Lemme de Zolotarev et réciprocité 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 $x \in \mathrm{G}$ tel que $a = x^2$.
Dans la suite on considèrera particulièrement le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$ pour un nombre premier p.
On note alors

$$\mathrm{K}_p = \left\{x^2 \mid x \in (\mathbb{Z}/p\mathbb{Z})^\times\right\}$$

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

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

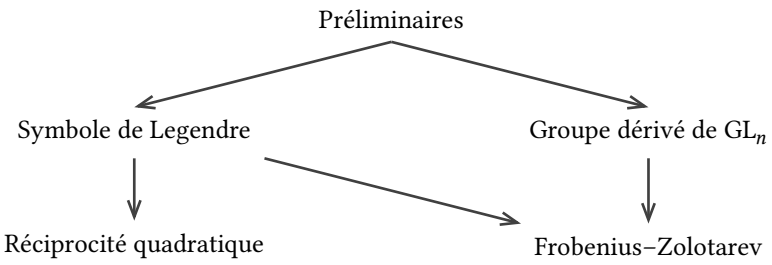
Plus généralement étant donné $a \in \mathbb{Z}$ premier avec p on dit que a est un carré modulo p ssi $\overline{a}$ est un carré dans $(\mathbb{Z}/p\mathbb{Z})^\times$, ce qui revient donc à l'existence de $b \in \mathbb{Z}$ premier avec p tel que $a \equiv b^2 \pmod{p}$.
On définit de même pour $a \in \mathbb{Z}$ et p un nombre premier le symbole de Legendre

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

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 réciprocité 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

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

Q1. Soit p un nombre premier.
Montrer que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.
Cf. cours.

Q2. Soient G, H des groupes, G fini et $\varphi : \mathrm{G} \to \mathrm{H}$ un morphisme de groupes.
Montrer que

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

Pour tous $x_1, x_2 \in \mathrm{G}$, on $\varphi(x_1) = \varphi(x_2)$ ssi $\varphi\left(x_1 (x_2)^{-1}\right) = e_\mathrm{H}$ c'est à dire ssi $x_1 (x_2)^{-1} \in \mathrm{Ker}(\varphi)$ 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

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

Q3. Soit G un groupe fini et H un sous-groupe de G.

On suppose

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

Soit $\alpha \in \mathrm{G} \setminus \mathrm{H}$.

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

- *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*

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

Q4. Soient $\mathbb{K}$ un corps et $n \geq 2$ un entier.

Montrer que toute matrice de $\mathrm{SL}_n(\mathbb{K})$ est un produit de transvections.

Q5. Soit $(\mathrm{E}, \leq)$ un ensemble fini totalement ordonné et $\sigma \in \mathrm{S}(\mathrm{E})$.

On note

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

Montrer que

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

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.

(À détailler)

Soient $x_1, \ldots, x_n$ des complexes distincts.

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 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

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

B. Propriétés du symbole de Legendre

Q6. Soit $a \in \mathbb{Z}$. Que dire de $\left(\frac{a}{2}\right)$?

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

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

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

Q7. Montrer que K_p est un sous-groupe de $(\mathbb{Z}/p\mathbb{Z})^\times$ et que

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

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 **Q2** on en déduit*

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

Q8. En déduire que

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

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 **Q7** 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

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

Q9. En déduire que pour tout $a \in \mathbb{Z}$,

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

Soit $a \in \mathbb{Z}$. Si p divise a, les deux membres sont congrus à 0 modulo p.
Sinon, posons $x = \overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$. 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 **Q8**, cette puissance vaut 1 ssi $x \in \mathrm{K}_p$, et vaut donc -1 sinon.*
On a ainsi dans tous les cas

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

Q10. Montrer que

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

est un morphisme de groupes.
*On a d'après la question **Q9** que pour tout $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, l'égalité*

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

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

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

Q11. Soit

$$\varphi : (\mathbb{Z}/p\mathbb{Z})^\times \to \{-1,+1\}$$
$$a \mapsto \varphi(a)$$

un morphisme de groupes.
Montrer que $\varphi = 1$ (l'application constante égale à 1) ou $\varphi = \left(\frac{\cdot}{p}\right)$.
Remarque : $\left(\frac{\cdot}{p}\right)$ est donc l'unique morphisme non trivial de $(\mathbb{Z}/p\mathbb{Z})^\times$ vers $\{1,-1\}$.
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 **Q7**, la question **Q3** 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

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

et donc φ est constante égale à 1 sur K_p.

Ensuite, par disjonction de cas

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

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

et donc

$$\varphi=1.$$

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

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

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*

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

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

$$\begin{aligned} f_{a,b}:\mathbb{Z}/p\mathbb{Z}&\to\mathbb{Z}/p\mathbb{Z}\\ x&\mapsto ax+b\end{aligned}$$

et on note

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

Q12. Montrer que $\mathrm{GA}_1(\mathbb{Z}/p\mathbb{Z})$ est un sous-groupe de $\mathrm{S}(\mathbb{Z}/p\mathbb{Z})$.

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*

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

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

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

Q13. En déduire le **lemme de Zolotarev**: pour tout $(a,b)\in(\mathbb{Z}/p\mathbb{Z})^\times\times\mathbb{Z}/p\mathbb{Z}$,

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

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

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

- *Par récurrence on obtient donc que*

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

- *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

$$\varepsilon \circ \sigma : (\mathbb{Z}/p\mathbb{Z})^\times \to \{-1,+1\}$$
$$a \mapsto \varepsilon\big(f_{a,0}\big)$$

est un morphisme de groupes.

Et donc par la question ***Q11*** *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****.*
  D'après la question ***Q1****,* $(\mathbb{Z}/p\mathbb{Z})^\times$ *est cyclique. Soit* ζ *un générateur de* $(\mathbb{Z}/p\mathbb{Z})^\times$*. Alors* $f_{\zeta,0}$ *est le* $(p-1)$*-cycle* $\big(1\ \zeta\ \zeta^2 \cdots \zeta^{p-2}\big)$ *(et fixe* 0*) et donc*
  $$\varepsilon\big(f_{\zeta,0}\big) = (-1)^{p-2} = -1.$$
  Donc $\varepsilon \circ \sigma \neq 1$*, d'où finalement*
  $$\forall a \in (\mathbb{Z}/p\mathbb{Z})^\times, \varepsilon\big(f_{a,0}\big) = \left(\frac{a}{p}\right).$$
- *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 $(a,b) \in (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/p\mathbb{Z}$*,*
  $$\varepsilon\big(f_{a,b}\big) = \varepsilon\big(f_{1,b}\big) \times \varepsilon\big(f_{a,0}\big) = 1 \times \left(\frac{a}{p}\right) = \left(\frac{a}{p}\right).$$

C. Groupe dérivé de GL_n

Étant donné un groupe G on définit le **groupe dérivé** de G par
$$\mathrm{D}(\mathrm{G}) = \big\langle \{xyx^{-1}y^{-1}, x, y \in \mathrm{G}\} \big\rangle$$
c'est-à-dire le sous-groupe de G engendré par les **commutateurs** (éléments de la forme $xyx^{-1}y^{-1}$) de G.

Q14. Soit G, H des groupes et $\varphi : \mathrm{G} \to \mathrm{H}$ un morphisme de groupes.
Montrer que $\varphi(\mathrm{D}(\mathrm{G})) = \mathrm{D}(\varphi(\mathrm{G}))$.
En déduire en particulier que D(G) est stable par conjugaison (c'est-à-dire que pour tout $g \in \mathrm{G}$ et tout $x \in \mathrm{D}(\mathrm{G})$ on a $gxg^{-1} \in \mathrm{D}(\mathrm{G})$).
On a pour tous $x, y \in \mathrm{G}$*,*
$$\varphi\big(xyx^{-1}y^{-1}\big) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1}.$$
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*
$$\varphi(\mathrm{D}(\mathrm{G})) = \mathrm{D}(\varphi(\mathrm{G})).$$
Pour $g \in \mathrm{G}$*, appliquons ce résultat à l'automorphisme* $\varphi_g : x \mapsto gxg^{-1}$*. On a*
$$\varphi_{g(\mathrm{D}(\mathrm{G}))} = \mathrm{D}\big(\varphi_{g(\mathrm{G})}\big) = \mathrm{D}(\mathrm{G}),$$
d'où la stabilité de D(G) *par conjugaison.*

Q15. Soit G, H des groupes et $\varphi : \mathrm{G} \to \mathrm{H}$ un morphisme de groupes.
Montrer que $\mathrm{Im}(\varphi)$ est abélien ssi $\mathrm{D}(\mathrm{G}) \subset \mathrm{Ker}(\varphi)$.
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* ***Q14****), ssi* $\mathrm{D}(\mathrm{G}) \subset \mathrm{Ker}(\varphi)$*.*
On a donc bien
$$\mathrm{Im}(\varphi) \text{ est abélien} \iff \mathrm{D}(\mathrm{G}) \subset \mathrm{Ker}(\varphi).$$

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

Q16. Montrer que $\mathrm{D}(\mathrm{GL}_n(\mathbb{K})) \subset \mathrm{SL}_n(\mathbb{K})$.
On a $\mathbb{K}^\times$ *est abélien et*
$$\det : \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^\times$$
$$\mathrm{A} \mapsto \det(\mathrm{A})$$
est un morphisme de groupes, d'où par la question ***Q15*** *on a*
$$\mathrm{D}(\mathrm{GL}_n(\mathbb{K})) \subset \mathrm{Ker}(\det) = \mathrm{SL}_n(\mathbb{K}).$$

Q17. Soient $i, j \in [\![1, n]\!]$ tels que $i \neq j$, $\lambda \in \mathbb{K}$ et $d_1, \ldots, d_n \in \mathbb{K}^\times$.
On pose $\mathrm{D} = \mathrm{diag}(d_1, \ldots, d_n)$ et $\mathrm{T} = \mathrm{I}_n + \lambda \mathrm{E}_{i,j}$.
Calculer le commutateur

$$\mathrm{DTD}^{-1}\mathrm{T}^{-1}.$$

On a

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

et par conséquent

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

d'où

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

Q18. Conclure que

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

*On sait déjà par la question **Q16** que* $\mathrm{D}(\mathrm{GL}_n(\mathbb{K})) \subset \mathrm{SL}_n(\mathbb{K})$.

*De plus on sait par la question **Q4** que* $\mathrm{SL}_n(\mathbb{K})$ *est engendré par les transvections. Comme* $\mathrm{D}(\mathrm{GL}_n(\mathbb{K}))$ *est un groupe il suffit de montrer que **toute transvection est dans*** $\mathrm{D}(\mathrm{GL}_n(\mathbb{K}))$.

Soient T *une transvection,* $i, j \in [\![1, n]\!]$ *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 **Q17** 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

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

Q19. Pour $a \in \mathbb{K}^\times$ on pose

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

Montrer que $\mathscr{D}$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{K})$ et que pour tout $\mathrm{A} \in \mathrm{GL}_n(\mathbb{K})$ il existe un unique couple $(\Delta, \mathrm{S}) \in \mathscr{D} \times \mathrm{SL}_n(\mathbb{K})$ tel que

$$\mathrm{A} = \Delta \mathrm{S}.$$

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 $(\Delta, \mathrm{S}) \in \mathscr{D} \times \mathrm{SL}_n(\mathbb{K})$ *tel 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 $A = \Delta S$ *et* $\det(S) = \det(\Delta)^{-1}\det(A) = 1$, *donc* $S \in \mathrm{SL}_n(\mathbb{K})$.
D'où l'existence.

Q20. Soit H un groupe **abélien** et

$$\varphi : \mathrm{GL}_n(\mathbb{K}) \to H$$

un morphisme de groupes.
Montrer qu'il existe

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

un morphisme de groupes tel que

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

Posons

$$\begin{aligned}\psi : \mathbb{K}^\times &\to H\\ a &\mapsto \varphi(\Delta_a).\end{aligned}$$

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* ***Q19****.*
Comme H *est abélien, on a* $D(H) = \{1\}$ *et par les questions* ***Q15*** *et* ***Q18*** *on a donc*

$$\forall S \in \mathrm{SL}_n(\mathbb{K}), \varphi(S) = 1.$$

Soit $A \in \mathrm{GL}_n(\mathbb{K})$.
L'analyse menée à la question ***Q19*** *montre qu'il existe* $S \in \mathrm{SL}_n(\mathbb{K})$ *tel que*

$$A = \Delta_{\det(A)} S$$

d'où

$$\varphi(A) = \varphi\big(\Delta_{\det(A)}\big)\varphi(S) = \psi(\det(A)) \times 1 = \psi(\det(A)).$$

Ainsi

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

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**

$$E = [\![0, p-1]\!] \times [\![0, q-1]\!],$$

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

$$L_i = \{i\} \times [\![0, q-1]\!] \quad \text{et} \quad C_j = [\![0, p-1]\!] \times \{j\}$$

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 $[\![0, N-1]\!]$.
Pour $(i,j) \in E$ on pose dans la suite

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

et

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

Q21. Montrer que ℓ, c et θ sont des numérotations de E.

- *La division euclidienne par* q *montre que tout* $k \in [\![0,N-1]\!]$ *s'écrit de manière unique* $k = qi + j$ *avec* $i \in [\![0, p-1]\!]$ *et* $j \in [\![0, q-1]\!]$ *:* ℓ *est bijective.*
- *De même la division euclidienne par* p *montre que tout* $k \in [\![0,N-1]\!]$ *s'écrit de manière unique* $k = i + pj$ *avec* $i \in [\![0, p-1]\!]$ *et* $j \in [\![0, q-1]\!]$ *:* c *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*

$$\begin{aligned}[\![0,N-1]\!] &\to E\\ k &\mapsto (k\%p, k\%q)\end{aligned}$$

est bijective. Or θ *est exactement sa bijection réciproque, d'où*

θ est bijective.

Q22. 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 à chacun des schémas (I), (II) et (III) celle des trois numérotations ℓ, c et θ qui le définit.

Tracer les trois numérotations correspondantes pour $p = 3$ et $q = 5$.

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

Q23. Montrer que pour tout $i \in [\![0, p-1]\!]$,

$$\big(\theta^{-1} \circ c\big)(\mathrm{L}_i) = \mathrm{L}_i$$

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

Soit $i \in [\![0, p-1]\!]$.

On a

$$c(\mathrm{L}_i) = \big\{i + pj, j \in [\![0, q-1]\!]\big\}.$$

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

$$\big(\theta^{-1} \circ c\big)(\mathrm{L}_i) = \mathrm{L}_i$$

et la permutation induite est

$$\begin{aligned} \mathrm{L}_i &\to \mathrm{L}_i \\ (i, j) &\mapsto (i, (i + pj)\%q) \end{aligned}$$

Q24. Montrer que

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

- ***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

  $$\begin{aligned} \rho_i : \mathrm{L}_i &\to \mathrm{L}_i \\ (i, j) &\mapsto (i, (i + pj)\%q). \end{aligned}$$

  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 **Q5** 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

  $$u_i : \mathrm{L}_i \to \mathbb{Z}/q\mathbb{Z}$$
  $$(i, j) \mapsto \overline{j}.$$

  Comme $\overline{(i+pj)\%q} = \overline{p}\overline{j} + \overline{i}$, on a

  $$u_i \circ \rho_i \circ u_i^{-1} = f_{\overline{p},\overline{i}}.$$

  Les permutations ρ_i et $f_{\overline{p},\overline{i}}$ ont donc des cycles de mêmes longueurs, et par conséquent la même signature.

  *Comme $p \neq q$ sont premiers on a $\overline{p} \in (\mathbb{Z}/q\mathbb{Z})^\times$, donc $f_{\overline{p},\overline{i}} \in \mathrm{GA}_1(\mathbb{Z}/q\mathbb{Z})$ et la question **Q13**, appliquée au nombre premier impair q, donne*

  $$\varepsilon(\rho_i) = \varepsilon\left(f_{\overline{p},\overline{i}}\right) = \left(\frac{p}{q}\right).$$

- ***Conclusion***

  On a donc

  $$\varepsilon(\rho) = \prod_{i=0}^{p-1} \varepsilon(\rho_i) = \left(\frac{p}{q}\right)^p = \left(\frac{p}{q}\right)$$

  *car p est **impair**.*

On admet qu'exactement le même raisonnement donne

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

Q25. Montrer que

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

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

- ***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 ***Q5*** *on en déduit*

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

Q26. En déduire la **loi de réciprocité quadratique** :

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

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 ***Q24*** *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 ***Q25*** *donne alors*

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

E. Frobenius-Zolotarev

Dans cette partie on fixe $n \geq 2$ et p un nombre premier impair. On cherche à généraliser la question **Q13** à $\mathrm{GA}_n(\mathbb{Z}/p\mathbb{Z})$.
Étant donnés $\mathrm{A} \in \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ et $\mathrm{B} \in (\mathbb{Z}/p\mathbb{Z})^n$, on note

$$\begin{aligned} f_{\mathrm{A,B}} : (\mathbb{Z}/p\mathbb{Z})^n &\to (\mathbb{Z}/p\mathbb{Z})^n \\ \mathrm{X} &\mapsto \mathrm{AX} + \mathrm{B} \end{aligned}$$

et on note

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

De même qu'à la question **Q12**, on montre que $\mathrm{GA}_n(\mathbb{Z}/p\mathbb{Z})$ est un sous-groupe de $\mathrm{S}\big((\mathbb{Z}/p\mathbb{Z})^n\big)$ (il n'est pas demandé de le démontrer).

Q27. Montrer que pour tout $\mathrm{B} \in (\mathbb{Z}/p\mathbb{Z})^n$,

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

Q28. Soient ζ un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$ et $\Delta_\zeta = \mathrm{diag}(\zeta, 1, \ldots, 1) \in \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$. Montrer que

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

Q29. Conclure que

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