JOURNAL

DE

MATHÉMATIQUES

PURES ET APPLIQUÉES

FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874

PAR JOSEPH LIOUVILLE

J. LIOUVILLE

Sur la loi de réciprocité dans la théorie des résidus quadratiques

Journal de mathématiques pures et appliquées 1re série, tome 12 (1847), p. 95-96.

<http://www.numdam.org/item?id=JMPA_1847_1_12__95_0>

SUR LA LOI DE RÉCIPROCITÉ

DANS LA THÉORIE DES RÉSIDUS QUADRATIQUES;

PAR J. LIOUVILLE.

(Extrait des *Comptes rendus de l'Académie des Sciences*, tome XXIV.)

Pour démontrer la *loi de réciprocité* entre deux nombres premiers impairs p et q, dans la théorie des résidus quadratiques, on peut partir de la formule élémentaire connue, et d'ailleurs facile à vérifier,

$$\frac{A^p - B^p}{A - B} = (A\rho - B\rho^{-1})(A\rho^2 - B\rho^{-2})\ldots(A\rho^{p-1} - B\rho^{-p+1}),$$

où ρ désigne une racine imaginaire de l'équation $\rho^p = 1$. En posant $B = A$, on en déduit aisément

$$p = (-1)^{\frac{p-1}{2}}(\rho - \rho^{-1})^2(\rho^2 - \rho^{-2})^2\ldots\left(\rho^{\frac{p-1}{2}} - \rho^{-\frac{p-1}{2}}\right)^2.$$

En élevant les deux membres à la puissance $\frac{q-1}{2}$, et omettant les multiples de q, on trouve ensuite, d'après une notation de Legendre,

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\,\Pi\,\frac{\rho^{\alpha q} - \rho^{-\alpha q}}{\rho^{\alpha} - \rho^{-\alpha}}.$$

le signe de multiplication Π s'étendant aux valeurs $1, 2, 3, \ldots, \frac{p-1}{2}$ de α. Or on démontre sans peine que

$$\Pi\,\frac{\rho^{\alpha q} - \rho^{-\alpha q}}{\rho^{\alpha} - \rho^{-\alpha}} = \left(\frac{q}{p}\right);$$

il suffit, par exemple, de se rappeler le lemme de M. Gauss, relatif aux produits αq réduits à leurs résidus minima, positifs ou négatifs, par rapport au module p. En effet, soit μ le nombre de ceux de ces résidus qui portent le signe — ; M. Gauss prouve que

$$\left(\frac{q}{p}\right) = (-1)^{\mu},$$

et, d'un autre côté, il est évident que

$$\Pi \frac{\rho^{\alpha q} - \rho^{-\alpha q}}{\rho^{\alpha} - \rho^{-\alpha}} = (-1)^{\mu}.$$

Donc

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{q}{p}\right),$$

ce qu'il fallait démontrer. On peut aussi se passer du lemme de M. Gauss, et arriver au même résultat, sans compliquer la démonstration, en décomposant chaque facteur du produit Π à l'aide des racines de l'équation $r^q = 1$. Je me bornerai ici à cette indication générale, me réservant de revenir sur ce sujet dans une autre occasion avec tous les développements convenables; je rapprocherai alors l'analyse précédente (considérée sous les diverses formes dont elle est susceptible) des démonstrations déjà connues qui peuvent avoir avec elle quelque analogie.