Über Eisensteins Beweis des quadratischen Reciprocitätsgesetzes.*)

Von **Ernst Fischer** in Wien.

Ausgehend vom Gauß'schen Lemma gelangt Eisenstein zu der für jedes Paar ungerader positiver Primzahlen p, q giltigen Formel

$$\left(\frac{q}{p}\right) = \prod\left(4\sin^2\frac{2b\pi}{q} - 4\sin^2\frac{2a\pi}{p}\right) \qquad \begin{pmatrix} a = 1, 2, \ldots, \frac{p-1}{2} \\ b = 1, 2, \ldots, \frac{q-1}{2} \end{pmatrix},$$

aus welcher das Reciprocitätsgesetz unmittelbar abgelesen werden kann. Diese Darstellung des Legendre'schen Symbols als Resultante zweier ganzen rationalen und ganzzahligen Functionen einer Veränderlichen wird im Folgenden ohne Entfernung aus dem Gebiete der ganzen rationalen und ganzzahligen Functionen unbestimmter Größen abgeleitet, wobei die Benutzung des Gauß'chen Lemmas entfällt.

Dass die allgemeine Theorie der Resultante durchaus dem genannten Gebiete angehört, kann wohl als bekannt gelten. Ich werde die nach x genommene Resultante zweier Functionen

$$g = a_0 x^\mu + a_1 x^{\mu-1} + \cdots + a_\mu, \quad h = b_0 x^\nu + b_1 x^{\nu-1} + \cdots + b_\nu$$

von x, von welchen auch eine den Grad 0 haben darf, mit

$$R(g, h)$$

bezeichnen, wobei ich mir den seit der Definition der Resultante als einer Function der Coefficienten bisweilen unbestimmt gelassenen Zahlenfactor derart bestimmt denke, dass das Potenzproduct $a_0^\nu b_\nu^\mu$ den Coefficienten 1 erhält.

---

[1]) Applications de l'Algèbre à l'Arithmétique transcendante. Crelle's Journal, Bd. 29.

I.

Es seien x_1, x_2 Unbestimmte, und man setze

$$x_1 + x_2 = \sigma_1, \quad x_1 x_2 = \sigma, \quad x_1^\varkappa + x_2^\varkappa = s_\varkappa.$$

Unter n eine ganze positive ungerade Zahl verstehend, denke man sich s_n als ganze rationale Function von σ_1, σ_2 ausgedrückt, wobei der Gradverhältnisse wegen nur solche Potenzproducte $\sigma_1^\alpha \sigma_2^\beta$ vorkommen können, in welchen $\alpha + 2\beta = n$, also α ungerade ist. Setzt man

$$(1) \qquad s_n = \sigma_1 f_n(\sigma_1^2, \sigma_2),$$

$$f_n(x_1, x_2) = c_{n0} x_1^{\frac{n-1}{2}} + c_{n1} x_1^{\frac{n-3}{2}} x_2 + \cdots + c_{n\,\frac{n-3}{2}} x_1 x_2^{\frac{n-3}{2}} + c_{n\,\frac{n-1}{2}} x_2^{\frac{n-1}{2}}$$

so sind hiedurch die Coefficienten c völlig bestimmt und haben ganzzahlige Werte.

Setzt man in (1) $x_2 = 0$, so ergibt sich $c_{n0} = 1$; setzt man, nachdem man duch σ_1 dividiert hat, $x_2 = -x_1$, so erweist sich $c_{n\,\frac{n-1}{2}} = (-1)^{\frac{n-1}{2}} n$. Ist insbesondere n eine Primzahl p, so hat man

$$s_p = \sigma_1^p + p\,\Gamma(x_1, x_2),$$

wobei Γ eine ganze ganzzahlige Function von x_1, x_2, bedeutet; nun ist Γ symmetrisch und daher als ganze ganzzahlige Function von σ_1, σ_2 darstellbar, woraus man leicht erkennt, dass $c_{p1}, c_{p2}, \ldots c_{p\,\frac{p-1}{2}}$ sämmtlich durch p theilbar sind.

Ist m eine zweite ganze positive ungerade Zahl, so ist

$$R(f_m(x, 1), f_n(x, 1))$$

eine ganze Zahl, deren Abhängigkeit von m und n den Gegenstand unserer Untersuchung bildet. Zur Abkürzung werde $f_n(x, 1)$ mit $f_n(x)$ bezeichnet.

Unmittelbar ersichtlich ist die Richtigkeit der Gleichung

$$R(f_n, f_m) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}} R(f_m, f_n);$$

denn $m - 1$ und $n - 1$ sind die Grade von f_m und f_n.

II.

Haben m und n einen gemeinsamen Theiler $\delta > 1$, so sind $x^m - 1$ und $x^n - 1$ durch $x^\delta - 1$, daher s_m und s_n durch s_δ theilbar.

Da δ ebenfalls ungerade sein muss, erhält man

$$\sigma_1 f_m(\sigma_1^2, \sigma_2) = M(x_1, x_2)\, \sigma_1 f_\delta(\sigma_1^2, \sigma_2),$$
$$\sigma_1 f_m(\sigma_1^2, \sigma_2) = N(x_1, x_2)\, \sigma_1 f_\delta(\sigma_1^2, \sigma_2),$$

worin M, N ganze und offenbar symmetrische Functionen bedeuten, bei deren Darstellung durch σ_1, σ_2 der Gradverhältnisse wegen nur solche Potenzproducte $\sigma_1^\alpha \sigma_2^\beta$ entstehen können, in welchen α gerade ist; ersetzt man daher σ_1^2 durch x, σ_2 durch 1, so erweisen sich $f_m(x)$ und $f_n(x)$ durch $f_\delta(x)$ theilbar, mithin $R(f_m, f_n) = 0$.

Sind hingegen m und n theilerfremd, so ist $R(f_m, f_n)$ keiner anderen Werte fähig als $+1$ und -1.

Zum Beweise genügt die Herstellung einer identischen Gleichung

$$1 = A(x) f_m(x) + B(x) f_n(x),$$

in welcher A und B ganze Zahlen zu Coefficienten haben; in der That würde aus derselben folgen:

$$R(f_m, 1) = R(f_m, A f_m + B f_n),$$

woraus die Theilbarkeit von $R(f_m, 1) = 1$ durch $R(f_m, f_n)$ ersichtlich wäre.

Zur Gewinnung einer solchen Identität hatte ich ursprünglich ein dem Euklid'schen Algorithmus des größten gemeinsamen Theilers nachgebildetes Verfahren angewendet, welches auf der Theilbarkeit von $f_{n+2h} + f_{n-2h}$ durch f_n (siehe unten) beruhte, wobei jedoch mittelst der Festsetzung $f_{-\varkappa} = f_\varkappa$ auch negative Stellenzeiger in Betracht gezogen werden mussten.

Herr Professor Mertens hat mich indessen auf folgenden näheren Weg aufmerksam gemacht.

Man kann zunächst, wie bekannt,

$$x - 1 = P(x)(x^m - 1) + Q(x)(x^n - 1)$$

setzen, wobei P und Q, wie auch die weiteren in dieser Rechnung eingeführten Zeichen, ganze ganzzahlige Functionen bedeuten sollen.

Durch Homogenmachen mit $-x_2$ erhält man

$$\sigma_1 x_2^\nu = H(x_1, x_2)\, s_m + K(x_1, x_2)\, s_n,$$

woraus durch Vertauschung von x_1 und x_2 noch

$$\sigma_1 x_1^\nu = H(x_2, x_1)\, s_m + K(x_2, x_1)\, s_n$$

hervorgeht.

Addiert man diese Gleichungen, nachdem man die erste mit $x_1^{\nu+1}$, die zweite mit $x_2^{\nu+1}$ multipliciert hat, so ergibt sich

$$\sigma_1^2 \sigma_2^\nu = U(\sigma_1, \sigma_2)\, s_m + V(\sigma_1, \sigma_3)\, s_n.$$

In U braucht man nur solche Potenzproducte $\sigma_1^\alpha \sigma_2^\beta$ zu dulden, in welchen $\alpha + 2\beta + m = 2 + 2\nu$, also α ungerade ist; setzt man daher $U(\sigma_1, \sigma_2) = \sigma_1 A(\sigma_1^2, \sigma_2)$ und aus ähnlichen Gründen $V(\sigma_1, \sigma_2) = \sigma_1 . B(\sigma_1^2, \sigma_2)$, so entsteht die Gleichung

$$\sigma_2^\nu = A(\sigma_1^2, \sigma_2) f_m(\sigma_1^2, \sigma_2) + B(\sigma_1^2, \sigma_2) f_n(\sigma_1^2, \sigma_2),$$

aus welcher die gewünschte Identität

$$1 = A(x, 1) f_m(x) + B(x, 1) f_n(x)$$

folgt.

III.

Wird in der identischen Gleichung

$$s_{n+h} + s_{n-h}\, \sigma_2^h = s_n\, s_h \tag{2}$$

in welcher $n > h$ vorausgesetzt ist, n gerade, h ungerade angenommen, so kann sie in die Form

$$\sigma_1 f_{n+h}(\sigma_1^2, \sigma_2) + \sigma_1 f_{n-h}(\sigma_1^2, \sigma_2)\, \sigma_1^h = L(\sigma_1^2, \sigma_2)\, \sigma_1 f_h(\sigma_1^2, \sigma_2)$$

gesetzt werden; dividiert man durch σ_1 und ersetzt hierauf σ_1^2 und σ_2 durch x und 1, so erkennt man die algebraische Theilbarkeit von $f_{n+h}(x) + f_{n-h}(x)$ durch $f_h(x)$. Folglich ist

$$\begin{aligned} R(f_{n+h}, f_h) &= (-1)^{\frac{n+h-1}{2}\frac{h-1}{2}} R(f_h, f_{n+h}) \\ &= (-1)^{\frac{n+h-1}{2}\frac{h-1}{2} + \frac{h-1}{2}} R(f_h, f_{n-h}) \\ &= (-1)^{\frac{n+h-1}{2}\frac{h-1}{2} + \frac{h-1}{2} + \frac{h-1}{2}\frac{n-h-1}{2}} R(f_{n-h}, f_h) \\ &= R(f_{n-h}, f_h). \end{aligned}$$

Sind daher m, m' zwei positive ungerade Zahlen und $m \equiv m' \pmod{h}$, so ist

$$R(f_m, f_h) = R(f_{m'}, f_h).$$

Wird dagegen in (2) n ungerade, h gerade angenommen, so führt eine ähnliche Rechnung zu der Formel

$$R(f_{n+h}, f_n) = (-1)^{\frac{n-1}{2}} R(f_{n-h}, f_n).$$

Für $h = n-1$ wird also

$$R(f_{2n-1}, f_n) = (-1)^{\frac{n-1}{2}} R(f_1, f_n) = (-1)^{\frac{n-1}{2}}.$$

Hingegen entsteht für $h = 2$

$$\begin{aligned} R(f_{n+2}, f_n) &= (-1)^{\frac{n-1}{2}} R(f_{n-1}, f_n) \\ &= (-1)^{\frac{n-1}{2}} R(f_n, f_{n-2}); \end{aligned}$$

ist um $n-2 > 1$, so hat man ebenso weiter

$$\begin{aligned} R(f_n, f_{n-2} &= (-1)^{\frac{n-3}{2}} R(f_{n-2}, f_{n-4}), \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ R(f_5, f_3) &= -R(f_3, f_1) \\ &= -1; \end{aligned}$$

durch Multiplication liefern diese Gleichungen die Formel

$$R(f_{n+2}, f_n) = (-1)^{1+2+\ldots+\frac{n-1}{2}} = (-1)^{\frac{n^2-1}{8}}.$$

IV.

Es sei nun p eine positive ungerade Primzahl. Dann ist

$$\begin{aligned} R(f_m, f_p) &\equiv R(f_m, x^{\frac{p-1}{2}}) \pmod{p} \\ &\equiv (-1)^{\frac{m-1}{2}\frac{p-1}{2}} R(x^{\frac{p-1}{2}}, c_{m\,\frac{m-1}{2}}) \pmod{p} \\ &\equiv m^{\frac{p-1}{2}} \pmod{p}. \end{aligned}$$

Folglich ist $R(f_m, f_p)$ identisch mit dem Legendre'schen Symbole $\left(\frac{m}{p}\right)$.

Ferner folgt aus der Congruenz

$$\sigma_1^p \equiv s_p \pmod{p},$$

wenn x_1, x_2 durch x_1^n, x_2^n ersetzt werden,

$$s_n^p \equiv s_{np} \pmod{p};$$

mithin ist

$$\sigma_1^p s_{np} \equiv s_p s_n^p \pmod{p}.$$

Wenn daher n eine positive ungerade Zahl bedeutet, ist

$$\sigma_1^p \sigma_1 f_{np}(\sigma_1^2, \sigma_2) = \sigma_1 f_p(\sigma_1^2, \sigma_2) \sigma_1^p f_n^p(\sigma_1^2, \sigma_2) + p L(\sigma_1, \sigma_2),$$

worin L eine ganze ganzzahlige Function vorstellt.

Hieraus folgt

$$x^{p+1} f_{np}(x^2) = x^{p+1} f_p(x^2) f_n^p(x^2) + p L_0(x),$$

worin wieder L_0 ganze Zahlen zu Coefficienten hat.

Aus dieser Gleichung schließt man leicht:

$$f_{np}(x) \equiv f_p(x) f_n^p(x) \pmod{p}.$$

Dann ist aber

$$R(f_{np}, f_m) \equiv R^p(f_n, f_m) R(f_p, f_m) \pmod{p},$$

folglich, da $p \equiv 1 \pmod 2$ ist,

$$R(f_{np}, f_m) = R(f_n, f_m) R(f_p, f_m).$$

Sind daher $n_1, n_2 \ldots, n_\nu$ ungerade positive Zahlen, N ihr Product, so ist

$$R(f_N, f_m) = R(f_{n_1}, f_m) R(f_{n_2}, f_m) \ldots R(f_{n_\nu}, f_m).$$

Aus denselben Gründen ist aber

$$R(f_m, f_N) = R(f_m, f_{n_1}) R(f_m, f_{n_2}) \ldots R(f_m, f_{n_\nu}).$$

Hiedurch ist die Identität von $R(f_m, f_n)$ mit dem Jacobi'schen Symbole $\left(\frac{m}{n}\right)$ dargethan und die vorhin bewiesenen Formeln fallen zusammen mit den bekannten Gleichungen

$$\left(\frac{m}{h}\right) = \left(\frac{m'}{h}\right), \text{ wenn } m \equiv m' \text{ (mod. } h),$$

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

$$\left(\frac{n_1 \cdot n_2 \cdots n_\nu}{m}\right) = \left(\frac{n_1}{m}\right)\left(\frac{n_1}{m}\right)\cdots\left(\frac{n_\nu}{m}\right),$$

$$\left(\frac{m}{n_1 \cdot n_2 \cdots n_\nu}\right) = \left(\frac{m}{n_1}\right)\left(\frac{m}{n_2}\right)\cdots\left(\frac{m}{n_\nu}\right),$$

während die letzte Formel (I) das Reciprocitätsgesetz

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

enthält.