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>

UNE DEMONSTRATION DE LA LOI

DE RECIPROCITE QUADRATIQUE

S. AGOU

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

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

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

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

---

Soit $\varepsilon = \pm 1$. On utilise le lemme 1 en y faisant $k = \frac{p+\varepsilon}{4}$ lorsque $p + \varepsilon \equiv 0 \ (4)$; on en déduit que $2^{\frac{p-1}{2}} = (-1)^{\frac{p+\varepsilon}{4}} = (-1)^{\frac{p^2-1}{8}}$ 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 $X_1, \ldots, X_q$ ses racines dans une extension convenable de $\mathbb{F}_p[X]$. Dans cette extension on a l'identité :

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

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

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

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

Chaque déterminant de (2) est donc égal à :

$$X^{\sum_{h=1}^{q-1} \left[\frac{hp}{q}\right]} \cdot \operatorname{sgn} \begin{pmatrix} q-1, \dots, 1 \\ j_{q-1}, \dots, j_1 \end{pmatrix} \begin{vmatrix} X_1^{q-1} & \dots & X_1 & 1 \\ \cdot & & \cdot & \cdot \\ \cdot & & \cdot & \cdot \\ X_q^{q-1} & \dots & X_q & 1 \end{vmatrix} .$$

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

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

Mais

(1). $$\left(\begin{vmatrix} X_1^{q-1} & \dots & 1 \\ \cdot & & \cdot \\ \cdot & & \cdot \\ X_q^{q-1} & \dots & 1 \end{vmatrix}\right)^{p-1} = \left((-1)^{\frac{q-1}{2}} q^q X^{q-1}\right)^{\frac{p-1}{2}} ,$$

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

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

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

On décompose la permutation en cycles. Si $a \in [1,.,q-1]$ le cycle $(a, pa, p^2a, \dots, p^{\rho-1}a)$ est d'ordre $\rho = r$, 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 $\frac{q-1}{r} = 2.\frac{q-1}{2r}$. Donc $\operatorname{sgn}\begin{pmatrix} q-1 & \dots & 1 \\ j_{q-1} & \dots & j_1 \end{pmatrix} = (-1)^{2(r-1)\frac{q-1}{2r}} = 1 = \left(\frac{p}{q}\right)$. 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

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

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.

Manuscrit remis en Mars 1973.

S. AGOU
Maître-Assistant
Département de Mathématiques
43, bd du 11 novembre 1918.
69621 - VILLEURBANNE