BULLETIN DES SCIENCES
MATHÉMATIQUES ET ASTRONOMIQUES

KRONECKER

Sur la loi de réciprocité

Bulletin des sciences mathématiques et astronomiques 2^e série, tome 4, n° 1 (1880), p. 182-192

<http://www.numdam.org/item?id=BSMA_1880_2_4_1_182_1>

SUR LA LOI DE RÉCIPROCITÉ;

PAR M. KRONECKER.

I.

Soient r et s deux nombres entiers positifs ou négatifs, l, m, n trois nombres impairs; soient enfin $\gamma = \pm 1$, $\delta = \pm 1$, $\varepsilon = \pm 1$, les signes étant choisis de façon que $\gamma l, \delta m, \varepsilon n$ soient positifs. Si l'on pose, en généralisant une expression donnée par Eisenstein,

$$(\mathfrak{A}) \qquad \left(\frac{r}{n}\right) = \prod_{k} \frac{\sin\frac{2rk\pi}{n}}{\sin\frac{2k\pi}{n}} \quad \left[k = 1, 2, \ldots, \tfrac{1}{2}(\varepsilon n - 1)\right],$$

on peut remarquer tout d'abord que ce produit conserve la même

valeur lorsqu'on l'étend à tous les systèmes de $\frac{1}{2}(\varepsilon n - 1)$ nombres k, qui forment, pour ainsi dire, un demi-système de résidus relativement au module n, c'est-à-dire dont tous les restes, pris de manière à être, en valeur absolue, moindres que $\frac{\varepsilon n}{2}$, sont différents. Le symbole $\left(\frac{r}{n}\right)$, défini par l'équation (♋), jouit des propriétés suivantes.

1. Sa valeur est zéro ou ± 1 : elle est zéro si r et n ont un commun diviseur, car alors un des facteurs du numérateur s'annule évidemment; elle est ± 1 quand les deux nombres r et n sont premiers entre eux, car chaque facteur du numérateur coïncide, abstraction faite du signe, avec un facteur du dénominateur.

2. La définition conduit immédiatement aux relations

$$(\mathrm{A}) \qquad \begin{cases} \left(\frac{r}{n}\right) = \left(\frac{r}{-n}\right), \quad \left(\frac{r}{n}\right) = \left(\frac{r'}{n}\right) \quad \text{si} \quad r \equiv r' \,(\mathrm{mod.}\, n), \\ \left(\frac{1}{n}\right) = 1, \quad \left(\frac{-1}{n}\right) = (-1)^{\frac{1}{2}(\varepsilon n - 1)}. \end{cases}$$

Or, comme on a

$$\left(\frac{2}{n}\right) = \prod_{k} 2\cos\frac{2k\pi}{n}, \quad \left[k = 1, 2, \ldots, \tfrac{1}{2}(\varepsilon n - 1)\right],$$

le nombre des facteurs négatifs $\cos\frac{2k\pi}{n}$ étant $\frac{1}{4}(\varepsilon n \pm 1)$ et ayant la même parité que $\frac{1}{8}(n^2 - 1)$, il s'ensuit

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

3. La remarque faite au début sur les systèmes des nombres k montre que l'on peut écrire

$$\left(\frac{s}{n}\right) = \prod_{k} \frac{\sin\frac{2rsk\pi}{n}}{\sin\frac{2rk\pi}{n}} \quad \left[k = 1, 2, \ldots, \tfrac{1}{2}(\varepsilon n - 1)\right],$$

et par suite que l'on a

$$(\mathrm{A}') \qquad \left(\frac{r}{n}\right)\left(\frac{s}{n}\right) = \left(\frac{rs}{n}\right).$$

4. En prenant $r = m$ et en mettant à la place des nombres k les nombres $\frac{1}{2}(n+1)k$, il vient

$$\left(\frac{m}{n}\right) = \prod_k \frac{\sin\frac{mk\pi}{n}}{\sin\frac{k\pi}{n}},$$

où les k forment un demi-système de résidus par rapport au module n; puis, en utilisant les relations

$$\delta \frac{\sin m\varphi}{\sin\varphi} = \prod_h 2\sin\left(\frac{h\pi}{m}+\varphi\right) 2\sin\left(\frac{h\pi}{m}-\varphi\right),$$

$$\delta^{\frac{1}{2}(\varepsilon n-1)}\left(\frac{m}{n}\right) = \left(\frac{\delta}{n}\right)\left(\frac{m}{n}\right) = \left(\frac{\delta m}{n}\right),$$

on arrive à l'équation

$$(\mathfrak{B}) \qquad \left(\frac{\delta m}{n}\right) = \prod 2\sin\left(\frac{h\pi}{m}+\frac{k\pi}{n}\right) 2\sin\left(\frac{h\pi}{m}-\frac{k\pi}{n}\right),$$

où le produit s'étend aux $\frac{1}{2}(\delta m-1)$ nombres h et aux $\frac{1}{2}(\varepsilon n-1)$ nombres k qui forment les uns un demi-système de résidus par rapport au module m, les autres un demi-système de résidus par rapport au module n.

L'équation $(\mathfrak{B})$ subsiste, il convient de le remarquer, lors même que m est un nombre pair; toutefois, il faut prendre alors pour k seulement des nombres pairs, remplacer h dans un seul des deux facteurs du second membre par $\frac{1}{2}m$, et enfin, partout ailleurs, faire parcourir à h dans les deux facteurs $\frac{1}{2}\delta m-1$ nombres qui, en valeur absolue, soient incongrus entre eux et avec $\frac{1}{2}m$ par rapport au module m.

De l'équation $(\mathfrak{B})$ résulte immédiatement l'équation de réciprocité

$$\left(\frac{\delta m}{n}\right)\left(\frac{\varepsilon n}{m}\right) = (-1)^{\frac{1}{4}(\delta m-1)(\varepsilon n-1)},$$

ou

$$(B)\qquad \left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=(-1)^{\frac{1}{4}(m-1)(n-1)+\frac{1}{4}(\delta-1)(\varepsilon-1)}.$$

5. En posant $l=r+mn$ ou $l=r$, selon que r est pair ou impair, l sera impair et le produit

$$\left(\frac{l}{mn}\right)\left(\frac{mn}{l}\right)\quad\text{ou}\quad\left(\frac{l}{mn}\right)\left(\frac{m}{l}\right)\left(\frac{n}{l}\right)$$

sera une puissance de -1 dont l'exposant sera

$$\tfrac{1}{4}(l-1)(mn-1)+\tfrac{1}{4}(\gamma-1)(\delta\varepsilon-1);$$

de même, le produit $\left(\frac{l}{m}\right)\left(\frac{m}{l}\right)\left(\frac{l}{n}\right)\left(\frac{n}{l}\right)$ sera une puissance de -1 dont l'exposant sera

$$\tfrac{1}{4}(l-1)(m+n-2)+\tfrac{1}{4}(\gamma-1)(\delta+\varepsilon-2).$$

La différence des deux exposants

$$\tfrac{1}{4}(l-1)(m-1)(n-1)+\tfrac{1}{4}(\gamma-1)(\delta-1)(\varepsilon-1)$$

étant paire, on a

$$\left(\frac{l}{mn}\right)=\left(\frac{l}{m}\right)\left(\frac{l}{n}\right),$$

et par conséquent

$$(C)\qquad \left(\frac{r}{mn}\right)=\left(\frac{r}{m}\right)\left(\frac{r}{n}\right).$$

6. Les nombres k formant un demi-système de résidus par rapport au module n, à chaque nombre k correspond un nombre k' pour lequel on a

$$rk\equiv\pm k'\pmod{n},$$

et par suite

$$rk\equiv k'\frac{\sin\frac{2rk\pi}{n}}{\sin\frac{2k'\pi}{n}}\pmod{n};$$

De là résulte

$$r^{\frac{1}{2}(\varepsilon n-1)}\prod_k k \equiv \left(\frac{r}{n}\right)\prod_k k \pmod{n}.$$

Si n est un nombre premier, le produit Πk n'est pas divisible par n, et dans ce cas on a, par conséquent,

$$\left(\frac{r}{n}\right) \equiv r^{\frac{1}{2}(\varepsilon n-1)} \pmod{n}. \tag{D}$$

Cette dernière congruence montre que, si n est un nombre premier, le symbole $\left(\frac{r}{n}\right)$ défini par l'équation (A) coïncide avec le symbole de *Legendre*, et ensuite il résulte de l'équation (C) que, si n est un nombre quelconque, le symbole $\left(\frac{r}{n}\right)$ est identique avec celui qu'a introduit *Jacobi* en généralisant le symbole de Legendre.

II.

m et n étant supposés premiers entre eux, l'interprétation arithmétique de l'équation (A) donne la généralisation du lemme de *Gauss*, qui a été communiquée par M. *Schering*. Si en effet les nombres k', k'', ... forment un demi-système de résidus relativement au module n, et que l'on ait toujours pour ce module

$$rk' \equiv \rho' k'', \quad rk'' \equiv \rho'' k''', \quad \ldots \quad \rho' = \pm 1, \quad \rho'' = \pm 1, \quad \ldots),$$

l'équation (A) donne pour le symbole $\left(\frac{r}{n}\right)$ la définition arithmétique

$$\left(\frac{r}{n}\right) = \prod \rho, \tag{A'}$$

entièrement équivalente à celle qui apparaît d'abord sous une forme transcendante.

L'interprétation arithmétique de l'équation (B), si l'on prend

$$h = 1, 2, \ldots, \tfrac{1}{2}(\delta m - 1), \quad k = 1, 2, \ldots, \tfrac{1}{2}(\varepsilon n - 1),$$

permet de définir le signe de $\left(\frac{\delta m}{n}\right)$ par le signe du produit

$$\prod_{h,k}\left(\frac{h^2}{m^2}-\frac{k^2}{n^2}\right),$$

ou, si l'on veut, par les conditions

$$\left(\frac{\delta m}{n}\right)=\pm 1, \quad \left(\frac{\delta m}{n}\right)\prod_{h,k}\left(\frac{h}{\delta m}-\frac{k}{\varepsilon n}\right)>0.$$

Si l'on suppose, comme on le fera désormais pour plus de simplicité, m et n positifs, le signe de $\left(\frac{m}{n}\right)$ est le signe de

$$(\mathfrak{B}') \qquad \prod\left(\frac{h}{m}-\frac{k}{n}\right),$$

où le produit s'étend aux valeurs

$$h=1, 2, \ldots, \tfrac{1}{2}(m-1), \quad k=1, 2, \ldots, \tfrac{1}{2}(n-1).$$

Le produit $(\mathfrak{B}')$, ainsi que celui qui figure dans l'équation $(\mathfrak{B})$, s'annule si m et n ne sont pas premiers entre eux; de même, la définition du symbole $\left(\frac{r}{n}\right)$ donnée par l'équation $(\mathfrak{A}')$ peut être énoncée de telle manière que la coïncidence avec celle qui résulte de l'équation $(\mathfrak{A})$ soit encore conservée quand r et n ne sont pas premiers entre eux. La définition arithmétique du symbole $\left(\frac{r}{n}\right)$ donnée par l'équation $(\mathfrak{A}')$ conduit aussi immédiatement que la définition $(\mathfrak{A})$ aux propriétés qu'expriment les équations (A) et (A'); d'un autre côté, la définition arithmétique $(\mathfrak{B}')$ met, tout aussi bien que la définition $(\mathfrak{B})$, l'équation de réciprocité (B) en évidence : en sorte que, pour lier aux définitions arithmétiques $(\mathfrak{A}')$ et $(\mathfrak{B}')$ toute l'analyse déduite dans le § I des définitions correspondantes $(\mathfrak{A})$ et $(\mathfrak{B})$, et pour constituer de cette manière la théorie complète du symbole $\left(\frac{r}{n}\right)$, il ne manque plus qu'un procédé purement arithmétique pour passer de l'une à l'autre; on y parvient aisément comme il suit.

Dans la définition $(\mathfrak{A}')$, prenons pour les nombres k', k'', ... les nombres impairs positifs moindres que $n-1$; chaque produit km

sera congru suivant le module n à la valeur positive ou négative de l'un des nombres k suivant que la partie entière $\mathrm{E}\left(\frac{km}{n}\right)$ de $\left(\frac{km}{n}\right)$ sera paire ou impaire. Par suite, le symbole $\left(\frac{m}{n}\right)$ représente une puissance de -1 dont l'exposant est

$$\mathrm{E}\left(\frac{m}{n}\right)+\mathrm{E}\left(\frac{3m}{n}\right)+\mathrm{E}\left(\frac{5m}{n}\right)+\cdots+\mathrm{E}\left[\frac{(n-2)m}{n}\right],$$

et cette somme, en vertu de la relation

$$\mathrm{E}\left(\frac{am}{n}\right)+\mathrm{E}\left[\frac{(n-a)m}{n}\right]=m-1 \quad (0<a<n),$$

peut être remplacée par

$$\sum_{k}\mathrm{E}\left(\frac{km}{n}\right) \quad \left[k=1, 2, \ldots, \tfrac{1}{2}(n-1)\right].$$

Or c'est évidemment cette même puissance de -1 qui détermine le signe du produit $(\mathfrak{W}')$, puisque $\mathrm{E}\left(\frac{km}{n}\right)$ est le nombre de valeurs de h pour lesquelles $\frac{h}{m}-\frac{k}{n}$ est négatif.

Ce passage de la définition $(\mathfrak{A}')$ à la définition $(\mathfrak{W}')$ remplace, au point de vue arithmétique, le passage de la définition $(\mathfrak{A})$ à la définition $(\mathfrak{W})$ obtenu par la méthode d'Eisenstein au moyen de la formule qui donne $\sin m\nu$; de même, il remplace chacune des différentes déductions qui, partant du lemme de Gauss, conduisent à la loi de réciprocité. Mais le nœud de toutes les démonstrations de la loi de réciprocité qui rentrent dans cette catégorie apparaîtra plus nettement encore en laissant, comme nous le ferons désormais, le lemme de Gauss de côté et en s'arrêtant à la définition $(\mathfrak{W}')$.

III.

Le symbole $\left(\frac{m}{n}\right)$ relatif aux nombres positifs impairs m, n étant défini par le signe de

$$\prod\left(\frac{h}{m}-\frac{k}{n}\right) \quad \left[\begin{matrix}h=1, 2, \ldots, \frac{1}{2}(m-1)\\ k=1, 2, \ldots, \frac{1}{2}(n-1)\end{matrix}\right],$$

l'équation de réciprocité

$$(\alpha) \qquad \left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{1}{4}(m-1)(n-1)}$$

résulte immédiatement de cette définition, ainsi que la relation

$$\left(\frac{m}{n}\right) = (-1)^{\sum_k \mathrm{E}\left(\frac{km}{n}\right)} \quad \left[k = 1, 2 \ldots, \tfrac{1}{2}(n-1)\right].$$

De là résulte aussi que, pour les nombres positifs impairs l et m, congrus entre eux suivant le module n et par suite suivant le module $2n$, on a

$$(\beta) \qquad \left(\frac{l}{n}\right) = \left(\frac{m}{n}\right);$$

mais, dans le cas où $l = -m \pmod{n}$, on aura

$$(\beta') \qquad \left(\frac{l}{n}\right) = \left(\frac{m}{n}\right)(-1)^{\frac{n-1}{2}}.$$

Si maintenant on a $km = \pm k' \pmod{n}$, en désignant les nombres k' ou $n - k'$ suivant les deux cas par r, on aura

$$\mathrm{E}\left(\frac{k'm}{n}\right) = l\,\mathrm{E}\left(\frac{km}{n}\right) + \mathrm{E}\left(\frac{lr}{n}\right)$$

et

$$\mathrm{E}\left(\frac{lr}{n}\right) + \mathrm{E}\left[\frac{l(n-r)}{n}\right] = l - 1;$$

ainsi

$$\mathrm{E}\left(\frac{klm}{n}\right) \equiv \mathrm{E}\left(\frac{km}{n}\right) + \mathrm{E}\left(\frac{k'l}{n}\right) \pmod 2,$$

et par suite

$$(\gamma) \qquad \left(\frac{lm}{n}\right) = \left(\frac{l}{n}\right)\left(\frac{m}{n}\right).$$

En appliquant à chacun des trois symboles l'équation de réciprocité (α) et en permutant l avec n, on parvient, comme dans le § I, 5, à la relation

$$(\gamma') \qquad \left(\frac{l}{mn}\right) = \left(\frac{l}{m}\right)\left(\frac{l}{n}\right),$$

qui montre que le symbole défini précédemment sera identique avec celui de Legendre-Jacobi si, pour le nombre premier n, le symbole $\left(\frac{m}{n}\right)$ est $+1$ ou -1, suivant le caractère quadratique de m par rapport au module n. Or l'équation (γ), pour $m = l$, jointe à l'équation (β), montre d'abord que, pour tout résidu quadratique l de n, on a en effet $\left(\frac{l}{n}\right) = 1$; si maintenant pour un seul nombre m le symbole $\left(\frac{m}{n}\right)$ est négatif, m sera nécessairement non-résidu, et le symbole sera -1 pour tous les non-résidus, ainsi que cela résulte des équations (β) et (γ), qui montrent qu'alors on aura

$$\left(\frac{lm}{n}\right) = -1$$

si l est résidu quadratique : or lm peut représenter tous les non-résidus. Il ne reste plus qu'à prouver que pour tout nombre n il existe un nombre m qui satisfait à l'équation $\left(\frac{m}{n}\right) = -1$. Soit d'abord $n \equiv -1 \pmod 4$; il suit de l'équation (β') que pour $m = 2n - 1$ le symbole $\left(\frac{m}{n}\right)$ est négatif; si, en second lieu, $n \equiv 5 \pmod 8$ et si l'on prend $m = \frac{1}{2}(n+1)$, on aura, à cause de (β'),

$$\left(\frac{n}{m}\right) = \left(\frac{2m-n}{m}\right)(-1)^{\frac{1}{2}(m-1)} = -1,$$

et par suite, à cause de (α),

$$\left(\frac{m}{n}\right) = -1.$$

En troisième lieu, si le nombre n est de la forme $8\nu + 1$, supposons que pour tous les nombres inférieurs à n' existent des nombres m satisfaisant à la condition imposée : les développements précédents prouvent l'identité du symbole $\left(\frac{m}{n}\right)$ avec celui de Legendre-Jacobi pour *tous* les nombres m et n inférieurs à n'. Or le théorème de Gauss (*Disqu. arithm.*, sect. IV, art. 129) montre qu'il y a toujours au moins *un* nombre premier m inférieur à $2\sqrt{n'}$ par rapport auquel

n' est non-résidu quadratique : dès lors, les deux nombres positifs m et $n' - 2m$ étant inférieurs à n', $\left(\frac{n'-2m}{m}\right)$ est identique au symbole de Legendre-Jacobi, et par conséquent négatif, et l'équation (β) donne

$$\left(\frac{n'-2m}{m}\right) = \left(\frac{n'}{m}\right) = -1;$$

et enfin, en vertu de l'équation de réciprocité, on aura

$$\left(\frac{m}{n'}\right) = -1.$$

L'existence de ce nombre m, pour le nombre n', complète la démonstration, par voie d'induction, de l'identité du symbole défini par le signe du produit

$$\prod \left(\frac{h}{m} - \frac{k}{n}\right) \quad \left[\begin{matrix} h = 1, 2, \ldots, \frac{1}{2}(m-1) \\ k = 1, 2, \ldots, \frac{1}{2}(n-1) \end{matrix}\right]$$

avec le symbole de Legendre-Jacobi.

Les développements qui précèdent constituent donc une démonstration de la loi de réciprocité qui appartient essentiellement à la même catégorie que la troisième et la cinquième démonstration de Gauss. Elle a cela de commun avec la première démonstration de Gauss qu'elle ne sort point du domaine de la proposition à démontrer ; elle lui emprunte en outre son principal point d'appui, à savoir le théorème de l'article 129 des *Disquisitiones arithmeticæ*, et aussi, du moins en partie, sa marche inductive. Naturellement la troisième et la cinquième preuve de Gauss, et toutes celles qui rentrent dans cette catégorie, peuvent être établies de la même façon que les développements précédents et débarrassées du lemme de l'article 108 des *Disquisitiones arithmeticæ*. Si l'on voulait se rattacher à la cinquième démonstration de Gauss, il faudrait faire abstraction du § I, utiliser seulement le contenu du § II, où l'équation de réciprocité (α) est établie en regardant le symbole $\left(\frac{m}{n}\right)$ relatif à deux nombres premiers entre eux m, n comme défini par le signe du produit des résidus par rapport au module n, pris en valeur absolue

moindre que $\frac{n}{2}$, des nombres

$$m,\ 2m,\ 3m,\ \ldots,\ \tfrac{1}{2}(n-1)m.$$

De cette définition du symbole $\left(\frac{m}{n}\right)$ résultent immédiatement les équations (β), (β'), (γ), et l'on a tout ce qu'il faut pour établir comme plus haut l'identité du symbole $\left(\frac{m}{n}\right)$ avec celui de Legendre-Jacobi, sans avoir besoin, comme dans l'article 1 de la cinquième preuve de Gauss, d'invoquer le lemme de l'article 106 des *Disquisitiones*. Or, à la place de ce lemme, on utilise la plus importante des propositions sur lesquelles s'appuie la première preuve de Gauss. Que ce soit justement cette proposition à l'aide de laquelle on puisse éviter les congruences de degré supérieur qui figurent dans le lemme, cela me semble éclairer une fois de plus le caractère profond de cette déduction si singulière et si cachée qui a conduit pour la première fois à la démonstration rigoureuse de la loi de réciprocité et qui, tendant directement au but en surmontant tous les obstacles, se présente comme une épreuve de force du génie de Gauss.