Leçons : 105 , 108.

Th de Frobenius - Zolotarev

Énoncés : • lemme 1 : K de caractéristique $\neq 2$, $n \geq 1$. Alors $D(GL_n(K)) = SL_n(K)$.

• lemme 2 : p premier impair. Le symbole de Legendre $\left(\frac{\cdot}{p}\right)$ est l'unique morphisme $\mathbb{F}_p^* \to \{-1,1\}$ non trivial.

• th : p premier impair, $n \geq 1$. Pour $u \in GL(\mathbb{F}_p^n) \subset \mathfrak{S}(\mathbb{F}_p^n)$, la signature de u vu comme permutation est $\varepsilon(u) = \left(\frac{\det u}{p}\right)$.

⊛ Lemme 1.

$\boxed{\subset}$ Les commutateurs ont déterminant 1 donc sont dans $SL_n(K)$.

$\boxed{\supset}$ $SL_n(K)$ est engendré par les transvections : il suffit de prouver qu'une transvection peut s'écrire comme un commutateur. Pour $i \neq j$ ds $[\![1,n]\!]$ et $\lambda \in K$ on note $T_{i,j}(\lambda)$ la transvection $I_n + \lambda E_{i,j}$.

On rappelle que pour $i \neq j$ et $\lambda, \mu \in K$, $T_{i,j}(\lambda) T_{i,j}(\mu) = T_{i,j}(\lambda + \mu)$. En particulier $T_{i,j}(\lambda)^{-1} = T_{i,j}(-\lambda)$.

On note $D_i(\mu) = \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & \mu & & \\ & & & 1 & \\ & & & & 1 \end{bmatrix} \leftarrow \text{pos. } i$ pour $\mu \in K^*$.

Calculons : $[D_i(2), T_{i,j}(\lambda)] = D_i(2) \cdot T_{i,j}(\lambda) \cdot D_i(2^{-1}) \cdot T_{i,j}(-\lambda)$

$$= \left(\begin{array}{c} \begin{array}{cccccc} & & \text{pos } i & \text{pos } j & \\ & & \downarrow & \downarrow & \end{array} \\ \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 2 & 2\lambda & \\ & & & 1 & \\ & & & & 1 \end{bmatrix} \leftarrow \text{pos } i \end{array} \right) \cdot D_i(2^{-1}) \cdot T_{i,j}(-\lambda)$$

car multiplier à gauche par $D_i(\mu)$ multiplie la i^e ligne par μ

$$= T_{i,j}(2\lambda) \cdot T_{i,j}(-\lambda)$$

car multiplier à droite par $D_i(\mu)$ multiplie la i^e colonne par μ

$$= T_{i,j}(\lambda).$$

□

⊛ Lemme 2.

$\mathbb{F}_p^*$ est cyclique : soit α un générateur. Alors les morphismes $\varphi : \mathbb{F}_p^* \to \{-1,1\}$ sont caractérisés par $\varphi(\alpha)$; il y en a deux possibles (-1 et 1) donc il y a au plus deux morphismes $\mathbb{F}_p^* \to \{-1,1\}$. Comme 1 et $\left(\frac{\cdot}{p}\right)$ en sont deux distincts le lemme est montré. □

⊛ Th.

• On note ε la restriction du morphisme signature à $GL(\mathbb{F}_p^n)$, qui est un sg de $\mathfrak{S}(\mathbb{F}_p^n)$. ε est à valeurs dans un groupe abélien donc $D(GL(\mathbb{F}_p^n)) \subset \operatorname{Ker} \varepsilon$, cad d'après le lemme 1 $SL(\mathbb{F}_p^n) \subset \operatorname{Ker} \varepsilon$. On peut donc factoriser $\varepsilon = \bar{\varepsilon} \circ \pi$ avec $\bar{\varepsilon} : GL(\mathbb{F}_p^n)/SL(\mathbb{F}_p^n) \to \{-1,1\}$ et $\pi : GL(\mathbb{F}_p^n) \to GL(\mathbb{F}_p^n)/SL(\mathbb{F}_p^n)$ la proj canonique.

On a aussi $SL(\mathbb{F}_p^n) = \operatorname{Ker} \det$ où $\det : GL(\mathbb{F}_p^n) \to \mathbb{F}_p^*$ est surjectif : on factorise $\det = \overline{\det} \circ \pi$ avec $\overline{\det} : GL(\mathbb{F}_p^n)/SL(\mathbb{F}_p^n) \to \mathbb{F}_p^*$ qui est un isomorphisme.

$$\begin{tikzcd}
\mathbb{F}_p^* & GL(\mathbb{F}_p^n) \arrow[l, "\det"'] \arrow[r, "\varepsilon"] \arrow[d, "\pi"] & \{-1,1\} \\
& GL(\mathbb{F}_p^n)/SL(\mathbb{F}_p^n) \arrow[ul, dashed, "\overline{\det}"] \arrow[ur, dashed, "\overline{\varepsilon}"'] &
\end{tikzcd}$$

On peut alors écrire : $\varepsilon = \overline{\varepsilon} \circ \pi = \overline{\varepsilon} \circ \overline{\det}^{-1} \circ \det$.

- Reste à mq $\overline{\varepsilon} \circ \overline{\det}^{-1} = \left(\frac{\cdot}{p}\right)$. C'est un morphisme $\mathbb{F}_p^* \to \{-1,1\}$ donc d'après le lemme 2 il suffit de mq il n'est pas trivial, et par la factorisation $\varepsilon = (\overline{\varepsilon} \circ \overline{\det}^{-1}) \circ \det$ il suffit de mq ε n'est pas trivial.

  On note $q = p^n$: alors $\mathbb{F}_p^n \simeq \mathbb{F}_q$ et $GL(\mathbb{F}_p^n) \simeq GL(\mathbb{F}_q)$, et on cherche $u \in GL(\mathbb{F}_q)$ tq $\varepsilon(u) = -1$. $\mathbb{F}_q^*$ est cyclique : soit α un générateur. On pose $u = (x \mapsto \alpha x) \in GL(\mathbb{F}_q)$: on peut réécrire $u = (1\ \alpha\ \alpha^2\ \dots\ \alpha^{q-2})$ comme un cycle de longueur $q-1$. Alors $\varepsilon(u) = (-1)^{q-1-1} = (-1)^q = -1$ car q est, comme p, impair. $\square$

Réf : • Beck – Objectif agrégation : exo 5.4, p 251 (sauf lemme 1).
• Gourdon – Algèbre : p 156 (lemme 1).
• Rombaldi : p 432 (réf alternative).

↳ On admet que $\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^* \to \{-1,1\}$ est un morphisme non trivial. Cela découle d'une part du fait que $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)$ pour $a \in \mathbb{F}_p$, et d'autre part de la non surjectivité du morphisme $\begin{cases} \mathbb{F}_p^* \to \mathbb{F}_p^* \\ x \mapsto x^2 \end{cases}$, qui a un noyau non trivial.

↳ Le lemme 1 n'est pas fait dans Obj. agreg mais le livre renvoie à Perrin ou Gourdon. Gourdon ne le fait pas pareil qu'ici, mais même idée avec les transvections.