Sur la loi de réciprocité quadratique *

O. Serman

9 novembre 2002

Nous donnons dans ces notes une démonstration de la loi de réciprocité quadratique d'après des idées de Zolotarev et de Rousseau (cf. [R]).

1. Rappels

1.1. Si p est un nombre premier, et n un entier, on définit le *symbole de Legendre* $\left(\frac{n}{p}\right)$ par

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & p \mid n, \\ 1 & \text{si } n \in (\mathbb{Z}/n\mathbb{Z}^*)^2, \\ -1 & \text{sinon.} \end{cases}$$

Si p est un nombre premier impair, $\left(\frac{n}{p}\right) = n^{\frac{p-1}{2}} \mod p$ (cf. [Se] I.3.1).

1.2. La loi de réciprocité quadratique affirme que, si p et q sont deux premiers impairs distincts, alors

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{1.2.1}$$

On a par ailleurs la loi complémentaire $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

2. Le symbole de Zolotarev

2.1. Soient $a, n \in \mathbb{Z}$ avec $n \geqslant 1$ et $(a, n) = 1$. On définit le *symbole de Zolotarev* $\left(\frac{a}{n}\right)_Z$ par

$$\left(\frac{a}{n}\right)_Z = \varepsilon(s_a) \tag{2.1.1}$$

où s_a désigne la multiplication par a dans $\mathbb{Z}/n\mathbb{Z}$ et où $\varepsilon(\sigma)$ est la signature de la permutation σ.

Le symbole de Zolotarev $\left(\frac{a}{n}\right)_Z$ ne dépend que de la classe de $a \mod n$. C'est un symbole multiplicatif en haut, i.e. si a et b sont deux entiers premiers à n on a

$$\left(\frac{ab}{n}\right)_Z = \left(\frac{a}{n}\right)_Z \left(\frac{b}{n}\right)_Z \tag{2.1.2}$$

Cela résulte des égalités suivantes : $\left(\frac{ab}{n}\right)_Z = \varepsilon(s_{ab}) = \varepsilon(s_a \circ s_b) = \left(\frac{a}{n}\right)_Z \left(\frac{b}{n}\right)_Z$.

Proposition 2.2. *Soient p un nombre premier et n un entier non divisible par p ; alors $\left(\frac{n}{p}\right) = \left(\frac{n}{p}\right)_Z$.*

*d'après un exposé de D. Zagier à l'ENS le 22 octobre 2002.

Le cas $p = 2$ est évident. Soit donc p premier impair. Si $n = a^2 \mod p$, alors $\left(\frac{n}{p}\right)_Z = \left(\frac{a^2}{p}\right)_Z = \left(\frac{a}{p}\right)_Z^2 = 1 = \left(\frac{n}{p}\right)$. Sinon pour tout a, $n \neq a^2 \mod p$; remarquons alors que $s_n = \beta \circ \alpha$ où α et β sont les involutions de $\mathbb{Z}/p\mathbb{Z}$ définies par

$$\alpha\colon \begin{cases} 0 \mapsto 0 \\ x \mapsto x^{-1} \quad \text{si } x \neq 0 \end{cases} \quad ; \quad \beta\colon \begin{cases} 0 \mapsto 0 \\ x \mapsto nx^{-1} \quad \text{si } x \neq 0 \end{cases}.$$

Ainsi $\left(\frac{n}{p}\right)_Z = \varepsilon(\beta)\varepsilon(\alpha)$. Mais puisque une involution se décompose, en tant que permutation d'ordre 2, en produit de transpositions à supports deux à deux disjoints, la signature d'une involution τ de $\mathbb{Z}/p\mathbb{Z}$ est égale à $(-1)^{\frac{p-|Fix(\tau)|}{2}}$ où $Fix(\tau)$ désigne l'ensemble des points fixes de τ. Or $Fix(\alpha) = \{0, 1, -1\}$, et $Fix(\beta) = \{0\}$, car un point fixe $a \neq 0 \mod p$ de β vérifie $n = a^2$ ce qui est exclu. Donc $\left(\frac{n}{p}\right)_Z = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-3}{2}} = -1 = \left(\frac{n}{p}\right)$.

Vérifions maintenant la loi de réciprocité quadratique pour le symbole de Zolotarev, ce qui établira (1.2.1) en vertu de 2.2.

Théorème 2.3. *Si m et n sont deux entiers naturels impairs premiers entre eux, alors*

$$\left(\frac{m}{n}\right)_Z \left(\frac{n}{m}\right)_Z = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}. \tag{2.3.1}$$

On range de trois manières différentes les entiers de 0 à $mn-1$ en définissant trois matrices (m, n) V, H et D, la première correspondant à un remplissage vertical, la deuxième à un remplissage horizontal et la troisième à un remplissage diagonal. Plus précisement on definit $V = (v_{i,j})$ par $v_{i,j} = m(j-1) + i - 1$, $H = (h_{i,j})$ par $h_{i,j} = n(i-1) + j - 1$. La définition de $D = (d_{i,j})$ est plus délicate : il faut être sûr de ne pas répéter le même nombre. Définissons donc $d_{i,j}$ à l'aide du lemme chinois comme l'unique entier compris entre 0 et $mn - 1$ congru à $i - 1 \mod m$ et à $j - 1 \mod n$, ce qui est possible puisque $(m, n) = 1$. Exhibons les matrices ainsi obtenues dans le cas $(m, n) = (3, 5)$.

$$V = \begin{pmatrix} 0 & 3 & 6 & 9 & 12 \\ 1 & 4 & 7 & 10 & 13 \\ 2 & 5 & 8 & 11 & 14 \end{pmatrix} \qquad H = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 & 9 \\ 10 & 11 & 12 & 13 & 14 \end{pmatrix}$$

$$D = \begin{pmatrix} 0 & 6 & 12 & 3 & 9 \\ 10 & 1 & 7 & 13 & 4 \\ 5 & 11 & 2 & 8 & 14 \end{pmatrix}$$

On dispose des trois permutations de $\{0, 1, ..., mn-1\}$ que sont $\sigma_{D,V}\colon v_{i,j} \mapsto d_{i,j}$, $\sigma_{H,D}\colon d_{i,j} \mapsto h_{i,j}$ et $\sigma_{V,H}\colon h_{i,j} \mapsto v_{i,j}$, liées par la relation $\sigma_{V,H} \circ \sigma_{H,D} \circ \sigma_{D,V} = id$. Le théorème résulte alors immédiatement des deux lemmes suivants :

Lemme 2.4. *$\varepsilon(\sigma_{D,V}) = \left(\frac{m}{n}\right)_Z$ et $\varepsilon(\sigma_{H,D}) = \left(\frac{n}{m}\right)_Z$.*

Lemme 2.5. *$\varepsilon(\sigma_{V,H}) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$.*

Prouvons 2.4 : la permutation $\sigma_{D,V}$ conserve les lignes, puisque $\{v_{i,j}, j = 1, \cdots, n\} = \{k \in \{0, \cdots, mn-1\}, k = i - 1 \mod m\} = \{d_{i,j}, j = 1, \cdots, n\}$. $\sigma_{D,V}$ est donc le produit de m permutations de n éléments, chaque permutation correspondant à l'action de $\sigma_{D,V}$ sur une ligne.

Fixons donc $i \in \{1, \cdots, m\}$ et calculons la signature de la permutation ρ_i induite par $\sigma_{D,V}$ sur la i-ème ligne. Grâce au lemme chinois un élément de la i-ème ligne

de D ou de V est uniquement déterminé par sa classe dans $\mathbb{Z}/n\mathbb{Z}$. Ainsi ρ_i^{-1} est la permutation de $\mathbb{Z}/n\mathbb{Z}$ qui envoie $j-1$ sur $m(j-1)+i-1$, i.e. $\rho_i^{-1} = T_{i-1} \circ s_m$ où T_a désigne la translation $k \in \mathbb{Z}/n\mathbb{Z} \mapsto k+a$. Mais, pour tout a, $\varepsilon(T_a) = 1$: il suffit de voir que $T_a = \underbrace{T_1 \circ \cdots \circ T_1}_{a \text{ fois}}$ (on peut toujours supposer $a \geqslant 0$), d'où $\varepsilon(T_a) = \varepsilon(T_1)^a = 1$ car T_1 est un cycle de longueur impaire n (on peut aussi décomposer T_a en produit de n/r cycles à supports disjoints de même longueur impaire r, ce qui permet d'écrire $\varepsilon(T_a) = ((-1)^{r-1})^{\frac{n}{r}} = 1$). Donc $\varepsilon(\rho_i) = \varepsilon(T_a)\varepsilon(s_m) = \left(\frac{m}{n}\right)_Z$. Alors $\varepsilon(\sigma_{D,V}) = \prod_{i=1}^{m} \varepsilon(\rho_i) = (\left(\frac{m}{n}\right)_Z)^m = \left(\frac{m}{n}\right)_Z$ puisque m est impair. En remarquant que $\sigma_{H,D}$ conserve les colonnes, on montre de même que $\varepsilon(\sigma_{H,D}) = \left(\frac{n}{m}\right)_Z$.

Prouvons 2.5 : on va pour cela calculer le nombre d'inversions de $\sigma_{V,H}$. On a $(v_{i,j} < v_{k,l}) \Leftrightarrow (m(j-1)+i-1 < m(k-1)+l-1) \Leftrightarrow (j < l \text{ ou } (j = l \text{ et } i < k))$. De même $(h_{i,j} < h_{k,l}) \Leftrightarrow (i < k \text{ ou } (i = k \text{ et } j < l))$. On a donc $(v_{i,j} < v_{k,l} \text{ et } h_{i,j} > h_{k,l}) \Leftrightarrow (j < l \text{ et } k < i)$; le nombre d'inversions est donc égal à $\binom{m}{2}\binom{n}{2} = m\frac{m-1}{2}n\frac{n-1}{2}$ et, puisque mn est impair, on a $\varepsilon(\sigma_{V,H}) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$, ce qui achève la démonstration de 2.5 et de 2.3.

Remarque 2.6. (a) La loi de réciprocité 2.3 contient la multiplicativité en bas du symbole de Zolotarev : si m et n sont des entiers impairs et si a est premier à mn, on a

$$\left(\frac{a}{mn}\right)_Z = \left(\frac{a}{m}\right)_Z \left(\frac{a}{n}\right)_Z \tag{2.6.1}$$

En effet si r est un entier (donné par le lemme chinois) congru à $1 \mod 4$ et à $a \mod mn$, on a $\left(\frac{a}{mn}\right)_Z = \left(\frac{r}{mn}\right)_Z = (-1)^{\frac{r-1}{2}\frac{mn-1}{2}} \left(\frac{mn}{r}\right)_Z = \left(\frac{m}{r}\right)_Z \left(\frac{n}{r}\right)_Z = \left(\frac{r}{m}\right)_Z \left(\frac{r}{n}\right)_Z = \left(\frac{a}{m}\right)_Z \left(\frac{a}{n}\right)_Z$.

On en déduit aussitôt que le symbole de Zolotarev est égal au symbole de Jacobi défini pour les couples (m,n) d'entiers premiers entre eux avec n impair comme l'unique symbole multiplicatif en haut et en bas prolongeant le symbole de Legendre (cf. [C]). On retrouve aussi la loi de réciprocité quadratique relative au symbole de Jacobi.

(b) Il découle de 2.3 que, si n est un entier impair, on a

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} \tag{2.6.2}$$

ce qui étend au symbole de Jacobi la loi complémentaire rappelée en 1.2. L'entier n étant impair, on a $(n, n-2) = 1$, ce qui permet d'appliquer 2.3 : $\left(\frac{2}{n}\right) = \left(\frac{2}{n}\right)_Z = \left(\frac{-(n-2)}{n}\right)_Z = \left(\frac{-1}{n}\right)_Z \left(\frac{n-2}{n}\right)_Z = (-1)^{\frac{n-1}{2}}(-1)^{\frac{n-1}{2}\frac{n-3}{2}} \left(\frac{n}{n-2}\right)_Z = (-1)^{\frac{n-1}{2}} \left(\frac{2}{n-2}\right)_Z$. Si on note $n = 2k+1$ il est alors clair que $\left(\frac{2}{n}\right)_Z = (-1)^{\frac{k(k+1)}{2}} = \begin{cases} 1 & \text{si } n = \pm 1 \mod 8 \\ -1 & \text{sinon} \end{cases}$, ce qui est la loi annoncée.

Bibliographie

[C] P. Cartier, *Sur une généralisation des symboles de Legendre-Jacobi*, L'enseignement mathématique **16** (1970), 31-48.

[R] G. Rousseau, *Exterior algebras and the quadratic reciprocity law*, L'enseignement mathématique **36** (1990), 303-308.

[Se] J.-P. Serre, *A Course in Arithmetic*, Graduate Texts in Math. **7**, Springer-Verlag 1973.