Lemme de Zolotarev et réciprocité quadratique

A. Préliminaires

Q1. *Pour tous $x_1, x_2 \in \mathrm{G}$, on a $\varphi(x_1) = \varphi(x_2)$ ssi $\varphi\left((x_2)^{-1}x_1\right) = e_{\mathrm{H}}$, c'est-à-dire ssi $(x_2)^{-1}x_1 \in \mathrm{Ker}(\varphi)$, c'est-à-dire ssi $x_1 \in x_2\,\mathrm{Ker}(\varphi)$.*
Ainsi pour $y \in \mathrm{Im}(\varphi)$, avec x_p une «solution particulière» de l'équation $\varphi(x) = y$, on a

$$\varphi^{-1}(\{y\}) = x_p\,\mathrm{Ker}(\varphi)$$

en particulier comme

$$\mathrm{Ker}(\varphi) \to x_p\,\mathrm{Ker}(\varphi)$$

$$k \mapsto x_p k$$

est bijective (de réciproque $x \mapsto x_p^{-1}x$), on a

$$\forall y \in \mathrm{Im}(\varphi), \left|\varphi^{-1}(\{y\})\right| = |\mathrm{Ker}(\varphi)|.$$

Et comme on a

$$\mathrm{G} = \bigsqcup_{y\in\mathrm{Im}(\varphi)} \varphi^{-1}(\{y\})$$

on en déduit (principe des bergers)

$$|\mathrm{G}| = \sum_{y\in\mathrm{Im}(\varphi)} \left|\varphi^{-1}(\{y\})\right|$$

et donc finalement

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

Q2. ▸ *Supposons par l'absurde que $\mathrm{H} \cap \alpha\mathrm{H} \neq \emptyset$.*
Soit $x \in \mathrm{H} \cap \alpha\mathrm{H}$. Alors il existe $h \in \mathrm{H}$ tel que $x = \alpha h$, et donc $\alpha = xh^{-1} \in \mathrm{H}$, ce qui est absurde.
Donc $\mathrm{H} \cap \alpha\mathrm{H} = \emptyset$.
▸ *On a l'application*

$$\mathrm{H} \to \alpha\mathrm{H}$$

$$h \mapsto \alpha h$$

est bien définie et bijective (de réciproque $y \mapsto \alpha^{-1}y$), et donc $|\alpha\mathrm{H}| = |\mathrm{H}|$.
▸ *Comme de plus $|\mathrm{H}| = \frac{|\mathrm{G}|}{2}$, par cardinalité on en déduit que*

$$\boxed{\mathrm{G} = \mathrm{H} \cup \alpha\mathrm{H}}$$

Q3. *Il y a plusieurs façons de procéder (par exemple en utilisant le fait que les transpositions de la forme $(k\ k+1)$ génèrent S_n).*
Proposons une démonstration reposant sur les déterminants de Vandermonde.
Si $|\mathrm{E}| \leq 1$, le résultat est immédiat. Sinon, posons $n = |\mathrm{E}|$ et soit $u : [\![1,n]\!] \to \mathrm{E}$ la bijection croissante. La permutation $\tau = u^{-1} \circ \sigma \circ u$ a les mêmes longueurs de cycles que σ, donc $\varepsilon(\tau) = \varepsilon(\sigma)$. Comme u est croissante, $(i,j) \mapsto (u(i), u(j))$ met en bijection leurs ensembles d'inversions, donc $d_\tau = d_\sigma$. Quitte à conjuguer par u, on peut donc supposer $\mathrm{E} = [\![1,n]\!]$, muni de l'ordre usuel.
On travaille désormais avec $\sigma \in \mathrm{S}_n$. Choisissons des complexes distincts $x_1, \ldots, x_n$, qui serviront à calculer sa signature au moyen d'un déterminant de Vandermonde.
On sait que

$$\mathrm{V}(x_1, \ldots, x_n) = \det\left(\begin{pmatrix} 1 & x_1 & \cdots & x_1^{n-1} \\ 1 & x_2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & x_n & \ldots & x_n^{n-1} \end{pmatrix}\right) = \prod_{1\leq i<j\leq n} (x_j - x_i).$$

En effectuant la permutation σ sur les lignes, on obtient

$$\mathrm{V}\left(x_{\sigma(1)}, \ldots, x_{\sigma(n)}\right) = \varepsilon(\sigma)\mathrm{V}(x_1, \ldots, x_n) = \varepsilon(\sigma) \prod_{1\leq i<j\leq n} (x_j - x_i).$$

et, toujours par le déterminant de Vandermonde,

$$\mathrm{V}\left(x_{\sigma(1)}, \ldots, x_{\sigma(n)}\right) = \prod_{1\leq i<j\leq n} \left(x_{\sigma(j)} - x_{\sigma(i)}\right).$$

D'où finalement (le déterminant est non nul)

$$\varepsilon(\sigma) = \frac{\prod_{1\leq i<j\leq n}\left(x_{\sigma(j)} - x_{\sigma(i)}\right)}{\prod_{1\leq i<j\leq n}\left(x_j - x_i\right)}.$$

Les termes du numérateur et du dénominateur sont les mêmes au signe près, et le nombre de termes du numérateur qui sont de signe opposé à ceux du dénominateur est exactement le nombre d'inversions d_σ.
D'où

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

B. Propriétés du symbole de Legendre

Q4. *Tous les éléments non nuls de $\mathbb{Z}/2\mathbb{Z}$ sont des carrés (car $1^2 = 1$) et par conséquent*

$$\boxed{\left(\frac{a}{2}\right) = \begin{cases} 0 \text{ si } a \text{ pair} \\ 1 \text{ sinon.} \end{cases}}$$

Q5. *Considérons*

$$\gamma : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$$
$$x \mapsto x^2.$$

C'est une application ***bien définie****, un* ***morphisme de groupes*** *(car pour tous $x, y \in (\mathbb{Z}/p\mathbb{Z})^\times$, par commutativité, $(xy)^2 = x^2y^2$) et on a*

$$\mathrm{K}_p = \mathrm{Im}(\gamma)$$

d'où

$$\mathrm{K}_p \text{ est un sous-groupe de } (\mathbb{Z}/p\mathbb{Z})^\times.$$

De plus

$$\mathrm{Ker}(\gamma) = \left\{x \in (\mathbb{Z}/p\mathbb{Z})^\times \mid x^2 = 1\right\}.$$

Or comme $\mathbb{Z}/p\mathbb{Z}$ est un ***corps****, on a pour tout $x \in \mathbb{Z}/p\mathbb{Z}$,*

$$x^2 - 1 = 0 \iff x = 1 \text{ ou } x = -1.$$

Comme $1 \neq -1$ on en déduit que

$$\mathrm{Ker}(\gamma) = \{1, -1\} \text{ et } |\mathrm{Ker}(\gamma)| = 2.$$

De plus comme $\mathbb{Z}/p\mathbb{Z}$ est un corps on a

$$(\mathbb{Z}/p\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\} \text{ d'où } \left|(\mathbb{Z}/p\mathbb{Z})^\times\right| = p - 1.$$

Par la question ***Q1*** *on en déduit*

$$\boxed{\left|\mathrm{K}_p\right| = \frac{p-1}{2}.}$$

Q6. *Procédons par inclusion et inégalité des cardinaux.*
Notons

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

- ***Inclusion*** $\mathrm{K}_p \subset \mathrm{R}_p$
  Soit $a \in \mathrm{K}_p$. Alors il existe $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $a = x^2$. On a donc, par le petit théorème de Fermat,

$$\begin{aligned} a^{\frac{p-1}{2}} - 1 &= \left(x^2\right)^{\frac{p-1}{2}} - 1 \\ &= x^{p-1} - 1 \\ &= 0 \end{aligned}$$

  et donc

$$\mathrm{K}_p \subset \mathrm{R}_p.$$

- ***Inégalité de cardinaux*** $\left|\mathrm{K}_p\right| \geq \left|\mathrm{R}_p\right|$
  On a R_p est l'ensemble des racines du polynôme de degré $\frac{p-1}{2}$

$$\mathrm{X}^{\frac{p-1}{2}} - 1 \in (\mathbb{Z}/p\mathbb{Z})[\mathrm{X}].$$

  Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, ce polynôme a au plus $\frac{p-1}{2}$ racines dans $\mathbb{Z}/p\mathbb{Z}$ et donc

$$\left|\mathrm{R}_p\right| \leq \frac{p-1}{2}.$$

  Par la question ***Q5*** *on a donc*

$$\left|\mathrm{K}_p\right| \geq \left|\mathrm{R}_p\right|.$$

- ***Conclusion***
  Par inclusion et inégalité des cardinaux on en déduit que

$$\mathrm{K}_p = \mathrm{R}_p$$

  c'est-à-dire

$$\boxed{\mathrm{K}_p = \left\{a \in (\mathbb{Z}/p\mathbb{Z})^\times \mid a^{\frac{p-1}{2}} - 1 = 0\right\}}$$

Q7. *Soit $a \in \mathbb{Z}$. Si p divise a, les deux membres sont congrus à 0 modulo p.*
Sinon, posons $x = [a]_p \in (\mathbb{Z}/p\mathbb{Z})^\times$. Par le petit théorème de Fermat on a

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

Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, on en déduit que $x^{\frac{p-1}{2}} \in \{1, -1\}$. Par la question ***Q6****, cette puissance vaut 1 ssi $x \in \mathrm{K}_p$, et vaut donc -1 sinon.*
On a ainsi dans tous les cas

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

Q8. *Pour tout $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, la question* ***Q7****, appliquée à un représentant entier de a, donne l'égalité*

$$\left[\left(\frac{a}{p}\right)\right]_p = a^{\frac{p-1}{2}}$$

dans $\mathbb{Z}/p\mathbb{Z}$, et comme $(\mathbb{Z}/p\mathbb{Z})^\times$ est commutatif,

$$(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$$
$$a \mapsto a^{\frac{p-1}{2}}$$

est un morphisme de groupes.
Comme p est impair on a $[1]_p \neq [-1]_p$, et $x \mapsto [x]_p$ réalise un isomorphisme de $\{1,-1\}$ sur le sous-groupe $\{[1]_p, [-1]_p\}$ de $(\mathbb{Z}/p\mathbb{Z})^\times$, qui contient l'image du morphisme ci-dessus. On en déduit que

$$\boxed{\left(\frac{\cdot}{p}\right) \text{ est un morphisme de groupes.}}$$

Q9. *Soit $\alpha \in (\mathbb{Z}/p\mathbb{Z})^\times \setminus \mathrm{K}_p$.*
*Comme $\left|(\mathbb{Z}/p\mathbb{Z})^\times\right| / \left|\mathrm{K}_p\right| = 2$ par la question **Q5**, la question **Q2** donne que $\left(\mathrm{K}_p, \alpha\mathrm{K}_p\right)$ est une partition de $(\mathbb{Z}/p\mathbb{Z})^\times$.*
Tout d'abord pour tout $a \in \mathrm{K}_p$ avec $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $a = x^2$, on a

$$\psi(a) = \psi\left(x^2\right) = \psi(x)^2 = 1$$

et donc ψ est constante égale à 1 sur K_p.
Ensuite, par disjonction de cas

- ***si** $\psi(\alpha) = 1$, alors pour tout $b \in \alpha\mathrm{K}_p$ on a*

$$\psi(b) = \psi\left(\alpha\left(\alpha^{-1}b\right)\right) = \psi(\alpha) \times \psi\left(\underbrace{\alpha^{-1}b}_{\in \mathrm{K}_p}\right) = 1 \times 1 = 1$$

et donc

$$\psi = 1.$$

- ***si** $\psi(\alpha) = -1$, alors pour tout $b \in \alpha\mathrm{K}_p$ on a*

$$\psi(b) = \psi\left(\alpha\left(\alpha^{-1}b\right)\right) = \psi(\alpha) \times \psi\left(\underbrace{\alpha^{-1}b}_{\in \mathrm{K}_p}\right) = -1 \times 1 = -1$$

et comme $\left(\frac{\cdot}{p}\right)$ vaut 1 sur K_p et -1 sur $\alpha\mathrm{K}_p$ (le complémentaire de K_p dans $(\mathbb{Z}/p\mathbb{Z})^\times$), on en déduit que

$$\boxed{\psi = \left(\frac{\cdot}{p}\right).}$$

Q10. *Soient $a_1, a_2 \in (\mathbb{Z}/p\mathbb{Z})^\times$ et $b_1, b_2 \in \mathbb{Z}/p\mathbb{Z}$. Alors pour tout $x \in \mathbb{Z}/p\mathbb{Z}$ on a*

$$\begin{aligned} f_{a_1,b_1}\left(f_{a_2,b_2}(x)\right) &= a_1(a_2x + b_2) + b_1 \\ &= (a_1a_2)x + (a_1b_2 + b_1) \end{aligned}$$

et donc

$$f_{a_1,b_1} \circ f_{a_2,b_2} = f_{a_1a_2, a_1b_2+b_1}.$$

En particulier, comme de plus $\mathrm{Id}_{\mathbb{Z}/p\mathbb{Z}} = f_{1,0}$, on a :

- ***Inclusion***
  Soit $\varphi \in \mathrm{GA}_1(\mathbb{Z}/p\mathbb{Z})$ et $(a,b) \in (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/p\mathbb{Z}$ tels que $\varphi = f_{a,b}$. Alors

$$\begin{aligned} \varphi \circ f_{a^{-1},-a^{-1}b} &= f_{a^{-1},-a^{-1}b} \circ \varphi \\ &= f_{1,0} \end{aligned}$$

  et donc φ est bien bijective.
  D'où

$$\mathrm{GA}_1(\mathbb{Z}/p\mathbb{Z}) \subset \mathrm{S}(\mathbb{Z}/p\mathbb{Z})$$

- ***Non-vacuité** : on a déjà vu que $\mathrm{Id}_{\mathbb{Z}/p\mathbb{Z}} = f_{1,0} \in \mathrm{GA}_1(\mathbb{Z}/p\mathbb{Z})$.*
- ***Stabilité par produit** : on a déjà vu que $f_{a_1,b_1} \circ f_{a_2,b_2} = f_{a_1a_2,a_1b_2+b_1} \in \mathrm{GA}_1(\mathbb{Z}/p\mathbb{Z})$.*
- ***Stabilité par inverse** : on a déjà vu que $f_{a,b}^{-1} = f_{a^{-1},-a^{-1}b} \in \mathrm{GA}_1(\mathbb{Z}/p\mathbb{Z})$.*

Et donc

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

Q11.

- *On a $f_{1,1} : x \mapsto x+1$ est un p-cycle, et par conséquent, comme p est **impair**,*

$$\varepsilon\left(f_{1,1}\right) = (-1)^{p-1} = 1.$$

- *Par récurrence sur les représentants dans $[\![0, p-1]\!]$, on obtient donc que*

$$\forall b \in \mathbb{Z}/p\mathbb{Z}, \varepsilon\left(f_{1,b}\right) = 1.$$

- *L'application*

$$\begin{aligned} \sigma : (\mathbb{Z}/p\mathbb{Z})^\times &\to \mathrm{S}(\mathbb{Z}/p\mathbb{Z}) \\ a &\mapsto f_{a,0} \end{aligned}$$

  est un morphisme de groupes (car pour tous $a_1, a_2 \in (\mathbb{Z}/p\mathbb{Z})^\times$ on a $a_1(a_2x) = (a_1a_2)x$).
  Par conséquent

$$\begin{aligned} \varepsilon \circ \sigma : (\mathbb{Z}/p\mathbb{Z})^\times &\to \{-1,+1\} \\ a &\mapsto \varepsilon\left(f_{a,0}\right) \end{aligned}$$

  est un morphisme de groupes.
  *Et donc par la question **Q9** il s'agit soit de l'application constante égale à 1, soit de $\left(\frac{\cdot}{p}\right)$.*

- *Montrons que ce n'est **pas l'application triviale**.*
  Or $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique. Soit ζ un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$. Alors $f_{\zeta,0}$ est le $(p-1)$-cycle $\left(1\ \zeta\ \zeta^2\ \cdots\ \zeta^{p-2}\right)$ (et fixe 0) et donc

$$\varepsilon\left(f_{\zeta,0}\right) = (-1)^{p-2} = -1.$$

  Donc $\varepsilon \circ \sigma \neq 1$, d'où finalement

$$\forall a \in (\mathbb{Z}/p\mathbb{Z})^\times, \varepsilon(f_{a,0}) = \left(\frac{a}{p}\right).$$

- *Comme pour tout* $(a,b) \in (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/p\mathbb{Z}$ *on a*
$$f_{a,b} = f_{1,b} \circ f_{a,0}$$
on en déduit que pour tout $(a,b) \in (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/p\mathbb{Z}$,
$$\varepsilon(f_{a,b}) = \varepsilon(f_{1,b}) \times \varepsilon(f_{a,0}) = 1 \times \left(\frac{a}{p}\right)$$
et donc
$$\boxed{\varepsilon(f_{a,b}) = \left(\frac{a}{p}\right).}$$

C. Groupe dérivé de GL_n

Q12. *Soient* $M_1, M_2 \in G$.
Soient (A_1, C_1, L_1) *et* (A_2, C_2, L_2) *tels que* $M_1 = \begin{pmatrix} I_3 & C_1 & A_1 \\ 0 & I_1 & L_1 \\ 0 & 0 & I_3 \end{pmatrix}$ *et* $M_2 = \begin{pmatrix} I_3 & C_2 & A_2 \\ 0 & I_1 & L_2 \\ 0 & 0 & I_3 \end{pmatrix}$.
On a alors par produit par blocs
$$M_1M_2 = \begin{pmatrix} I_3 & C_1 + C_2 & A_1 + A_2 + C_1L_2 \\ 0 & I_1 & L_1 + L_2 \\ 0 & 0 & I_3 \end{pmatrix}.$$
On a donc
- $I_7 = \begin{pmatrix} I_3 & 0 & 0 \\ 0 & I_1 & 0 \\ 0 & 0 & I_3 \end{pmatrix} \in G$,
- *par le calcul précédent* G *est stable par produit,*
- *pour tout* $M \in G$ *avec* (A, C, L) *tels que* $M = \begin{pmatrix} I_3 & C & A \\ 0 & I_1 & L \\ 0 & 0 & I_3 \end{pmatrix}$ *on a, toujours par le calcul précédent*
$$\begin{pmatrix} I_3 & C & A \\ 0 & I_1 & L \\ 0 & 0 & I_3 \end{pmatrix}\begin{pmatrix} I_3 & -C & -A+CL \\ 0 & I_1 & -L \\ 0 & 0 & I_3 \end{pmatrix} = I_7$$

et donc $M^{-1} = \begin{pmatrix} I_3 & -C & -A+CL \\ 0 & I_1 & -L \\ 0 & 0 & I_3 \end{pmatrix} \in G$.
D'où $\boxed{G \text{ est un sous-groupe de } \mathrm{GL}_7(\mathbb{R}).}$
De plus, toujours par les calculs précédents, pour $M_1 = \begin{pmatrix} I_3 & C_1 & A_1 \\ 0 & I_1 & L_1 \\ 0 & 0 & I_3 \end{pmatrix}$ *et* $M_2 = \begin{pmatrix} I_3 & C_2 & A_2 \\ 0 & I_1 & L_2 \\ 0 & 0 & I_3 \end{pmatrix}$ *on a*
$$M_1M_2M_1^{-1}M_2^{-1} = \begin{pmatrix} I_3 & 0 & C_1L_2 - C_2L_1 \\ 0 & I_1 & 0 \\ 0 & 0 & I_3 \end{pmatrix}.$$
Or pour tous $C_1, C_2 \in M_{3,1}(\mathbb{R})$ *et* $L_1, L_2 \in M_{1,3}(\mathbb{R})$ *on a*
$$\mathrm{rg}(C_1L_2 - C_2L_1) \leq \dim(\mathrm{Vect}(C_1, C_2)) \leq 2.$$
Réciproquement, toute matrice $A \in M_{3,3}(\mathbb{R})$ *de rang inférieur ou égal à 2 s'écrit sous la forme* $C_1L_2 - C_2L_1$. *En notant* E_1, E_2, E_3 *la base canonique de* $\mathbb{R}^3$,
- *si* $\mathrm{rg}(A) = 0$ *alors* $A = 0_{3,1}0_{1,3} - 0_{3,1}0_{1,3}$,
- *si* $\mathrm{rg}(A) = 1$ *alors il existe* $(C_1, L_2) \in M_{3,1}(\mathbb{R}) \times M_{1,3}(\mathbb{R})$ *tels que* $A = C_1L_2$ *et donc* $A = C_1L_2 - 0_{3,1}0_{1,3}$,
- *si* $\mathrm{rg}(A) = 2$ *alors il existe* $P, Q \in \mathrm{GL}_3(\mathbb{R})$ *tels que* $A = P\,\mathrm{diag}(1,1,0)Q^{-1} = P\left(E_1E_1^\top + E_2E_2^\top\right)Q^{-1}$ *et donc avec* $C_1 = PE_1$, $C_2 = PE_2$, $L_2 = E_1^\top Q^{-1}$ *et* $L_1 = -E_2^\top Q^{-1}$ *on a* $A = C_1L_2 - C_2L_1$.

D'où
$$\left\{xyx^{-1}y^{-1}, (x,y) \in G^2\right\} = \left\{\begin{pmatrix} I_3 & 0 & A \\ 0 & I_1 & 0 \\ 0 & 0 & I_3 \end{pmatrix}, A \in M_{3,3}(\mathbb{R}) \mid \mathrm{rg}(A) \leq 2\right\}.$$
Notons $N(A) = \begin{pmatrix} I_3 & 0 & A \\ 0 & I_1 & 0 \\ 0 & 0 & I_3 \end{pmatrix}$. *On a déjà vu que pour tous* $A_1, A_2 \in M_{3,3}(\mathbb{R})$,
$$N(A_1)N(A_2) = N(A_1 + A_2).$$
Comme $N(0) = I_7$ *et* $N(A)^{-1} = N(-A)$, *l'ensemble des* $N(A)$ *est un sous-groupe de* G *contenant tous les commutateurs. Il contient donc* D(G).
Réciproquement, pour toute matrice $A = (a_{i,j}) \in M_{3,3}(\mathbb{R})$, *chaque* $a_{i,j}E_{i,j}$ *est de rang inférieur ou égal à* 1, *donc* $N(a_{i,j}E_{i,j})$ *est un commutateur. Comme* $A = \sum_{i=1}^3 \sum_{j=1}^3 a_{i,j}E_{i,j}$, *la formule de produit donne* $N(A) \in D(G)$.
On obtient donc
$$D(G) = \left\{\begin{pmatrix} I_3 & 0 & A \\ 0 & I_1 & 0 \\ 0 & 0 & I_3 \end{pmatrix}, A \in M_{3,3}(\mathbb{R})\right\}.$$
Et comme il existe des matrices 3×3 *qui ne sont pas de rang inférieur ou égal à 2* (I_3 *par exemple), on en déduit que*
$$\boxed{\left\{xyx^{-1}y^{-1}, (x,y) \in G^2\right\} \neq D(G).}$$

Q13. *On a pour tous* $(x,y) \in G^2$,

$$\varphi\left(xyx^{-1}y^{-1}\right) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1}.$$

Les images des commutateurs de G *sont donc exactement les commutateurs de* $\varphi(\mathrm{G})$. *Comme l'image d'un sous-groupe engendré est le sous-groupe engendré par les images des générateurs, on en déduit*

$$\boxed{\varphi(\mathrm{D}(\mathrm{G})) = \mathrm{D}(\varphi(\mathrm{G})).}$$

Pour $g \in \mathrm{G}$, *appliquons ce résultat à l'automorphisme* $\varphi_g : x \mapsto gxg^{-1}$. *On a*

$$\varphi_g(\mathrm{D}(\mathrm{G})) = \mathrm{D}\left(\varphi_{g(\mathrm{G})}\right) = \mathrm{D}(\mathrm{G}),$$

d'où la $\boxed{\text{stabilité de } \mathrm{D}(\mathrm{G}) \text{ par conjugaison.}}$

Q14. *Remarquons tout d'abord qu'un groupe* K *est abélien ssi pour tous* $x, y \in \mathrm{K}$ *on a* $xy = yx$, *ssi pour tous* $x, y \in \mathrm{K}$ *on a* $xyx^{-1}y^{-1} = 1$, *ssi* $\mathrm{D}(\mathrm{K}) = \{1\}$.
Par conséquent $\mathrm{Im}(\varphi)$ *est abélien ssi* $\mathrm{D}(\mathrm{Im}(\varphi)) = \{1\}$, *ssi* $\varphi(\mathrm{D}(\mathrm{G})) = \{1\}$ *(par la question* ***Q13****), ssi* $\mathrm{D}(\mathrm{G}) \subset \mathrm{Ker}(\varphi)$.
On a donc bien

$$\boxed{\mathrm{Im}(\varphi) \text{ est abélien} \iff \mathrm{D}(\mathrm{G}) \subset \mathrm{Ker}(\varphi).}$$

Q15. *On a* $\mathbb{K}^\times$ *est abélien et*

$$\begin{aligned} \det : \mathrm{GL}_n(\mathbb{K}) &\to \mathbb{K}^\times \\ \mathrm{A} &\mapsto \det(\mathrm{A}) \end{aligned}$$

est un morphisme de groupes, d'où par la question ***Q14*** *on a*

$$\boxed{\mathrm{D}(\mathrm{GL}_n(\mathbb{K})) \subset \mathrm{Ker}(\det) = \mathrm{SL}_n(\mathbb{K}).}$$

Q16. *On a*

$$\mathrm{T}^{-1} = \mathrm{I}_n - \lambda \mathrm{E}_{i,j}$$

et par conséquent

$$\begin{aligned} \mathrm{DTD}^{-1}\mathrm{T}^{-1} &= \mathrm{D}\left(\mathrm{I}_n + \lambda \mathrm{E}_{i,j}\right)\mathrm{D}^{-1}\left(\mathrm{I}_n - \lambda \mathrm{E}_{i,j}\right) \\ &= \mathrm{I}_n + \mathrm{D}\lambda \mathrm{E}_{i,j}\mathrm{D}^{-1} - \lambda \mathrm{E}_{i,j} - \mathrm{D}\lambda \mathrm{E}_{i,j}\mathrm{D}^{-1}\lambda \mathrm{E}_{i,j} \\ &= \mathrm{I}_n + \lambda \frac{d_i}{d_j}\mathrm{E}_{i,j} - \lambda \mathrm{E}_{i,j} - 0 \end{aligned}$$

d'où

$$\boxed{\mathrm{DTD}^{-1}\mathrm{T}^{-1} = \mathrm{I}_n + \lambda\left(\frac{d_i}{d_j} - 1\right)\mathrm{E}_{i,j}.}$$

Q17. *On sait déjà par la question* ***Q15*** *que* $\mathrm{D}(\mathrm{GL}_n(\mathbb{K})) \subset \mathrm{SL}_n(\mathbb{K})$.
De plus on sait que $\mathrm{SL}_n(\mathbb{K})$ *est engendré par les transvections élémentaires. Comme* $\mathrm{D}(\mathrm{GL}_n(\mathbb{K}))$ *est un groupe il suffit de montrer que* ***toute transvection élémentaire est dans*** $\mathrm{D}(\mathrm{GL}_n(\mathbb{K}))$.
Soient T *une transvection élémentaire,* $i, j \in [\![1, n]\!]$ *tels que* $i \neq j$ *et* $\lambda \in \mathbb{K}$ *tels que* $\mathrm{T} = \mathrm{I}_n + \lambda \mathrm{E}_{i,j}$.
Comme $\mathbb{K}$ *possède au moins trois éléments, il existe* $a \in \mathbb{K}^\times \setminus \{1\}$.
Posons

$$\mathrm{A} = \mathrm{diag}(1, \ldots, 1, a, 1, \ldots, 1)$$

la matrice diagonale avec a *en position* (i, i) *et* 1 *ailleurs, et*

$$\mathrm{B} = \mathrm{I}_n + \frac{\lambda}{a-1}\mathrm{E}_{i,j}.$$

Par la question ***Q16*** *on a*

$$\mathrm{ABA}^{-1}\mathrm{B}^{-1} = \mathrm{I}_n + \lambda \mathrm{E}_{i,j}$$

et donc en particulier

$$\mathrm{T} \in \mathrm{D}(\mathrm{GL}_n(\mathbb{K})).$$

D'où finalement

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

Q18. *On a pour* $a, b \in \mathbb{K}^\times$,

$$\Delta_a \Delta_b = \Delta_{ab}$$

et donc

$$\mathscr{D} \text{ est un sous-groupe de } \mathrm{GL}_n(\mathbb{K})$$

comme image du morphisme de groupes

$$\begin{aligned} \mathbb{K}^\times &\to \mathrm{GL}_n(\mathbb{K}) \\ a &\mapsto \Delta_a. \end{aligned}$$

Soit $\mathrm{A} \in \mathrm{GL}_n(\mathbb{K})$. *Procédons par analyse-synthèse.*

- ***Analyse***
  Soient $(\Delta, \mathrm{S}) \in \mathscr{D} \times \mathrm{SL}_n(\mathbb{K})$ *tels que* $\mathrm{A} = \Delta\mathrm{S}$ *et* $a \in \mathbb{K}^\times$ *tel que* $\Delta = \Delta_a$. *Alors*
  $$\det(\mathrm{A}) = \det(\Delta)\det(\mathrm{S}) = \det(\Delta_a) = a$$
  et on en déduit que $\Delta = \Delta_{\det(\mathrm{A})}$ *et donc* $\mathrm{S} = \Delta^{-1}\mathrm{A}$.
  D'où l'unicité.
- ***Synthèse***
  Posons $\Delta = \Delta_{\det(\mathrm{A})} \in \mathscr{D}$ *et* $\mathrm{S} = \Delta^{-1}\mathrm{A}$.
  On a bien $\mathrm{A} = \Delta\mathrm{S}$ *et* $\det(\mathrm{S}) = \det(\Delta)^{-1}\det(\mathrm{A}) = 1$, *donc* $\mathrm{S} \in \mathrm{SL}_n(\mathbb{K})$.
  D'où l'existence.

Q19. *Posons*

$$\psi : \mathbb{K}^\times \to \mathrm{H}$$
$$a \mapsto \varphi(\Delta_a).$$

*C'est un morphisme de groupes, comme composée de φ et du morphisme de groupes $a \mapsto \Delta_a$ mis en évidence à la question **Q18**.*
*Comme H est abélien, on a $\mathrm{D}(\mathrm{H}) = \{1\}$ et par les questions **Q14** et **Q17** on a donc*
$$\forall \mathrm{S} \in \mathrm{SL}_n(\mathbb{K}), \varphi(\mathrm{S}) = 1.$$

Soit $\mathrm{A} \in \mathrm{GL}_n(\mathbb{K})$.
*La question **Q18** montre qu'il existe $\mathrm{S} \in \mathrm{SL}_n(\mathbb{K})$ tel que*
$$\mathrm{A} = \Delta_{\det(\mathrm{A})}\mathrm{S}$$
d'où
$$\varphi(\mathrm{A}) = \varphi\big(\Delta_{\det(\mathrm{A})}\big)\varphi(\mathrm{S}) = \psi(\det(\mathrm{A})) \times 1 = \psi(\det(\mathrm{A})).$$
Ainsi
$$\boxed{\varphi = \psi \circ \det.}$$

D. Loi de réciprocité quadratique

Q20.
- *La division euclidienne par q montre que tout $k \in [\![0, \mathrm{N}-1]\!]$ s'écrit de manière unique $k = qi + j$ avec $i \in [\![0, p-1]\!]$ et $j \in [\![0, q-1]\!]$: $\boxed{\ell \text{ est bijective.}}$*
- *De même la division euclidienne par p montre que tout $k \in [\![0, \mathrm{N}-1]\!]$ s'écrit de manière unique $k = i + pj$ avec $i \in [\![0, p-1]\!]$ et $j \in [\![0, q-1]\!]$: $\boxed{c \text{ est bijective.}}$*
- *Comme p et q sont deux nombres premiers distincts, $p \wedge q = 1$ et le théorème des restes chinois montre que θ est **bien définie** et que*
$$[\![0, \mathrm{N}-1]\!] \to \mathrm{E}$$
$$k \mapsto (k\%p, k\%q)$$
est bijective. Or θ est exactement sa bijection réciproque, d'où $\boxed{\theta \text{ est bijective.}}$

Q21. *On a le tableau de correspondance*

(I)	*(II)*	*(III)*
ℓ	c	θ

Pour $p = 3$ et $q = 5$, on obtient

$i \setminus j$	0	1	2	3	4
0	0	1	2	3	4
1	5	6	7	8	9
2	10	11	12	13	14

ℓ : par lignes

$i \setminus j$	0	1	2	3	4
0	0	3	6	9	12
1	1	4	7	10	13
2	2	5	8	11	14

c : par colonnes

$i \setminus j$	0	1	2	3	4
0	0	6	12	3	9
1	10	1	7	13	4
2	5	11	2	8	14

θ : par restes chinois

Q22. *Soit $i \in [\![0, p-1]\!]$.*
On a
$$c(\mathrm{L}_i) = \{i + pj, j \in [\![0, q-1]\!]\}.$$
Soit $j \in [\![0, q-1]\!]$.
On a
$$i + pj \equiv i \pmod{p}$$
d'où
$$\theta^{-1}(i + pj) = (i, (i + pj)\%q).$$
On en déduit donc que
$$\big(\theta^{-1} \circ c\big)(\mathrm{L}_i) \subset \mathrm{L}_i.$$
Et comme $\theta^{-1} \circ c$ est bijective (composée de bijections) et L_i est fini, on a bien
$$\boxed{\big(\theta^{-1} \circ c\big)(\mathrm{L}_i) = \mathrm{L}_i}$$
et la permutation induite est
$$\boxed{\begin{aligned} \mathrm{L}_i &\to \mathrm{L}_i \\ (i, j) &\mapsto (i, (i + pj)\%q) \end{aligned}}$$

Q23.
- ***Décomposition en lignes***
Notons $\rho = \theta^{-1} \circ c$. On a déjà vu que ρ laisse stable chaque ligne L_i et induit sur celle-ci la permutation
$$\rho_i : \mathrm{L}_i \to \mathrm{L}_i$$
$$(i, j) \mapsto (i, (i + pj)\%q).$$
Munissons E de l'ordre total donné par la numérotation ℓ, c'est-à-dire
$$(i, j) < (i', j') \iff \ell(i, j) < \ell(i', j').$$
Dans cet ordre, tous les éléments de L_i précèdent ceux de $\mathrm{L}_{i'}$ lorsque $i < i'$. Comme ρ laisse stable chaque ligne, un couple d'éléments appartenant à deux lignes distinctes ne peut donc pas être une inversion de ρ.
Les inversions de ρ sont ainsi exactement les inversions des ρ_i, chaque ligne étant munie de l'ordre induit. On a donc
$$d_\rho = \sum_{i=0}^{p-1} d_{\rho_i}$$
*et par la question **Q3** on en déduit*

$$\varepsilon(\rho) = (-1)^{d_\rho} = \prod_{i=0}^{p-1} (-1)^{d_{\rho_i}} = \prod_{i=0}^{p-1} \varepsilon(\rho_i).$$

- ***Signature de la permutation induite sur une ligne***
  Soit $i \in [\![0, p-1]\!]$.
  On a la bijection
  $$u_i : \mathrm{L}_i \to \mathbb{Z}/q\mathbb{Z}$$
  $$(i,j) \mapsto [j]_q.$$
  Comme $[(i+pj)\%q]_q = [p]_q[j]_q + [i]_q$, on a
  $$u_i \circ \rho_i \circ u_i^{-1} = f_{[p]_q,[i]_q}.$$
  Les permutations ρ_i et $f_{[p]_q,[i]_q}$ ont donc des cycles de mêmes longueurs, et par conséquent la même signature.
  *Comme p et q sont premiers et distincts, on a $[p]_q \in (\mathbb{Z}/q\mathbb{Z})^\times$, donc $f_{[p]_q,[i]_q} \in \mathrm{GA}_1(\mathbb{Z}/q\mathbb{Z})$ et la question **Q11**, appliquée au nombre premier impair q, donne*
  $$\varepsilon(\rho_i) = \varepsilon\Big(f_{[p]_q,[i]_q}\Big) = \left(\frac{p}{q}\right).$$

- ***Conclusion***
  On a donc
  $$\varepsilon(\rho) = \prod_{i=0}^{p-1} \varepsilon(\rho_i) = \left(\frac{p}{q}\right)^p$$
  *et comme p est **impair** on a donc bien*
  $$\boxed{\varepsilon\big(\theta^{-1} \circ c\big) = \left(\frac{p}{q}\right).}$$

Q24. *Notons $\sigma = \ell^{-1} \circ c$ et munissons E de l'ordre total donné par ℓ, comme à la question **Q23**.*

- ***Caractérisation des inversions***
  On a pour tout $(i,j) \in \mathrm{E}$,
  $$\ell(\sigma(i,j)) = c(i,j).$$
  Un couple $((i,j),(i',j')) \in \mathrm{E}^2$ est donc une inversion de σ ssi
  $$\ell(i,j) < \ell(i',j') \quad \text{et} \quad c(i,j) > c(i',j').$$
  Or les numérotations par lignes et par colonnes donnent respectivement
  $$\ell(i,j) < \ell(i',j') \iff i < i' \text{ ou } (i = i' \text{ et } j < j'),$$
  $$c(i,j) > c(i',j') \iff j > j' \text{ ou } (j = j' \text{ et } i > i').$$
  Si $i = i'$, ces deux conditions imposent à la fois $j < j'$ et $j > j'$, ce qui est impossible. De même, le cas $j = j'$ est impossible.
  On en déduit que $((i,j),(i',j'))$ est une inversion de σ ssi
  $$i < i' \quad \text{et} \quad j > j'.$$

- ***Nombre d'inversions***
  Il suffit donc de choisir deux lignes distinctes $i < i'$ et deux colonnes distinctes $j' < j$. Elles donnent exactement une inversion, le couple $((i,j),(i',j'))$, formé par les deux cases grisées ci-dessous :

	j'	j
i	(i,j')	(i,j)
i'	(i',j')	(i',j)

  On a donc
  $$d_\sigma = \binom{p}{2}\binom{q}{2} = \frac{p(p-1)}{2} \times \frac{q(q-1)}{2} = pq \times \frac{p-1}{2} \times \frac{q-1}{2}.$$

- ***Conclusion***
  *Comme pq est **impair**, on a*
  $$d_\sigma \equiv \frac{p-1}{2} \times \frac{q-1}{2} \pmod 2.$$
  *Par la question **Q3** on a*
  $$\varepsilon\big(\ell^{-1} \circ c\big) = (-1)^{d_\sigma}$$
  d'où finalement
  $$\boxed{\varepsilon\big(\ell^{-1} \circ c\big) = (-1)^{\frac{p-1}{2} \times \frac{q-1}{2}}.}$$

Q25. *On a*
$$\ell^{-1} \circ c = \big(\theta^{-1} \circ \ell\big)^{-1} \circ \big(\theta^{-1} \circ c\big).$$
Comme la signature est un morphisme de groupes et qu'une permutation a la même signature que son inverse, on en déduit
$$\varepsilon\big(\ell^{-1} \circ c\big) = \varepsilon\big(\theta^{-1} \circ \ell\big) \times \varepsilon\big(\theta^{-1} \circ c\big).$$
*Par la question **Q23** et le résultat admis qui la suit, on a donc*
$$\varepsilon\big(\ell^{-1} \circ c\big) = \left(\frac{q}{p}\right)\left(\frac{p}{q}\right).$$
*La question **Q24** donne alors*
$$\boxed{\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \times \frac{q-1}{2}}.}$$

E. Frobenius-Zolotarev

Q26. *Notons* $\mathrm{E}_1, \dots, \mathrm{E}_n$ *la base canonique de* $(\mathbb{Z}/p\mathbb{Z})^n$ *et* $\mathrm{B} = (b_1, \dots, b_n) \in (\mathbb{Z}/p\mathbb{Z})^n$. *On a*

$$f_{\mathrm{I}_n,\mathrm{B}} = f_{\mathrm{I}_n,b_1\mathrm{E}_1} \circ \dots \circ f_{\mathrm{I}_n,b_n\mathrm{E}_n}.$$

Pour tout $i \in [\![1,n]\!]$, *choisissons* $k_i \in [\![0, p-1]\!]$ *tel que* $b_i = [k_i]_p$. *On a alors*

$$f_{\mathrm{I}_n,b_i\mathrm{E}_i} = \left(f_{\mathrm{I}_n,\mathrm{E}_i}\right)^{k_i}.$$

Il suffit donc, comme à la question ***Q11****, de montrer que* $\varepsilon\left(f_{\mathrm{I}_n,\mathrm{E}_i}\right) = 1$ *pour tout* $i \in [\![1,n]\!]$.
Soit $i \in [\![1,n]\!]$.
On peut décomposer $(\mathbb{Z}/p\mathbb{Z})^n$ *en la réunion disjointe des droites affines*

$$(\mathbb{Z}/p\mathbb{Z})^n = \bigsqcup_{(a_1,\dots,a_{i-1},a_{i+1},\dots,a_n)\in(\mathbb{Z}/p\mathbb{Z})^{n-1}} \left\{ \begin{pmatrix} a_1 \\ \dots \\ a_{i-1} \\ x \\ a_{i+1} \\ \dots \\ a_n \end{pmatrix}, x \in \mathbb{Z}/p\mathbb{Z} \right\}$$

De plus $f_{\mathrm{I}_n,\mathrm{E}_i}$ *laisse invariante chacune de ces droites affines et agit sur chacune d'elles comme la translation* $x \mapsto x+1$ *de* $\mathbb{Z}/p\mathbb{Z}$, *qui, cf. question* ***Q11****, est une permutation de signature* $+1$. *La signature de* $f_{\mathrm{I}_n,\mathrm{E}_i}$ *est le produit des signatures de ces restrictions, donc vaut* 1.
Par conséquent, pour tout $\mathrm{B} \in (\mathbb{Z}/p\mathbb{Z})^n$,

$$\boxed{\varepsilon\left(f_{\mathrm{I}_n,\mathrm{B}}\right) = 1.}$$

Q27. *On peut décomposer* $(\mathbb{Z}/p\mathbb{Z})^n$ *en la réunion disjointe des droites affines*

$$(\mathbb{Z}/p\mathbb{Z})^n = \bigsqcup_{(a_2,\dots,a_n)\in(\mathbb{Z}/p\mathbb{Z})^{n-1}} \left\{ \begin{pmatrix} x \\ a_2 \\ \dots \\ a_n \end{pmatrix}, x \in \mathbb{Z}/p\mathbb{Z} \right\}$$

De plus $f_{\Delta_\zeta,0}$ *laisse invariante chacune de ces droites affines et agit sur chacune d'elles comme la multiplication par* ζ *de* $\mathbb{Z}/p\mathbb{Z}$. *Cette permutation fixe* 0 *et permute les éléments non nuls en un* $(p-1)$*-cycle, donc sa signature vaut* $(-1)^{p-2} = -1$, *comme à la question* ***Q11****.*
Comme p^{n-1} *est impair, on en déduit que*

$$\boxed{\varepsilon\left(f_{\Delta_\zeta,0}\right) = (-1)^{p^{n-1}} = -1.}$$

Q28. *Pour tous* $(\mathrm{A},\mathrm{B}) \in \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})^n$, *on peut écrire*

$$f_{\mathrm{A},\mathrm{B}} = f_{\mathrm{I}_n,\mathrm{B}} \circ f_{\mathrm{A},0}$$

et donc par la question ***Q26****,*

$$\varepsilon\left(f_{\mathrm{A},\mathrm{B}}\right) = \varepsilon\left(f_{\mathrm{I}_n,\mathrm{B}}\right)\varepsilon\left(f_{\mathrm{A},0}\right) = \varepsilon\left(f_{\mathrm{A},0}\right).$$

De plus pour tous $\mathrm{A}_1, \mathrm{A}_2 \in \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$, *on a*

$$f_{\mathrm{A}_1\mathrm{A}_2,0} = f_{\mathrm{A}_1,0} \circ f_{\mathrm{A}_2,0}$$

et donc

$$\varphi : \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z}) \to \{+1,-1\}, \quad \mathrm{A} \mapsto \varepsilon\left(f_{\mathrm{A},0}\right)$$

est un morphisme de groupes.
Comme $(\{+1,-1\},\times)$ *est abélien, par la question* ***Q19****, il existe un morphisme de groupes* $\psi : (\mathbb{Z}/p\mathbb{Z})^\times \to \{+1,-1\}$ *tel que* $\varphi = \psi \circ \det$.
Par la question ***Q9****,* $\psi = 1$ *ou* $\psi = \left(\frac{\cdot}{p}\right)$. *Pour le générateur* ζ *choisi à la question* ***Q27****, on a* $\det\left(\Delta_\zeta\right) = \zeta$, *donc*

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

Ainsi $\psi \neq 1$.
Et donc $\psi = \left(\frac{\cdot}{p}\right)$, *c'est-à-dire que pour tout* $\mathrm{A} \in \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$,

$$\varepsilon\left(f_{\mathrm{A},0}\right) = \psi(\det(\mathrm{A})) = \left(\frac{\det(\mathrm{A})}{p}\right).$$

On a donc bien montré le résultat (dit théorème de Frobenius-Zolotarev) :

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