

Signature et déterminant

Nouvelle rédaction

Février 2004

La démonstration qui suit peut être proposée comme développement dans plusieurs leçons :

- corps finis ;
- groupe symétrique ;
- déterminant ;
- arithmétique.

Elle avait un certain succès il y a quelques années.

Théorème (Frobenius-Zolotarev) *Soient \mathbb{F}_p le corps fini à p éléments, où $p \geq 3$, et V un espace vectoriel sur \mathbb{F}_p de dimension finie. Alors, pour tout $u \in \mathbf{GL}(V)$, on a*

$$\text{signature}(u) = \left(\frac{\det(u)}{p} \right).$$

La démonstration repose sur les deux propriétés suivantes qui seront démontrées plus bas.

1. *Pour tout homomorphisme $\alpha : \mathbf{GL}(V) \rightarrow A$, où A est un groupe commutatif, il existe un unique homomorphisme de groupes $f : \mathbb{F}_p^\times \rightarrow A$ tel que $\alpha = f \circ \det$*

2. *Il existe un automorphisme u de V de signature -1 .*

D'après la propriété 1, il existe un unique homomorphisme de groupes $f : \mathbb{F}_p^\times \rightarrow \{\pm 1\}$ rendant commutatif le carré suivant :

$$\begin{array}{ccc} \mathbf{GL}(V) & \subset & \mathfrak{S}_V \\ \det \downarrow & & \downarrow \text{signature} \\ \mathbb{F}_p^\times & \xrightarrow{f} & \{\pm 1\} \end{array}$$

Il s'agit de montrer que f est le symbole de Legendre. Or, ce dernier est caractérisé par la propriété suivante : c'est l'unique homomorphisme $\mathbb{F}_p^\times \rightarrow \{\pm 1\}$ qui envoie un générateur du groupe cyclique \mathbb{F}_p^\times sur -1 ; en effet, être ou non un carré dans \mathbb{F}_p^\times équivaut à être une puissance paire, ou bien impaire, de ce générateur. Or, d'après la propriété 2, il existe $u \in \mathbf{GL}(V)$ tel que

$$-1 = \varepsilon(u) = f(\det(u)).$$

Cela implique que f n'est pas l'homomorphisme trivial (qui envoie tous les éléments sur 1), et donc que l'image d'un générateur est -1 .

Montrons la propriété 1. Par définition de $\mathbf{SL}(V)$, le déterminant induit un isomorphisme de groupes

$$\mathbf{GL}(V)/\mathbf{SL}(V) \xrightarrow{\cong} \mathbb{F}_p^\times.$$

Il s'agit donc de vérifier que pour tout homomorphisme de groupes $\alpha : \mathbf{GL}(V) \rightarrow A$, où A est un groupe abélien, on a $\alpha(\mathbf{SL}(V)) = 1$. Si $\dim(V) = 0$, alors $\mathbf{GL}(V) = 1$; si $\dim(V) = 1$, alors $\mathbf{GL}(V) = \mathbb{F}_p^\times$, $\det = \text{id}$, donc $\mathbf{SL}(V) = 1$. Si $\dim(V) \geq 2$ (et si $p \geq 3$) alors c'est une conséquence de ce que le groupe dérivé de $\mathbf{GL}(V)$ est égal $\mathbf{SL}(V)$ (Perrin, ch. IV, § 3). À cet endroit Perrin est moins clair que d'habitude, peut-être parce qu'il veut démontrer du même mouvement l'assertion analogue pour $\mathbf{SL}(V)$. Reprenons donc l'argument. Tout d'abord, $\mathbf{SL}(V)$ est engendré par les transvections, c'est-à-dire par les automorphismes u de V tels que $u - 1$ soit de rang 1 et de

carré nul (2.11). Comme deux transvections sont représentables par la *même* matrice sur des bases convenables (2.2, 6)), elles sont conjuguées dans $\mathbf{GL}(V)$ (2.17). Soit u une transvection. La relation $(u - 1)^2 = 0$ s'écrit aussi $u^2 - 1 = 2(u - 1)$; cela montre déjà que $u^2 - 1$ est de carré nul; mais comme 2 est inversible dans le corps \mathbb{F}_p ($p \geq 3$), $u^2 - 1$ est de rang 1, donc u^2 est une transvection; ainsi, il existe $v \in \mathbf{GL}(V)$ tel que $u^2 = vuv^{-1}$, d'où $u = vuv^{-1}u^{-1}$, ce qui implique bien $\alpha(u) = 1$.

Il reste finalement à vérifier la propriété 2. Elle provient de deux résultats centraux de la théorie des corps finis. Tout d'abord, il existe une extension $\mathbb{F}_p \subset \mathbb{F}_q$ de degré $d = \dim(V)$ (on a donc $q = p^d$); vus comme espaces vectoriels sur \mathbb{F}_p , V et \mathbb{F}_q sont isomorphes; il suffit donc de trouver une bijection \mathbb{F}_p -linéaire de \mathbb{F}_q , de signature -1 . Or, le groupe multiplicatif \mathbb{F}_q^\times est cyclique d'ordre $q - 1$; soit g un générateur de ce groupe; la permutation (\mathbb{F}_p -linéaire) $x \mapsto g.x$ de \mathbb{F}_q laisse 0 fixe, et comporte l'unique cycle $\{g, g^2, \dots, g^{q-1}\}$ qui est de longueur paire $q - 1$; la signature de cette permutation est donc $(-1)^q = -1$.

Remarque 1 Soit V un espace vectoriel de dimension d sur un corps quelconque K , de caractéristique $\neq 2$. Le choix d'une base (e_1, \dots, e_d) de V permet de faire opérer \mathfrak{S}_d sur V , par les conditions $\sigma(e_i) = e_{\sigma i}$; on obtient ainsi un homomorphisme injectif $\mathfrak{S}_d \rightarrow \mathbf{GL}(V)$. Comme le déterminant de la matrice d'une permutation d'une base est égal à la signature de cette permutation, on a un carré commutatif

$$\begin{array}{ccc} \mathfrak{S}_d & \longrightarrow & \mathbf{GL}(V) \\ \text{signature} \downarrow & & \downarrow \det \\ \{\pm 1\} & \subset & K^\times \end{array}$$

Ni l'homomorphisme $\mathfrak{S}_d \rightarrow \mathbf{GL}(V)$, ni ce carré n'ont quoi que ce soit à voir avec ceux du théorème; d'ailleurs, si $K = \mathbb{F}_p$, alors V a p^d éléments et le théorème concerne un homomorphisme $\mathbf{GL}(V) \rightarrow \mathfrak{S}_{p^d}$.

Remarque 2 Ce résultat, ainsi que quatre définitions possibles de la signature, et leurs liens avec le symbole de Legendre-Jacobi, sont longuement discutés dans plusieurs articles élémentaires et lumineux de Pierre CARTIER, parus dans *L'Enseignement Mathématique*, t. XVI, fasc.1 .

Daniel Ferrand