L'oral à l'agreg - Isenmann (p.203)

Théorème de Frobenius-Zolotarev

105 106 108 120 121 123

Définition : Une matrice de dilatation de $GL_n(\mathbb{K})$ est de la forme $\begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 & \\ & & & \lambda \end{pmatrix}$ avec $\lambda \in \mathbb{K}^*$ (dans une certaine base).
Soit H hyperplan de E et G son supplémentaire i.e. $E = H \oplus G$. La dilatation f de base H, direction G et rapport $\lambda \in \mathbb{K}^*$ est telle que :
$\forall h, u \in H \times G, \ f(h+u) = h + \lambda u$

Théorème : Soit $\mathbb{K}$ d'au moins 3 éléments.
Alors les dilatations engendrent $GL(V)$

Lemme : (1) L'application $\varphi : \begin{array}{l} \mathbb{F}_p^* \to \{\pm 1\} \\ a \mapsto \left(\frac{a}{p}\right) \end{array}$ est un morphisme de groupes.
(2) Soit p premier impair.
Alors : il y a $\frac{p+1}{2}$ carrés et $\frac{p-1}{2}$ non-carrés dans $\mathbb{F}_p$.

Théorème : Soit $\mathbb{K}$ corps fini
Alors il existe $a \in \mathbb{K}^*$ tel que $\mathbb{K}^* = \langle a \rangle$

Théorème (de Frobenius - Zolotarev) :
Soit p premier impair et V un $\mathbb{F}_p$ espace vectoriel de dimension n.
Alors : pour tout $u \in GL(V)$, $\varepsilon(u) = \left(\frac{\det(u)}{p}\right)$

Preuve :

oral

L'idée pour montrer ce théorème est de :
① Montrer qu'il suffit de montrer l'égalité pour les dilatations uniquement.
② Montrer que pour toute dilatation f, $\left(\frac{\det(f)}{p}\right) = -1$
③ Montrer que l'on peut assimiler les dilatations à des permutations et montrer que $\varepsilon(f) = -1$
④ Conclure pour tout $u \in GL(V)$ par structure de morphismes de ε, $\det$ et φ.

① Soit $\mathbb{K} = \mathbb{F}_p$ et $a \in \mathbb{K}^*$ tel que $\mathbb{K}^* = \langle a \rangle$ (par le théorème).
Toutes les dilatations sont des puissances d'une dilatation de rapport a.

En effet, soit $\lambda \in \mathbb{K}^*$, H hyperplan et G supplémentaire de H tq : $E = H \oplus G$.
Soit f, g dilatations de base H, direction G et rapports λ, a respectivement, et $k \in \mathbb{N}$ tq : $\lambda = a^k$.
Ainsi, $\forall h, u \in H \times G$, $f(h+u) = h + \lambda u = h + a^k u = g^k(h+u)$
Puisque les dilatations engendrent $GL(V)$, il suffit de montrer le résultat pour les dilatations de rapport a. Ops f dilatation de rapport a.

② Montrons $\left(\frac{\det(f)}{p}\right) = -1$.
Supposons par l'absurde que $\left(\frac{\det(f)}{p}\right) = 1$
i.e. $\left(\frac{a}{p}\right) = 1$. Or : $\mathbb{K}^* = \langle a \rangle$ donc $\forall x \in \mathbb{K}^*$, $\left(\frac{x}{p}\right) = 1$
ABSURDE puisqu'il y a des non-carrés dans $\mathbb{K}$.

③ On remarque qu'en oubliant toute structure sur V, on peut l'assimiler à un ensemble de cardinal p^n et alors assimiler $f : V \to V$ à une permutation $\begin{pmatrix} h & x & x^2 & \cdots & x^{p-2} \\ \downarrow & \downarrow & \downarrow & & \downarrow \\ h & f(x) = x^2 & x^3 & & x \end{pmatrix} \in S_{p^n}$

Puisque les orbites de V sous l'action de f, donnée par $\begin{array}{l} \langle f \rangle \times V \to V \\ (f^k ; x) \mapsto f^k(x) \end{array}$, forme une partition de V, il suffit d'étudier ces orbites.

- Soit $h \in H$. $Orb(h) = \{h\}$
Ainsi $|Orb(h)| = 1$ et alors elle compte pour un signe $+$ dans $\varepsilon(f)$.
- Soit $x = h + u \in V$ avec $h, u \in H \times G \setminus \{0\}$
Montrons que $Orb(x) = \{x ; \dots ; f^{p-2}(x)\}$.
Par petit théorème de Fermat, $a^{p-1} = 1$ et alors $f^{p-1}(x) = x$ d'où : $Orb(x) \subseteq \{x ; \dots ; f^{p-2}(x)\}$.
Par ailleurs, supposons par l'absurde qu'il existe $1 \leq i < j < p$ tels que $f^i(x) = f^j(x)$.
Ainsi, $h + a^i u = h + a^j u$ i.e. $a^{j-i}\underbrace{(a^i - 1)}_{\neq 0}\underbrace{u}_{\neq 0} = 0$
donc $a^{j-i} = 0$ i.e. $a = 0$
ABSURDE
Ainsi, $Orb(x) = \{x ; \dots ; f^{p-2}(x)\}$ et puisque $|Orb(x)| = p-1$, $Orb(x)$ définit un cycle de longueur $p-1$ qui compte pour un signe $-$ dans $\varepsilon(f)$

Ainsi, le nombre d'orbites de cardinal $(p-1)$ est l'ensemble des éléments de la forme : $h + u$ avec $h \in H$, $u \in G \setminus \{0\}$ de cardinal $p^{n-1}(p-1)$
Il y en a alors p^{n-1} qui est impair et donc $\varepsilon(f) = -1$.

Preuves résultats utilisés

Lemme : (1) $\varphi : \begin{array}{l} \mathbb{F}_p^\times \to \{\pm 1\} \\ a \mapsto \left(\frac{a}{p}\right) \end{array}$ est un morphisme de groupes.

(2) Il y a $\frac{p+1}{2}$ carrés et $\frac{p-1}{2}$ non-carrés dans $\mathbb{F}_p$.

Preuve :

(1) Soit $a, b \in \mathbb{F}_p^\times$.

$\varphi(ab) = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} [p] = \varphi(a)\varphi(b) [p]$

(2) Soit $f : \begin{array}{l} \mathbb{F}_p^\times \to \mathbb{F}_p^\times \\ x \mapsto x^2 \end{array}$ morphisme avec :

$\ker(f) = \{x^2 - 1 = 0 \mid x \in \mathbb{F}_p^\times\}$

$= \{x \in \mathbb{F}_p^\times \mid (x+1)(x-1) = 0\}$

$= \{\pm 1\}$ (par intégrité du corps $\mathbb{F}_p$)

Par premier théorème d'isomorphisme,

$\mathbb{F}_p^\times / \{\pm 1\} \simeq \mathrm{Im}(f)$ donc $|\mathrm{Im}(f)| = \frac{p-1}{2}$

et alors $|\mathbb{F}_p^\times \setminus \mathrm{Im}(f)| = \frac{p-1}{2}$.

Ainsi, en comptant 0, il y a $\frac{p+1}{2}$ carrés dans $\mathbb{F}_p$ et $\frac{p-1}{2}$ non-carrés dans $\mathbb{F}_p$.

Théorème : Soit $\mathbb{K}$ à au moins 3 éléments

Alors : $GL(E)$ est engendré par les dilatations

Preuve :

Puisque de manière générale, $GL(E)$ est engendré par les transvections et les dilatations, il suffit de montrer que toute transvection peut s'écrire comme produit de dilatations.

Soit τ transvection de $GL(E)$.

- Si $\tau = id$, alors ok
- Si $\tau = \tau_{\varphi,a} \neq id$ avec $\varphi \in E^* \setminus \{0\}$, $a \in \ker(\varphi) \setminus \{0\}$,

pour toutes dilatations δ_{φ_1, a_1}, δ_{φ_2, a_2} avec $\varphi_k \in E^* \setminus \{0\}$, $a_k \notin \ker(\varphi_k)$, l'égalité $\tau_{\varphi,a} = \delta_{\varphi_1,a_1} \circ \delta_{\varphi_2,a_2}$ s'écrit : $\forall x \in E$, $x + \varphi(x) a = \delta_{\varphi_1,a_1}(x + \varphi_2(x) a_2)$

$$= x + \varphi_2(x) a_2 + \varphi_1(x + \varphi_2(x) a_2) a_1$$

En prenant φ_1, φ_2 telles que $\varphi_1(a) \neq 0$ et $\varphi_2(a) \neq 0$, $a_1 = a_2 = a$, on a : $\varphi(x) a = [\varphi_2(x) + \varphi_1(x + \varphi_2(x) a)] a$

Soit $\varphi(x) = \varphi_1(x) + \varphi_2(x)(1 + \varphi_1(a))$

Soit alors $\varphi_1 \in E^* \setminus \{0\}$ telle que $\varphi_1(a) = 1 \notin \{-1; 0\}$ (licite car $\exists a \in \mathbb{K} \setminus \{0; -1\}$) et $\varphi_2 \in E^* \setminus \{0\}$ telle que :

$\varphi_2(x) = \dfrac{\varphi(x) - \varphi_1(x)}{2}$ (on a : $\varphi_2(a) = \dfrac{\varphi(a) - \varphi_1(a)}{2} = -\frac{1}{2} \neq 0$)

Ainsi, $\tau_{\varphi,a} = \delta_{\varphi_1,a_1} \circ \delta_{\varphi_2,a_2}$.

Théorème : Soit $\mathbb{K}$ corps fini :

Alors : $\mathbb{K}^*$ est cyclique i.e. $\exists a \in \mathbb{K}^* \mid \mathbb{K}^* = \langle a \rangle$

Preuve :

Soit G sous-groupe d'ordre n de $\mathbb{K}^*$.

Montrons que G est cyclique.

Puisque G est abélien, $\exists g_0 \in G \mid \mathrm{ord}(g_0) = m \leq n$ tel que : $m = \mathrm{PPCM}(\{\mathrm{ord}(g) \mid g \in G\})$.

Puisque $\forall g \in G$, $\mathrm{ord}(g) \mid m$, alors tous les éléments de G sont racines de $X^m - 1$.

On a alors n racines distinctes d'un polynôme à au plus m racines donc $n \leq m$.

Ainsi, $m = n$ et alors G a un élément d'ordre n donc G est cyclique.

Temps
15' 26"