Théorème Frobenius-Zolotarev

réf: Objectif Agrégation, p 51.

Théorème:

Soient p premier impair, $n \geq 1$ un entier. Alors on a:

$$\forall u \in GL_n(\mathbb{F}_p),\ \varepsilon(u) = \left(\frac{\det(u)}{p}\right).$$

Rappel:
- $\varepsilon(u)$ est la signature de u, vu comme une permutation de $\mathbb{F}_p^n$
- $\left(\frac{\cdot}{p}\right)$ correspond au symbole de legendre i.e: $\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ si } a=0 \\ 1 \text{ si } a \text{ est un carré de } \mathbb{F}_p \\ -1 \text{ sinon} \end{cases}$

Preuve:

Soit $u \in GL_n(\mathbb{F}_p)$ en particulier $u: \mathbb{F}_p^n \longrightarrow \mathbb{F}_p^n$ et est bijectif c'est bien une permutation, sa signature à donc un sens.

On va montrer que $\varepsilon = \left(\frac{\cdot}{p}\right) \circ \det$ est une factorisation de la signature.

Lemme 1:

Soit K un corps tel que $K \neq \mathbb{F}_2$ et $n \neq 2$. Soit M un groupe abélien et $\varphi: GL_n(K) \to M$ un morphisme de groupes alors il se factorise par le déterminant i.e il existe un unique morphisme de groupes $\delta: K^\times \to M$ tel que $\varphi = \delta \circ \det$.

Preuve:

Comme $K \neq \mathbb{F}_2$ et $n \neq 2$ on a $\mathcal{D}(GL_n(K)) = SL_n(K)$.

Or pour $x, y \in GL_n(K)$ on a $\varphi([x,y]) = [\varphi(x), \varphi(y)] = e$ car M abélien. Or $\mathcal{D}(GL_n(K)) = SL_n(K)$ est engendré par les commutateurs donc $SL_n(K) = \mathcal{D}(GL_n(K)) \subset \ker(\varphi)$.

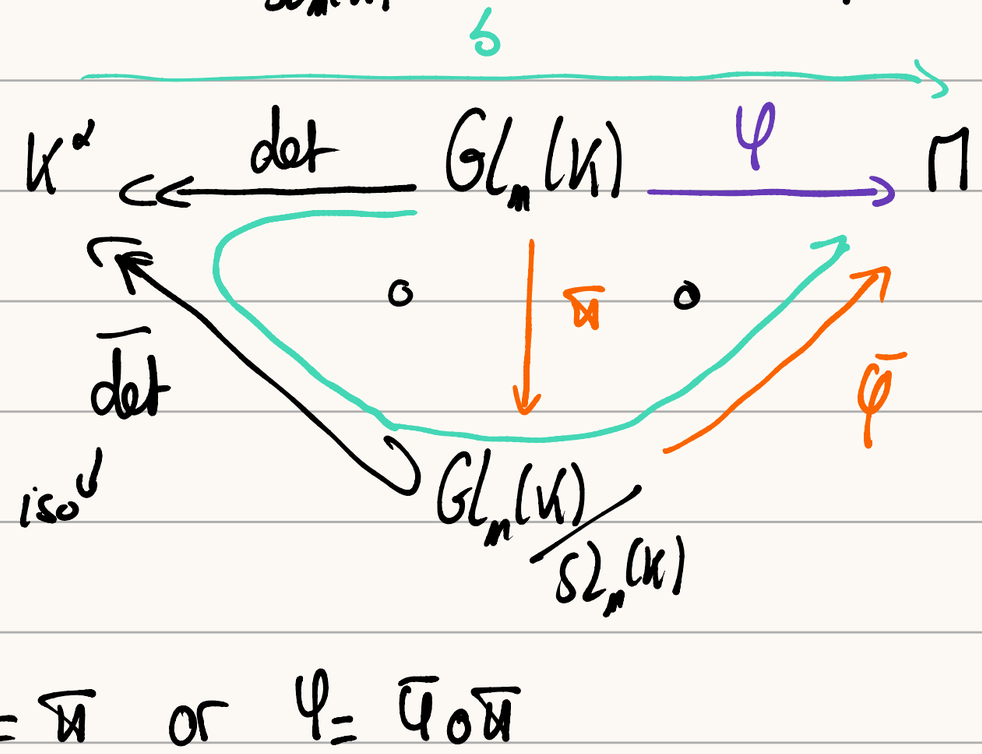
Ainsi φ se factorise:

$$\begin{array}{ccc} GL_n(K) & \xrightarrow{\varphi} & M \\ \pi \downarrow & \circ & \nearrow \bar{\varphi} \\ GL_n(K)/SL_n(K) & & \end{array} \qquad \text{i.e } \varphi = \bar{\varphi} \circ \pi.$$

Or $\det: GL_n(K) \longrightarrow K^\times$ est un morphisme surjectif de noyau $SL_n(K)$. On peut donc factoriser

$\det$ i.e il existe un unique $\overline{\det} : GL_n(K)/SL_n(K) \longrightarrow K^\times$ automorphisme tel que : $\det = \overline{\det} \circ \pi$.

On a donc :



Donc $(\overline{\det})^{-1} \circ \det = \pi$ or $\varphi = \bar{\varphi} \circ \pi$

donc $\varphi = \bar{\varphi} \circ (\overline{\det})^{-1} \circ \det$

donc $\varphi = b \circ \det$ où $b : K^\times \longrightarrow \Pi$ est un morphisme de groupe.

De plus $\det$ étant surjectif, b est unique.

☑

Lemme 2 :

Soit p un nombre premier impair, le symbole de Legendre est l'unique morphisme non trivial de $\mathbb{F}_p^\times$ dans $\{-1, 1\}$

Preuve :

Le symbol de Legendre est un morphisme de $\mathbb{F}_p^\times$ dans $\{-1, 1\}$ non trivial car il y a $\frac{p-1}{2}$ éléments qui ne sont pas des carrés.

Réciproquement soit $\alpha : \mathbb{F}_p^\times \longrightarrow \{-1, 1\}$ un morphisme non trivial.
Par le premier théorème d'isomorphisme :

$$[\mathbb{F}_p^\times : \operatorname{Ker}\alpha] = \#\operatorname{Im}\alpha = 2.$$

Ainsi $\operatorname{Ker}(\alpha)$ est un sous-groupe d'indice 2 de $\mathbb{F}_p^\times$.

Or $\mathbb{F}_p^\times$ est de cardinal $p-1$ donc pair et est cyclique, ainsi il existe un unique sous-groupe de $\mathbb{F}_p^\times$ d'indice 2 que l'on note H et donc $\operatorname{Ker}(\alpha) = H$.

On a alors la partition $\mathbb{F}_p^\times = H \sqcup gH$ avec $g \notin H$.

$$\text{et } \alpha(g) = \begin{cases} 1 \text{ si } g \in H = \operatorname{Ker}(\alpha) \\ -1 \text{ sinon} \end{cases}$$

Ainsi α est entièrement déterminé donc unique.

☑

On a que $\varepsilon : GL_n(\mathbb{F}_p) \longrightarrow \{-1,1\}$ qui est un morphisme de groupe.
Par le lemme 1, il existe $\delta : \mathbb{F}_p^\times \to \{-1,1\}$ un morphisme de groupe tel que :

$$\varepsilon = \delta \circ \det.$$

Il reste à montrer que $\delta = \left(\frac{\cdot}{p}\right)$ donc par le lemme 2 que δ n'est pas trivial.
Pour cela il suffit de trouver $u \in GL_n(\mathbb{F}_p)$ tel que :

$$\varepsilon(u) = \delta \circ \det(u) = -1.$$

On pose $q = p^n$ alors $\mathbb{F}_q$ et $\mathbb{F}_p^n$ sont isomorphes en tant que $\mathbb{F}_p$-espaces vectoriels.
Or $\mathbb{F}_q^\times$ est cyclique d'ordre $q-1$, soit g un générateur de ce groupe, on pose :

$$u : x \longmapsto gx \text{ qui est clairement } \mathbb{F}_p\text{-linéaire.}$$

u fixe 0 et agit comme le cycle $(g\ g^2 \dots g^{q-1})$ de longueur $q-1$ car $\mathbb{F}_q = \{0, g, \dots, g^{q-1}\}$.
Ainsi sa signature est :

$$\varepsilon(u) = (-1)^q = -1 \text{ car } (q = p^n \text{ est impair}).$$

D'où le résultat.

☑

Application :

1) Soit $u : \mathbb{F}_q \longrightarrow \mathbb{F}_q$, $x \longmapsto ax$ où $a \in \mathbb{F}_q \simeq \mathbb{F}_p^n$ alors $\det(u) = a$ donc $\varepsilon(u) = \left(\frac{a}{p}\right)$

2) Calcul de $\left(\frac{2}{p}\right)$. On pose $u : \mathbb{F}_p \longrightarrow \mathbb{F}_p$ de déterminant 2.

$x \longmapsto 2x$

On calcul sa signature :

x	0	1	2	$\dots$	$\frac{p-1}{2}$	$\frac{p+1}{2}$	$\dots$	$p-2$	$p-1$
$u(x)$	0	2	4		$p-1$	1		$p-4$	$p-2$

On calcul le nombre d'inversion, pour $k \geqslant \frac{p+1}{2}$ l'élément voit sa position relative à $p-k$ éléments inversée par u. Le nombre total d'inversions est alors :

$$\sum_{k=\frac{p+1}{2}}^{p-1} p-k = \sum_{j=1}^{\frac{p-1}{2}} j = \frac{\frac{p-1}{2}\,\frac{p+1}{2}}{2} = \frac{p^2-1}{8}$$

Ainsi, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. ☐

Théorème : p16 Rombaldi.

Soit $n \geq 2$ et $G = \langle a \rangle$ un groupe cyclique d'ordre n.

1 - Les sous-groupes de $G = \langle a \rangle$ sont tous cycliques d'ordre n

2 - Soit d positif tel que $d \mid n$, il existe un unique sous-groupe d'ordre d de G. Ce sous-groupe est le groupe cyclique $H = \langle a^{\frac{n}{d}} \rangle$. C'est également l'ensemble de tous les éléments d'ordre divisant d et les générateurs de H sont tous les éléments d'ordre d de G.

Preuve :

1 - Soit H un sous-groupe de G d'ordre d.

Le théorème de Lagrange nous dit que $d \mid n$ donc $n = qd \in \mathbb{N}^*$.

Pour tout élément $h = a^k \in H$ on a :

$$h^d = a^{kd} = 1$$

Ainsi, l'ordre de a étant n, on a : $n \mid kd$ i.e $\exists j \in \mathbb{N}$ tq $kd = jn = jqd$.

donc $k = jq$.

Ainsi $h = a^k = (a^q)^j$ donc $h \in \langle a^q \rangle$.

donc $H \subset \langle a^q \rangle$ et $d \mid |\langle a^q \rangle|$

Or $(a^q)^d = a^n = 1$ donc $|\langle a^q \rangle| \mid d$.

Ainsi $d = |\langle a^q \rangle|$ et donc $H = \langle a^q \rangle$.

Un sous-groupe d'ordre d de G, s'il en existe, est donc unique.

2 - Réciproquement, soient d un diviseur de n, $q = \frac{n}{d}$ et $H = \langle a^q \rangle$ le sous-groupe de G engendré par a^q.

Soit b l'ordre de H, on a $(a^q)^b = a^{qb} = 1$ donc $n \mid qb$.

donc $qb = kn = kqd$ $(\exists k \in \mathbb{N})$

donc $b = kd$.

donc $d \mid b$.

Or on a aussi $(a^q)^d = a^n = 1$ donc $b \mid d$ d'où $b = d$.

En conclusion $\langle a^q \rangle$ est l'unique sous-groupe d'ordre d de G.

Le théorème de Lagrange nous dit que tous les éléments de H ont un ordre qui divise d.
Réciproquement si $h = a^k \in G$ est d'ordre divisant d on a alors $h^d = a^{kd} = 1$ donc $n = qd \mid kd$.

donc $q \mid k$

Ainsi $k = qj$ donc $h = (a^q)^j \in \langle a^q \rangle = H$.
Le groupe H est donc l'ensemble de tous les éléments de G d'ordre divisant d. Les générateurs de H sont tous d'ordre d et réciproquement tout élément de G d'ordre d est dans H et l'engendre.

Rmq :

Un groupe commutatif fini d'ordre n est cyclique ssi pour tout $d \mid n$, il existe un unique sous-groupe d'ordre d de G.