Obj. Agreg

Théorème de Frobenius - Zolotarev

103, 105, 106, 108, 123, 152

<u>Théorème</u> : Soient $n \in \mathbb{N}^*$, p premier impair.

$$\forall u \in GL_n(\mathbb{F}_p). \quad \varepsilon(u) = \left(\frac{\det u}{p}\right) \quad \text{où} \quad \left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a \equiv 0\,[p] \\ 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p \\ -1 & \text{sinon.} \end{cases}$$

<u>Lemme</u> : Soient K un corps, M un groupe abélien, $n \neq 2$, $K \neq \mathbb{F}_2$.
Tout morphisme de groupes $\varphi : GL_n(K) \to M$ se factorise par le déterminant.
$\exists!\, \delta : K^\times \to M$, $\varphi = \delta \circ \det$.

$D(GL_n(K)) = SL_n(K)$.
$\forall x, y \in GL_n(K)$, $\varphi([x,y]) = [\varphi(x), \varphi(y)] = 0$ car M abélien, donc $D(GL_n(K)) \subset \ker \varphi$
Donc $\exists!\, \bar{\varphi} : GL_n(K)/SL_n(K) \to M$ morphisme surjectif.
D'autre part, $\det : GL_n(K) \to K^\times$ est surjectif de noyau $SL_n(K)$
donc $\exists!\, \overline{\det} : GL_n(K)/SL_n(K) \to K^\times$ isomorphisme.
De là, $\varphi = \delta \circ \det$ avec $\delta = \bar{\varphi} \circ (\overline{\det})^{-1}$
unique car det surjectif.

$$\begin{tikzcd} K^\times & GL_n(K) \arrow[l, "\det"'] \arrow[r, "\varphi"] \arrow[d, "\pi"] & M \\ & GL_n(K)/SL_n(K) \arrow[ul, bend left, "\overline{\det}"] \arrow[ur, bend right, "\bar{\varphi}"'] & \end{tikzcd}$$

Ici, $\exists!\, \delta : \mathbb{F}_p^\times \to \{\pm 1\}$, $\varepsilon = \delta \circ \det$.

<u>Lemme</u> : le symbole de Legendre est l'unique morphisme de groupes non trivial de $\mathbb{F}_p^\times$ dans $\{\pm 1\}$.

$\forall a \in \mathbb{F}_p^*$, $a^{p-1} \equiv 1\,[p]$ par Fermat donc $a^{\frac{p-1}{2}} \equiv \pm 1\,[p]$
Or $\varphi : \mathbb{F}_p^* \to \mathbb{F}_p^*$, $x \mapsto x^2$ a $\{\pm 1\}$ pour noyau, donc il y a $\frac{p-1}{2}$ carrés dans $\mathbb{F}_p^*$.
Donc : si $a \in \mathbb{F}_p^{*2}$, alors $a^{\frac{p-1}{2}} \equiv 1\,[p]$ et sinon, $a^{\frac{p-1}{2}} \equiv -1\,[p]$
i.e. $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\,[p]$.
Le symbole de Legendre est donc un morphisme non trivial de $\mathbb{F}_p^\times \to \{\pm 1\}$.
. Si $\alpha : \mathbb{F}_p^\times \to \{\pm 1\}$ non trivial, alors $H = \ker \alpha$ est l'unique (car $2 \mid p-1$ et $\mathbb{F}_p^\times$ cyclique) ss-gpe d'indice 2 de $\mathbb{F}_p^\times$: $\mathbb{F}_p^\times = H \sqcup xH$ où $x \notin H$
et $\alpha(y) = \begin{cases} 1 & \text{si } y \in H \\ -1 & \text{sinon} \end{cases}$: α entièrement déterminé.

La signature $\varepsilon : GL_n(\mathbb{F}_p) \to \{\pm 1\}$ est un morphisme de groupes donc par lemme, $\exists \delta$, $\varepsilon = \delta \circ \det$, avec δ morphisme de groupes $\mathbb{F}_p^\times \to \{\pm 1\}$.
Soit $q = p^n$. Vus comme $\mathbb{F}_p$-ev, $\mathbb{F}_q$ et $\mathbb{F}_p^n$ sont isomorphes
De plus, $\mathbb{F}_q^\times$ cyclique donc si $\langle g \rangle = \mathbb{F}_q^\times$, la permutation $x \mapsto gx$ (fixe 0 et $\mathbb{F}_p$-linéaire) peut être vue comme le cycle $(g, g^2, \dots, g^{q-1})$ de signature $(-1)^q = -1$ car q impair.
... trivial, i.e. $\delta = \left(\frac{\cdot}{p}\right)$