Développement: Théorème de Frobenius-Zolotarev

Adrien Fontaine

4 avril 2013

Référence : Objectif Agrégation

Théorème 1

Soit $p \geq 3$ un nombre premier et V un $\mathbb{F}_p$ espace vectoriel de dimension finie. Alors, tout $u \in GL(V)$ est une permutation de V dont on note $\varepsilon(u)$ la signature. Le théorème de Frobenius-Zolotarev affirme que

$$\varepsilon(u) = \left(\frac{det(u)}{p}\right)$$

où $(\frac{\cdot}{p})$ désigne le symbole de Legendre ($(\frac{x}{p}) = 1$ si x est un carré dans $\mathbb{F}_p$ et -1 sinon).

Démonstration : On sait que la restriction de ε à $GL(V)$ est un morphisme de groupes à valeurs dans $\{-1, 1\}$. Montrons le lemme suivant :

Lemme 1

Tout morphisme de $GL(V) \to \{-1, 1\}$ se factorise de manière unique par le déterminant.

Démonstration : Soit Φ un morphisme de $GL(V)$ dans $\{-1, 1\}$. Comme $p \geq 3$, le groupe dérivé de $GL(V)$ est $SL(V)$. Ainsi, on a $\Phi(SL(V)) = 1$. En effet, soit $v \in SL(V) = D(GL(V))$. v s'écrit par définition du groupe dérivé, sous la forme $v = v_1...v_n$ où les v_i sont des commutateurs (*i.e* de la forme $v_i = f_i g_i f_i^{-1} g_i^{-1}$). Par conséquent, $\Phi(v_i) = \Phi(f_i)\Phi(g_i)\Phi(f_i)^{-1}\Phi(g_i)^{-1}$. Comme $\mathbb{Z}/2\mathbb{Z}$ est commutatif, on a $\Phi(v_i) = 1$ et donc $\Phi(v) = 1$. Donc, $SL(V) \subset Ker(\Phi)$.
$SL(V) = D(GL(V))$ donc $SL(V)$ est distingué dans $GL(V)$. Notons Π la surjection canonique de $GL(V)$ dans $SL(V)$. D'après le premier théorème d'isomorphisme, il existe un morphisme $\overline{\Phi} : Gl(V)/SL(V) \to \mathbb{Z}/2\mathbb{Z}$ tel que $\Phi = \overline{\Phi} \circ \Pi$.
Il s'agit maintenant d'exprimer Π en fonction du déterminant. On sait que le noyau du déterminant est (par définition) $SL(V)$. *det* étant un morphisme surjectif de $GL(V)$ dans $\mathbb{F}_p^*$, on a, toujours d'après le premier théorème d'isomorphisme, l'existence d'un isomorphisme $f : GL(V)/SL(V) \to \mathbb{F}_p^*$ tel que $det = f \circ \Pi$. Et f étant un isomorphisme, on a donc $\Pi = f^{-1} \circ \Pi$.
En conclusion, on a donc $\Phi = (\overline{\Phi} \circ f^{-1}) \circ det$. En posant, $g = \overline{\Phi} \circ f^{-1}$, on a donc montré l'existence d'un $g : \mathbb{F}_p^* \to \mathbb{Z}/2\mathbb{Z}$ tel que $\Phi = g \circ det$, *i.e* qui factorise Φ par le déterminant.
Prouvons maintenant l'unicité de g. On a $\Phi = g \circ det$. Soit g' tel que $\Phi = g' \circ det$. Soit $x \in \mathbb{F}_p^*$. Par surjectivité du déterminant, il existe $a \in GL(V)$ tel que $x = det(a)$. Alors, $g(x) = g \circ det(a) = \Phi(a) = g' \circ det(a) = g'(x)$. ■

Le lemme que l'on vient de démontrer nous permet d'affirmer l'existence d'un unique morphisme $g : \mathbb{F}_p^* \to \mathbb{Z}/2\mathbb{Z}$ tel que $\varepsilon = g \circ det$. Le lemme suivant nous permet de voir que g est soit le morphisme trivial, soit le symbole de Legendre.

Lemme 2

Soit $p \geq 3$ un nombre premier. Le symbole de Legendre $(\frac{\cdot}{p}) : \mathbb{F}_p^* \to \{-1, 1\}$ est l'unique morphisme non trivial de $\mathbb{F}_p^*$ dans $\{-1, 1\}$.

Démonstration : $\mathbb{F}_p^*$ est cyclique. Soit α un générateur de $\mathbb{F}_p^*$. Alors, un morphisme $\sigma : \mathbb{F}_p^* \to \{-1, 1\}$ est entièrement déterminé par $\sigma(\alpha)$. On a alors deux cas :

- Si $\sigma(\alpha) = 1$, alors $\forall x \in \mathbb{F}_p^*, \sigma(x) = 1$ et donc σ est le morphisme trivial.
- Si $\sigma(\alpha) = -1$, alors pour tout $x \in \mathbb{F}_p^*$, $\sigma(x) = 1$, si, et seulement si, x est une puissance paire de α. Or, les puissances paires de α sont exactement les carrés de $\mathbb{F}_p^*$, et donc σ est le symbole de Legendre. ■

Il reste maintenant à voir que g est non trivial, et on aura alors montré que g est le symbole de Legendre. Si g était trivial, alors on aurait pour tout $u \in GL(V)$, $\varepsilon(u) = g(det(u)) = 1$. Il s'agit donc d'exhiber un élément $u \in GL(V)$ tel que $\varepsilon(u) = -1$.
Notons d la dimension de V en tant que $\mathbb{F}_p$ espace vectoriel. Alors, si $q = p^d$, V et $\mathbb{F}_q$ sont isomorphes en tant que $\mathbb{F}_p$ espaces vectoriels. Il suffit donc de trouver une bijection de $\mathbb{F}_q$ qui soit $\mathbb{F}_p$ linéaire et de signature -1. Soit β un générateur du groupe multiplicatif $\mathbb{F}_q^*$. La multiplication par β est clairement une bijection $\mathbb{F}_p$-linéaire. Par ailleurs, elle est égale au cycle $(\beta, \beta^2, ..., \beta^{q-1})$ qui est de taille $q - 1$, et donc de signature $(-1)^q = -1$.
g est donc le symbole de Legendre et donc :

$$\forall u \in GL(V), \varepsilon(u) = \left(\frac{det(u)}{p}\right)$$

■