Zur Theorie der komplexen Multiplikation. II.

Von *Masao Sugawara* in Tokyo.

In einer früheren Arbeit [1]) habe ich folgende Vermutung ausgesprochen:

Es sei Ω ein imaginär quadratischer Zahlkörper und $\mathfrak{m}$ ein ganzes Ideal in Ω. Der Strahlklassenkörper mod $\mathfrak{m}$ *über Ω entsteht dann dadurch, daß man eine Hassesche Strahlklasseninvariante $\tau(\mathfrak{k}^*)$ zu Ω adjungiert.*

Beweisen konnte ich sie dort unter der Annahme:

$$\text{(I)} \qquad 4 \mid \mathfrak{m}, \quad \mathfrak{m} \neq 4\,.$$

Inzwischen ist es mir gelungen, diese Vermutung noch in weiteren Fällen zu bestätigen. Der Beweis in S. I läßt sich nämlich vereinfachen und verschärfen; man braucht statt (I) nur folgendes vorauszusetzen:

(I′) *Es existiert ein Primfaktor $\mathfrak{p}$ von 2 in Ω mit $\mathfrak{p}^2 \mid \mathfrak{m}$ und $\varphi(\mathfrak{m}) \geqq 6$.*

Ist insbesondere $\mathfrak{p}$ vom absolut ersten Grade, so kann es wegen $\varphi(\mathfrak{p}) = 1$ nie im Führer einer Idealgruppe in Ω genau in der ersten Potenz aufgehen. Zieht man also bei der Voraussetzung (I′) nur solche Werte von $\mathfrak{m}$ in Betracht, die wirklich als Führer einer Idealgruppe in Ω auftreten können, so ist hiermit meine obige Vermutung für „fast alle" durch einen Primfaktor ersten Grades von 2 teilbaren Moduln $\mathfrak{m}$ bestätigt. — „Fast alle" soll hier wie im folgenden „bis auf endlich viele Ausnahmen" bedeuten.

Eine ähnliche Methode, die von einer anderen Form des Additionstheorems der $\wp$-Funktion Gebrauch macht, gestattet nun, die Behauptung auch unter folgender Voraussetzung zu beweisen:

$$\text{(II)} \qquad \Psi(\mathfrak{m}) = N(\mathfrak{m}) \prod_{\mathfrak{p} \mid \mathfrak{m}} \left(1 - \frac{2}{N(\mathfrak{p})}\right) \geqq 5\,.$$

Soweit $\mathfrak{m}$ nicht durch einen Primfaktor ersten Grades von 2 teilbar ist, ist $\Psi(\mathfrak{m})$ eine *positive* ganze rationale Zahl; und es gibt offenbar nur endlich viele Werte von $\mathfrak{m}$ für die $0 < \Psi(\mathfrak{m}) < 5$ gilt. Meine Vermutung ist damit überhaupt für „fast alle" $\mathfrak{m}$ bestätigt.

Zum Beweis setze ich die Kenntnis von S. I voraus und kann mich dementsprechend kurz fassen. Ferner lasse ich die Körper $\Omega = \mathrm{P}(\sqrt{-1})$, $\mathrm{P}(\sqrt{-3})$ außer Betracht; für sie ist ja, wie bereits in S. I erwähnt, meine Vermutung bereits auf Grund der klassischen Theorie richtig.

Beweis unter der Annahme (I′).

---

[1]) M. Sugawara, Zur Theorie der komplexen Multiplikation. I, ds. Journal **174** (1936); im folgenden zitiert mit S. I.

Es sei $\tau(\mathfrak{k}^*) = \tau(\varrho \mid \mathfrak{a})$ eine Strahlklasseninvariante mod $\mathfrak{m}$ und ω eine durch $\frac{\mathfrak{m}}{\mathfrak{p}}$ teilbare ganze Zahl in Ω, die aber $\not\equiv 0$ mod$^+$ $\mathfrak{m}$ ist. $\omega\varrho$ ist dann offenbar eine Halbperiode der Funktion $\tau(u \mid \mathfrak{a})$.

Beachtet man nun, daß in der in S. I zugrunde gelegten Additionsformel

$$(1) \qquad (\tau(u+h) + \tau(u) + \tau(h))(\tau(u) - \tau(h))^2 = \tau(u)^3 - A\tau(u) + B$$

die rechte Seite für $u = h$ verschwindet, daß also das Polynom $x^3 - Ax + B$ durch $x - \tau(h)$ teilbar ist, so kann man diese Formel durch Division beider Seiten mit $\tau(u) - \tau(h)$ in die folgende einfachere Gestalt bringen:

$$(1') \qquad (\tau(u+h) + \tau(u) + \tau(h))(\tau(u) - \tau(h)) = \tau(u)^2 + \tau(u)\tau(h) + \tau(h)^2 - A\,,$$

oder

$$(1'') \qquad (2\,\tau(h)^2 - A) + \tau(h)\,(\tau(u) + \tau(u+h)) = \tau(u)\,\tau(u+h)\,.$$

Nach unseren Voraussetzungen $\varphi(\mathfrak{m}) \geqq 6$ und $\Omega \neq \mathsf{P}(\sqrt{-1}), \mathsf{P}(\sqrt{-3})$ gibt es nun sicher drei zu $\mathfrak{m}$ prime Zahlen $\omega_1, \omega_2, \omega_3$, die in verschiedenen Strahlklassen mod $\mathfrak{m}$ liegen. In (1′) bzw. (1″) setzen wir $h = \omega\varrho$, $u = \omega_i\varrho$ $(i = 1, 2, 3)$. Wie in S. I sieht man dann leicht ein, daß die $\tau(\omega_i\varrho \mid \mathfrak{a})$ und die $\tau((\omega_i + \omega)\varrho \mid \mathfrak{a})$ verschiedene Strahlklasseninvarianten mod $\mathfrak{m}$ sind. Ferner ist es unmöglich, daß die drei Zahlen

$$\sigma_i = \tau((\omega_i + \omega)\,\varrho \mid \mathfrak{a}) + \tau(\omega_i\varrho \mid \mathfrak{a})$$

sämtlich einander gleich ausfallen. Denn sonst sei σ ihr gemeinsamer Wert. Das Polynom zweiten Grades in x,

$$(\sigma + \tau(\omega\varrho))(x - \tau(\omega\varrho)) - (x^2 + x\tau(\omega\varrho) + \tau(\omega\varrho)^2 - A)\,,$$

hätte dann nach (1′) die drei verschiedenen Wurzeln $\tau(\omega_i\varrho \mid \mathfrak{a})$.

Es sei also etwa $\sigma_1 \neq \sigma_2$. Aus den nach (1″) gültigen Formeln

$$(2\,\tau(\omega\varrho)^2 - A) + \sigma_i\,\tau(\omega\varrho) = \tau(\omega_i\varrho)\,\tau((\omega_i + \omega)\varrho) \qquad (i = 1, 2)$$

ergibt sich dann durch Subtraktion, daß $\tau(\omega\varrho)$ in $\Omega(\tau(\mathfrak{k}^*))$ liegt. Nach (1′) und (1″) gehören mithin auch die Zahlen A, B zu $\Omega(\tau(\mathfrak{k}^*))$. Nach S. I, § 1 bzw. § 3 ist damit der Beweis erbracht.

Beweis unter der Annahme (II) [2].

Zunächst beweisen wir folgenden

Hilfssatz. *Wenn* $\Omega \neq \mathsf{P}(\sqrt{-1}), \mathsf{P}(\sqrt{-3})$ *und*

$$(2) \qquad \Psi(\mathfrak{m}) \geqq 5,$$

so gibt es in Ω *sicher drei Zahlen* $\omega_1, \omega_2, \omega_3$ *von der Art, daß* ω_i *und* $\omega_i + 1$ *prim zu* $\mathfrak{m}$ *sind und überdies die drei durch* ω_i *und* $\omega_i + 1$ mod $\mathfrak{m}$ *bestimmten Paare von Strahlklassen* mod $\mathfrak{m}$, *die wir im folgenden mit*

$$\{(\omega_i), (\omega_i + 1)\} \text{ mod } \mathfrak{m} \qquad (i = 1, 2, 3)$$

bezeichnen, voneinander verschieden sind.

Dabei sollen zwei Paare $\{\alpha, \beta\}$ und $\{\gamma, \delta\}$ dann und nur dann als „gleich" gelten, wenn $\alpha = \gamma$, $\beta = \delta$ oder $\alpha = \delta$, $\beta = \gamma$ ist.

---

[2]) Die folgende Beweisanordnung verdanke ich Herrn Iyanaga; mein ursprünglicher Beweis war komplizierter. Ich möchte Herrn Iyanaga auch an dieser Stelle meinen herzlichen Dank für seine Verbesserungen aussprechen.

Beweis. $\Psi(\mathfrak{m})$ gibt, wie leicht ersichtlich, die Anzahl der $\bmod^+ \mathfrak{m}$ inkongruenten Zahlen ω von der Art an, daß ω und $\omega + 1$ beide zu $\mathfrak{m}$ prim sind. Zwei Strahlklassenpaare mod $\mathfrak{m}$,

$$\{(\omega), (\omega + 1)\} \quad \text{und} \quad \{(\omega'), (\omega' + 1)\},$$

sind aber für $\mathfrak{m} \nmid 2$ — und das ist auf Grund der Voraussetzung (2) sicher der Fall — dann und nur dann gleich, wenn eine der beiden folgenden Kongruenzen stattfindet:

$$\omega' \equiv \omega \qquad (\bmod^+ \mathfrak{m})$$
$$\omega' \equiv -\omega - 1 \qquad (\bmod^+ \mathfrak{m}).$$

Ist also $\Psi(\mathfrak{m}) > 2 \cdot 2$, d. h. gilt (2), so gibt es mehr als zwei Werte ω derart, daß $\{(\omega), (\omega + 1)\}$ verschiedene zu $\mathfrak{m}$ prime Restklassenpaare $\bmod^+ \mathfrak{m}$ darstellt; w. z. b. w.

Unser Beweis wird nun auf Grund der folgenden Additionsformel [3]) der $\wp$-Funktion geführt:

$$(p_1 + p_2 + p_3)(4\,p_1 p_2 p_3 - g_3) = \left(p_1 p_2 + p_2 p_3 + p_3 p_1 + \frac{g^2}{4}\right)^2,$$

wobei

$$p_1 = \wp(u), \qquad p_2 = \wp(v), \qquad p_3 = \wp(u + v).$$

Es sei $\tau(\mathfrak{k}^*) = \tau(\varrho \,|\, \mathfrak{a})$ eine Strahlklasseninvariante mod $\mathfrak{m}$. Rechnet man die eben angegebene Formel auf die Funktion $\tau(u) = \tau(u \,|\, \mathfrak{a})$ um, so findet man

$$(3) \qquad 4\,(\tau_1 + \tau_2 + \tau_3)(\tau_1\tau_2\tau_3 + B) = (\tau_1\tau_2 + \tau_2\tau_3 + \tau_3\tau_1 + A)^2,$$

wobei

$$\tau_1 = \tau(u), \qquad \tau_2 = \tau(v), \qquad \tau_3 = \tau(u + v),$$
$$A = 3\,j(\mathfrak{a})\,(j(\mathfrak{a}) - 2^6 \cdot 3^3),$$
$$B = 2\,j(\mathfrak{a})\,(j(\mathfrak{a}) - 2^6 \cdot 3^3)^2$$

gesetzt ist, oder auch

$$(3') \qquad 4\,(\tau_1 + x)(\tau_1 y + B) = (\tau_1 x + y + A)^2,$$

wo

$$\tau_2 + \tau_3 = x, \qquad \tau_2\tau_3 = y$$

gesetzt ist.

Denkt man sich nun in (3′) τ_1, A, B als Konstante, x, y als Variable, so stellt (3′) eine Parabel in der x, y-Ebene dar, die nur dann ausartet, wenn die Determinante

$$D = \begin{vmatrix} \tau_1^2 & -\tau_1 & \tau_1 A - 2B \\ -\tau_1 & 1 & A - 2\tau_1^2 \\ \tau_1 A - 2B & A - 2\tau_1^2 & A^2 - 4\tau_1 B \end{vmatrix} = -4(\tau_1^3 - A\tau_1 + B)^2$$

verschwindet.

Unter der Annahme (2) gibt es nun offenbar zwei Werte von ω so, daß $\tau(\omega\varrho \,|\, \mathfrak{a})$ verschiedene Strahlklasseninvarianten mod $\mathfrak{m}$ sind. Verschwindet $D = D(u \,|\, \mathfrak{a})$ für $u = \omega\varrho$ mit diesen zwei Werten von ω, so kann man die so entstehenden zwei Gleichungen als lineare inhomogene Gleichungen für die Zahlen A, B auffassen, und damit durch Auflösung A, B als Zahlen in $\Omega(\tau(\mathfrak{k}^*))$ finden.

Da sich also der Beweis in diesem Fall mit unserem Schluß aus S. I durchführen läßt, nehmen wir weiterhin an, daß es ein ϱ mit $D(\varrho \,|\, \mathfrak{a}) \neq 0$ gibt. Wir setzen dann in (3) $u = \varrho$, $v = \omega_i \varrho$, wo die ω_i $(i = 1, 2, 3)$ gemäß unserem Hilfssatz bestimmt sind.

[3]) Siehe etwa Hurwitz-Courant, Funktionentheorie (Berlin 1925), S. 172.

Setzen wir ferner

$$\tau(\omega_i \varrho \mid \mathfrak{a}) + \tau((1 + \omega_i)\varrho \mid \mathfrak{a}) = x_i$$
$$\tau(\omega_i \varrho \mid \mathfrak{a}) \cdot \tau((1 + \omega_i)\varrho \mid \mathfrak{a}) = y_i ,$$

so sind ersichtlich

$$(x_i, y_i) \qquad (i = 1, 2, 3)$$

drei verschiedene Punkte auf der nicht ausgearteten Parabel (3′) mit $\tau_1 = \tau(\varrho \mid \mathfrak{a})$. Diese Punkte können daher nicht auf einer Geraden liegen, d. h. es ist die Determinante

$$d = \begin{vmatrix} 1 & x_1 & y_1 \\ 1 & x_2 & y_2 \\ 1 & x_3 & y_3 \end{vmatrix} \neq 0 .$$

Die drei aus (3′) entspringenden Formeln

$$4(\tau_1 + x_i)(\tau_1 y_i + B) = (\tau_1 x_i + y_i + A)^2 \qquad (i = 1, 2, 3)$$

sind nun wieder drei lineare inhomogene Gleichungen für die Zahlen

$$A^2, \quad 2A, \quad -4B$$

mit der Determinante

$$\begin{vmatrix} 1 & \tau_1 x_1 + y_1 & x_1 + \tau_1 \\ 1 & \tau_1 x_2 + y_2 & x_2 + \tau_1 \\ 1 & \tau_1 x_3 + y_3 & x_3 + \tau_1 \end{vmatrix} = -d \neq 0 .$$

Unser Beweis ist also auch in diesem Fall nach dem Schema aus S. I durchführbar.

Eingegangen 8. Juli 1935.