sous-groupe de G engendré par les **commutateurs** (éléments de la forme $xyx^{-1}y^{-1}$) de G .

Q12. On pose dans cette question

$$G = \left\{ \begin{pmatrix} I_3 & C & A \\ 0 & I_1 & L \\ 0 & 0 & I_3 \end{pmatrix}, (A, C, L) \in M_{3,3}(\mathbb{R}) \times M_{3,1}(\mathbb{R}) \times M_{1,3}(\mathbb{R}) \right\} \subset \text{GL}_7(\mathbb{R}).$$

Montrer que G est un groupe et que

$$\{xyx^{-1}y^{-1}, (x, y) \in G^2\} \neq D(G).$$

Q13. Soient G, H des groupes et $\varphi : G \rightarrow H$ un morphisme de groupes.

Montrer que $\varphi(D(G)) = D(\varphi(G))$.

En déduire en particulier que $D(G)$ est stable par conjugaison (c'est-à-dire que pour tout $g \in G$ et tout $x \in D(G)$ on a $gxg^{-1} \in D(G)$).

Q14. Soient G, H des groupes et $\varphi : G \rightarrow H$ un morphisme de groupes.

Montrer que $\text{Im}(\varphi)$ est abélien ssi $D(G) \subset \text{Ker}(\varphi)$.

On fixe dans la suite un corps $\mathbb{K}$ possédant au moins trois éléments et un entier $n \geq 2$, et on cherche à déterminer $D(\text{GL}_n(\mathbb{K}))$.

Q15. Montrer que $D(\text{GL}_n(\mathbb{K})) \subset \text{SL}_n(\mathbb{K})$.

Q16. Soient $i, j \in \llbracket 1, n \rrbracket$ tels que $i \neq j$, $\lambda \in \mathbb{K}$ et $d_1, \dots, d_n \in \mathbb{K}^\times$.

On pose $D = \text{diag}(d_1, \dots, d_n)$ et $T = I_n + \lambda E_{i,j}$.

Calculer le commutateur

$$D T D^{-1} T^{-1}.$$

Q17. Conclure que

$$\text{SL}_n(\mathbb{K}) = D(\text{GL}_n(\mathbb{K})).$$

Q18. Pour $a \in \mathbb{K}^\times$ on pose

$$\Delta_a = \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \quad \text{et} \quad \mathcal{D} = \{\Delta_a, a \in \mathbb{K}^\times\}.$$

Montrer que $\mathcal{D}$ est un sous-groupe de $GL_n(\mathbb{K})$ et que pour tout $A \in GL_n(\mathbb{K})$ il existe un unique couple $(\Delta, S) \in \mathcal{D} \times SL_n(\mathbb{K})$ tel que $A = \Delta S$.

Q19. Soit H un groupe **abélien** et

$$\varphi : GL_n(\mathbb{K}) \rightarrow H$$

un morphisme de groupes.
Montrer qu’il existe

$$\psi : \mathbb{K}^\times \rightarrow H$$

un morphisme de groupes tel que

$$\varphi = \psi \circ \det.$$

D. Loi de réciprocité quadratique

Soient p, q deux nombres premiers impairs **distincts**. On cherche à démontrer, dans cette partie, le résultat suivant, appelé **loi de réciprocité quadratique** :

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

On note $N = pq$ et on considère la **grille**

$$E = \llbracket 0, p-1 \rrbracket \times \llbracket 0, q-1 \rrbracket,$$

à p lignes et q colonnes ; pour $(i, j) \in E$, on note

$$L_i = \{i\} \times \llbracket 0, q-1 \rrbracket \quad \text{et} \quad C_j = \llbracket 0, p-1 \rrbracket \times \{j\}$$

la ligne i et la colonne j de la grille, ainsi $L_i \cap C_j = \{(i, j)\}$.

On appelle **numérotation** de E toute bijection de E vers $\llbracket 0, N-1 \rrbracket$.

Pour $(i, j) \in E$, on pose dans la suite

$$\ell(i, j) = qi + j,$$

$$c(i, j) = i + pj,$$

et

$$\theta(i, j) = \text{l'unique élément de } \llbracket 0, N-1 \rrbracket \text{ tel que } \begin{cases} \theta(i, j) \equiv i \pmod{p} \\ \theta(i, j) \equiv j \pmod{q} \end{cases}$$

Q20. Montrer que ℓ, c et θ sont des numérotations de E .

Q21. Pour $p = 5$ et $q = 7$, on a tracé ci-dessous les numérotations ℓ, c et θ , sans préciser laquelle est laquelle.

$i \setminus j$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	7	8	9	10	11	12	13
2	14	15	16	17	18	19	20
3	21	22	23	24	25	26	27
4	28	29	30	31	32	33	34

(I)

$i \setminus j$	0	1	2	3	4	5	6
0	0	5	10	15	20	25	30
1	1	6	11	16	21	26	31
2	2	7	12	17	22	27	32
3	3	8	13	18	23	28	33
4	4	9	14	19	24	29	34

(II)

$i \setminus j$	0	1	2	3	4	5	6
0	0	15	30	10	25	5	20
1	21	1	16	31	11	26	6
2	7	22	2	17	32	12	27
3	28	8	23	3	18	33	13
4	14	29	9	24	4	19	34

(III)

Associer (*sans justification*) à chacun des schémas (I), (II) et (III) celle des trois numérotations ℓ, c et θ qui le définit.
Tracer (*sans justification*) les trois numérotations correspondantes pour $p = 3$ et $q = 5$.

Q22. Montrer que pour tout $i \in \llbracket 0, p-1 \rrbracket$,

$$(\theta^{-1} \circ c)(L_i) = L_i$$

et exprimer la permutation induite par $\theta^{-1} \circ c$ sur L_i .

Q23. Montrer que

$$\varepsilon(\theta^{-1} \circ c) = \left(\frac{p}{q}\right).$$

On admet qu’exactement le même raisonnement donne

$$\varepsilon(\theta^{-1} \circ \ell) = \left(\frac{q}{p}\right).$$

Q24. Montrer que

$$\varepsilon(\ell^{-1} \circ c) = (-1)^{\frac{p-1}{2} \times \frac{q-1}{2}}.$$

Q25. En déduire la **loi de réciprocité quadratique** :

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

E. Frobenius-Zolotarev

Dans cette partie, on fixe un entier $n \geq 2$ et un nombre premier impair p . On cherche à généraliser la question **Q11** à $\text{GA}_n(\mathbb{Z}/p\mathbb{Z})$. Étant donnés $A \in \text{GL}_n(\mathbb{Z}/p\mathbb{Z})$ et $B \in (\mathbb{Z}/p\mathbb{Z})^n$, on note

$$f_{A,B} : (\mathbb{Z}/p\mathbb{Z})^n \rightarrow (\mathbb{Z}/p\mathbb{Z})^n$$

$$X \mapsto AX + B$$

et on note

$$\text{GA}_n(\mathbb{Z}/p\mathbb{Z}) = \{f_{A,B}, (A, B) \in \text{GL}_n(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})^n\}.$$

De même qu'à la question **Q10**, on montre que $\text{GA}_n(\mathbb{Z}/p\mathbb{Z})$ est un sous-groupe de $S((\mathbb{Z}/p\mathbb{Z})^n)$ (il n'est pas demandé de le démontrer).

Q26. Montrer que pour tout $B \in (\mathbb{Z}/p\mathbb{Z})^n$,

$$\varepsilon(f_{I_n, B}) = 1.$$

Q27. Soient ζ un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$ et $\Delta_\zeta = \text{diag}(\zeta, 1, \dots, 1) \in \text{GL}_n(\mathbb{Z}/p\mathbb{Z})$. Montrer que

$$\varepsilon(f_{\Delta_\zeta, 0}) = -1.$$

Q28. Conclure que

$$\forall (A, B) \in \text{GL}_n(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})^n, \quad \varepsilon(f_{A,B}) = \left(\frac{\det(A)}{p} \right).$$