SUR LA SIGNATURE DE L'AUTOMORPHISME DE FROBENIUS

par

Stef Graillat

Résumé. — Dans cette note, nous calculons la signature de l'automorphisme de Frobenius dans un corps fini. Nous serons amené pour cela à calculer la signature de la multiplication par n dans $\mathbf{Z}/m\mathbf{Z}$ avec n et m premiers entre eux.

Abstract. — In this note, we compute the sign of the Frobenius' automorphism on a finite field.

Table des matières

1. Introduction et notations

Dans toute cette note, nous noterons $\mathbf{F}_q$ le *corps fini* à q éléments, où $q = p^n$ avec p un nombre premier et n un entier naturel non nul. On rappelle que l'*automorphisme de Frobenius* est l'application $\varphi : \mathbf{F}_q \to \mathbf{F}_q$, $x \mapsto x^p$. Le caractère bijectif de φ résulte dans la finitude de $\mathbf{F}_q$ et dans l'injectivité de φ. L'automorphisme de Frobenius est donc une permutation de l'ensemble $\mathbf{F}_q$ (ensemble à q éléments). On peut donc se demander quelle est la signature de cette permutation. C'est la question à laquelle nous allons répondre.

Si $\mathbf{K}$ est un corps, nous noterons $\mathbf{K}^\star$ l'ensemble $\mathbf{K}\backslash\{0\}$. Si A est un anneau, nous noterons $\mathrm{A}^\times$ l'ensemble des éléments inversibles de A (qui forme un groupe multiplicatif).

Dans la première section, nous allons calculer cette signature dans deux cas particuliers assez simples que sont celui de $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ et celui de $\mathbf{F}_q$ où $q = p^n$ avec n impair. Nous verrons à la fin de cette section que la signature de l'automorphisme de Frobenius est égale à celle de la multiplication par p dans $\mathbf{Z}/(q-1)\mathbf{Z}$. Cela nous amènera dans la deuxième section à étudier la signature de la multiplication par n dans $\mathbf{Z}/m\mathbf{Z}$ avec n et m premiers entre eux. Nous aurons alors besoin de différencier les démonstrations en fonction de la

parité de n.

Les références qui ont été utilisées sont principalement [NQ92, Zah99]. Nous avons aussi utilisé [Art91, Per95, Rao01] pour certains résultats intermédiaires.

2. Les cas simples

2.1. Dans $\mathbf{F}_p$. — Le cas de $\mathbf{F}_p$ est relativement simple. En effet, $(\mathbf{Z}/p\mathbf{Z})^\star$ étant un groupe multiplicatif d'ordre $p-1$, il vient que $x^{p-1}=1$ pour tout $x\neq 0$. On en déduit donc que pour tout $x\in\mathbf{F}_p$, $\varphi(x)=x$. La signature de φ est donc celle de l'identité qui est bien sûr 1.

2.2. Dans $\mathbf{F}_q$ où n est impair. — Comme $\mathbf{F}_q^\star$ est un groupe multiplicatif d'ordre $q-1$, on a $x^{q-1}=1$ pour tout $x\neq 0$. Par conséquent, $x^q=x$ ceci pour tout x dans $\mathbf{F}_q$. Or comme $q=p^n$, on a

$$x^q = x^{p^n} = \underbrace{\varphi\circ\cdots\circ\varphi}_{n\text{ fois}}(x) = \varphi^n(x).$$

Par conséquent, $\varphi^n=\mathrm{Id}$. La signature ε étant un homomorphisme, on a

$$\varepsilon(\varphi^n)=\varepsilon(\varphi)^n=1,$$

et donc $\varepsilon(\varphi)=1$ car n est impair.

2.3. Où l'on va dans $\mathbf{Z}/(q-1)\mathbf{Z}$. — Intéressons-nous maintenant au cas général. On va sortir de $\mathbf{F}_q$ que l'on ne connaît pas très bien pour aller dans $\mathbf{Z}/(q-1)\mathbf{Z}$ que l'on connaît beaucoup mieux. Par ce faire, on va utiliser le théorème fondamental suivant.

THÉORÈME 2.1. — *Soit* $\mathbf{K}$ *un corps (commutatif) et* G *un sous-groupe fini du groupe multiplicatif* $\mathbf{K}^\star$. *Alors* G *est un* groupe cyclique.

Démonstration. — La démonstration que nous proposons ici (tirée de [Art91]) utilise le *théorème de structure des groupes abéliens finis* et la fait qu'un polynôme *non nul* de degré n sur un corps (commutatif) a au plus n racines.

Puisque le corps $\mathbf{K}$ est commutatif, le groupe G est lui un groupe abélien fini. Le *théorème de structure des groupes abéliens finis* nous permet de dire qu'il existe des entiers $d_1|d_2|\ldots|d_r$, $d_1>1$, vérifiant $\mathrm{G}\simeq\mathbf{Z}/d_1\mathbf{Z}\times\cdots\times\mathbf{Z}/d_r\mathbf{Z}$. Si on note n le cardinal de G, on a $n=d_1d_2\ldots d_r$. Pour tout $x\in\mathrm{G}$, on a donc $x^{d_r}=1$ (attention : on jongle entre la notation additive et multiplicative). Or le groupe G étant inclus dans $\mathbf{K}$, l'équation $x^{d_r}=1$ ne peut avoir plus de d_r solutions. On a donc $d_r\geqslant n=d_1d_2\ldots d_r$. Par conséquent $r=1$ et $d_1=n$, donc $\mathrm{G}\simeq\mathbf{Z}/n\mathbf{Z}$. □

Comme le corps $\mathbf{F}_q$ est fini, on déduit que $\mathbf{F}_q^\star$ est *cyclique*. Notons g un générateur de $\mathbf{F}_q^\star$. On a donc $\mathbf{F}_q^\star=\{1,g,g^2,\ldots,g^{q-2}\}$, et par conséquent $\mathbf{F}_q=\{0,1,g,g^2,\ldots,g^{q-2}\}$. Regardons comment agit l' automorphisme de Frobenius sur $\mathbf{F}_q$. Le tableau suivant résume cette action sur les exposants de g.

x	0	$1=g^0$	g	$\cdots$	g^i	$\cdots$	g^{q-1}
$\varphi(x)$	0	$1=g^0$	g^p	$\cdots$	$g^{pi \pmod{q-1}}$	$\cdots$	$g^{p(q-1) \pmod{q-1}}$

On remarque que l'automorphisme agit sur les exposants comme la multiplication par p dans $\mathbf{Z}/(q-1)\mathbf{Z}$. Comme p est premier avec $q-1=p^n-1$, la multiplication par p dans

$\mathbf{Z}/(q-1)\mathbf{Z}$ est donc une permutation de $\mathbf{Z}/(q-1)\mathbf{Z}$ dont la signature est égale à celle de l'automorphisme de Frobenius. Nous allons maintenant nous intéresser à ce problème mais de manière plus générale : on va chercher la signature de la multiplication par n dans $\mathbf{Z}/m\mathbf{Z}$ avec n et m premiers entre eux.

3. Étude de la signature de la multiplication par n dans $\mathbf{Z}/m\mathbf{Z}$

Dans toute cette section, n et m seront deux entiers naturels *premiers entre eux*. Nous noterons $\pi_{n,m}$ la multiplication par n dans $\mathbf{Z}/m\mathbf{Z}$. Il s'agit de l'application $\pi_{n,m} : \mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$, $x \mapsto nx$. Comme n et m sont par hypothèse premier entre eux, n est inversible dans $\mathbf{Z}/m\mathbf{Z}$, et donc $\pi_{n,m}$ est une bijection et donc une *permutation*. Nous définirons le *symbole de Zolotarev* $(n \mid m) := \varepsilon(\pi_{n,m})$ comme étant la signature de $\pi_{n,m}$.

Nous allons nous intéresser aux permutations classiques dans $\mathbf{Z}/m\mathbf{Z}$.

LEMME 3.1. — *La signature de la permutation de* $\mathbf{Z}/m\mathbf{Z}$, $x \mapsto x + r$ *est* $(-1)^{r(m-1)}$.

Démonstration. — La translation $x \mapsto x+1$ dans $\mathbf{Z}/m\mathbf{Z}$ est un cycle de longueur m donc de signature $(-1)^{m-1}$. La translation $x \mapsto x + r$ est la puissance r-ième de $x \mapsto x+1$. Par conséquent sa signature est $(-1)^{r(m-1)}$. □

Soit I un ensemble fini et $\sigma : \mathrm{I} \to \mathrm{I}$ une permutation de I. Si on munit I d'une structure d'ordre total quelconque et si $\mathrm{Inv}(\sigma)$ désigne l'ensemble des *inversions* de σ, c'est-à-dire des couples (i, j) avec $i < j$ et $\sigma(i) > \sigma(j)$, on rappelle qu'alors $\varepsilon(\sigma) = (-1)^{\mathrm{card}(\mathrm{Inv}(\sigma))}$.

LEMME 3.2. — *Soient* I *et* J *deux ensembles finis et* $\sigma : \mathrm{I} \to \mathrm{I}$, $\tau : \mathrm{J} \to \mathrm{J}$ *deux permutations. On définit la permutation* $\sigma \times \tau : \mathrm{I} \times \mathrm{J} \to \mathrm{I} \times \mathrm{J}$ *par* $(\sigma \times \tau)(i, j) = (\sigma(i), \tau(j))$. *Alors*

$$\varepsilon(\sigma \times \tau) = \varepsilon(\sigma)^{\mathrm{card}(\mathrm{J})} \varepsilon(\tau)^{\mathrm{card}(\mathrm{I})}.$$

Démonstration. — Nous munissons $\mathrm{I} \times \mathrm{J}$ de l'ordre lexicographique. On rappelle que cela signifie que $(i, j) < (i', j')$ si

- $i < i'$ ou
- $i = i'$ et $j < j'$.

Le couple $((i, j), (i', j'))$ est donc une inversion de $\sigma \times \tau$ si $(i, j) < (i', j')$ implique $(\sigma \times \tau)(i, j) > (\sigma \times \tau)(i', j')$. Ce qui s'écrit aussi

$$\begin{cases} i < i' \\ \text{ou} \\ i = i' \text{ et } j < j' \end{cases} \quad \text{implique} \quad \begin{cases} \sigma(i) > \sigma(i') \\ \text{ou} \\ \sigma(i) = \sigma(i') \text{ et } \tau(j) > \tau(j'). \end{cases}$$

Soit maintenant (i, i') une inversion de σ. Alors on déduit de ce qui précède que pour tout j, j' dans J, le couple $((i, j), (i', j'))$ est une inversion de $\sigma \times \tau$. On en a donc $\mathrm{card}(\mathrm{J})^2 \,\mathrm{card}(\mathrm{Inv}(\sigma))$. De la même façon, si (j, j') est une inversion de τ, alors les couples $((i, j), (i, j'))$ pour i dans I sont des inversions de $\sigma \times \tau$. Il y en a $\mathrm{card}(\mathrm{I})\,\mathrm{card}(\mathrm{Inv}(\tau))$. Au total, on a donc

$$\mathrm{card}\,\mathrm{Inv}(\sigma \times \tau) = \mathrm{card}(\mathrm{J})^2\,\mathrm{card}(\mathrm{Inv}(\sigma)) + \mathrm{card}(\mathrm{I})\,\mathrm{card}(\mathrm{Inv}(\tau)).$$

On a donc

$$\begin{aligned}\varepsilon(\sigma\times\tau) &= (-1)^{\operatorname{card}\operatorname{Inv}(\sigma\times\tau)}\\ &= \varepsilon(\sigma)^{\operatorname{card}(\mathrm{J})^2}\varepsilon(\tau)^{\operatorname{card}(\mathrm{I})}.\end{aligned}$$

Comme pour tout entier x dans $\mathbf{Z}$, x et x^2 ont même parité, on déduit que $\varepsilon(\sigma\times\tau) = \varepsilon(\sigma)^{\operatorname{card}(\mathrm{J})}\varepsilon(\tau)^{\operatorname{card}(\mathrm{I})}$. □

LEMME 3.3. — *Soient* I *et* J *deux ensembles finis totalement ordonnés. La permutation de* $\mathrm{I}\times\mathrm{J}$ *qui consiste à passer de l'ordre lexicographique de gauche à droite (l'unique application strictement croissante d'un ordre vers l'autre) a pour signature* $(-1)^{\frac{n(n-1)}{2}\frac{m(m-1)}{2}}$.

Démonstration. — On compte les inversions : $(i,j) < (i',j') \Leftrightarrow i < i'$ ou $(i = i'$ et $j < j')$ pour l'ordre lexicographique gauche et $(i,j) > (i',j') \Leftrightarrow j > j'$ ou $(j = j'$ et $i > i')$ pour l'ordre lexicographique droit. Les seules possibilités sont : $i < i'$ et $j > j'$. Il y a donc $\mathrm{C}_n^2\mathrm{C}_m^2 = \frac{n(n-1)}{2}\frac{m(m-1)}{2}$ inversions. D'où le résultat. □

3.1. Cas où m est impair. — Dans le cas où m est impair, nous allons montrer que le *symbole de Zolotarev* $(n \mid m)$ coïncide avec le *symbole de Jacobi* $\left(\frac{n}{m}\right)$.

PROPOSITION 3.4. — *Le symbole de Zolotarev vérifie les propriétés suivantes :*

(i) $(nn' \mid m) = (n \mid m)(n' \mid m)$ *;*
(ii) $(2 \mid m) = (-1)^{\frac{m^2-1}{8}}$ *;*
(iii) $(n \mid m) \equiv n^{\frac{m-1}{2}} \pmod{m}$ *si m est premier.*

Démonstration. — *(i)* : En utilisant le fait que $\pi_{nn',m} = \pi_{n,m}\circ\pi_{n',m}$ et que la signature est un morphisme, on obtient

$$(nn' \mid m) = \varepsilon(\pi_{nn',m}) = \varepsilon(\pi_{n,m})\varepsilon(\pi_{n',m}) = (n \mid m)(n' \mid m).$$

(ii) : Comme m est impair, $m = 2q+1$ avec $q \in \mathbf{Z}$. La multiplication par 2 dans $\mathbf{Z}/m\mathbf{Z}$ est

$$\begin{pmatrix} 0 & 1 & 2 & \cdots & q & q+1 & q+2 & \cdots & 2q \\ 0 & 2 & 4 & \cdots & 2q & 1 & 3 & \cdots & 2q-1 \end{pmatrix},$$

et la nombre d'inversions est $1+2+\cdots+q = \frac{q(q+1)}{2} = \frac{m^2-1}{8}$.
(iii) : Comme m est premier, la formule

$$\varepsilon(\pi_{n,m}) = \prod_{1\leqslant i<j\leqslant m} \frac{\pi_{n,m}(j) - \pi_{n,m}(i)}{j-i}$$

peut se calculer dans $\mathbf{F}_m$ (qui est un corps). On a donc, toujours modulo m,

$$\varepsilon(\pi_{n,m}) = \prod_{1\leqslant i<j\leqslant m} \frac{nj-ni}{j-i} = \prod_{1\leqslant i<j\leqslant m} n.$$

Comme il y a $\mathrm{C}_m^2 = \frac{m(m-1)}{2}$ paires $\{i,j\}$ avec $i \neq j$ dans $[\![1;m]\!]$, on a $\varepsilon(\pi_{n,m}) = n^{\frac{m(m-1)}{2}}$ ceci dans $\mathbf{F}_m$. D'après le petit théorème de Fermat, $n^m = n$ dans $\mathbf{F}_m$. Par conséquent, $(n \mid m) = \varepsilon(\pi_{n,m}) = n^{\frac{m-1}{2}}$ dans $\mathbf{F}_m$. □

THÉORÈME 3.5. — *Si n et m sont* impairs *et* premiers entre eux, *alors le symbole de Zolotarev vérifie la* loi de réciprocité quadratique *:*

$$(n \mid m)(m \mid n) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}.$$

Démonstration. — On définit les deux permutations σ et τ de $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ par $\sigma(i,j) = (mi+j, j)$ et $\tau(i,j) = (i, nj+i)$. La restriction σ_j de σ à $\mathbf{Z}/n\mathbf{Z} \times \{j\}$ est l'application de $\mathbf{Z}/n\mathbf{Z}$, $i \mapsto mi+j$. Comme n est impair, d'après le lemme 3.1, la signature des translations est 1. Par conséquent, $\varepsilon(\sigma_j) = \varepsilon(\pi_{m,n}) = (n \mid m)$. D'après le lemme 3.2, on en déduit que $\varepsilon(\sigma) = (n \mid m)^m = (n \mid m)$ car m est impair. De la même façon, on démontre que $\varepsilon(\tau) = (m \mid n)$

Notons $\theta : \mathbf{Z}/nm\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ l'homomorphisme d'anneaux du *théorème des restes chinois*. On a alors $\theta(mi+j) = (mi+j, j)$ et $\theta(nj+i) = (i, nj+i)$. En notant $\lambda : \mathbf{Z}/nm\mathbf{Z} \to \mathbf{Z}/nm\mathbf{Z}$ la permutation $nj+i \mapsto mi+j$, on a $\lambda \circ \theta^{-1} \circ \sigma = \theta^{-1} \circ \tau$. Or la permutation λ, étant conjuguée à la permutation qui renverse l'ordre lexicographique du $\mathbf{Z}/nm\mathbf{Z}$, est de signature $(-1)^{\frac{n-1}{2}\frac{m-1}{2}}$. Par conséquent, on trouve bien que

$$(n \mid m)(m \mid n) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}.$$

□

LEMME 3.6. — *Pour tous entiers m et m' impairs et n quelconque, on a*

$$(n \mid m)(n \mid m') = (n \mid mm').$$

Démonstration. — Nous allons différencier deux cas :

– Cas où n est impair :

D'après la *loi de réciprocité quadratique*, on a $(n \mid m) = (m \mid n)(-1)^{\frac{n-1}{2}\frac{m-1}{2}}$ et $(n \mid m') = (m' \mid n)(-1)^{\frac{n-1}{2}\frac{m'-1}{2}}$. Par conséquent,

$$\begin{aligned}(n \mid m)(n \mid m') &= (m \mid n)(m' \mid n)(-1)^{\frac{n-1}{2}\frac{m-1}{2}}(-1)^{\frac{n-1}{2}\frac{m'-1}{2}} \\ &= (mm' \mid n)(-1)^{\frac{n-1}{2}(\frac{m-1}{2}+\frac{m'-1}{2})}.\end{aligned}$$

En appliquant la *loi de réciprocité quadratique* à $(mm' \mid n)$, on obtient

$$(n \mid m)(n \mid m') = (n \mid mm')(-1)^{\frac{n-1}{2}(\frac{m-1}{2}+\frac{m'-1}{2}+\frac{mm'-1}{2})}.$$

Nous allons montrer que $\frac{m-1}{2} + \frac{m'-1}{2} + \frac{mm'-1}{2}$ est pair. En effet, comme m et m' sont impair, on a $m = 2k+1$ et $m' = 2k'+1$. D'ou on déduit que $\frac{m-1}{2} + \frac{m'-1}{2} + \frac{mm'-1}{2} = 2k + 2k' + 2kk'$ qui est bien pair. Par conséquent, $(n \mid m)(n \mid m') = (n \mid mm')$.

– Cas où n est pair :

Comme n est pair, on a $n = 2^i r$ avec $i \geqslant 1$ et r impair. On a donc

$$\begin{aligned}(n \mid m)(n \mid m') &= (2^i \mid m)(2^i \mid m')(r \mid m)(r \mid m') \\ &= ((2 \mid m)(2 \mid m'))^i (r \mid mm'),\end{aligned}$$

car r est impair (*cf.* le premier cas au dessus). De plus

$$(2 \mid m)(2 \mid m') = (-1)^{\frac{m^2-1}{8}}(-1)^{\frac{m'^2-1}{8}} = (-1)^{\frac{m^2+m'^2-1}{8}}.$$

Or comme $\frac{m^2+m'^2-2}{8}$ et $\frac{(mm')^2-1}{8}$ ont même parité, on en déduit que $(2 \mid m)(2 \mid m') = (-1)^{\frac{(mm')^2-1}{8}} = (2 \mid mm')$. Par conséquent,

$$(n \mid m)(n \mid m') = (2 \mid mm')^i (r \mid mm') = (2^i \mid mm')(r \mid mm') = (n \mid mm').$$

Il ne reste plus qu'à montrer que $\frac{m^2+m'^2-2}{8}$ et $\frac{(mm')^2-1}{8}$ ont même parité. En effet $m = 4k+\delta$ et $m' = 4k'+\delta'$ avec $\delta, \delta' \in \{1,3\}$. Alors $\frac{m^2+m'^2-2}{8}$ = nombre pair $+ \frac{\delta^2+\delta'^2-2}{8}$ et $\frac{(mm')^2-1}{8}$ = nombre pair $+ \frac{(\delta\delta')^2-1}{8}$. Or $\frac{\delta^2+\delta'^2-2}{8}$ et $\frac{(\delta\delta')^2-1}{8}$ ont la même parité pour $\delta, \delta' \in \{1,3\}$.

□

On peut maintenant montrer que le symbole de Zolotarev et de Jacobi coïncident.

THÉORÈME 3.7. — *Pour tous entiers m impairs et n quelconque, on a*

$$(n \mid m) = \left(\frac{n}{m}\right).$$

Démonstration. — Soit $m = \prod_{i=1}^r p_i^{\alpha_i}$ la décomposition de m en produit de nombres premiers. On a alors, d'après ce qui précède,

$$(n \mid m) = (n \mid \prod_{i=1}^r p_i^{\alpha_i}) = \prod_{i=1}^r (n \mid p_i)^{\alpha_i}.$$

Or d'après la proposition 3.4(iii), on a $(n \mid p_i) = \left(\frac{n}{p_i}\right)$. D'où

$$(n \mid m) = \prod_{i=1}^r \left(\frac{n}{p_i}\right)^{\alpha_i} = \left(\frac{n}{\prod_{i=1}^r p_i^{\alpha_i}}\right) = \left(\frac{n}{m}\right).$$

□

3.2. Cas où m est pair. — Dans cette section, nous allons démontrer le théorème suivant.

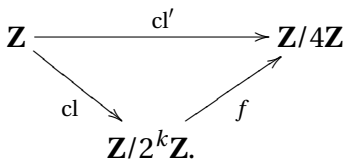
THÉORÈME 3.8. — *Soit m un entier* pair *et n un entier* premier *avec m. Alors la signature de $\pi_{n,m}$, la multiplication par n dans $\mathbf{Z}/m\mathbf{Z}$, est égale à $(-1)^{(\frac{m}{2}+1)(\frac{n-1}{2})}$.*

Pour ce faire, nous aurons besoin des deux lemmes suivants.

LEMME 3.9. — *Les groupes $(\mathbf{Z}/2\mathbf{Z})^\times$ et $(\mathbf{Z}/4\mathbf{Z})^\times$ sont cycliques d'ordre 1 et 2 respectivement. Pour tout $k \geqslant 3$, le groupe $(\mathbf{Z}/2^k\mathbf{Z})^\times$ est isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{k-2}\mathbf{Z}$. Il est engendré par -1 et 5.*

Remarque 3.10. — Autrement dit, le lemme précédent nous assure que tout nombre impair s'écrit $\pm 5^j \pmod{2^k}$.

Démonstration du lemme 3.9. — Soit $\mathrm{cl}' : \mathbf{Z} \to \mathbf{Z}/4\mathbf{Z}$ la surjection canonique. Comme $2^k\mathbf{Z}$ est inclus dans le noyau de cl′, on peut donc passer au quotient :



Le noyau $\mathrm{Ker}\, f$ est l'ensemble des $1+4x$ avec $0<x<2^{k-2}$. Il est donc de cardinal 2^{k-2}. On va montrer qu'il est cyclique en montrant que 5 est d'ordre 2^{k-2}.

Pour ce faire, nous allons montrer par récurrence que pour tout $k\geqslant 1$, $5^{2^k}=1+\lambda 2^{k+2}$ avec λ impair. Ceci est clair pour $k=1$, puisque $5^2=1+3\times 8$. Supposons l'égalité vraie au rang k et montrons la au rang $k+1$. De l'égalité $5^{2^k}=1+\lambda 2^{k+2}$, on tire $5^{2^{k+1}}=1+\lambda 2^{k+3}+\lambda^2 2^{2k+4}=1+2^{k+3}(\lambda+2^{k+1}\lambda^2)$ qui est bien de la forme voulue.

On peut donc dire maintenant que 5 est d'ordre 2^{k-2} et donc que $\mathrm{Ker}\, f$ est cyclique avec 5 comme générateur.

Tout nombre impair s'écrivant sous la forme $\pm(1+4x)$, $x\in\mathbf{Z}$, on en déduit que le morphisme $\{\pm 1\}\times\mathrm{Ker}\, f\to(\mathbf{Z}/2^k\mathbf{Z})^\times$, $(\delta,x)\mapsto\delta x$ est surjectif et donc bijectif par égalité des cardinaux. Il s'agit donc bien d'un isomorphisme. Puisque $\{\pm 1\}\times\mathrm{Ker}\, f$ est engendré par $(-1,1)$ et $(1,5)$, on en déduit que -1 et 5 engendre $(\mathbf{Z}/2^k\mathbf{Z})^\times$. □

LEMME 3.11. — *Soit k un entier supérieur ou égal à 2 et n un entier* impair. *Alors la signature de $\pi_{n,2^k}$, la multiplication par n dans $\mathbf{Z}/2^k\mathbf{Z}$, est égale à $(-1)^{\frac{n-1}{2}}$.*

Démonstration du lemme 3.11. — Le cas $k=2$ est clair. Intéressons-nous au cas $k\geqslant 3$. Pour n et n' deux entiers impairs, on a $\varepsilon(\pi_{nn',2^k})=\varepsilon(\pi_{n,2^k})\varepsilon(\pi_{n',2^k})$. De même, on a $(-1)^{\frac{nn'-1}{2}}=(-1)^{\frac{n-1}{2}}(-1)^{\frac{n'-1}{2}}$. Par conséquent, l'égalité que nous voulons montrer, $\varepsilon(\pi_{n,2^k})=(-1)^{\frac{n-1}{2}}$ est multiplicative en $n\in(\mathbf{Z}/2^k\mathbf{Z})^\times$. Il suffit donc de la montrer pour les générateurs de $(\mathbf{Z}/2^k\mathbf{Z})^\times$ que sont -1 et 5 d'après le lemme 3.9.

– Cas où $n=-1$:
Pour 0 et 2^{k-1}, la multiplication par -1 les laisse fixes. Pour le reste, la multiplication par -1 est un produit de transpositions. Par conséquent, $\varepsilon(\pi_{-1,2^k})=(-1)^{\frac{2^k-2}{2}}=-1$.

– Cas où $n=5$:
Soit x un élément non nul de $(\mathbf{Z}/2^k\mathbf{Z})^\times$ (disons ici que x est le représentant appartenant à $[\![0,2^{k-1}]\!]$). On va montrer que la valuation 2-adique de x ne dépend pas du représentant choisi. Soit $x=2^r m$ avec m impair et $\widehat{x}=2^r m+s2^k$ un autre représentant. On a $\widehat{x}=2^r(m+s2^{k-r})$ avec $m+s2^{k-r}$ impair. Sa valuation 2-adique est bien r (on notera $v_2(x)=r$). On peut donc introduire pour chaque entier $r\in[\![0,k]\!]$, l'ensemble $\mathrm{V}_r:=\{x\in(\mathbf{Z}/2^k\mathbf{Z})^\times : v_2(x)=r\}$. Chaque élément de V_r s'écrit sous la forme $x=2^r m$ avec m impair. Or on a vu ci-dessus que tout nombre impair s'écrit sous la forme $\pm 5^j$ dans $\mathbf{Z}/2^k\mathbf{Z}$. Par conséquent, pour $r\in[\![0,k-2]\!]$ on a $\mathrm{V}_r=\{\pm 2^r 5,\pm 2^r 5^2,\dots,\pm 2^r 5^{2^{k-r-2}}\}$ et $\mathrm{V}_{k-1}=\{2^{k-1}\}$ ainsi que $\mathrm{V}_k=\{0=2^k\}$. Les parties V_r sont stables par $\pi_{5,2^k}$ (*i.e.* $\pi_{5,2^k}(\mathrm{V}_r)=\mathrm{V}_r$). De plus, pour $r\in[\![0,k-3]\!]$, $\pi_{5,2^k}$ restreint à V_r est le produit de deux cycles de longueur 2^{k-r-2} :

$$(2^r 5,2^r 5^2,\dots,2^r 5^{k-r-2}=2^r)(-2^r 5^2,\dots,-2^r 5^{k-r-2}=-2^r).$$

Pour $r\geqslant k-2$, $\pi_{5,2^k}$ vaut l'identité sur V_r. Par suite, il vient que $\varepsilon(\pi_{5,2^k})=1$.

□

Démonstration du théorème 3.8. — Comme m est pair, il s'écrit $m=2^k r$ avec r impair et $k\geqslant 1$. D'après le théorème des restes chinois, on a $\mathbf{Z}/m\mathbf{Z}\simeq\mathbf{Z}/2^k\mathbf{Z}\times\mathbf{Z}/r\mathbf{Z}$. D'après le lemme

3.2 et si $k \geqslant 2$, la signature est donnée par

$$((-1)^{\frac{n-1}{2}})^r (n \mid r)^{2^k} = ((-1)^{\frac{n-1}{2}})^r.$$

Si $k = 1$, la signature vaut 1. On peut résumer ceci en disant que la signature est

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

□

4. Étude de la signature de l'automorphisme de Frobenius

Maintenant que nous avons calculer la signature de la multiplication par n dans $\mathbf{Z}/m\mathbf{Z}$, nous pouvons facile calculer celle de la multiplication par p dans $\mathbf{Z}/(q-1)\mathbf{Z}$ (qui n'est rien d'autre que la signature de l'automorphisme de Frobenius).

Il nous faut distinguer, comme dans l'étude précedente, deux cas selon la partité de p. Si $p \neq 2$ alors p est impair et donc $q-1$ est pair. Dans ce cas la signature est $(-1)^{(\frac{q-1}{2}+1)(\frac{p-1}{2})}$. Si maintenant $p = 2$, la signature est $(p \mid q-1) = (2 \mid 2^n - 1)$. D'après la proposition 3.4(ii), on alors $(p \mid q-1) = (-1)^{\frac{(q-1)^2-1}{8}}$.

On peut donc énoncer le théorème suivant.

THÉORÈME 4.1. — *Soit* $\mathbf{F}_q$ *le* corps fini *à* q *éléments, où* $q = p^n$ *avec* p *un nombre premier et* n *un entier naturel. Soit* $\varphi : \mathbf{F}_q \to \mathbf{F}_q$, $x \mapsto x^p$ *l'*automorphisme de Frobenius. *La signature de* φ *est alors*

$$\varepsilon(\varphi) = \begin{cases} (-1)^{\frac{(q-1)^2-1}{8}} & \text{si } p = 2\,; \\ (-1)^{(\frac{q-1}{2}+1)(\frac{p-1}{2})} & \text{si } p \neq 2. \end{cases}$$

5. Conclusion

On trouva dans [Fer01] le théorème de Frobenius-Zolotarev qui permet de relier la signature d'un automorphisme sur un corps fini (qui est bien une permutation d'un ensemble fini) avec le symbole de Legendre du déterminant de ce même automorphisme. Voici l'énoncé de ce théorème.

THÉORÈME 5.1. — *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* $u \in \mathrm{GL}(V)$ *on a*

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

Références

[Art91] M. ARTIN – *Algebra*, Prentice Hall, 1991.

[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.

[NQ92] P. NAUDIN & C. QUITTÉ – *Algorithmique algébrique, avec exercices corrigés*, Masson, 1992.

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

[Rao01] J.-C. RAOULT – *Résidus quadratiques*, Université de Rennes I, 2001, disponible à l'adresse http://agreg-maths.univ-rennes1.fr/documentation/docs/quadratique.pdf.

[Zah99] M. ZAHIDI – « Symboles des restes quadratiques et discriminants », Thèse, Université de Limoge, 1999.

---

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