

Prop Soit $n \in \mathbb{N}^+$, $p \in \mathbb{P}$, $p \geq 3$
 Soit $u \in GL_n(\mathbb{F}_p) \cong GL(\mathbb{F}_p^n)$
 Alors $u \in S(\mathbb{F}_p^n) \subseteq G_{\mathbb{F}_p}$ et
 $\varepsilon(u) = \left(\frac{\det(u)}{p} \right)$

Pg ε ne dépend pas de l'identification.

$S(\mathbb{F}_p^n) \cong G_{\mathbb{F}_p}$
 Notons $q = p^n$, et $\begin{matrix} \downarrow b_1 \\ \mathbb{F}_p^n \end{matrix} \xrightarrow{\sim} [1, q]$
 $\downarrow b_2 \quad \mathbb{F}_p^n \xrightarrow{\sim} [1, q]$

$$\begin{array}{ccc} [1, q] & \xleftarrow{b_2} \mathbb{F}_p^n & \xrightarrow{b_1} [1, q] \\ \downarrow u & \downarrow u & \downarrow u_2 \\ [1, q] & \xleftarrow{b_2} \mathbb{F}_p^n & \xrightarrow{b_1} [1, q] \end{array}$$

Alors $\mu_1 = B^{-1} \circ \mu_2 \circ B$
 où $B = b_2 \circ b_1^{-1} \in S_q$.

lemme $D(GL_n(\mathbb{F}_p)) = SL_n(\mathbb{F}_p)$.

En effet:

* $SL_n(\mathbb{F}_p) = \langle \text{transvections} \rangle$
 (pivot de Gauss)

* les transvections ont toutes conjuguées dans $GL_n(\mathbb{F}_p)$.

Exemple $T_{12}(1) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{matrix} e_1 \\ e_2 \\ e_3 \end{matrix}$
 $\sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{matrix} e_3 \\ e_1 \\ e_2 \end{matrix}$

* Toute transvection est un commutateur.
 $S \ A = T_{ij}(1), A^2 = T_{ij}(2)$
 où $i \neq j$ car $p \geq 2$

donc $A^2 = B^{-1} A B$ et $A = A^{-1} B^{-1} A B$.

Autre: $SL_n(\mathbb{F}_p) \subseteq D(GL_n(\mathbb{F}_p))$
 $D(GL_n(\mathbb{F}_p)) \subseteq SL_n(\mathbb{F}_p)$
 Car $\det(ab^{-1}b) = 1$.

Preuve de la proposition:

$$\begin{array}{ccc} GL_n(\mathbb{F}_p) & \xrightarrow{\varepsilon} & \{\pm 1\} \subseteq \mathbb{F}_p^* \\ \downarrow \pi & \nearrow \varepsilon & \\ GL_n(\mathbb{F}_p)^{ab} & & \end{array}$$

$GL_n(\mathbb{F}_p)^{ab} = GL_n(\mathbb{F}_p) / D(GL_n(\mathbb{F}_p)) = D(GL_n(\mathbb{F}_p))$ Car $\mathbb{F}_p^*$ est abélien.

$$\begin{array}{ccc} GL_n(\mathbb{F}_p) & \xrightarrow{\det} & \mathbb{F}_p^* \\ \downarrow \pi & \nearrow \det & \\ GL_n(\mathbb{F}_p)^{ab} & & \end{array}$$

Or $D(GL_n) = \ker \det$

d'où $\varepsilon = \overline{\det} \circ \pi$
 $\det = \det \pi$
 $\boxed{\varepsilon = \delta \det}$ où $\delta = \overline{\det} \circ \det^{-1}$
 * un morphisme $\mathbb{F}_p^* \rightarrow \{\pm 1\}$

Or $\mathbb{F}_p^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$ donc δ est déterminé par $\delta(g)$ où $\langle g \rangle = \mathbb{F}_p^*$.

Or: $\left(\frac{\cdot}{p} \right)$ est un morphisme non trivial de $\mathbb{F}_p^* \rightarrow \{\pm 1\}$.

But: Montrer que δ est non trivial.

$\Leftrightarrow$ Suffit de montrer que ε est non trivial.

On a $\mathbb{F}_p^n \cong \mathbb{F}_q$ en tant que $\mathbb{F}_p$ -v.
 d'où $GL(\mathbb{F}_p^n) \cong GL(\mathbb{F}_q)$
 groupes

Soit g un générateur de $\mathbb{F}_q^*$
 cyclotome - Landau
 $\mu: \mathbb{F}_q \rightarrow \mathbb{F}_q$
 $n \mapsto g^n$

$\mathbb{F}_p$ -linéaire et de cyclope $x \mapsto g^x$.

Alors $\mu = (1, g, g^2, \dots, g^{q-2})$

car $\mu(0) = 0$, d'où:
 $\varepsilon(\mu) = (-1)^{(q-1)+1}$
 $= (-1)^q$
 impair

$\varepsilon(\mu) = -1 \neq 1$. $\square$

Application $p \neq 2$, $\left(\frac{2}{p} \right) = (-1)^{\frac{p-1}{2}}$

On considère $\mu: \mathbb{F}_p \rightarrow \mathbb{F}_p$
 $n \mapsto 2n$
 $\det(\mu) = 2$ d'où

$\left(\frac{2}{p} \right) = \varepsilon(\mu)$. Comparons les matrices

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

Preuve: i, j sur la première ligne.
 $Hy =$ une relation $i \leq \frac{p-1}{2}$.

appel v et $y =$ nombre in
 $j \leq \frac{p-1}{2} + 1$

d'où $\sum_{i=1}^{p-1} i = \frac{(p-1)(p-2)}{2} = \frac{p^2-1}{8}$
 d'où $\dots$

Prop Soit $n \in \mathbb{N}^*$, $p \in \mathbb{P}$, $p \geq 3$
 Soit $u \in GL(\mathbb{F}_p^n) \cong GL(\mathbb{F}_p^n)$
 Alors $u \in S(\mathbb{F}_p^n) \cong G_{p^n}$ et
 $\Sigma(u) = \left(\frac{\det(u)}{p} \right)$.

Rq Σ ne dépend pas de l'identification.

$S(\mathbb{F}_p^n) \cong G_{p^n}$
 Notons $q = p^n$, et $\begin{cases} b_1: \mathbb{F}_p^n \xrightarrow{\sim} [1, q] \\ b_2: \mathbb{F}_p^n \xrightarrow{\sim} [1, q] \end{cases}$

$$\begin{array}{ccccc} [1, q] & \xleftarrow{b_2} & \mathbb{F}_p^n & \xrightarrow{b_1} & [1, q] \\ \downarrow u_1 & & \downarrow u & & \downarrow u_2 \\ [1, q] & \xleftarrow{b_2} & \mathbb{F}_p^n & \xrightarrow{b_1} & [1, q] \end{array}$$

Alors $u_1 = B^{-1} \circ u_2 \circ B$
 où $B = b_2 \circ b_1^{-1} \in S_q$.

Lemme $D(GL_n(\mathbb{F}_p)) = SL_n(\mathbb{F}_p)$.

En effet:

* $SL_n(\mathbb{F}_p) = \langle \text{transvections} \rangle$
 (pivot de Gauss)

* des transvections sont toutes conjuguées dans $GL_n(\mathbb{F}_p)$.

Exemple: $T_{12}(1) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{matrix} e_1 \\ e_2 \\ e_3 \end{matrix}$

$$\sim \begin{array}{ccc|c} 1 & 0 & 0 & e_3 \\ 0 & 1 & 1 & e_1 \\ 0 & 0 & 1 & e_2 \end{array}$$

* Toute transvection est un commutateur.
 S: $A = T_{ij}(1)$, $A^2 = T_{ij}(2)$
 $\neq 0$ car $p \neq 2$

d'où $A^2 = B^{-1}AB$ et $A = A^{-1}B^{-1}AB$.

Alors $SL_n(\mathbb{F}_p) \leq D(GL_n(\mathbb{F}_p))$.

$$D(GL_n(\mathbb{F}_p)) \leq SL_n(\mathbb{F}_p),$$

Ceci conclut.

$$\text{car } \det(ab^{-1}b^{-1}) = 1.$$

Preuve de la proposition:

$$\begin{array}{ccc} GL_n(\mathbb{F}_p) & \xrightarrow{\Sigma} & \{ \pm 1 \} \subseteq \mathbb{F}_p^* \\ \pi \downarrow & \nearrow \bar{\Sigma} & \\ GL_n(\mathbb{F}_p)^{ab} & = & GL_n(\mathbb{F}_p) / SL_n(\mathbb{F}_p) \\ & = & D(GL_n(\mathbb{F}_p)) \end{array}$$

Car $\mathbb{F}_p^*$ est abélien.

$$\text{et } GL_n(\mathbb{F}_p) \xrightarrow{\det} \mathbb{F}_p^*$$

$$\begin{array}{ccc} GL_n(\mathbb{F}_p) & & \\ \pi \downarrow & \nearrow \det & \\ GL_n(\mathbb{F}_p)^{ab} & & \end{array}$$

Car $DGL_n = \ker \det$.

$$\text{d'où } \Sigma = \bar{\Sigma} \text{ et } \det = \det.$$

$$\Sigma = \delta \det$$

est un morphisme.

On $\mathbb{F}_p^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$
 défini par $\delta(g)$

On: $\left(\frac{\cdot}{p} \right)$ est un morphisme de $\mathbb{F}_p^*$ vers $\mathbb{Z}/(p-1)\mathbb{Z}$.

But montrer que Σ

est suffisant de montrer que Σ est non triviale!

$$\begin{aligned} \pi(\mathbb{F}_p) &\subseteq \mathrm{DGL}_n(\mathbb{F}_p) \\ \pi(\mathbb{F}_p) &\subseteq \mathrm{SL}_n(\mathbb{F}_p), \\ \text{car } \det(ab^{-1}b^{-1}) &= 1. \end{aligned}$$

proposition:

$$\begin{array}{ccc} \pi(\mathbb{F}_p) & \xrightarrow{\varepsilon} & \{\pm 1\} \subseteq \mathbb{F}_p^* \\ & \nearrow \bar{\varepsilon} & \end{array}$$

$$\begin{array}{ccc} \pi(\mathbb{F}_p) & \xrightarrow{\det} & \mathbb{F}_p^* \\ & \nearrow \bar{\det} & \end{array}$$

$$\pi(\mathbb{F}_p) \xrightarrow{\det} \mathbb{F}_p^*$$

$$\pi(\mathbb{F}_p) \xrightarrow{\det} \mathbb{F}_p^*$$

$$\mathrm{DGL}_n = \ker \det$$

$$\begin{aligned} \text{donc: } \varepsilon &= \bar{\varepsilon} \pi \\ \det &= \det \pi \end{aligned}$$

$$\boxed{\varepsilon = \delta \det} \text{ où } \delta = \bar{\varepsilon} \circ \det^{-1}$$

est un morphisme $\mathbb{F}_p^* \rightarrow \{\pm 1\}$

On $\mathbb{F}_p^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$ donc δ est déterminé par $\delta(g)$ où $\langle g \rangle = \mathbb{F}_p^*$.

On: $\left(\frac{\cdot}{p}\right)$ est un morphisme non trivial de $\mathbb{F}_p^* \rightarrow \{\pm 1\}$.

But montrer que δ est non trivial.

Il suffit de montrer que ε est non trivial.

On a $\mathbb{F}_p^* \cong \mathbb{F}_q^*$ en tant que $\mathbb{F}_p$ -v

donc $\mathrm{GL}(\mathbb{F}_p^n) \cong \mathrm{GL}(\mathbb{F}_q^n)$
groupes

Soit g un générateur de $\mathbb{F}_q^*$

cyclique - condition:

$$\begin{aligned} m: \mathbb{F}_q &\rightarrow \mathbb{F}_q \\ n &\mapsto g^n, \end{aligned}$$

$\mathbb{F}_p$ -linéaire et de l'éprouve $n \mapsto g^{-1}n$.

$$\text{Alors } m = (1, g, g^2, \dots, g^{q-2})$$

car $m(0) = 0$, donc:

$$\begin{aligned} \varepsilon(m) &= (-1)^{(q-1)+1} \\ &= (-1)^q \\ &\quad \text{impair} \end{aligned}$$

$$\varepsilon(m) = -1 \neq 1.$$

□

$$\text{Application } p \neq 2, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

On considère $m: \mathbb{F}_p \rightarrow \mathbb{F}_p$
 $n \mapsto 2n$

$$\det(m) = 2 \text{ donc}$$

$$\left(\frac{2}{p}\right) = \varepsilon(m) \text{ - Comptons les inversions.}$$

i	0	1	2	...	$\frac{p-1}{2}$	$\frac{p+1}{2}$	...	$p-2$	$p-1$
$2n$	0	2	4		$p-1$	1		$p-4$	$p-2$

Prendre $i < j$ sur la première ligne.

Il y a inversion seulement si $i \leq \frac{p-1}{2}$,

car si $i > \frac{p-1}{2}$ et $j < \frac{p-1}{2} + 1$

$$j < \frac{p-1}{2} + 1$$

$$\text{donc } \sum_{i=1}^{\frac{p-1}{2}} i = \frac{\frac{p-1}{2} \cdot \frac{p+1}{2}}{2} = \frac{p^2-1}{8}$$

Inversions -