

ANWENDUNG JACOBISCHER THETAFUNKTIONEN AUF DIE POTENZRESTE

TOMIO KUBOTA

Eisenstein führte in seiner Abhandlung [1] einen durchsichtigen, analytischen Beweis des Reziprozitätsgesetzes der Potenzreste im rationalen und Gausschen Zahlkörper. Zur kurzen Fassung seiner Methode im rationalen Fall, seien m und n positive ganzrationale Zahlen und sei

$$f(z) = e^{2\pi iz} - e^{-2\pi iz}.$$

Dann ist ersichtlich $f(-z) = -f(z)$ und zudem gilt die folgende Multiplikationsformel

$$f(nz) = f(z) f\left(z + \frac{1}{n}\right) \cdots f\left(z + \frac{n-1}{n}\right).$$

Ist andererseits M eine Menge ganzrationaler Zahlen, für die die Vereinigung $\{0, M, -M\}$ ¹⁾ ein vollkommenes Restsystem mod. m bildet, so ergibt sich nach dem Gausschen Lemma²⁾

$$\left(\frac{n}{m}\right) = \prod_{a \in M} \frac{f\left(\frac{na}{m}\right)}{f\left(\frac{a}{m}\right)}.$$

Wenn wir wie die Menge M eine gleichbedeutende Menge N in bezug auf n auswählen, so gilt auch

$$\left(\frac{m}{n}\right) = \prod_{b \in N} \frac{f\left(\frac{mb}{n}\right)}{f\left(\frac{b}{n}\right)}.$$

Wegen der obigen Multiplikationsformel ist nun

Received May 19, 1961.

¹⁾ Allgemein bedeutet aM die Menge aller am mit $m \in M$. Insbesondere ist $-M = (-1)M$.

²⁾ In dieser Hinsicht siehe Reichardt [4].

$$\binom{n}{m} = \prod_{a \in \mathcal{M}} \prod_{\substack{b \bmod n \\ i: \frac{a}{m} + \frac{b}{n} \\ i: \frac{a}{m} - \frac{b}{n}}} f\left(\frac{a}{m} + \frac{b}{n}\right) = \prod_{a \in \mathcal{M}, b \in \mathcal{N}} f\left(\frac{a}{m} + \frac{b}{n}\right) f\left(\frac{a}{m} - \frac{b}{n}\right)$$

und also

$$\binom{n}{m} = \prod_{a \in \mathcal{M}, b \in \mathcal{N}} \varphi\left(\frac{a}{m}, \frac{b}{n}\right)$$

mit $\varphi(x, y) = f(x+y)f(x-y)$. Ganz analog ist

$$\binom{m}{n} = \prod_{a \in \mathcal{M}, b \in \mathcal{N}} \varphi\left(\frac{b}{n}, \frac{a}{m}\right).$$

Aus diesen zwei Formeln, wenn nur $\varphi(y, x) = -\varphi(x, y)$ beachtet wird, folgt sogleich das Reziprozitätsgesetz

$$\binom{n}{m} \binom{m}{n} = (-1)^{(m-1)/2 \cdot (n-1)/2}.$$

Eisenstein betrachtete in [2] auf derselben Grundlage ausführlich die 4-ten Potenzreste im Gaußschen Körper und fasste dann in einer längeren Arbeit [3] auch mit einem wesentlich gleichen Gedankengang die 4-ten Potenzreste im Gaußschen Körper und die 6-ten Potenzreste im Körper der dritten Einheitswurzeln (sogenannten Eisensteinschen Körper) zusammen, wobei die Thetafunktion eingetreten ist.

Was wir in der vorliegenden Arbeit entwickeln wollen, ist eine möglichst klare Darstellung Eisensteinscher Idee. Nämlich soll erwiesen werden, dass das Reziprozitätsgesetz der Potenzreste in einem beliebigen imaginären Zahlkörper in seiner allgemeinsten Form sehr glatt unter Verwendung der seitdem entwickelten Theorie der Jacobischen Thetafunktionen hervorkommt. Dabei braucht man weder Erweiterungskörper noch Ideale, sondern nur die fundamentalen Transformationsformeln der Thetafunktionen. Es wird vielmehr gezeigt, dass das Reziprozitätsgesetz der Potenzreste recht einfach aus Eigenschaften analytischer Mannigfaltigkeit (elliptischer Kurve) abgeleitet werden kann.

§ 1. Einführung gewisser normierten elliptischen Funktionen

Es sei F ein imaginär-quadratischer Zahlkörper und $1, \omega$ eine Ganzheitsbasis von F , wo ω einen positiven imaginären Teil $\text{Im } \omega > 0$ hat. Die elliptische Funktion mit den Perioden $1, \omega$ und mit dem Divisor

$$(1) \quad (f) = (0) + \left(\frac{1+\omega}{2}\right) - \left(\frac{1}{2}\right) - \left(\frac{\omega}{2}\right)^3$$

bestimmt sich bis auf einen konstanten Faktor, also wird eine solche Funktion dadurch eindeutig normiert, dass

$$(2) \quad f\left(\frac{1}{4}\right) = 1$$

ist. Nach dieser Normierung ergibt sich nun

$$(3) \quad f(z) = i \frac{\vartheta(z)\vartheta\left(z + \frac{1+\omega}{2}\right)}{\vartheta\left(z + \frac{1}{2}\right)\vartheta\left(z + \frac{\omega}{2}\right)}$$

mit

$$\vartheta(z) = \vartheta(z|\omega) = 2 \sum_{n=0}^{\infty} (-1)^n e^{((n+1)/2)^2 \pi i \omega} \sin(2n+1)\pi z, \quad \vartheta(0) = 0.$$

In der Tat folgt (2) aus den beiden fundamentalen Eigenschaften der Theta-funktion

$$(4) \quad \vartheta(z+1) = -\vartheta(z), \quad \vartheta(z+\omega) = -e^{-\pi i(2z+\omega)} \vartheta(z),$$

d.h.,

$$\begin{aligned} f\left(\frac{1}{4}\right) &= i \frac{\vartheta\left(\frac{1}{4}\right)\vartheta\left(\frac{1}{4} + \frac{1+\omega}{2}\right)}{\vartheta\left(\frac{1}{4} + \frac{1}{2}\right)\vartheta\left(\frac{1}{4} + \frac{\omega}{2}\right)} = i \frac{\vartheta\left(-\frac{3}{4} + 1\right)\vartheta\left(\frac{3}{4} + \frac{\omega}{2}\right)}{\vartheta\left(\frac{3}{4}\right)\vartheta\left(-\frac{3}{4} - \frac{\omega}{2} + 1 + \omega\right)} \\ &= -i \frac{\vartheta\left(-\frac{3}{4}\right)\vartheta\left(\frac{3}{4} + \frac{\omega}{2}\right)}{\vartheta\left(\frac{3}{4}\right)\vartheta\left(-\frac{3}{4} - \frac{\omega}{2}\right) e^{\pi i(-3/2-\omega+\omega)}} = -ie^{-3\pi i/2} = 1. \end{aligned}$$

Ähnlicherweise ist

$$\begin{aligned} f\left(\frac{\omega}{4}\right) &= i \frac{\vartheta\left(\frac{\omega}{4}\right)\vartheta\left(\frac{\omega}{4} + \frac{1+\omega}{2}\right)}{\vartheta\left(\frac{\omega}{4} + \frac{1}{2}\right)\vartheta\left(\frac{\omega}{4} + \frac{\omega}{2}\right)} = i \frac{\vartheta\left(-\frac{3\omega}{4} + \omega\right)\vartheta\left(\frac{3\omega}{4} + \frac{1}{2}\right)}{\vartheta\left(-\frac{3\omega}{4} - \frac{1}{2} + 1 + \omega\right)\vartheta\left(\frac{3\omega}{4}\right)} \\ &= -ie^{-\pi i(-3\omega/2+\omega)} e^{\pi i(-3\omega/2-1+\omega)} = -ie^{-\pi i} = i, \end{aligned}$$

i.e.,

³⁾ Hier bedeutet (z) den der komplexen Zahl z zugeordneten Punkt auf der elliptischen Kurve \mathcal{C} , die durch $1, \omega$ bestimmt wird.

$$(5) \quad f\left(\frac{\omega}{4}\right) = i.$$

Ferner ist ersichtlich

$$(6) \quad f(-z) = -f(z)$$

und aus (2), (5) und (6) folgt

$$(7) \quad f(z)f\left(z + \frac{1}{2}\right) = -1, \quad f(z)f\left(z + \frac{\omega}{2}\right) = 1.$$

Zum Beweis des quadratischen Reziprozitätsgesetzes in imaginär-quadratischen Körpern reicht diese einzige Funktion f aus. Auch für die biquadratische Reziprozität im Gaußschen Körper wird die Funktion f verwendet, allerdings mit der Festsetzung $\omega = i$. Dabei erfüllt f überdies

$$(8) \quad f(iz) = if(z).$$

Wollen wir im Eisensteinschen Körper $F = \mathbf{Q}(\rho)$ ($\rho = e^{2\pi i/3}$, \mathbf{Q} : der rationale Zahlkörper) die 3-ten und 6-ten Potenzreste behandeln, so soll eine andere Funktion eingeführt werden. Es ist nämlich die elliptische Funktion g mit den Perioden 1, ω und mit dem Divisor

$$(9) \quad (g) = -2(0) + (\gamma) + (-\gamma),$$

wo $\omega = \rho$ und $\gamma = \frac{2+\rho}{3}$ ist. Normiert eindeutig durch

$$(10) \quad g\left(\frac{1}{3}\right) = 1,$$

hat g die Form

$$(11) \quad g(z) = e^{2\pi i(1+\gamma)/3} \frac{\vartheta(z+\gamma)\vartheta(z-\gamma)}{\vartheta(z)^2},$$

denn aus (4) und

$$(12) \quad \vartheta(\rho z) = \rho e^{-\pi i \rho z^2} \vartheta(z), \quad \vartheta(\rho^2 z) = \rho^2 e^{\pi i \rho^2 z^2} \vartheta(z)$$

folgt

$$g\left(\frac{1}{3}\right) = e^{2\pi i(1+\gamma)/3} \frac{\vartheta\left(\frac{1}{3} + \gamma\right)\vartheta\left(\frac{1}{3} - \gamma\right)}{\vartheta\left(\frac{1}{3}\right)^2} = e^{2\pi i(1+\gamma)/3} \frac{\vartheta\left(\frac{\rho}{3} + 1\right)\vartheta\left(\frac{\rho^2}{3}\right)}{\vartheta\left(\frac{1}{3}\right)^2}$$

$$\begin{aligned}
&= -e^{2\pi i(1+\gamma)/3} \frac{\vartheta\left(\frac{\rho}{3}\right)\vartheta\left(\frac{\rho^2}{3}\right)}{\vartheta\left(\frac{1}{3}\right)^2} = -e^{2\pi i(1+\gamma)/3} \cdot \rho e^{-(\pi i\rho/9)} \cdot \rho^2 e^{\pi i\rho^2/9} \\
&= -e^{2\pi i(1+\gamma)/3} e^{\pi i(-1-2\rho)/9} = -e^{\pi i(4+2\rho+6-1-2\rho)/9} = 1.
\end{aligned}$$

Ferner hat man

$$(13) \quad g(-z) = g(z), \quad g(\rho z) = \rho g(z)$$

und aus (10) und (13) folgt

$$g(z)g(z+\gamma)g(z-\gamma) = 1.$$

Diese letzte Formel ist eine fundamentale Eigenschaft von g , wovon jedoch im folgenden keinen Gebrauch gemacht wird.

§ 2. Multiplikationsformeln

Für einen imaginär-quadratischen Körper F mit einer Ganzheitsbasis $1, \omega$, wo $\text{Im } \omega > 0$ ist, wird jetzt die in § 1 definierte elliptische Funktion f betrachtet. Der Einfachheit halber setzen wir dabei voraus, dass

$$\omega \notin 1$$

ist, wenn nur 2 sich in F verzweigt und $2 = \mathfrak{l}^2$ mit einem Primideal \mathfrak{l} von F vorkommt.

Nun sei ν eine zu 2 prime ganze Zahl von F , die $\nu \equiv 1 \pmod{2}$ genügt, falls 2 in F prim ist. Dann bleibt der Divisor (f) in (1) unverändert beim von ν bestimmten Endomorphismus der von $1, \omega$ bestimmten elliptischen Kurve \mathcal{C} . Der Divisor von $f(\nu z)$ stimmt also mit dem von $\prod_{\beta \bmod \nu} f\left(z + \frac{\beta}{\nu}\right)$ überein, und die Gleichung

$$(14) \quad f(\nu z) = \varepsilon_\nu \prod_{\beta \bmod \nu} f\left(z + \frac{\beta}{\nu}\right)$$

ergibt sich mit einer Konstante ε_ν .

Um ε_ν zu bestimmen, betrachtet man das Produkt

$$(15) \quad \prod'_{\beta \bmod \nu} f\left(\frac{1}{4} + \frac{\beta}{\nu}\right),$$

wo mit dem Strich die Ausschließung von $\beta \equiv 0 \pmod{\nu}$ gemeint wird. Es sei N eine Menge von ganzen Zahlen von F , für die die Vereinigung $\{0, N, -N\}$

ein vollkommenes Restsystem mod. ν ist. Wenn β in (15) dann die Vereinigung $\{N, -N\}$ durchläuft, so ist

$$(16) \quad \sum'_{\beta \bmod \nu} \frac{\beta}{\nu} = 0.$$

Wegen (3), (4) und (16) ergibt sich jetzt

$$\begin{aligned} \prod'_{\beta \bmod \nu} f\left(\frac{1}{4} + \frac{\beta}{\nu}\right) &= \prod'_{\beta \bmod \nu} \frac{i\vartheta\left(\frac{1}{4} + \frac{\beta}{\nu}\right)\vartheta\left(\frac{1}{4} + \frac{\beta}{\nu} + \frac{1+\omega}{2}\right)}{\vartheta\left(\frac{1}{4} + \frac{\beta}{\nu} + \frac{1}{2}\right)\vartheta\left(\frac{1}{4} + \frac{\beta}{\nu} + \frac{\omega}{2}\right)} \\ &= \prod'_{\beta \bmod \nu} \frac{i\vartheta\left(-\frac{3}{4} - \frac{\beta}{\nu} + 1\right)\vartheta\left(\frac{3}{4} + \frac{\beta}{\nu} + \frac{\omega}{2}\right)}{\vartheta\left(\frac{3}{4} + \frac{\beta}{\nu}\right)\vartheta\left(-\frac{3}{4} - \frac{\beta}{\nu} - \frac{\omega}{2} + 1 + \omega\right)} \\ &= (-1)^{(N\nu-1)/2} \prod'_{\beta \bmod \nu} e^{\pi i(-3/2-2\beta/\nu-\omega+\omega)} = e^{-2\pi i \sum' \beta/\nu} = 1, \end{aligned}$$

also ist

$$(17) \quad \prod'_{\beta \bmod \nu} f\left(\frac{1}{4} + \frac{\beta}{\nu}\right) = 1.$$

Diese Formel wird hergeleitet nur aus der Voraussetzung $(\nu, 2) = 1$. Setzt man $z = \frac{1}{4}$ in (14), so kann die Konstante ε_ν sofort wegen (2) und (17) bestimmt werden:

$$f\left(\frac{\nu}{4}\right) = \varepsilon_\nu.$$

Die Konstante ε_ν bestimmt sich noch näher durch (2), (5), (6) und (7). Wenn nämlich 2 sich nicht in F verzweigt, so ist $\varepsilon_\nu = 1$ oder $\varepsilon_\nu = -1$ für ν mit $\nu \equiv 1 \pmod{2}$ ⁴⁾, je nachdem $\nu \equiv 1, 1+2\omega \pmod{4}$ oder $\nu \equiv -1, -1+2\omega \pmod{4}$ ist. Wenn ferner 2 sich in F verzweigt, so hat ε_ν den gleichen Wert wie oben für $\nu \equiv 1 \pmod{2}$, aber für sonstige ν ist $\varepsilon_\nu = i$ oder $\varepsilon_\nu = -i$, je nachdem $\nu \equiv \omega, \omega+2 \pmod{4}$ oder $\nu \equiv -\omega, -\omega+2 \pmod{4}$ ist. Ist insbesondere F der Gausssche Körper und $\omega = i$, so gilt

$$(18) \quad \varepsilon_\nu = (-1)^{(N\nu-1)/4} \sigma_\nu,$$

wo σ_ν die Potenz von i mit $\sigma_\nu \equiv \nu \pmod{l^2}$, $l^2 = 2$ ist.

Da wir die Multiplikationsformel (14) mit explizitem Wert von ε_ν erledigten,

⁴⁾ Wenn 2 in F vollzerlegt ist, so ist stets $\nu \equiv 1 \pmod{2}$.

wollen wir uns nächstens der Funktion g in §1 zuwenden. Es sei \mathcal{C} die der Ganzheitsbasis 1, ρ vom Eisensteinischen Körper $F = \mathbf{Q}(\rho)$ zugeordnete elliptische Kurve. Ist ν dann eine zu 3 prime ganze Zahl von F , so bleibt der Divisor (g) in (9) beim von ν bestimmten Endomorphismus von \mathcal{C} unverändert. Also haben $g(\nu z)$ und $\prod_{\beta \bmod \nu} g\left(z + \frac{\beta}{\nu}\right)$ einen und denselben Divisor, und die Gleichung

$$(19) \quad g(\nu z) = \delta_\nu \prod_{\beta \bmod \nu} g\left(z + \frac{\beta}{\nu}\right)$$

gilt mit einer Konstante δ_ν . Wie bei der Funktion f , wird hier das Produkt

$$(20) \quad \prod'_{\beta \bmod \nu} g\left(\frac{1}{3} + \frac{\beta}{\nu}\right)$$

untersucht. Ist N eine Menge ganzer Zahlen von F , für die die Vereinigung $\{0, N, \rho N, \rho^2 N\}$ ein vollkommenes Restsystem mod. ν ist, und durchläuft β in (20) die Vereinigungsmenge $\{N, \rho N, \rho^2 N\}$, so ist

$$(21) \quad \sum'_{\beta \bmod \nu} \frac{\beta}{\nu} = 0, \quad \sum'_{\beta \bmod \nu} \frac{\beta^2}{\nu^2} = 0.$$

Wegen (4), (11), (12) und (21) gilt also

$$\begin{aligned} \prod'_{\beta \bmod \nu} g\left(\frac{1}{3} + \frac{\beta}{\nu}\right) &= \prod'_{\beta \bmod \nu} \frac{e^{2\pi i(1+\tau)/3} \vartheta\left(\frac{1}{3} + \frac{\beta}{\nu} + \tau\right) \vartheta\left(\frac{1}{3} + \frac{\beta}{\nu} - \tau\right)}{\vartheta\left(\frac{1}{3} + \frac{\beta}{\nu}\right)^2} \\ &= \prod'_{\beta \bmod \nu} \frac{e^{2\pi i(1+\tau)/3} \vartheta\left(\frac{\rho}{3} + \frac{\rho\beta}{\nu} + 1\right) \vartheta\left(\frac{\rho^2}{3} + \frac{\rho^2\beta}{\nu}\right)}{\vartheta\left(\frac{1}{3} + \frac{\beta}{\nu}\right)^2} \\ &= (-1)^{N\nu-1} \prod'_{\beta \bmod \nu} e^{-\pi i \rho(1/3 + \beta/\nu)^2 + \pi i \rho^2(1/3 + \beta/\nu)^2 + 2\pi i(1+\tau)/3} \\ &= (-1)^{N\nu-1} \prod'_{\beta \bmod \nu} e^{\pi i - 2\pi i(\rho - \rho^2)/3 \cdot \Sigma' \beta/\nu - \pi i(\rho - \rho^2) \Sigma' \beta^2/\nu^2} = 1. \end{aligned}$$

Wenn daher $z = \frac{1}{3}$ in (19) gesetzt wird, so folgt aus (10), dass

$$g\left(\frac{\nu}{3}\right) = \delta_\nu$$

ist. Wegen (13) lässt sich diese δ_ν noch deutlicher bestimmen, d.h., $\delta_\nu = 1$, $\delta_\nu = \rho$ oder $\delta_\nu = \rho^2$, je nachdem $\nu \equiv \pm 1$, $\nu \equiv \pm \rho$ oder $\nu \equiv \pm \rho^2 \pmod{3}$ ist. Mit anderen Worten: δ_ν ist eine dritte Einheitswurzel, die $\delta_\nu \equiv \pm \nu \pmod{3}$ erfüllt.

§ 3. Quadratische und biquadratische Reste

Anfänglich wird das quadratische Reziprozitätsgesetz in einem imaginär-quadratischen Zahlkörper gewonnen. Es sei F ein imaginär-quadratischer Zahlkörper, $1, \omega$ seine Ganzheitsbasis und f die vorher besprochene elliptische Funktion. Sind dann μ, ν miteinander prime und auch zu 2 prime ganze Zahlen von F , die, falls 2 in F prim ist, noch der Bedingung $\mu \equiv \nu \equiv 1 \pmod{2}$ Genüge leisten sollen, so gilt nach dem Gauss'schen Lemma

$$(22) \quad \left(\frac{\nu}{\mu}\right) = \prod_{\alpha \in \mathcal{V}} \frac{f\left(\frac{\nu\alpha}{\mu}\right)}{f\left(\frac{\alpha}{\mu}\right)}$$

wo M eine Menge der ganzen Zahlen von F , für die die Vereinigung $\{0, M, -M\}$ ein vollkommenes Restsystem mod. μ ist. Mit einer gleichbedeutenden Menge N für ν ergibt sich ferner

$$(23) \quad \left(\frac{\mu}{\nu}\right) = \prod_{\beta \in \mathcal{V}} \frac{f\left(\frac{\mu\beta}{\nu}\right)}{f\left(\frac{\beta}{\nu}\right)}$$

Ist $\varphi(x, y) = f(x+y)f(x-y)$, so ist

$$(24) \quad \varphi(x, y) = -\varphi(y, x)$$

und wegen der Multiplikationsformel (14) gibt (22) die Beziehung

$$\prod_{\alpha \in M} \varepsilon_{\nu} \prod_{\beta \in \mathcal{V}, -\mathcal{V}} f\left(\frac{\alpha}{\mu} + \frac{\beta}{\nu}\right) = \varepsilon_{\nu}^{(N\mu-1)/2} \prod_{\alpha \in M, \beta \in N} \varphi\left(\frac{\alpha}{\mu}, \frac{\beta}{\nu}\right),$$

also

$$(25) \quad \left(\frac{\nu}{\mu}\right) = \varepsilon_{\nu}^{(N\mu-1)/2} \prod_{\alpha \in M, \beta \in N} \varphi\left(\frac{\alpha}{\mu}, \frac{\beta}{\nu}\right).$$

Wegen (23) gilt ähnlicherweise

$$(26) \quad \left(\frac{\mu}{\nu}\right) = \varepsilon_{\mu}^{(N\nu-1)/2} \prod_{\alpha \in M, \beta \in N} \varphi\left(\frac{\beta}{\nu}, \frac{\alpha}{\mu}\right)$$

und jetzt folgt aus (24), (25) und (26) das Reziprozitätsgesetz⁵⁾

⁵⁾ Dies Gesetz gilt, wenn μ oder ν eine Einheit ist. Denn der obige Gedankengang bleibt bei solchem Fall noch richtig, sobald man ein eventuell vorkommendes leeres Produkt in (14) als 1 ansieht.

$$(27) \quad \left(\frac{\nu}{\mu}\right)\left(\frac{\mu}{\nu}\right) = (-1)^{(N\mu-1)/2 \cdot (N\nu-1)/2} \frac{\varepsilon_\nu^{(N\mu-1)/2}}{\varepsilon_\mu^{(N\nu-1)/2}}.$$

Da ε_ν nur von $\nu \pmod{4}$ abhängt, folgt aus (27) selbstverständlich

$$(28) \quad \left(\frac{\nu}{\mu}\right) = \left(\frac{\mu}{\nu}\right) \text{ f\u00fcr } \nu \equiv 1 \pmod{4}, (\mu, 2) = 1,$$

falls 2 in F nicht prim ist. Aber (28) gilt auch dann, wenn 2 in F prim ist, weil in diesem Fall $\left(\frac{\nu}{\mu}\right) = \left(\frac{\nu}{\mu^3}\right)$, $\left(\frac{\mu}{\nu}\right) = \left(\frac{\mu^3}{\nu}\right)$ und $\mu^3 \equiv 1 \pmod{2}$ bestehen und zudem (28) f\u00fcr $\mu \equiv 1 \pmod{2}$ vorhanden ist.

Nun soll das Gesetz (27) zu einer noch bequemeren Gestalt umgeformt werden. Ist 2 in F vollzerlegt, so ist ε_ν ein Kongruenzcharakter mod. 4, der den Wert -1 f\u00fcr $\nu = -1$ annimmt. Es gibt zwei solche Charaktere, aber beide k\u00f6nnen als ε_ν bei verschiedenen ausgew\u00e4hlten ω vorkommen. Darum k\u00f6nnen wir erschliessen, dass

$$(29) \quad \left(\frac{\nu}{\mu}\right)\left(\frac{\mu}{\nu}\right) = (-1)^{(N\mu-1)/2 \cdot (N\nu-1)/2} \chi(\nu)^{(N\mu-1)/2} \chi(\mu)^{(N\nu-1)/2},$$

$$((\mu, \nu) = (\mu, 2) = (\nu, 2) = 1),$$

f\u00fcr einen beliebigen Kongruenzcharakter χ mod. 4 mit $\chi^2 = 1$, $\chi(-1) = -1$ von F ist.

Ist 2 in F prim, so gibt es nach der Struktur der Restklassen mod. 4 auch zwei Kongruenzcharaktere mod. 4 mit $\chi^2 = 1$, $\chi(-1) = -1$, und zwar k\u00f6nnen die beide ε_ν sein, wenn man sie auf ν mit $\nu \equiv 1 \pmod{2}$ beschr\u00e4nkt. Also besteht (29) f\u00fcr $\nu \equiv \mu \equiv 1$. Da aber $\left(\frac{\nu}{\mu}\right) = \left(\frac{\nu^3}{\mu^3}\right)$, $\nu^3 \equiv \mu^3 \equiv 1 \pmod{2}$ f\u00fcr beliebige μ, ν mit $(\mu, \nu) = (\mu, 2) = (\nu, 2) = 1$ gilt und ferner $N\mu^3 - 1 \equiv N\mu - 1 \pmod{4}$, $\chi(\mu^3) = \chi(\mu)$ ist, ist (29) auch f\u00fcr diesen Fall allgemein richtig.

F\u00fcr einen imagin\u00e4r-quadratischen K\u00f6rper F , worin 2 sich verzweigt, sind andere Formeln als (29) n\u00f6tig. Diesen Fall teilen wir noch in zwei F\u00e4lle und setzen vorerst voraus, dass $F = \mathbf{Q}(\sqrt{m})$ mit einer quadratfreien, ungeraden ganzrationalen Zahl m ist. Es sei $2 = i^2$ in F und sei $\eta_\nu = 1$ oder -1 , je nachdem $\nu \equiv 1 \pmod{2}$ oder nicht f\u00fcr eine ganze Zahl ν von F . Dann ist $\varepsilon_\nu^2 = \eta_\nu$ und es ist $N\nu \equiv 1 \pmod{4}$ f\u00fcr den betreffenden K\u00f6rper F . Nach (27) ist also

$$(30) \quad \left(\frac{\nu}{\mu}\right)\left(\frac{\mu}{\nu}\right) = \eta_\nu^{(N\mu-1)/4} \eta_\mu^{(N\nu-1)/4}.$$

Der zun\u00e4chst zu betrachtende Fall ist der von F mit $F = \mathbf{Q}(\sqrt{m})$, wo m

eine gerade, quadratfreie ganzrationale Zahl ist. Es sei hier $\theta_\nu = 0$ oder 1, je nachdem $\nu \equiv 1 \pmod{2}$ oder nicht und es sei χ ein Kongruenzcharakter mod. 4 mit $\chi^2 = 1$, $\chi(-1) = -1$ von F . Da dann $1 + 2\omega$ ein quadratischer Rest mod. 4 ist ($\omega^2 \equiv 1 + 2\omega \pmod{4}$), folgt aus der expliziten Wertangabe von ε_ν in § 2, dass $\varepsilon_\nu = \chi(\nu)i^{0\nu}$ oder $\varepsilon_\nu = \chi(\nu)i^{-0\nu}$ stattfindet. Andererseits für $\nu \equiv 1 \pmod{2}$ ist die Zahl $(N_\nu - 1)/2$ durch 4 teilbar und für sonstige ν ist sie ungerade und gehört einer festen Restklasse mod 4. Daraus ergibt sich

$$\frac{\varepsilon_\nu^{(N_\nu - 1)/2}}{\varepsilon_\mu^{(N_\mu - 1)/2}} = \chi(\nu)^{(N_\mu - 1)/2} \chi(\mu)^{(N_\nu - 1)/2}$$

und kommt (29) wieder vor.

Beiläufig soll bemerkt werden, dass das wohlbekannte Reziprozitätsgesetz

$$\left(\frac{\nu}{\mu}\right)\left(\frac{\mu}{\nu}\right) = (-1)^{S((\mu-1)/2 \cdot (\nu-1)/2)}, \quad (\mu \equiv \nu \equiv 1 \pmod{2}),$$

für einen beliebigen imaginär-quadratischen Zahlkörper ohne Mühe von den bisher erhaltenen Tatsachen erledigt wird.

Auch kann das Gesetz (29) etwas anderes ausgesprochen werden. Es sei nämlich $(\nu) \rightarrow \nu^* \in F$ eine solche multiplikative Abbildung von zu 2 primen Idealen von F , dass $(\nu^*) = (\nu)$ ist und aus $\nu \equiv 1 \pmod{4}$ die Gleichheit $\nu^* = \nu$ folgt. Dann ist ν^* ein sogenannter Größencharakter mod. 4 und (29) gibt

$$(31) \quad \left(\frac{\nu^*}{\mu}\right)\left(\frac{\mu}{\nu}\right) = (-1)^{(N_\mu - 1)/2 \cdot (N_\nu - 1)/2}.$$

Es ist noch zu beachten, dass man (30) ebenfalls als eine Umformung von (29) oder (31) verstehen kann, indem man einen Kongruenzcharakter χ mod. 4 mit den Eigenschaften $\chi^4 = 1$, $\chi(-1) = -1$ aufnimmt und formal

$$\left(\frac{i}{\mu}\right) = (-1)^{(N_\mu - 1)/4}$$

setzt.

Da wir schon die quadratischen Reste vollständig durchsehen haben, wollen wir nun die 4-ten Reste im Gausschen Körper $F = \mathbf{Q}(i)$ behandeln. Es geht ganz ähnlich wie bisher. Es seien μ, ν zwei zueinander und zu 2 prime ganze Zahlen von F , und f die mit $\omega = i$ definierte Funktion in § 1. Dann ist nach (8) und dem Gausschen Lemma

$$\left(\frac{\nu}{\mu}\right)_4 = \prod_{\alpha \in M} \frac{f\left(\frac{\nu\alpha}{\mu}\right)}{f\left(\frac{\alpha}{\mu}\right)},$$

wo M eine Menge ganzer Zahlen von F , für die die Vereinigung $\{0, M, iM, -M, -iM\}$ ein vollkommenes Restsystem mod. μ ist. Ist ferner $\varphi(x, y) = f(x+y)f(x+iy)f(x-y)f(x-iy)$, so ist

$$(32) \quad \varphi(x, y) = -\varphi(y, x)$$

und wie bei quadratischen Resten ist

$$(33) \quad \left(\frac{\nu}{\mu}\right)_4 = \varepsilon_\nu^{(N_\mu-1)/4} \prod_{\alpha \in M, \beta \in N} \varphi\left(\frac{\alpha}{\mu}, \frac{\beta}{\nu}\right),$$

wo N von gleicher Bedeutung für ν ist. Da andererseits

$$(34) \quad \left(\frac{\mu}{\nu}\right)_4 = \varepsilon_\mu^{(N_\nu-1)/4} \prod_{\alpha \in M, \beta \in N} \varphi\left(\frac{\beta}{\nu}, \frac{\alpha}{\mu}\right)$$

entsteht, folgt aus (32), (33) und (34) die Beziehung

$$\left(\frac{\nu}{\mu}\right)_4 \left(\frac{\mu}{\nu}\right)_4^{-1} = (-1)^{(N_\mu-1)/4 + (N_\nu-1)/4} \frac{\varepsilon_\nu^{(N_\mu-1)/4}}{\varepsilon_\mu^{(N_\nu-1)/4}},$$

und wegen (18) ergibt sich das Reziprozitätsgesetz in bekannter Form

$$(35) \quad \left(\frac{\nu}{\mu}\right)_4 \left(\frac{\mu}{\nu}\right)_4^{-1} = (-1)^{(N_\mu-1)/4 + (N_\nu-1)/4} \frac{\sigma_\nu^{(N_\mu-1)/4}}{\sigma_\mu^{(N_\nu-1)/4}}.$$

Im Gausschen Körper gibt es nur einen Kongruenzcharakter mod. 4, der vom Hauptcharakter verschieden ist und auf den Einheiten trivial wird, i.e., den Charakter $(-1)^{(N_\nu-1)/4}$. Daher wird wie oben eine Erklärung von (35) mittels Größencharakter erhalten. Es sei nämlich $(\nu) \rightarrow \nu^* \in F$ eine multiplikative Abbildung zu 2 primen Zahlen von F , wobei $(\nu^*) = (\nu)$ ist und $\nu^* = \nu$ für $\nu \equiv 1 \pmod{4}$ eintritt. Wegen (35) ist dann

$$\left(\frac{\nu^*}{\mu}\right)_4 \left(\frac{\mu^*}{\nu}\right)_4^{-1} = (-1)^{(N_\mu-1)/4 + (N_\nu-1)/4}.$$

§ 4. 3-te und 6-te Reste

Da die 3-ten und 6-ten Reste nichts wesentlich verschiedenes entspringen lassen, wollen wir sie nur kurz betrachten. Es sei $F = \mathbf{Q}(\rho)$ der Eisensteinsche Körper und μ, ν seien zueinander und zu 3 prime ganze Zahlen von F . Ist dann

g die in § 1 definierte elliptische Funktion, so folgt aus (13) und dem Gausschen Lemma

$$(36) \quad \left(\frac{\nu}{\mu}\right)_3 = \prod_{\alpha \in M} \frac{g\left(\frac{\nu\alpha}{\mu}\right)}{g\left(\frac{\alpha}{\mu}\right)},$$

wo M eine Menge ganzer Zahlen von F , für die die Vereinigung $\{0, M, \rho M, \rho^2 M\}$ ein vollkommenes Restsystem mod. μ ist. Es sei N eine gleichbedeutende Menge für ν und sei $\varphi(x, y) = g(x + y)g(x + \rho y)g(x + \rho^2 y)$. Dann ist

$$(37) \quad \varphi(x, y) = \varphi(y, x),$$

und aus (36) und aus der Multiplikationsformel (19) ergibt sich

$$(38) \quad \left(\frac{\nu}{\mu}\right)_3 = \delta_\nu^{(N\mu-1)/3} \prod_{\alpha \in M, \beta \in N} \varphi\left(\frac{\alpha}{\mu}, \frac{\beta}{\nu}\right),$$

nebst

$$(39) \quad \left(\frac{\mu}{\nu}\right)_3 = \delta_\mu^{(N\nu-1)/3} \prod_{\alpha \in M, \beta \in N} \varphi\left(\frac{\beta}{\nu}, \frac{\alpha}{\mu}\right).$$

Aus (37), (38) und (39) folgt sogleich das 3-te Reziprozitätsgesetz

$$\left(\frac{\nu}{\mu}\right)_3 \left(\frac{\mu}{\nu}\right)_3^{-1} = \frac{\delta_\nu^{(N\mu-1)/3}}{\delta_\mu^{(N\nu-1)/4}}.$$

was mit

$$(40) \quad \left(\frac{\nu}{\mu}\right)_3 \left(\frac{\mu}{\nu}\right)_3^{-1} = \left(\frac{\delta_\nu}{\mu}\right)_3 \left(\frac{\delta_\mu}{\nu}\right)_3^{-1}$$

gleichbedeutend ist.

Wenn ferner (29) und (40) miteinander verbunden werden, so besteht nach der Relation $\left(\frac{\nu}{\mu}\right)_6 = \left(\frac{\nu}{\mu}\right)_3 \left(\frac{\nu}{\mu}\right)_3^{-1}$ das 6-te Reziprozitätsgesetz folgender Gestalt

$$(41) \quad \left(\frac{\nu}{\mu}\right)_6 \left(\frac{\mu}{\nu}\right)_6^{-1} = (-1)^{(N\mu-1)/2 \cdot (N\nu-1)/2} \left(\frac{\chi(\nu)\delta_\nu}{\mu}\right)_6 \left(\frac{\chi(\mu)\delta_\mu}{\nu}\right)_6^{-1},$$

$$((\mu, \nu) = (\mu, 6) = (\nu, 6) = 1),$$

wo $\chi(\nu)$ ein Kongruenzcharakter mod. 4, der durch $\chi(\pm 1) = \pm 1, \chi(\pm 1 + 2\rho) = \pm 1$ und $\chi(\rho) = \chi(\rho^2) = 1$ bestimmt wird.

Ist $\nu^* = \nu(\chi(\nu)\delta_\nu)^{-1}$, so gibt $(\nu) \rightarrow \nu^*$ wie vorher einen Grössencharakter mod. 12 und (41) lässt sich in der Form

$$\left(\frac{\nu^*}{\mu}\right)_6 \left(\frac{\mu^*}{\nu}\right)_6^{-1} = (-1)^{(N\mu-1)/2 \cdot (N\nu-1)/2}$$

schreiben (vgl. (31)). Eine entsprechende Formulierung von (40) ist auch ohne weiteres zu sehen.

LITERATURVERZEICHNIS

- [1] G. Eisenstein, Application de l'algèbre à l'arithmétique transcendante, J. für reine u. angew. Math. **29** (1845), 177–184.
- [2] G. Eisenstein, Beiträge zur Theorie der elliptischen Functionen I, Ableitung des biquadratischen Fundamentaltheorems aus der Theorie der Lemniscatenfunctionen, nebst Bemerkungen zu den Multiplications- und Transformationsformeln, J. für reine u. angew. Math. **30** (1846), 185–210.
- [3] G. Eisenstein, Beiträge zur Theorie der elliptischen Functionen VI, Genaue Untersuchung der unendlichen Doppelproducte, aus welchen die elliptischen Functionen als Quotienten zusammengesetzt sind, J. für reine u. angew. Math. **35** (1847), 153–274.
- [4] H. Reichardt, Eine Bemerkung zur Theorie der Jacobischen Symbols, Math. Nachr. **19** (1958), 171–175.

*Mathematisches Institut,
Universität zu Nagoya*