Université de Rennes 1
Préparation à l'agrégation
de mathématiques
Auteur du document :

D. Ferrand

La signature de Frobenius

1.- Introduction

D'après une liste provenant de l'université de Strasbourg, la question de la signature de l'automorphisme de Frobenius d'un corps fini, aurait été posée à l'oral de l'agrégation, ou aurait pu l'être. Je ne connaissais pas la réponse, ni une référence la contenant, jusqu'à ce que Steph Graillat m'envoie sa solution déposée sur sa page personnelle :

http://gala.univ-perp.fr/~graillat

Je propose ci-dessous une autre méthode.

2.- Calcul de certaines signatures

Il arrive souvent qu'un ensemble fini C soit lié à un ensemble fini B de telle sorte que toute permutation de ce dernier induise une permutation de C, de façon compatible avec les compositions de permutations (en termes savants, c'est le cas si C dépend « fonctoriellement » de B) ; on dispose donc d'un homomorphisme de groupes

$$f : \mathfrak{S}_B \longrightarrow \mathfrak{S}_C$$

On cherche alors, pour $\sigma \in \mathfrak{S}_B$, à exprimer la signature de $f(\sigma)$ (qui est une permutation de C) en fonction de la signature de σ.

Notons ε_B et ε_C les signatures. Rappelons que tout homomorphisme $g : \mathfrak{S}_B \to A$ à valeurs dans un groupe *abélien* A se factorise par la signature au sens suivant : notant $\{\pm 1\}$ le groupe à deux éléments, il existe un homomorphisme $h : \{\pm 1\} \to A$ tel que $g = h \circ \varepsilon_B$ (La raison en est que deux transpositions sont conjuguées, et ont donc même image par g, et que cette image a un carré trivial). Par suite, comme l'homomorphisme $\varepsilon_C \circ f$ est à valeurs dans le groupe abélien $\{\pm 1\}$, il se factorise par ε_B. Comme tout endomorphisme du groupe cyclique $\{\pm 1\}$ est de la forme $s \mapsto s^a$, pour un entier a convenable (bien défini modulo 2), il existe un entier $a = a(f)$ tel que

$$\varepsilon_C \circ f = \varepsilon_B^a.$$

Autrement dit, le carré suivant est commutatif :

$$\begin{array}{ccc} \mathfrak{S}_B & \xrightarrow{f} & \mathfrak{S}_C \\ {\scriptstyle \varepsilon_B}\downarrow & & \downarrow{\scriptstyle \varepsilon_C} \\ \{\pm 1\} & \xrightarrow[s \mapsto s^a]{} & \{\pm 1\} \end{array}$$

Pour déterminer cet entier $a(f)$, il suffit de calculer $\varepsilon_C(f(\tau))$ pour une transposition τ de B. Appliquons ce principe.

Soit F un autre ensemble fini, et désignons par $\mathsf{M}(B, F)$ l'ensemble des applications de B vers F. À une permutation σ de B on associe la permutation de $\mathsf{M}(B, F)$ définie par $u \mapsto u \circ \sigma^{-1}$; on obtient ainsi un homomorphisme

$$f : \mathfrak{S}_B \longrightarrow \mathfrak{S}_{\mathsf{M}(B,F)}.$$

On va vérifier la formule suivante, où on a posé $n = \mathrm{Card}(B)$ et $p = \mathrm{Card}(F)$, et où on suppose que $n \geq 2$,

$$\varepsilon(f(\sigma)) = \varepsilon(\sigma)^{\frac{p-1}{2}.p^{n-1}}$$

Soient i et j deux éléments distincts dans B, et posons $B' = B - \{i, j\}$; l'application

$$\mathsf{M}(B, F) \quad \longrightarrow \quad \mathsf{M}(B', F) \times F^2, \qquad u \mapsto (u_{|B'}, u(i), u(j))$$

est bijective. Soit τ la transposition $(i\, j)$; $f(\tau)$ est l'identité sur le premier facteur $\mathsf{M}(B', F)$, et permute les deux autres ; il est clair que la permutation de F^2 définie par $(x, y) \mapsto (y, x)$ a pour signature $(-1)^{\frac{p^2-p}{2}}$; d'autre part,

$$\mathrm{Card}(\mathsf{M}(B', F)) = \mathrm{Card}(F)^{\mathrm{Card}(B')} = p^{n-2};$$

d'où la formule indiquée.

On utilisera le cas particulier suivant : soit ρ une permutation circulaire de B ; alors

$$\varepsilon(u \mapsto u \circ \rho^{-1}) = (-1)^{(n+1).\frac{p-1}{2}.p^{n-1}}.$$

Exercice.
Soient k un entier, C l'ensemble des parties à k éléments de B, et

$$g : \mathfrak{S}_B \longrightarrow \mathfrak{S}_C$$

l'homomorphisme évident ; montrer que l'exposant $a(g)$ peut être pris égal au coefficient binomial C_{n-2}^{k-1}.

3.- La signature de Frobenius

Soient K un corps fini à $q = p^n$ éléments, et φ son automorphisme de Frobenius, de sorte que $\varphi(x) = x^p$. On note $F = \mathbb{F}_p$ le sous-corps premier de K. Le choix d'une base B de K, vu comme $F-$espace vectoriel, fournit une bijection

$$K \quad \widetilde{\longrightarrow} \quad \mathsf{M}(B, F),$$

en associant à un élément de K ses coordonnées sur cette base B. Le *théorème de la base normale* montre qu'il existe une base B qui est une orbite sous le groupe de Galois, ce qui veut dire ici qu'il existe $x \in K$ tel que l'ensemble

$$B = \{x, \varphi(x), \ldots, \varphi^{n-1}(x)\}$$

soit une base (ce résultat figure dans tous les bons livres de théorie des corps, par exemple, dans Bourbaki, Algèbre, ch. V, p.69). L'automorphisme de Frobenius de K correspond, par la bijection signalée plus haut, à la bijection de $\mathsf{M}(B, F)$ induite par la permutation circulaire sur B. Le calcul indiqué en 2 donne donc la formule cherchée :

Dans le corps $\mathbb{F}_{p^n}$, avec $n \geq 2$, l'automorphisme de Frobenius a pour signature

$$(-1)^{(n+1).\frac{p-1}{2}.p^{n-1}}.$$

Daniel Ferrand (*Mars 2003*)