

S. AGOU

Une démonstration de la loi de réciprocité quadratique

Publications du Département de Mathématiques de Lyon, 1972, tome 9, fascicule 3
, p. 55-57

[<http://www.numdam.org/item?id=PDML_1972__9_3_55_0>](http://www.numdam.org/item?id=PDML_1972__9_3_55_0)

© Université de Lyon, 1972, tous droits réservés.

L'accès aux archives de la série « Publications du Département de mathématiques de Lyon » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

UNE DEMONSTRATION DE LA LOI

DE RECIPROCITE QUADRATIQUE

S. AGOU

LEMME 1. - Soit p un nombre premier impair, alors pour k entier,

$$0 \leq k \leq \frac{p-1}{2}, \text{ on a } 2^{2k} \binom{\frac{p-1}{2}}{k} = (-1)^k \binom{2k}{k} \text{ dans } \mathbb{F}_p.$$

$$\text{En effet } \binom{\frac{p-1}{2}}{k} = \frac{(-1)^k 1.3 \dots (2k-1)}{2^k k!} = (-1)^k \frac{\binom{2k}{k}}{2^{2k}} \text{ dans } \mathbb{F}_p.$$

$$\text{LOI COMPLEMENTAIRE : } - \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

Soit $\epsilon = \pm 1$. On utilise le lemme 1 en y faisant $k = \frac{p+\epsilon}{4}$ lorsque

$$p + \epsilon \equiv 0 \pmod{4}, \text{ on en déduit que } 2^{\frac{p-1}{2}} = (-1)^{\frac{p+\epsilon}{4}} = (-1)^{\frac{p^2-1}{8}} \text{ dans } \mathbb{F}_p.$$

Soient p et q deux nombres premiers impairs tels que $p \neq q$. Soient $Y^q - X \in \mathbb{F}_p[X, Y]$ un polynôme et $X_1, \dots, X_q$ ses racines dans une extension convenable de $\mathbb{F}_p[X]$. Dans cette extension on a l'identité :

$$\left(\begin{array}{cccc|c} X_1^{q-1} & X_1^{q-2} & \dots & X_1 & 1 \\ X_2^{q-1} & X_2^{q-2} & & X_2 & 1 \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ X_q^{q-1} & X_q^{q-2} & & X_q & 1 \end{array} \right)^p = \left(\begin{array}{cccc|c} X_1^{p(q-1)} & X_1^{p(q-2)} & \dots & X_1^p & 1 \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ X_q^{p(q-1)} & X_q^{p(q-2)} & \dots & X_q^p & 1 \end{array} \right) \quad (1).$$

Mais pour tout entier h , tel que $1 \leq h \leq q-1$, on a, si $hp \equiv j_h (q)$:

$$Y^{hp} = Y^{q \left[\frac{hp}{q} \right] + j_h} \equiv X^{\left[\frac{hp}{q} \right]} Y^{j_h} \pmod{Y^q - X}.$$

$$\text{Ainsi } \left(\begin{array}{cccc|c} X_1^{p(q-1)} & \dots & X_1^p & & 1 \\ & & \cdot & & \\ & & \cdot & & \\ & & \cdot & & \\ & & \cdot & & \\ X_q^{p(q-1)} & & X_q^p & & 1 \end{array} \right) = X^{\sum_{h=1}^{q-1} \left[\frac{hp}{q} \right]} \left(\begin{array}{cccc|c} X_1^{j_{q-1}} & X_1^{j_{q-2}} & \dots & X_1^{j_1} & 1 \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ X_q^{j_{q-1}} & X_q^{j_{q-2}} & \dots & X_q^{j_1} & 1 \end{array} \right) \quad (2).$$

Chaque déterminant de (2) est donc égal à :

$$X^{\sum_{h=1}^{q-1} \left[\frac{hp}{q} \right]} \cdot \text{sgn} \left(\begin{array}{c} q-1, \dots, 1 \\ j_{q-1}, \dots, j_1 \end{array} \right) \left(\begin{array}{cccc|c} X_1^{q-1} & \dots & X_1 & & 1 \\ \cdot & & \cdot & & \cdot \\ \cdot & & \cdot & & \cdot \\ \cdot & & \cdot & & \cdot \\ X_q^{q-1} & \dots & X_q & & 1 \end{array} \right).$$

Donc, puisque $p \neq q$, et compte tenu de (1) :

$$\left(\begin{array}{cccc|c} X_1^{q-1} & \dots & & & 1 \\ \cdot & & & & \\ \cdot & & & & \\ \cdot & & & & \\ X_q^{q-1} & \dots & & & 1 \end{array} \right)^{p-1} = X^{\sum_{h=1}^{q-1} \left[\frac{hp}{q} \right]} \cdot \text{sgn} \left(\begin{array}{c} q-1, \dots, 1 \\ j_{q-1}, \dots, j_1 \end{array} \right).$$

Mais

$$(1). \quad \left(\begin{array}{cccc} x_1^{q-1} & \dots & 1 \\ \vdots & & \vdots \\ x_q^{q-1} & \dots & 1 \end{array} \right)^{p-1} = ((-1)^{\frac{q-1}{2}} x^q x^{q-1})^{\frac{p-1}{2}},$$

Par suite on a : $\sum_{h=1}^{q-1} \left[\frac{hp}{q} \right] = \frac{(p-1)(q-1)}{2}$, ce qui est évident,

$$\text{et } (-1)^{\frac{p-1}{2}} \cdot \frac{q-1}{2} x^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} \cdot \frac{q-1}{2} \left(\frac{q}{p} \right) = \text{sgn} \left(\begin{array}{cccc} q-1 & \dots & 1 \\ j_{q-1} & \dots & j_1 \end{array} \right) \text{ dans } \mathbb{F}_p.$$

$$(2). \quad \text{LEMME 2. - } \text{sgn} \left(\begin{array}{cccc} q-1 & \dots & 1 \\ j_{q-1} & \dots & j_1 \end{array} \right) = \left(\frac{p}{q} \right).$$

On décompose la permutation en cycles. Si $a \in [1, \dots, q-1]$ le cycle $(a, pa, p^2a, \dots, p^{p-1}a)$ est d'ordre $p = r$, où r est l'ordre de p dans $\mathbb{F}_q^*$.

Donc tous les cycles sont de même ordre r . Si p est un résidu quadratique modulo q , alors le nombre de cycles est pair, car $p^{\frac{q-1}{2}} = 1$ et $\frac{q-1}{r} \equiv 2 \cdot \frac{q-1}{2r}$.

Donc $\text{sgn} \left(\begin{array}{cccc} q-1 & \dots & 1 \\ j_{q-1} & \dots & j_1 \end{array} \right) = (-1)^{2(r-1)\frac{q-1}{2r}} = 1 = \left(\frac{p}{q} \right)$. Si p n'est pas un résidu quadratique modulo q , alors r est pair. Mais $p^{\frac{q-1}{2}} = -1$ et $p^{\frac{r}{2}} = -1$ et $\frac{r}{2}$ divise $\frac{q-1}{2}$ par suite $\frac{q-1}{r}$ est impair, car

$$p^{\frac{q-1}{2}} = p^{\frac{r}{2} \cdot \frac{q-1}{r}} = (-1)^{\frac{q-1}{r}} = -1. \text{ Ainsi } \text{sgn} \left(\begin{array}{cccc} q-1 & \dots & 1 \\ j_{q-1} & \dots & j_1 \end{array} \right) = (-1)^{(r-1)\frac{q-1}{r}} = -1 = \left(\frac{p}{q} \right).$$

LOI DE RECIPROCITE QUADRATIQUE. - $\left(\frac{p}{q} \right) \left(\frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$ pour p et q premiers, distincts, impairs.

La démonstration résulte du lemme 2 et de ce qui précède.