

Théorème : Soit  $p$  nombre premier impair et  $n \in \mathbb{N}^*$  alors on a

$$\left[ \forall \nu \in GL_n(\mathbb{F}_q) = GL(\mathbb{F}_q^n), \quad \varepsilon(\nu) = \left( \frac{\det(\nu)}{p} \right) : \text{symbole de Legendre} \right.$$

Remarque :  $\varepsilon$  désigne la signature de  $\nu$ ,  $\nu$  comme permutation de  $\mathbb{F}_q^n$  : ensemble fini.  
 Il s'agit de montrer que  $\varepsilon$  se factorise  $\left( \frac{\cdot}{p} \right) \circ \det$ .

On commence par un lemme de factorisation :

Lemme 1 : Soit  $K$  un corps et  $\Gamma$  un groupe abélien,  $t_1 K \neq \mathbb{F}_2$  ou  $n \neq 2$   
 $n \in \mathbb{N}^*$

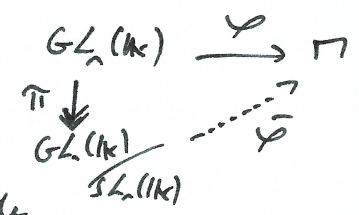
Alors tout  $\Psi : GL_n(K) \rightarrow \Gamma$  morphisme se factorise via  $\det$ .  
 i.e.  $\forall \Psi \in \text{Hom}_{\text{groupe}}(GL_n(K), \Gamma), \exists ! \delta \in \text{Hom}_{\text{groupe}}(K^\times, \Gamma) \text{ t.q. } \Psi = \delta \circ \det$

Preuve : notons que comme  $K \neq \mathbb{F}_2$  ou  $n \neq 2$ , on a  $D(GL_n(K)) = SL_n(K)$  (\*).

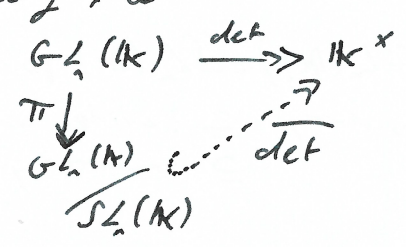
D'autre part, si  $(x, y) \in GL_n(K)$ ,  $\Psi((x, y)) = [\Psi(x), \Psi(y)] = 1_\Gamma$  car  $\Gamma$  abélien et  
 comme  $D(GL_n(K))$  est engendré par les commutateurs,  $SL_n(K) \subseteq \text{Ker}(\Psi)$ .

Donc  $\Psi : GL_n(K) \rightarrow \Gamma$  se factorise de façon unique

en  $\bar{\Psi} : \frac{GL_n(K)}{SL_n(K)} \rightarrow \Gamma$  t.q.  $\Psi = \bar{\Psi} \circ \pi$

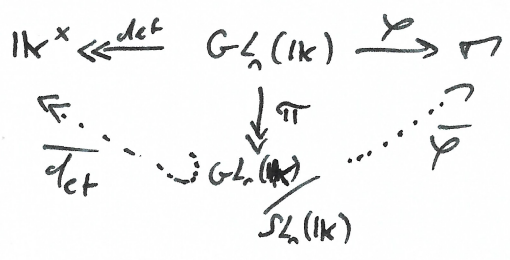


De plus  $\det : GL_n(K) \rightarrow K^\times$  est un morphisme surjectif, de  
 noyau  $SL_n(K)$ , d'où le diagramme commutatif



et  $\bar{\det}$  est un isomorphisme.

On peut résumer par le diagramme suivant



et donc

$$\begin{aligned} \Psi &= \bar{\Psi} \circ (\bar{\det}^{-1}) \circ \det \circ \pi \\ &= \underbrace{\bar{\Psi} \circ \bar{\det}^{-1}}_{=\delta} \circ \det \end{aligned}$$

La surjectivité de  $\det$  assure l'existence de la factorisation  $\det = \bar{\det} \circ \pi$  et aussi celle de  $\Psi = \delta \circ \det$ .

Lemme 2 : Soit  $p$  premier impair,  $\left( \frac{\cdot}{p} \right)$  est le seul morphisme non trivial de  $\mathbb{F}_p^\times \rightarrow \{-1, 1\}$ .

Preuve :  $\left( \frac{\cdot}{p} \right)$  est bien un morphisme non trivial de  $\mathbb{F}_p^\times \rightarrow \{-1, 1\}$  car  $\forall x \in \mathbb{F}_p^\times$ ,  
 $x^2 = (-x)^2$  et donc  $\left| \mathbb{F}_p^\times \rightarrow \mathbb{F}_p^\times \right.$  n'est pas injective ( $p \geq 3$ ), donc pas surjective  
 donc  $\exists x \in \mathbb{F}_p^\times$  t.q.  $\left( \frac{x}{p} \right) \neq 1$ . (□)

Réciproquement, si  $\alpha \in \text{Hom}_{\text{groupe}}(\mathbb{F}_p^x, \{-1, 1\})$  est non trivial,  $\text{Ker}(\alpha)$  est un sous-groupe d'indice 2 de  $\mathbb{F}_p^x$ . Or  $\mathbb{F}_p^x$  est cyclique d'ordre  $p-1$ : par conséquent il existe un unique sous-groupe  $H$  d'indice 2 de  $\mathbb{F}_p^x$  et on a  $\mathbb{F}_p^x = H \cup xH$  où  $x \notin H$  où  $\alpha(y) = \begin{cases} 1 & \text{si } y \in H \\ -1 & \text{sinon} \end{cases}$

( $\Delta$ )

Ainsi  $\alpha$  est entièrement déterminé par  $H$ , donc il existe un unique morphisme non trivial.

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

On passe à la preuve de la thèse:

On montre que  $\varepsilon : GL_n(\mathbb{F}_p) \rightarrow \{-1, 1\}$  n'est pas trivial.

En effet,  $\mathbb{F}_q := \mathbb{F}_{p^n} / \mathbb{F}_p$  est une extension de degré  $n$  de  $\mathbb{F}_p$ , isomorphe à  $(\mathbb{F}_p)^n$  vu

comme  $\mathbb{F}_p$  e.v. Il suffit de trouver une bijection de  $\mathbb{F}_q$  de signature  $-1$ .

Comme  $\mathbb{F}_q^x$  est cyclique d'ordre  $q-1$ ,  $\exists g \in \mathbb{F}_q^x$  t.q.  $\langle g \rangle = \mathbb{F}_q^x$  (vu comme groupe).

Alors  $x \mapsto gx$  est une bijection de  $\mathbb{F}_q$  qui correspond sur  $\mathbb{F}_q^x$  au  $(q-1)$ -cycle

$(g, \dots, g^{q-1})$  de signature  $(-1)^q = -1$  car  $q = p^n$  est impair

$\rightarrow \varepsilon$  est non trivial.

De plus, le lemme 1 fournit un unique morphisme  $\delta : \mathbb{F}_p^x \rightarrow \{-1, 1\}$  t.q.

$\varepsilon = \delta \circ \det$  comme  $\varepsilon$  et  $\det$  sont non triviaux,  $\delta$  est un morphisme

non trivial (lemme 2) et donc  $\delta = \left(\frac{\cdot}{p}\right)$  d'où finalement  $\varepsilon = \left(\frac{\det \cdot}{p}\right)$

Proposition 1 :

(\*) :  $D(GL_n(K)) = SL_n(K)$  pour  $(K, n) \neq (\mathbb{F}_2, 2) \rightarrow$  Perrin

$\hookrightarrow$  pas dur,  $\subseteq$  : évidente

$\supseteq$  : montrer que toute transvection est un commutateur (elles sont toutes conjuguées)

(II) :  $\left(\frac{\cdot}{p}\right)$  est un morphisme : si  $p$  est un entier premier impair

$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$  dans  $\mathbb{F}_p$

$\rightarrow \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

( $\Delta$ ) : Plus généralement : si  $G = \langle x \rangle$  est d'ordre  $n$ , alors  $\forall d | n$ ,  $\exists ! H < G$  t.q.  $|H| = d$  et  $H = \langle x^k \rangle$  où  $k = \frac{n}{d}$ . (Joseph cohen, III, 2.14)

En effet :  $\pi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$  projection,  $\bar{\varphi} : \mathbb{Z}/n\mathbb{Z} \rightarrow G$  est un isomorphisme donc tout

sous-groupe de  $G$  est l'image par  $\bar{\varphi}$  d'un sous-groupe de  $\mathbb{Z}/n\mathbb{Z}$  mais l'unique sous-groupe de  $\mathbb{Z}/n\mathbb{Z}$  d'ordre  $d | n$  est  $\mathbb{Z}/d\mathbb{Z}$ , engendré par  $\pi(x^{\frac{n}{d}})$

donc  $G$  admet un sous-groupe d'ordre  $d$ , unique, engendré par  $\bar{\varphi}(\pi(x^{\frac{n}{d}}))$ .

(objectif agrég)