Théorème de Frobenius Zolotarev

Leçon : 105, 106, 121, 123, 152

Réf : Objectif Agreg (lemme 2 et 3m), Perrin (lemme 1)

Lemme 1 On suppose que $(n,k) \neq (2, \mathbb{F}_2)$. Alors $\mathcal{D}(GL_n(k)) = SL_n(k)$.

Preuve On distingue les cas.

Si E est un k-ev de dimension n, alors clairement $\mathcal{D}(GL(E)) \subset SL(E)$

car si $g, h \in GL(E)$, $\det(ghg^{-1}h^{-1}) = \det([g,h]) = 1$.

Il suffit de prouver qu'une transvection u est un commutateur.

En effet, si $u = \underbrace{aba^{-1}b^{-1}}_{=[a,b]}$ avec $a, b \in GL(E)$, et si v est une autre transvection, u et v sont conjugués dans $GL(E)$, donc

$$v = gug^{-1}, \text{ avec } g \in GL(E).$$

Ainsi : $$v = gug^{-1} = gaba^{-1}b^{-1}g^{-1} = (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) = [gag^{-1}, gbg^{-1}].$$

Ainsi, comme les transvections engendrent $SL(E)$, on aurait $SL(E) \subset \mathcal{D}(GL(E))$.

→ Si $n \geq 3$ et $\mathrm{car}(k) \neq 2$

alors $u^2 \neq Id$ $\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \right)$

car $(k) \neq 2$, donc si u est transvection alors $u^2 \neq Id$, donc u^2 est aussi une transvection.

Or $n \geq 3$, donc u et u^2 sont conjugués dans $SL(E)$:

Il existe $s \in SL(E)$ tq $u^2 = sus^{-1} \Rightarrow u = sus^{-1}u^{-1}$
$\Rightarrow u \in \mathcal{D}(SL(E))$

on peut juste prendre $s \in GL(E)$, prendre $s \in SL(E)$ valable pour $\mathcal{D}(SL(E))$

et a fortiori, $u \in \mathcal{D}(GL(E))$.

→ Si $n = 2$ et $|k| \geq 4$, ie $k \neq (\mathbb{F}_2, \mathbb{F}_3)$.

On pose $t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $s = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ avec $\lambda \neq \pm 1, 0$ (possible car $|k| > 3$).

On a $\tau = sts^{-1}t^{-1} = \begin{pmatrix} \lambda & \lambda \\ 0 & \lambda^{-1} \end{pmatrix} \begin{pmatrix} \cdots \end{pmatrix} = \begin{pmatrix} 1 & \lambda^2 - 1 \\ 0 & 1 \end{pmatrix}$ → une transvection !

Pour $n>2$: m̂ méthode en prolongeant les matrices par des matrices identités

$\to$ Si $k=\mathbb{F}_2,\mathbb{F}_3$, $n\geq 3$,

$$u=\begin{pmatrix}1&0&1\\0&1&-1\\0&0&1\end{pmatrix},\ t=\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix},\ s=\begin{pmatrix}0&-1&0\\1&0&0\\0&0&1\end{pmatrix}$$

on a $u=tst^{-1}s^{-1}$, $s,t\in SL(E)$ et u est une transvection.

$\to$ Si $k=\mathbb{F}_3$, $n=2$

$$t=\begin{pmatrix}1&1\\0&1\end{pmatrix},\ s=\begin{pmatrix}1&0\\0&-1\end{pmatrix},\ \text{on a } sts^{-1}t^{-1}=t.$$

□

Lemme 2 Soient k un corps, $n\in\mathbb{N}^*$ et Π un groupe abélien. Alors tout morphisme de groupes $\varphi: GL_n(k)\to\Pi$ se factorise par le déterminant : il existe un unique morphisme de groupes $\delta: k^\times\to\Pi$ tel que
$$\varphi=\delta\circ\det. \qquad (\text{avec } (k,n)\neq(\mathbb{F}_2,2))$$

<u>Preuve</u>

$(k,n)\neq(\mathbb{F}_2,2)$, donc par le lemme 1, $\mathcal{D}(GL_n(k))=SL_n(k)$.

De plus il est clair que $\mathcal{D}(GL_n(k))\subset\operatorname{Ker}\varphi$, car Π est abélien

$(\varphi([x,y])=[\varphi(x),\varphi(y)]\underset{\Pi\text{ abélien}}{=}0)$

Ainsi il existe un unique morphisme $\bar\varphi : GL_n(k)/\mathcal{D}(GL_n(k))\to\Pi$

tel que le diagramme
$$\begin{tikzcd} GL_n(k) \arrow[r, "\varphi"] \arrow[d, two heads, "\pi"'] & \Pi \\ GL_n(k)/\mathcal{D}(GL_n(k)) = GL_n(k)/SL_n(k) \arrow[ur, "\bar\varphi"'] & \end{tikzcd}$$
commute.

Or $\det: GL_n(k)\twoheadrightarrow k^\times$ est un morphisme surjectif dont le noyau est $SL_n(k)$, on a donc le diagramme commutatif suivant :
$$\begin{tikzcd} GL_n(k) \arrow[r, two heads, "\det"] \arrow[dr, two heads, "\pi"'] & k^\times \\ & GL_n(k)/SL_n(k) \arrow[u, "\overline{\det}"'] \end{tikzcd}$$

L'application $\overline{\det}: GL_n(k)/SL_n(k)\xrightarrow{\sim}k^\times$ est de plus un isomorphisme.

Ainsi : $\varphi=\bar\varphi\circ\pi=\bar\varphi\circ\overline{\det}^{-1}\circ\underbrace{\overline{\det}\circ\pi}_{=\det}$, donc en posant $\delta=\bar\varphi\circ\overline{\det}^{-1}$,

on a $\boxed{\varphi=\delta\circ\det}$.

□

Théorème 3 Soient p un nombre premier ≥ 3, et V un $\mathbb{F}_p$-ev de dimension finie. Alors pour tout $u \in GL(V)$, on a

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

où ε est la signature de $u \in GL(V) \hookrightarrow \mathfrak{S}(V)$.

Preuve

$\varepsilon : GL(V) \to \{-1, 1\}$ est un morphisme de groupes, (si $n := \dim V$, $GL(V) \simeq GL_n(\mathbb{F}_p)$)

donc par le lemme 2 il existe $\delta : \mathbb{F}_p^\times \to \{-1, 1\}$ tel que $\varepsilon = \delta \circ \det$.

On veut montrer que $\delta = L : \mathbb{F}_p^\times \to \{-1, 1\}$

$$x \mapsto \left(\frac{x}{p}\right) = \begin{cases} 1 & \text{si } x \text{ est un carré mod } p \\ -1 & \text{sinon} \end{cases}$$

Rappel: Si p 1er impair, et $a \in \mathbb{Z}$, $\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a \equiv 0 \,[p] \\ 1 & \text{si } a \text{ est un carré mod } p \\ -1 & \text{sinon} \end{cases}$

On $\mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ donc il est cyclique. Ainsi, si g est un générateur de $\mathbb{F}_p^\times$, tout morphisme $\alpha : \mathbb{F}_p^\times \to \{\pm 1\}$ est uniquement déterminé par $\alpha(g)$.

Si $\alpha(g) = 1$, le morphisme est trivial. Nous allons voir qu'il existe un unique morphisme non-trivial: L, le symbole de Legendre.

- L est non trivial, il existe des éléments qui ne sont pas des carrés : il y en a même $\frac{q-1}{2}$ $\left[\begin{array}{l} (x \in \mathbb{F}_q^\times \text{ est un carré} \iff x^{\frac{q-1}{2}} = 1) \\ |\mathbb{F}_q^2| = \left|\frac{q+1}{2}\right| , \ |\mathbb{F}_q^{\times 2}| = \left|\frac{q-1}{2}\right| \end{array} \right]$

- Soit $\alpha : \mathbb{F}_p^\times \to \{\pm 1\}$ un morphisme non trivial. Alors $\operatorname{Ker}\alpha$ un sg d'indice 2 de $\mathbb{F}_p^\times$ (car $\underbrace{\{\pm 1\}}_{\alpha \text{ non trivial}} = \operatorname{Im}\alpha \simeq \mathbb{F}_p^\times / \operatorname{Ker}\alpha$).

  Or $\mathbb{F}_p^\times$ est cyclique, donc il existe un unique sg d'indice 2, que l'on note H. Ainsi, si $x \notin H$, on a la partition $\mathbb{F}_p^\times = H \sqcup xH$

  et $\alpha(g) = \begin{cases} 1 & \text{si } g \in H \\ -1 & \text{si } g \in xH \end{cases}$ $\to$ α est entièrement déterminé (x et H ne dépendent pas de α)

donc il y a un unique morphisme non trivial : 1.

Revenons à la preuve. Il suffit de montrer que δ n'est pas trivial, donc qu'il existe $u \in GL(V)$ tel que $\varepsilon(u) = \delta \circ \det(u) = -1$.

On note $n = \dim V$. Alors le corps $\mathbb{F}_q$, où $q = p^n$ est une extension de corps de $\mathbb{F}_p$ de degré n.

V et $\mathbb{F}_q$ sont isomorphes en tant que $\mathbb{F}_p$-espaces vectoriels.

Il faut donc trouver une bijection $\mathbb{F}_p$-linéaire de signature -1.

Or $\mathbb{F}_q^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z}$ est cyclique d'ordre $q-1$. Soit g un générateur.

Alors $\mathbb{F}_q = \{0, g, \dots, g^{q-1}\}$.

Ainsi la permutation $x \mapsto gx$ de $\mathbb{F}_q$ fixe 0 et agit comme le cycle $(g\, g^2 \dots g^{q-1})$, donc la signature de cette permutation est $(-1)^{q-1-1} = 1$ car $q = p^n$ est impair, elle est aussi clairement $\mathbb{F}_p$-linéaire

$\square$

Application ? Calcul de $\left(\frac{2}{p}\right)$. (pas dans le rdf, à connaître).

On pose $u : \mathbb{F}_p \to \mathbb{F}_p$, $x \mapsto 2x$. Donc $\det(u) = 2$.

Ainsi $\left(\frac{2}{p}\right) = \varepsilon(u)$. On construit un tableau.

x	0	1	2	$\dots$	$\frac{p-1}{2}$	$\frac{p+1}{2}$	$\frac{p+3}{2}$	$\dots$	$p-2$	$p-1$
$u(x)$	0	2	4	$\dots$	$p-1$	1	3	$\dots$	$p-4$	$p-2$

On cherche le nombre d'inversions.

inversion de 1 : $(1, \frac{p+1}{2})$

——— 2 : $(2, \frac{p+1}{2}), (2, \frac{p+3}{2})$

——— 3 : $(3, \frac{p+1}{2}), (3, \frac{p+3}{2}), (3, \frac{p+5}{2})$

...

$\hookrightarrow = (i, j)$, $i < j$, $\sigma(i) > \sigma(j)$

jusqu'à $\frac{p-1}{2}$ (qui a décalé de $\frac{p-1}{2}$).

$$\mathrm{Inv}(u) = \sum_{i=1}^{\frac{p-1}{2}} i = \frac{\frac{p-1}{2} \times \frac{p+1}{2}}{2} = \frac{p^2-1}{8}$$

$$\Rightarrow \left[\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \right]$$

autre app : signature de Frobenius, $\varepsilon(\varphi) = (-1)^{\frac{1}{2}((n+1)(p-1))}$