Note über das Legendre-Jacobi'sche Symbol

von

Leopold Gegenbauer,
c. M. k. Akad.

(Vorgelegt in der Sitzung am 9. Juli 1891.)

Zur Ermittlung von Ausdrücken für das von Jacobi verallgemeinerte Legendre'sche Symbol führt bekanntlich die folgende, zuerst von den Herren L. Kronecker und E. Schering in gänzlich verschiedener Weise bewiesene Verallgemeinerung des Gauss'schen Lemmas:

Sind m und n zwei theilerfremde ganze Zahlen, so hat das Legendre-Jacobi'sche Symbol $\left(\frac{n}{m}\right)$ den Werth $+1$ oder -1, je nachdem die Anzahl der negativen absolut kleinsten Reste, welche bei der Division der Producte

$$n,\ 2n,\ 3n,\ \ldots,\ \frac{m-1}{2}\,n$$

durch m auftreten, gerade oder ungerade ist.

Da selbstverständlich jede dieser Anzahl nach dem Modul 2 congruente Zahl zur Bestimmung des Zeichens in gleicher Weise verwendet werden kann, so soll jede solche eine durch das Kronecker-Schering'sche Lemma definirte charakteristische Zahl von n in Bezug auf m genannt und mit (n, m) bezeichnet werden.

Von den Darstellungen dieser charakteristischen Zahl pflegt man namentlich diejenigen zu benützen, welche so gebaut sind, dass man bei Vertauschung von n und m unmittelbar das Reciprocitätsgesetz erkennen kann. Ich will in dieser Beziehung nur die Gleichung

$$(n, m) = \sum_{x=1}^{x=\frac{m-1}{2}} \left[\frac{xn}{m}\right] \tag{1}$$

erwähnen, aus der man unter Benützung der durch die Relationen

$$\varepsilon(\alpha) = 1 \quad (\alpha \geqq 1); \qquad \varepsilon(\alpha) = 0 \quad (\alpha < 1)$$

definirten zahlentheoretischen Function $\varepsilon(\alpha)$ mit wenigen Worten das Reciprocitätsgesetz ableiten kann, sowie das dieser Darstellung von (n, m) entsprechende hochelegante Kronecker'sche Product für das Legendre-Jacobi'sche Symbol

$$\left(\frac{n}{m}\right) = \text{sign} \prod_{1}^{\frac{m-1}{2}}{}_{x} \prod_{1}^{\frac{n-1}{2}}{}_{y} \left(\frac{y}{n} - \frac{x}{m}\right).$$

Verschiedene Ausdrücke der charakteristischen Zahl, beziehungsweise des Symbols, von derselben Beschaffenheit wurden von den Herren Kronecker, Schering, mir u. A. bei diversen Gelegenheiten angegeben.

Nicht so unmittelbar führen andere Ausdrücke, von denen ich beispielsweise den im dritten Gauss'schen Beweise des quadratischen Reciprocitätsgesetzes auftretenden

$$(n, m) = \sum_{x=1}^{x=\frac{m-1}{2}} \left[\frac{2xn}{m}\right] \tag{2}$$

anführen will, auf das Reciprocitätsgesetz, man formt sie desshalb zumeist in andere um, denen die eben hervorgebobene Eigenschaft zukommt. So ergibt sich sofort aus dieser Darstellung die in 1) angeführte, wenn man nur die geraden Zahlen des Intervalles $\frac{m+1}{2} \ldots m$ durch $m-(2x_1-1)$ $\left(x_1 = 1, 2, \quad \frac{m-1}{2}\right)$ ersetzt und beachtet, dass in keinem der so entstehenden Glieder $\frac{(2x_1-1)\,n}{m}$ eine ganze Zahl sein kann, sowie dass für jedes nicht ganzzahlige α die Relation

$$[-\alpha] = -1-[\alpha]$$

besteht. Es mag hier nur bemerkt werden, dass man aus 2), wenn man alle geraden Zahlen in der eben angegebenen Weise darstellt, die Formel

$$(n, m) = \sum_{x=1}^{x=\frac{m-1}{2}} \left[\frac{(2x-1)n}{m}\right] \tag{3}$$

erhält.

Sieht man nun aber davon ab, dass das quadratische Reciprocitätsgesetz, wie dies in den angezogenen Fällen geschieht, mit Hilfe einer einzigen Darstellung der durch das Kronecker-Schering'sche Lemma definirten charakteristischen Zahl erschlossen werden soll, so lassen sich auch derartige Ausdrücke ohneweiters mit Vortheil zum Beweise desselben verwenden; man gelangt sogar durch Benützung zweier verschiedener Darstellungen der charakteristischen Zahl mitunter rascher und directer zum Ziele, als durch die Verwendung eines einzigen, namentlich dann, wenn die beiden Ausdrücke durch eine einfache Umformung aus einander ableitbar sind.

Es soll nun ein Beweis des quadratischen Reciprocitätsgesetzes angegeben werden, in welchem zwei verschiedene Darstellungen der charakteristischen Zahl mit einander verbunden werden. Hiebei wird sich auch die Gelegenheit ergeben, auf den innigen Zusammenhang einer Reihe von Darstellungen der ganzen Zahl (n, m) hinzuweisen.

Aus der durch die Gleichung 2) gegebenen Gauss'schen Darstellung von (n, m) kann man leicht die folgende herleiten

$$(n, m) = \sum_{x=1}^{x=n-1} \left[\frac{xm}{2n}\right]. \tag{4}$$

Es ist nämlich

$$\sum_{x=1}^{x=\frac{m-1}{2}} \left[\frac{2xn}{m}\right] = \sum_{x, y=1}^{x=\frac{m-1}{2},\, y=n-1} \varepsilon\left(\frac{2xn}{ym}\right)$$

$$\sum_{y=1}^{y=n-1} \left[\frac{ym}{2n}\right] = \sum_{x, y=1}^{x=\frac{m-1}{2},\, y=n-1} \varepsilon\left(\frac{ym}{2xn}\right)$$

Da nun von den zwei Brüchen $\frac{2xn}{ym}$, $\frac{ym}{2xn}$ für jedes in Betracht kommende Werthepaar x, y der eine grösser, der andere aber kleiner als 1 ist, so hat man

$$\sum_{x,y=1}^{x=\frac{m-1}{2},\, y=n-1} \left\{ \varepsilon\left(\frac{2xn}{ym}\right) + \varepsilon\left(\frac{ym}{2xn}\right) \right\} = \frac{(n-1)(m-1)}{2}$$
$$\equiv 0 \pmod{2},$$

und daher besteht die Congruenz

$$\sum_{x=1}^{x=\frac{m-1}{2}} \left[\frac{2xn}{ym}\right] \equiv \sum_{y=1}^{y=n-1} \left[\frac{ym}{2n}\right] \pmod{2},$$

durch welche die Gleichung 4) bewiesen wird. Man kann dieselbe übrigens auch, wie Herr E. Lucas[1] gezeigt hat, unmittelbar aus dem Lemma erschliessen, wenn man beachtet, dass $\left[\frac{ym}{2n}\right]$ die Anzahl derjenigen unter den Zahlen

$$n,\ 2n,\ 3n,\ \ldots,\ \frac{m-1}{2}\,n$$

ist, welche nicht grösser als $\frac{yn}{2}$ sind, sowie dass man bei der Division von $y_1 n$ durch m stets einen positiven oder negativen absolut kleinsten Rest erhält, je nachdem $y_1 n$ dem Intervalle $2\varkappa . \frac{m}{2} \quad (2\varkappa+1)\frac{m}{2}$ oder $(2\varkappa-1)\frac{m}{2} \quad 2\varkappa\frac{m}{2}$ angehört.

Es mag hier nur gelegentlich darauf hingewiesen werden, dass diese Darstellung von (n, m), in der als Nenner der zu benützenden Brüche das Doppelte des Zählers des zugehörigen

---

[1] „Sur la loi de réciprocité des residus quadratiques." Bulletin de l'académie impériale des sciences de St. Pétersburg. Nouvelle série, t. I (XXXIII), p. 495—496, 1890. Herr E. Lucas liefert a. a. O. unter alleiniger Benützung der Darstellung 4) von (n, m) einen höchst einfachen Beweis des quadratischen Reciprocitätsgesetzes für zwei Primzahlen und fügt bei, dass man auf demselben Wege bei einer Abänderung des Ausspruches des verallgemeinerten Fermat'schen Satzes dasselbe auch für zwei beliebige ungerade theilerfremde Zahlen beweisen kann.

Legendre-Jacobi'schen Zeichens auftritt, an die durch die Theorie der Gauss'schen Summen gelieferte Gleichung

$$W\left(\frac{-mi}{2n}\right) = (1+i^{m})(\sqrt{n})\left(\frac{n}{m}\right)$$

erinnert, die Herrn L. Kronecker zu einem ungemein eleganten Algorithmus zur Bestimmung des verallgemeinerten Legendre'-schen Symbols mit Hilfe der Kettenbruchentwicklung von $\frac{m}{2n}$ geführt hat.

Zu einer zweiten, für den beabsichtigten Zweck geeigneten Darstellung der charakteristischen Zahl (n, m) gelangt man durch die Überlegung, dass

$$\left[\frac{xn}{m} + \frac{1}{2}\right] = \left[\frac{xn}{m}\right] + \begin{cases} 0 \\ 1 \end{cases}$$

ist, je nachdem der Rest der Division von xn durch m kleiner als $\frac{m}{2}$ ist oder nicht, d. i. je nachdem der absolut kleinste Rest derselben positiv oder negativ ist; dieselbe ist also

$$(n, m) = \sum_{x=1}^{x=\frac{m-1}{2}} \left[\frac{xn}{m} + \frac{1}{2}\right] - \sum_{x-1}^{x=\frac{m-1}{2}} \left[\frac{xn}{m}\right]. \qquad 5)$$

Durch blosse Umformung der zweiten Summe auf der rechten Seite dieser Gleichung gelangt man nun unter Benützung der Gleichung 4) zu einem sehr einfachen Beweise des quadratischen Reciprocitätsgesetzes.

Man hat nämlich

$$\sum_{x=1}^{x=\frac{m-1}{2}} \left[\frac{xn}{m}\right] = \sum_{x=1}^{x=\frac{m-1}{2}} \left[\frac{2xn}{2m}\right]$$

$$= \sum_{x=1}^{x=m-1} \left[\frac{xn}{2m}\right] - \sum_{x=1}^{x=\frac{m-1}{2}} \left[\frac{(2x-1)\,n}{2m}\right]$$

Setzt man nun in der zweiten Summe auf der rechten Seite dieser Gleichung

$$x = \frac{m+1}{2} - x_1 \qquad \left(x_1 = 1, 2, \ldots, \frac{m-1}{2}\right),$$

so erhält man die Relation

$$\sum_{x=1}^{x=\frac{m-1}{2}} \left[\frac{(2x-1)\,n}{2m}\right] = \sum_{x=1}^{x=\frac{m-1}{2}} \left[\frac{n}{2} - \frac{xn}{m}\right]$$

$$= \frac{m-1}{2} \cdot \frac{n-1}{2} + \sum_{x=1}^{x=\frac{m-1}{2}} \left[\frac{1}{2} - \frac{xn}{m}\right]$$

$$\equiv \frac{m-1}{2} \cdot \frac{n-1}{2} + \sum_{x=1}^{x=\frac{m-1}{2}} \left[\frac{xn}{m} + \frac{1}{2}\right] \pmod{2}$$

und demnach ist

$$\sum_{x=1}^{x=\frac{m-1}{2}} \left[\frac{xn}{m} + \frac{1}{2}\right] - \sum_{x=1}^{x=\frac{m-1}{2}} \left[\frac{xn}{m}\right] \equiv \frac{m-1}{2} \cdot \frac{n-1}{2} - \sum_{x=1}^{x=m-1} \left[\frac{xn}{2m}\right] \pmod{2}$$

Verbindet man diese Congruenz mit der Gleichung 5), so erhält man unter Berücksichtigung von 4) die Congruenz

$$(n, m) + (m, n) \equiv \frac{m-1}{2} \cdot \frac{n-1}{2} \pmod{2},$$

durch welche das quadratische Reciprocitätsgesetz ausgesprochen wird.

Aus der Formel 4) lässt sich ein neuer Ausdruck für die charakteristische Zahl (n, m) ableiten, der in analoger Weise wie 4) zum Beweise des quadratischen Reciprocitätsgesetzes verwendet werden kann. Schreibt man diese Gleichung nämlich in der Form

$$(n, m) = \sum_{x=1}^{x=\frac{n-1}{2}} \left[\frac{xm}{2n}\right] + \sum_{x=\frac{n+1}{2}}^{x=n-1} \left[\frac{xm}{2n}\right]$$

und setzt sodann in der zweiten Summe auf der rechten Seite

$$x = n - x_1,$$

wo x_1 die ganzen Zahlen des Intervalles $1 \ldots \frac{n-1}{2}$ durchläuft, so verwandelt sich dieselbe in

$$(n, m) = \frac{m-1}{2} \cdot \frac{n-1}{2} + \sum_{x=1}^{x=\frac{n-1}{2}} \left[\frac{xm}{2n}\right] - \sum_{x=1}^{r=\frac{n-1}{2}} \left[\frac{xm}{2n} + \frac{1}{2}\right]. \qquad 6)$$

Wird nun in der ersten Summe auf der rechten Seite für $x : n - x_1$ gesetzt $\left(x_1 = \frac{n+1}{2}, \ldots, n-1\right)$, so ergibt sich sofort die bemerkenswerthe Gleichung

$$(n, m) = \sum_{x=1}^{x=n-1} \left[\frac{xm}{2n} + \frac{1}{2}\right], \qquad 7)$$

welche übrigens aus 3) in derselben Weise hätte abgeleitet werden können, wie 4) aus 2). Man sieht daher, dass die durch das Kronecker-Schering'sche Lemma definirte charakteristische Zahl von n in Bezug auf m sich durch die Summe, oder was dasselbe besagt, die Anzahl der ungeraden, in den Brüchen

$$\frac{m}{2n},\ 2\frac{m}{2n},\ 3\frac{m}{2n},\ \quad ,\ (n-1)\frac{m}{2n}$$

enthaltenen grössten und auch der ihnen zunächst liegenden ganzen Zahlen darstellen lässt.

Da bekanntlich $[2\alpha]$ gerade oder ungerade ist, je nachdem der in α enthaltene Bruchrest kleiner als $\frac{1}{2}$ ist oder nicht, so folgen aus 4) und 7) die neuen Gleichungen

$$(n, m) = \sum_{x=1}^{x=n-1} \left\{\left[\frac{xm}{4n} + \frac{1}{2}\right] - \left[\frac{xm}{4n}\right]\right\} \qquad 8)$$

$$(n, m) = \sum_{x=1}^{x=n-1} \left\{\left[\frac{xm}{4n} + \frac{3}{4}\right] - \left[\frac{xm}{4n} + \frac{1}{4}\right]\right\}, \qquad 9)$$

aus denen folgt:

$$\sum_{x=1}^{x=n-1}\left\{\left[\frac{xm}{4n}\right]+\left[\frac{xm}{4n}+\frac{1}{2}\right]\right\}\equiv\sum_{x=1}^{x=n-1}\left[\frac{xm}{4n}+\frac{1}{4}\right]+\left[\frac{xm}{4n}+\frac{3}{4}\right]\Big\} \pmod{2} \qquad 10)$$

Durch das quadratische Reciprocitätsgesetz ist bekanntlich das verallgemeinerte Legendre'sche Symbol für zwei ungerade theilerfremde Zahlen m und n vollkommen bestimmt, wesshalb es mit Recht als das Fundamenteltheorem dieser Theorie bezeichnet wird. Ja es kann durch dasselbe auch der quadratische Charakter $\left(\frac{2}{n}\right)$ von 2 in Bezug auf eine ungerade Zahl n ermittelt werden, wenn man nur die Gleichung

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

als bekannt voraussetzt, so dass also im Grunde genommen nur ein Ergänzungssatz zum Reciprocitätsgesetze nothwendig ist. Es ist nämlich nach dem Multiplicationssatze für die Symbole

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

oder nach dem Additionstheoreme

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

Da von den zwei ungeraden Zahlen $n-2$, n stets eine die Form $4s+1$ besitzt, so ist demnach nach dem quadratischen Reciprocitätsgesetze

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

und daher schliesslich

$$\left(\frac{2}{n}\right) = \prod_{0}^{\left[\frac{n-1}{2}\right]}{}_{\lambda} \left(\frac{-1}{n-2\lambda}\right)$$

$$= (-1)^{\frac{1}{2} \sum\limits_{\lambda=0}^{\lambda=\left[\frac{n-1}{2}\right]} (n-2\lambda-1)}$$

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

Besitzt man nun für zwei ungerade theilerfremde Zahlen m und n irgend einen Ausdruck für die durch das Kronecker-Schering'sche Lemma definirte charakteristische Zahl (n, m), so wird jede andere Function der beiden ganzen Zahlen m und n, welche, zu derselben hinzugefügt, eine Summe gibt, die nach dem Modul 2 congruent $\frac{m-1}{2} \cdot \frac{n-1}{2}$ ist, zu einer neuen Darstellung dieser charakteristischen Zahl führen. So folgt beispielsweise aus 6) unter Voraussetzung des Reciprocitätsgesetzes die Relation

$$(m, n) = \sum_{x=1}^{x=\frac{n-1}{3}} \left[\frac{xm}{2n} + \frac{1}{2}\right] - \left[\frac{xm}{2n}\right]\Big\},$$

aus welcher nach der oben gemachten Bemerkung sofort wieder die durch die Gleichung 1) angegebene Darstellung der charakteristischen Zahl fliesst, durch deren Vergleich mit 5) man die zuerst von Herrn Kronecker bewiesene Congruenz

$$\sum_{x=1}^{x=\frac{n-1}{2}} \left[\frac{xm}{n} + \frac{1}{2}\right] \equiv 0 \pmod{2} \qquad 11)$$

erhält. Vereinigt man dieselbe mit 7), so entsteht die neue Relation

$$(n, m) = \sum_{x=1}^{x=\frac{n-1}{2}} \left[\frac{(2x-1)m}{2n} + \frac{1}{2}\right],$$

während die Verbindung der aus ihr folgenden Congruenz

$$\sum_{x=1}^{x=\frac{n-1}{2}} \left\{ \left[\frac{xm}{2n} + \frac{3}{4}\right] + \left[\frac{xm}{2n} + \frac{1}{4}\right] \right\} \equiv 0 \pmod{2}$$

mit 10) nach einigen einfachen Umformungen zu der Beziehung

$$\sum_{x=1}^{x=n-1} \left[\frac{1}{2} + \left[\frac{n+1}{4}\right] - \frac{xn}{2m}\right] \equiv \frac{m-1}{2}\left[\frac{n-1}{4}\right] \pmod{2}$$

führt.