

Théorème de Frobenius-Zolotarev

Pierre Lissy

April 17, 2010

Lemme 1. *Soit k un corps et M un groupe abélien. On suppose que $k \neq \mathbb{F}_2$ ou que $n \neq 2$. Alors tout morphisme $\varphi : GL_n(k) \rightarrow M$ se factorise de manière unique par le déterminant.*

Proof. Le groupe dérivé de $GL_n(k)$ est dans ce cas $SL_n(k)$ tout entier. Donc on peut factoriser par le groupe dérivé pour obtenir un unique morphisme $\bar{\varphi} : GL_n(k)/SL_n(k) \rightarrow M$. Mais $\det$ est un morphisme de $GL_n(k)$ dans k^* dont le noyau est $SL_n(k)$, on peut donc le factoriser de manière unique en un morphisme $\bar{\det}$. De plus, ce morphisme est en fait un isomorphisme. Donc $\varphi = \bar{\varphi}\pi = \varphi\bar{\det}^{-1}\det\pi = \delta\det$. De plus, le morphisme δ est unique par surjectivité du déterminant: si pour tout A , $\delta(\det(A)) = \delta'(\det(A))$, alors pour tout élément de k^* on a $\delta(x) = \delta'(x)$, ie $\delta = \delta'$. $\square$

Lemme 2. *Soit p un nombre premier supérieur ou égal à 3. Alors le symbole de Legendre est l'unique morphisme non trivial de $\mathbb{F}_p^*$ dans $\{-1, 1\}$.*

Proof. Le symbole de Legendre n'est pas trivial car il y a toujours des éléments qui ne sont pas des carrés (il y en a même $(p-1)/2$). Réciproquement, considérons un morphisme non trivial de $\mathbb{F}_p^*$ dans $\{-1, 1\}$. Alors ce morphisme est nécessairement surjectif, ce qui entraîne que $\text{Ker}(\alpha)$ est un sous-groupe d'indice deux de $\mathbb{F}_p^*$. Mais on sait que $\mathbb{F}_p^*$ est un groupe cyclique. Il admet donc un unique sous-groupe de cardinal $(p-1)/2$, qui est son unique groupe d'indice 2, noté H . Or on connaît un groupe d'indice 2: le groupe des carrés, c'est donc celui-là. On a alors une partition de notre groupe en xH et H , avec $\alpha(x) = -1$ et $\alpha(h) = 1$ pour tout h dans H . Ainsi, α est entièrement défini et ne peut valoir que le symbole de Legendre. $\square$

Théorème 1 (Frobenius-Zolotarev). *On considère $u \in GL(V)$ où V est un $\mathbb{F}_p$ -ev. Alors u est une permutation de V et $\varepsilon(u)$ est le symbole de Legendre du déterminant de u dans $\mathbb{F}_p$.*

Proof. u est une bijection de l'ensemble fini V sur lui-même. On peut donc considérer u comme une permutation de V . On peut donc considérer la signature de u restreinte à $GL(V)$. C'est un morphisme du groupe $GL(V)$ dans le groupe commutatif $\{-1, 1\}$. D'après la première question, on peut le factoriser de manière unique δ de $\mathbb{F}_p^*$ et $\{-1, 1\}$ tel que $\delta\det = \varepsilon$. Il faut donc montrer que ce morphisme ne peut être que le symbole de Legendre. D'après la question 2, il suffit de montrer pour cela que ce morphisme δ est non trivial, autrement dit il suffit d'exhiber une matrice u telle que $\delta(\det(u)) = -1$. Appelons d la dimension de V . Alors comme il existe une extension de $\mathbb{F}_p$ de degré p , qui est isomorphe à V . Il suffit donc de trouver une bijection linéaire de $\mathbb{F}_q$ de signature -1 . Mais le groupe multiplicatif de $\mathbb{F}_q$ est cyclique. Considérons un générateur de ce groupe. On considère le morphisme $x \mapsto gx$. C'est une application clairement linéaire. De plus, cette application est bijective, fixe 0 et agit comme le cycle $(g, g^2, \dots, g^{q-1})$, de longueur $q-1$. C'est donc un morphisme de signature $(-1)^q = -1$ car q est impair. $\square$