LE THÉORÈME DE FROBENIUS-ZOLOTAREV

par

Stef Graillat

Le théorème de Frobenius-Zolotarev permet de relier la signature d'un automorphisme d'un espace vectoriel défini sur un corps fini (qui est bien une permutation d'un ensemble fini) avec le symbole de Legendre du déterminant de ce même automorphisme. Ce théorème trouve sa place dans les leçons :

- 104 : Sous-groupes distingués, groupes quotients. Exemples et applications.
- 106 : Groupe des permutations d'un ensemble fini. Applications.
- 109 : Congruence dans $\mathbf{Z}$, anneau $\mathbf{Z}/n\mathbf{Z}$. Applications.
- 110 : Nombres premiers. Applications.
- 112 : Corps finis. Applications.
- 122 : Déterminant. Applications.

Le démonstration que nous donnons ici est très largement inspirée de [Fer01].

THÉORÈME. — *Soient p un nombre premier $\geqslant 3$, $\mathbf{F}_p$ le corps fini à p éléments et* V *un espace vectoriel sur $\mathbf{F}_p$ de dimension finie. Alors, pour tout $u \in$ GL(V) on a*

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

Démonstration. — Comme $p \geqslant 3$, le groupe dérivé de GL(V) est le groupe SL(V) (voir par exemple [Per95, p.101] ou [Gou94, p.156]). Pour tout morphisme $\alpha : \text{GL(V)} \to \text{A}$, ou A est un groupe commutatif, on a $\alpha(\text{SL(V)}) = 1$. En effet, soit $v \in \text{SL(V)} = \mathscr{D}(\text{SL(V)})$; v s'écrit, par définition du groupe dérivé, sous la forme $v = v_1 \cdots v_m$ ou les v_i sont des commutateurs (*i.e.* sous la forme $v_i = f_i g_i f_i^{-1} g_i^{-1}$). Par conséquent, $\alpha(v_i) = \alpha(f_i)\alpha(g_i)\alpha(f_i^{-1})\alpha(g_i^{-1})$. Comme A est supposé commutatif, on a $\alpha(v_i) = 1$ et donc $\alpha(v) = 1$. Comme $\text{SL(V)} \subset \operatorname{Ker}\alpha$ (c'est ce que l'on vient juste de montrer), le théorème de factorisation (appelé aussi *propriété universelle* du quotient), nous donne le diagramme commutatif suivant

$$\begin{array}{ccc} \text{GL(V)} & \xrightarrow{\alpha} & \text{A} \\ {\scriptstyle \text{cl}}\downarrow & \nearrow_{\overline{\alpha}} & \\ \text{GL(V)}/\text{SL(V)}. & & \end{array}$$

Remarque. — En fait, on aurait pu appliquer directement la *propriété universelle* du groupe dérivé (voir [Gui97, p.48]), mais cette propriété étant moins connue, on l'a redémontrée à l'aide de celle du quotient (supposée connue).

Comme dét est un morphisme de GL(V) dans $\mathbf{F}_p^\times$ de noyau SL(V), là encore le théorème de factorisation nous donne le diagramme commutatif suivant

$$\begin{array}{ccc} \mathrm{GL(V)} & \xrightarrow{\text{dét}} & \mathbf{F}_p^\times \\ {\scriptstyle \mathrm{cl}}\downarrow & \nearrow_{\overline{f}} & \\ \mathrm{GL(V)/SL(V)}, & & \end{array}$$

avec le fait que $\overline{f}$ soit un isomorphisme.

En résumé, on a $\alpha = \overline{\alpha} \circ \mathrm{cl}$ et $\text{dét} = \overline{f} \circ \mathrm{cl}$. Par conséquent $\mathrm{cl} = \overline{f}^{-1} \circ \text{dét}$ et $\alpha = \overline{\alpha} \circ \overline{f}^{-1} \circ \text{dét}$. Posons $f : \mathbf{F}_p^\times \to \mathrm{A}$ définie par $f = \overline{\alpha} \circ \overline{f}^{-1}$. On a montré l'existence d'un morphisme f factorisant le diagramme

$$\begin{array}{ccc} \mathrm{GL(V)} & \xrightarrow{\alpha} & \mathrm{A} \\ {\scriptstyle \text{dét}}\downarrow & \nearrow_{f} & \\ \mathbf{F}_p^\times. & & \end{array}$$

Prouvons maintenant l'unicité de f. On a $\alpha = f \circ \text{dét}$ et soit f' tel que $\alpha = f' \circ \text{dét}$. L'unicité provient alors de la surjectivité du morphisme dét : $\mathrm{GL(V)} \to \mathbf{F}_p^\times$. On a alors $f(x) = f \circ \text{dét}\, a = \alpha(a) = f' \circ \text{dét}\, a = f'(a)$.

Désignons par $\varepsilon : \mathrm{GL(V)} \to \{\pm 1\}$ l'homomorphisme composé

$$\mathrm{GL(V)} \subset \mathfrak{S}(\mathrm{V}) \xrightarrow{\text{signature}} \{\pm 1\}.$$

On applique le résultat précédent à $\mathrm{A} = \{\pm 1\} = \mathbf{F}_2$. En conséquence, il existe un unique homomorphisme de groupes $f : \mathbf{F}_p^\times \to \{\pm 1\}$ rendant commutatif le diagramme

$$\begin{array}{ccc} \mathrm{GL(V)} & \hookrightarrow & \mathfrak{S}(\mathrm{V}) \\ {\scriptstyle \text{dét}}\downarrow & & \downarrow{\scriptstyle \text{signature}} \\ \mathbf{F}_p^\times & \xrightarrow[f]{} & \{\pm 1\}. \end{array}$$

Il s'agit maintenant de montrer que f correspond au symbole de Legendre. Le symbole de Legendre est caractérisé par le fait que c'est l'unique homomorphisme de $\mathbf{F}_p^\times$ dans $\{\pm 1\}$ qui envoie un générateur de $\mathbf{F}_p^\times$ sur -1. En effet, être un carré est équivalent à être une puissance paire de β un générateur de $\mathbf{F}_p^\times$ (En effet, si $a = b^2$ et b s'écrit $b = \beta^m$ alors $a = \beta^{2m}$. Réciproquement, si $a = \beta^{2m}$ alors $a = b^2$ ou $b = \alpha^m$.). Soit a un élément de $\mathbf{F}_p^\times$ qui ne soit pas un carré (il en existe car il y a $(p-1)/2$ éléments qui sont des carrés) ; il s'écrit sous la forme $a = \beta^{2m+1}$). On a alors

$$-1 = \left(\frac{a}{p}\right) = \left(\frac{\beta^{2m+1}}{p}\right) = \left(\frac{\beta}{p}\right)^{2m} \left(\frac{\beta}{p}\right),$$

et donc

$$\left(\frac{\beta}{p}\right) = -1.$$

Réciproquement, le symbole de Legendre envoie bien un générateur de $\mathbf{F}_p^\times$ sur -1 car sinon le symbole de Legendre vaudrait 1 et il n'y aurait pas de carrés ce qui est bien sûr faux.

On va maintenant montrer qu'il existe $u \in \mathrm{GL(V)}$ vérifiant $-1 = \varepsilon(u) = f \circ \det(u)$. Cela impliquera que f n'est pas le morphisme trivial et que par conséquent f est le symbole de Legendre.

Il reste donc à vérifier l'existence d'un automorphisme u de V de signature -1. Il existe une extension $\mathbf{F}_p \subset \mathbf{F}_q$ de degré $d = \dim \mathrm{V}$ (à savoir $\mathbf{F}_{p^d}$) ; vu comme espace vectoriel sur $\mathbf{F}_p$, V et $\mathbf{F}_q$ sont isomorphes. Il suffit donc de trouver une bijection $\mathbf{F}_p$-linéaire de $\mathbf{F}_q$, de signature -1. Or le groupe multiplicatif $\mathbf{F}_q^\times$ est cyclique d'ordre $q-1$. Soit g un générateur de ce groupe. La permutation $x \mapsto g \cdot x$ de $\mathbf{F}_q$ laisse 0 fixé et comporte l'unique cycle $(g, g^2, \ldots, g^{q-1})$ qui est de longueur $q-1$. La signature est donc $(-1)^q = -1$ (car $q = p^d$ est premier) et cette permutation est clairement $\mathbf{F}_p$-linéaire. □

Références

[Fer01] D. FERRAND – *Signature et déterminant*, Université de Rennes I, 2001, disponible à l'adresse http://agreg-maths.univ-rennes1.fr/documentation/docs/FrobZol.pdf.

[Gou94] X. GOURDON – *Les maths en tête : Algèbre*, Ellipses, 1994.

[Gui97] D. GUIN – *Algèbre, groupes et anneaux, tome 1*, Belin, 1997.

[Per95] D. PERRIN – *Cours d'algèbre*, Ellipses, 1995.

---

9 décembre 2004

STEF GRAILLAT, Université de Perpignan, 52, avenue Paul Alduy, F-66860 Perpignan Cedex
E-mail : graillat@univ-perp.fr • *Url :* http://gala.univ-perp.fr/~graillat