Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion

Herrn Professor Alexander Ostrowski zum 60. Geburtstag gewidmet

Von Martin Eichler in Münster

Einleitung

Es bedeute $F(x_i)$ eine quaternäre positiv definite quadratische Form mit ganzen rationalen Koeffizienten ohne gemeinsamen Teiler > 1. Die Determinante des Koeffizientenschemas sei D. Die Thetafunktion

$$\vartheta_F(\tau) = \sum_{x_i=-\infty}^{+\infty} e^{2\pi i \tau F(x_i)} = \sum_{n=0}^{\infty} \alpha_F(n)\, e^{2\pi i n \tau} \tag{1}$$

ist dann eine Modulfunktion — 2-ten Grades zu einer durch

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = 1, \quad c \equiv 0 \bmod Q$$

definierten Kongruenzuntergruppe $\mathfrak{G}(Q)$ der Modulgruppe zur Stufe Q, d. h. es besteht die Funktionalgleichung

$$\vartheta_F\left(\frac{a\tau+b}{c\tau+d}\right) = \chi(a)\,(c\tau+d)^2\,\vartheta_F(\tau) \tag{2}$$

mit

$$\chi(a) = \left(\frac{D}{a}\right). \tag{2a}$$

In Q gehen nur die Primteiler von D auf, und diese auch wirklich. Neben $\mathfrak{G}(Q)$ wird im folgenden noch die Untergruppe $\mathfrak{G}_1(Q)$ vom Index 2 oder 1 eine Rolle spielen, welche durch die Bedingung $\chi(a) = 1$ in $\mathfrak{G}(Q)$ herausgehoben wird. Bekanntlich besteht eine Zerlegung

$$\vartheta_F(\tau) = E_F(\tau) + S_F(\tau), \tag{3}$$

wobei

$$E_F(\tau) = \sum_{n=0}^{\infty} \varepsilon_F(n)\, e^{2\pi i n \tau}, \quad S_F(\tau) = \sum_{n=0}^{\infty} \sigma_F(n)\, e^{2\pi i n \tau}$$

eine Eisensteinreihe und eine Spitzenform zur Gruppe $\mathfrak{G}(Q)$ bezeichnen. Die Anzahl der Darstellungen einer natürlichen Zahl n durch die Form F ist mithin

$$\alpha_F(n) = \varepsilon_F(n) + \sigma_F(n). \tag{4}$$

Das Hauptglied $\varepsilon_F(n)$ in (4) ist die mittlere Darstellungsanzahl von n durch Formen des durch F definierten Geschlechts, es wird nach dem SIEGELschen Hauptsatz aus der analytischen Theorie der quadratischen Formen berechnet. Ist $(n, D) = 1$, so gilt mit einer von n unabhängigen Konstanten c_F

$$\varepsilon_F(n) = c_F\, n \sum_{t/n} \left(\frac{D}{t}\right) t^{-1}. \tag{5}$$

Für das Fehlerglied wollen wir hier die Abschätzung

$$|\sigma_F(n)| < \gamma_F(\varepsilon)\, n^{\frac{1}{2}+\varepsilon} \tag{6}$$

herleiten, dabei bedeute ε eine beliebig kleine positive Größe und $\gamma_F(\varepsilon)$ eine Konstante, die nur von F und ε abhängt. Für Primzahlen p gilt sogar

$$|\sigma_F(n)| < \gamma_F\, p^{\frac{1}{2}}. \tag{6a}$$

Zum Beweise betrachten wir einen gewissen Körper K von Modulfunktionen zur Gruppe $\mathfrak{G}_1(Q)$, dessen Konstantenkörper der rationale Zahlkörper k ist, sowie den Körper $\overline{K}$, der aus K durch algebraischen Abschluß des Konstantenkörpers entsteht. K ist eine Erweiterung 2-ten Grades des Körpers K_1 aller in K enthaltenen und bei der größeren Gruppe $\mathfrak{G}(Q)$ invarianten Modulfunktionen, und η bezeichne das von der Identität verschiedene Element der GALOISgruppe von K/K_1. (Die inkonsequente Benutzung des Index 1 erfolgt aus Gründen der Bequemlichkeit, der Körper K_1 ist nur zur Definition des Automorphismus η erforderlich und wird nie wieder vorkommen.) Bei der Reduktion von K modulo einer Primzahl p entsteht ein Körper $K(p)$, dessen Konstantenkörper der Primkörper der Charakteristik p ist; hierbei sind möglicherweise endlich viele p als unzulässig auszuschließen, was bei geeigneter Wahl von $\gamma_F(\varepsilon), \gamma_F$ keine Einschränkungen in (6a), (6) bedingt. Die HECKEschen Operatoren T_n [5] definieren Multiplikatoren τ_n von $\overline{K}$ in sich, und auch der eben erwähnte Automorphismus η ist ein solcher. Sie erzeugen einen Unterring $\mathfrak{M}_0$ in dem Ring $\mathfrak{M}$ aller Multiplikatoren von $\overline{K}$ in sich, und $\mathfrak{M}_0$ erfährt bei der Reduktion von K mod p eine isomorphe Abbildung auf einen Teil $\mathfrak{M}_0(p)$ des Multiplikatorenringes $\mathfrak{M}(p)$ von $\overline{K(p)}$ in sich, dabei bedeutet $\overline{K(p)}$ selbstverständlich den durch algebraischen Abschluß des Konstantenkörpers entstehenden Funktionenkörper. Die Bilder von η, τ_n in $\mathfrak{M}_0(p)$ mögen mit $\eta(p)$, $\tau_n(p)$ bezeichnet werden. Ferner bedeute $\pi(p)$ den durch gliedweise Potenzierung mit p definierten Multiplikator von $\overline{K(p)}$, und endlich der Stern den ROSATIschen Antiautomorphismus in $\mathfrak{M}$ bzw. $\mathfrak{M}(p)$. Mit diesen Bezeichnungen gilt jetzt

$$\tau_p(p) = \eta(p)^{\frac{1}{2}(1-\chi(p))}\, \pi(p) + \pi(p)^*; \tag{7}$$

wenn D eine Quadratzahl ist, also speziell:

$$\tau_p(p) = \pi(p) + \pi(p)^*. \tag{7a}$$

Diese Behauptungen werden in den beiden ersten Paragraphen begründet.

Die RIEMANNsche Vermutung für die Zetafunktion des Körpers $K(p)$ läßt sich in Form der Gleichung

$$|\pi_i(p)| = \sqrt{p} \tag{8}$$

für die Eigenwerte $\pi_i(p)$ des Operators $\pi(p)$ aussprechen; aus $\mathfrak{M}_0 \cong \mathfrak{M}_0(p)$ und (8) folgen dann leicht die Ungleichungen (6a) und (6) (§ 3).

Fortan sei D eine Quadratzahl, so daß also (7a) gilt. Das System der zu den Spitzenformen zur Gruppe $\mathfrak{G}(Q)$ gehörigen DIRICHLETreihen besitzt dann nach HECKE [5] eine EULERsche Produktentwicklung, deren Faktoren die g-reihigen Matrizen

$$Z_p(s) = (1_g - T_p\, p^{-s} + 1_g\, p^{1-2s})^{-1} \tag{9}$$

sind; 1_g ist die g-reihige Einheitsmatrix. Zieht man die bekannte Gleichung

$$\pi(p)\,\pi(p)^* = p \tag{10}$$

heran, und beachtet man die Isomorphie der Abbildungen $T_p \to \tau_p \to \tau_p(p)$, so folgt aus (7a) für die Determinante von (9) die Gleichung

$$|Z_p(s)|^{-1} = N((1-\pi(p)\,p^{-s})\,(1-\pi(p)^* p^{-s}))\,, \tag{11}$$

wobei N die Norm in einem gewissen noch näher zu präzisierenden Sinne bedeutet. Andererseits ist die Zetafunktion von $K(p)$:

$$\zeta_{K(p)}(s) = \frac{L(p^{-s})}{(1-p^{-s})(1-p^{1-s})} = \frac{N((1-\pi(p)\,p^{-s})\,(1-\pi(p)^* p^{-s}))}{(1-p^{-s})(1-p^{1-s})}\,. \tag{12}$$

Aus (11) und (12) folgt also: reduziert man K modulo fast allen Primzahlen p und bildet das Produkt über die Zetafunktionen der Körper $K(p)$, so entsteht im wesentlichen die Determinante der HECKEschen Matrix-Zetafunktion zu den Spitzenformen — 2-ten Grades von K. Genauer:

$$\prod_p \frac{1}{\zeta_{K(p)}(s)} \sim \frac{1}{\zeta(s)\,\zeta(s-1)} \prod_p |1_g - T_p\, p^{-s} + 1_g\, p^{1-2s}|^{-1}\,, \tag{13}$$

wobei das Äquivalenzzeichen andeutet, daß auf beiden Seiten möglicherweise endlich viele Faktoren auszulassen sind; $\zeta(s)$ ist die RIEMANNsche Zetafunktion. Die linke Seite ist demnach eine meromorphe Funktion und genügt einer Funktionalgleichung mit gewissen Gammafaktoren vom geläufigen Typ. Damit ist für den Fall des Körpers K eine zuerst von H. HASSE geäußerte Vermutung bewiesen. Die ersten Ergebnisse in dieser Richtung stammen von A. WEIL [10] ($K = k(x,y)$ mit $ax^m + by^n = 1$) und M. DEURING [4] (K = elliptische Funktionenkörper mit singulären Moduln).

1. Der Körper der Modulfunktionen

Wir brauchen im folgenden einen Körper K von solchen bei $\mathfrak{G}_1(Q)$ invarianten Modulfunktionen über dem Körper k der rationalen Zahlen, deren FOURIERentwicklungen rationale Koeffizienten haben, wobei die Nenner Potenzprodukte von endlich vielen Primzahlen sind. Mit zwei Funktionen haben offenbar ihre Summe, Differenz, Produkt und Quotient diese Eigenschaft. K läßt sich dann in der Weise $K = k(x, y)$ erzeugen, wobei eine absolut irreduzible Gleichung $F(x, y) = 0$ mit ganzen rationalen Koeffizienten besteht. Wir erzeugen K aus geeigneten Quotienten von Thetafunktionen, insbesondere $\vartheta_F(\tau)$, und EISENSTEINreihen, wobei wir ausdrücklich darauf achten müssen, daß nicht alle Funktionen von K schon bei $\mathfrak{G}(Q)$ invariant sind, falls D nicht eine Quadratzahl ist. Mit $\vartheta_F(\tau)$ und gewissen Funktionen $\varphi(\tau)$ von K sind dann weitere ganze Modulformen $\varphi(\tau)\,\vartheta_F(\tau)$ vom Grade -2 gegeben, welche ebenfalls FOURIERentwicklungen der eben genannten Art besitzen. Das gilt insbesondere für eine Basis $S_i(\tau)$ der Schar der Spitzenformen.

Es ist für das Folgende nicht erforderlich zu wissen, in welchem Verhältnis der konstruierte Körper K bzw. $\overline{K}$ zu dem Körper aller bei $\mathfrak{G}_1(Q)$ invarianten Modulfunktionen steht. Es bleibt also die Frage offen, ob es Modulfunktionen zu dieser Gruppe gibt, die sich nicht als rationale Funktionen von solchen darstellen lassen, welche rationalzahlige und sogar „fast" ganzzahlige FOURIERentwicklungen besitzen. Es bleibt ferner unerörtert, ob es mehrere Körper der genannten Art gibt; diese würden dann alle in einem umfassendsten enthalten sein.

Modulfunktionen zur Gruppe $\mathfrak{G}_1(Q)$ lassen sich stets als Summen von zwei Funktionen schreiben, welche das folgende Transformationsgesetz erfüllen:

$$(14)\quad x\left(\frac{a\tau+b}{c\tau+d}\right) = \chi(a)\,x(\tau) \text{ für } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathfrak{G}(Q), \text{ und mit } \chi(a) = 1 \text{ oder } = \left(\frac{D}{a}\right),$$

und zwar ist für die erste $\chi(a) = 1$, für die zweite $\chi(a) = \left(\frac{D}{a}\right)$ (sofern überhaupt $\mathfrak{G}(Q) \neq \mathfrak{G}_1(Q)$, d. h. $D \neq$ Quadratzahl ist). Entsprechendes gilt für Modulformen.

Das Geschlecht von K sei g. Einer Basis der Schar der Differentiale 1. Gattung von K entsprechen dann g linear unabhängige Spitzenformen $S_i(\tau)$. Offenbar kann man sie so wählen, daß ein Teil von ihnen die Funktionalgleichung (2) mit $\chi(a) = 1$, der andere mit $\chi(a) = \left(\frac{D}{a}\right)$ erfüllt. Die HECKEschen Operatoren T_n, an deren Definition im Falle einer zu D teilerfremden Primzahl $n = p$ wir hier erinnern müssen, nehmen auf diesen Multiplikator $\chi(a)$ Bezug; sie führen Modulformen in solche des gleichen Multiplikators über. Wichtig ist für uns indessen nur, daß sie die ganze Schar der Spitzenformen invariant lassen:

$$(15)\quad S_i(\tau) \mid T_p = \sum_{r \bmod p} \frac{1}{p} S_i\left(\frac{\tau+r}{p}\right) + \chi(p)\,p\,S_i(p\tau) = \sum_{k=1}^{g} t_{ik}(p)\,S_k(\tau).$$

Die rechts stehenden Matrizen $(t_{ik}(p))$ wollen wir mit dem gleichen Buchstaben T_p bezeichnen.

Jetzt schränken wir den Bereich der fortan zulässigen Primzahlen p ein: p soll nicht in den Nennern der FOURIERkoeffizienten der $S_i(\tau)$ vorkommen. Dadurch werden höchstens endlich viele p ausgeschlossen. Reduziert man diese FOURIERkoeffizienten mod p, so entstehen formale Potenzreihen in $e^{2\pi i\tau}$ mit Koeffizienten aus dem Restklassenkörper $k(p)$ von k mod p. Wir verlangen weiter, daß auch diese formalen Potenzreihen linear unabhängig sind. Das erfordert den Ausschluß von höchstens endlich vielen weiteren p.

Der Körper K besteht seiner Erzeugung gemäß aus Quotienten von Funktionen mit für p ganzen FOURIERentwicklungen. Es gibt demnach zu jeder Funktion $x(\tau)$ aus K eine Potenz von p so, daß $p^n x(\tau)$ eine p-ganze FOURIERentwicklung hat. Ordnet man jeder solchen Funktion ihre formale FOURIERentwicklung in $k(p)$ zu, so entsteht ein Körper $K(p)$ von Funktionen mit $k(p)$ als Konstantenkörper. $K(p)$ kann andererseits auch so erklärt werden: Es liege eine Erzeugung $K = k(x, y)$ mit $F(x, y) = 0$ vor, wobei F ganze rationale Koeffizienten hat und absolut irreduzibel ist. Bis auf endlich viele Ausnahmen ist $F(x, y)$ auch in $k(p)$ absolut irreduzibel [3], man setze dann $K(p) = k(p)\,(x, y)$ mit $F(x, y) \equiv 0$ mod p. Wir benutzen zunächst diese zweite Erklärung von $K(p)$, obwohl sie den Nachteil hat, auf eine willkürliche Erzeugung Bezug zu nehmen. Andererseits kann man im gleichen Zuge einsehen [3], daß $K(p)$ für fast alle p dasselbe Geschlecht g wie K hat; nur solche p kommen in Betracht. Nachträglich ist leicht festzustellen, daß für die zugelassenen p beide Erklärungen dasselbe liefern.

Außer den hier den p auferlegten Bedingungen werden wir endlich in § 3 $p > 2g$ voraussetzen müssen. Ob alle diese Einschränkungen wirklich erforderlich sind, bleibt eine offene Frage. Natürlich wird man vermuten, daß lediglich die Primteiler von D auszuschließen sind.

Es ist noch eine Bemerkung über die T_p anzuschließen, die wir gemäß (15) als g-reihige Matrizen auffassen. Sie erzeugen einen kommutativen halbeinfachen Ring, lassen sich also simultan auf Hauptachsen transformieren. Dabei werden die $S_i(\tau)$ gleichzeitig in g andere Spitzenformen

$$t_i(\tau) = \sum_{n=1}^{\infty} \tau_i(n)\, e^{2\pi i n\tau}\,, \quad \tau_i(1) = 1, \tag{16}$$

transformiert, die Eigenfunktionen der T_p. Hierbei sind die Entwicklungskoeffizienten $\tau_i(p)$ gerade die Eigenwerte der Matrix T_p [5]. Aus der linearen Unabhängigkeit der $t_i(\tau)$ geht dann hervor, daß der durch die T_p erzeugte Ring den Rang g hat.

Aus (15) und den Voraussetzungen über p folgt weiterhin, daß die T_l für jedes zulässige p p-ganze Koeffizienten $t_{ik}(l)$ haben und auch mod p genommen einen Ring vom Rang g erzeugen.

2. Der Multiplikatorenring

Die Multiplikatoren (für das Folgende vgl. [1, 2]) eines algebraischen Funktionenkörpers bilden einen Ring von Endomorphismen der Klassengruppe 0-ten Grades; ihre erzeugenden Elemente sind die folgendermaßen definierten Primmultiplikatoren τ: $\overline{K}_\tau$ sei ein mit $\overline{K}$ isomorpher Unterkörper einer endlich algebraischen Erweiterung $\overline{K}'$ von $\overline{K}$, so daß $\overline{K}'$ das Kompositum $\overline{K}\,\overline{K}_\tau$ ist. Eine Klasse C aus $\overline{K}$ werde nach $\overline{K}_\tau$ isomorph übertragen ($C \to C_\tau$) und die Norm

$$C^\tau = N_{\overline{K}K_\tau/\overline{K}}(C_\tau)$$

gebildet. Diese Definition gilt ebenso für $\overline{K(p)}$. Die τ erzeugen einen Ring $\mathfrak{M}$ (im Falle von $\overline{K}$) bzw. $\mathfrak{M}(p)$ (im Falle von $\overline{K(p)}$), beide Ringe sind halbeinfach und haben die Charakteristik 0 (für den letzteren s. [11, S. 59], bzw. [12, S. 142]). Der Körper $\overline{K}'$ kann auch als der Restklassenkörper des „Ringkompositums" $\overline{K}_1\overline{K}_2$ zweier mit $\overline{K}$ isomorpher und untereinander algebraisch unabhängiger Körper $\overline{K}_1$, $\overline{K}_2$ modulo einem Primideal $\mathfrak{T}$ von $\overline{K}_1\overline{K}_2$ verstanden werden [2, S. 32]. Das dem Multiplikator τ zugeordnete Primideal $\mathfrak{T}$ ist durch τ nicht eindeutig, sondern nur als Idealklasse festgelegt, während offenbar τ durch $\mathfrak{T}$ eindeutig bestimmt wird. Die Zuordnung eines Multiplikators τ zu einem beliebigen ganzen Ideal $\mathfrak{T} = \mathfrak{T}_1\,\mathfrak{T}_2 \ldots$ ohne mehrfache Primfaktoren geschieht folgendermaßen: Der Restklassenring $\overline{K}_1\overline{K}_2$ mod $\mathfrak{T}$ (abgekürzt: $\overline{K}_1\overline{K}_2(\mathfrak{T})$) ist die direkte Summe der Restklassenringe $\overline{K}_1\overline{K}_2(\mathfrak{T}_i)$, und die formale Übertragung der Definition lautet (C_1, C_2 = Bilder von C in $\overline{K}_1$, $\overline{K}_2$):

$$C_1^\tau = N_{\overline{K}_1\overline{K}_2(\mathfrak{T})/\overline{K}_1}(C_2) = \prod_i N_{\overline{K}_1\overline{K}_2(\mathfrak{T}_i)/\overline{K}_1}(C_2) = C_1^{\tau_1+\tau_2+\cdots}.$$

Treten in $\mathfrak{T}$ Primteiler mehrfach auf, so werden die τ_i rechts noch mit diesen Vielfachheiten multipliziert; das kommt für das Folgende aber nicht in Betracht.

Im Falle des Körpers $\overline{K}$ bekommt man auf Grund des ABELschen Theorems und des JACOBIschen Umkehrsatzes eine treue Darstellung von $\mathfrak{M}$ im Raume der Werte der ABELschen Integrale modulo deren Perioden (diese Darstellung hat den Grad $2g$), oder auch eine ebenfalls treue Darstellung g-ten Grades im Raume der Differentiale [1], [2] 1. Gattung. Diese letztere schreibt sich so:

$$S_i^\tau(\tau)\,d\tau = \mathrm{Spur}_{\overline{K}K_\tau/K}((S_i(\tau)d\tau)_\tau), \tag{17}$$

wobei man natürlich nicht die Variable τ mit dem Multiplikator τ verwechseln darf.

Multiplikatoren τ, die sich bereits für K (d. h. als Ideale in $K_1\,K_2$) definieren lassen, erhalten hiernach eine Darstellung, deren Koeffizienten in k liegen.

Es sei $x_1(\tau)$ eine Funktion aus K, welche sich gegenüber $\mathfrak{G}(Q)$ in einer der beiden Arten (14) verhält. Es handelt sich zunächst um die Aufgabe, die zu $x_1\begin{pmatrix}\tau\\ p\end{pmatrix}$ bezgl. K konjugierten Funktionen zu ermitteln. Sei $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ ein beliebiges Element aus $\mathfrak{G}_1(Q)$, also mit $\chi(\alpha) = 1$, dann läßt sich ein $\begin{pmatrix}a & b\\ c & d\end{pmatrix} \in \mathfrak{G}(Q)$ bekanntlich eindeutig so bestimmen, daß eine der folgenden $p+1$ Gleichungen besteht:

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} = \begin{pmatrix}a\alpha + pb\gamma & *\\ * & *\end{pmatrix} = \begin{pmatrix}1 & r\\ 0 & p\end{pmatrix} \text{ mit } r = 0, \ldots, p-1 \text{ oder} = \begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix},$$

und man erkennt $\chi(a) = 1$ in jedem der p ersten Fälle, dagegen $\chi(a) = \chi(p)$ im letzten. Daraus folgt, daß bei Anwendung aller Substitutionen $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathfrak{G}_1(Q)$ auf $x_1\begin{pmatrix} \tau \\ p \end{pmatrix}$ die Funktionen $x_1\begin{pmatrix} \tau + r \\ p \end{pmatrix}$ mit $r = 0, \ldots, p-1$ und $\chi(p)\, x_1(p\tau)$ entstehen, und daß diese durch die $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ permutiert werden. Daher genügt $x_2 = x_1\begin{pmatrix} \tau \\ p \end{pmatrix}$ in $K = K_1$ einer irreduziblen Gleichung $f(x_2) = 0$ vom Grade $p+1$. Das Letztere gilt aber ersichtlich auch für die Summe von zwei Funktionen $x_1(\tau)$ mit verschiedenen Multiplikatoren $\chi(a)$. Die Gesamtheit der so erhaltenen Gleichungen $f(x_2) = 0$ erzeugen dann ein Primideal $\mathfrak{T}_p$ in $K_1 K_2$ und folglich auch in $\overline{K}_1 \overline{K}_2$. Die Ausführung von (17) für den durch dieses $\mathfrak{T}_p$ definierten Multiplikator τ_p liefert nun gerade die Formel (15), sofern man voraussetzt, daß $S_i(\tau)$ eine Modulform vom Multiplikator $\chi(a)$ ist.

Hierauf sollen die T_l (l soll entweder p oder eine zu p teilerfremde Primzahl sein) auf den Körper $\overline{K(p)}$ übertragen werden.

$$x_1(\tau) = \sum_{n=0}^{\infty} \xi(n)\, e^{2\pi i n \tau}$$

genüge einer der Funktionalgleichungen (14) und habe rationale p-ganze Koeffizienten $\xi(n)$. Mit einer zu $k(p)$ zu adjungierenden primitiven l-ten Einheitswurzel ζ und einer $\left(e^{\frac{2\pi i \tau}{l}}\right)^l = e^{2\pi i \tau}$ genügenden Rechengröße $e^{\frac{2\pi i \tau}{l}}$ bilden wir die formalen Ausdrücke

$$(18) \qquad x_1\begin{pmatrix} \tau + r \\ l \end{pmatrix} = \sum_{n=0}^{\infty} \xi(n)\, \zeta^{rn} \left(e^{\frac{2\pi i \tau}{l}}\right)^n, \quad \chi(l)\, x_1(l\tau) = \chi(l) \sum_{n=0}^{\infty} \xi(n) (e^{2\pi i n \tau})^l,$$

wobei wir gleichzeitig die $\xi(n)$ durch ihre Reste mod p ersetzen. Ihre elementarsymmetrischen Funktionen stimmen mit den formalen mod p genommenen FOURIERreihen der entsprechenden Bildungen aus K überein. Speziell ist also $x_2 = x_1\begin{pmatrix} \tau \\ l \end{pmatrix}$ Lösung der Kongruenz $f(x_2) \equiv 0 \bmod p$, wo f die oben erklärte Bedeutung hat. Die Gesamtheit dieser f definiert dann auch in $K_1(p)\, K_2(p)$ sowie in $\overline{K_1(p)}\, \overline{K_2(p)}$ ein Ideal $\mathfrak{T}_l(p)$ und damit einen Multiplikator $\tau_l(p)$ von $\overline{K(p)}$.

Diese Abbildung $\tau_l \to \tau_l(p)$ ist offenbar ein Homomorphismus des durch die τ_l erzeugten Teilringes $\mathfrak{M}_0$ von $\mathfrak{M}$ auf einen Teil $\mathfrak{M}_0(p)$ des Multiplikatorenringes $\mathfrak{M}(p)$. Es wird behauptet, daß es sogar ein Isomorphismus ist. In § 1 war festgestellt worden, daß $\mathfrak{M}$ halbeinfach ist, und daß $\mathfrak{M}(p)$ die Charakteristik 0 hat. Die Abbildung $\mathfrak{M}_0 \to \mathfrak{M}_0(p)$ ist dann und nur dann isomorph, wenn hierbei kein direkter Summand von $\mathfrak{M}_0$ auf 0 abgebildet wird, d. h. wenn $\mathfrak{M}_0(p)$ denselben Rang wie $\mathfrak{M}_0$ hat. Daß dieses in der Tat zutrifft, folgt sofort aus der Matrixdarstellung (15) von $\mathfrak{M}_0$, wenn man nur weiß, daß (15) gleichzeitig eine Darstellung von $\mathfrak{M}_0(p)$ liefert, indem man für die $S_i(\tau)$ ihre formalen Potenzreihen mod p einsetzt: Es war ja gezeigt worden, daß der durch die T_l erzeugte Ring (von dem feststeht, daß er mit

$\mathfrak{M}_0$ isomorph ist) den Rang g hat. Unter den gemachten Voraussetzungen über die zulässigen p war ferner bewiesen worden, daß die T_l auch mod p genommen gemäß (15) einen Ring vom Rang g erzeugen. Es bleibt also übrig, in (15) auch die Darstellung von $\mathfrak{M}_0(p)$ im Raume der Differentiale 1. Gattung zu erkennen [2, S. 27], ebenso wie es sich im Falle des Körpers K verhält.

Die Differentiale in $K(p)$ erklärt man einfach durch formales Differenzieren der FOURIERreihen. Demnach erweisen sich die Bildungen $S_i(\tau)\,d\tau$ als Differentiale. Da $K(p)$ dasselbe Geschlecht g wie K hat, haben die ihnen zugeordneten Divisoren den Grad $2(g-1)$. Bei Restbildung mod p kann der Grad des Zählers des einem $S_i(\tau)\,d\tau$ zugeordneten Divisors offenbar nicht größer werden. Daher bleiben die $S_i(\tau)\,d\tau$ bei Restbildung mod p ganz, d. h. sie entsprechen auch mod p den Differentialen 1. Gattung, und (15) stimmt wiederum mit (17) überein.

Wichtig ist besonders der Multiplikator $\tau_p(p)$. Eine beliebige Funktion $x_1(\tau)$ aus K sei vorgelegt, sie sei in eine Summe von zwei (14) genügenden Funktionen $x_1'(\tau)$, $x_1''(\tau)$ zerlegt, welche zu verschiedenen Multiplikatoren $\chi(a)$ gehören. Aus (18) entnimmt man genau wie im klassischen Falle [9, S. 255] unter Benutzung von $\binom{p}{k} \equiv 0 \bmod p$ für $k \not\equiv 0, p$ sowie der Tatsache, daß die elementarsymmetrischen Funktionen der p-ten Einheitswurzeln und 1 bis auf die letzte durch p teilbar sind, daß die folgende Kongruenz in einer Unbestimmten x_2 besteht:

$$(19)\qquad f(x_2) = (x_2 - (x_1'(p\tau) + \chi(p)\,x_1''(p\tau))) \prod_{r=1}^{p-1} \left(x_2 - x_1\left(\frac{\tau + r}{p}\right)\right) \equiv$$
$$\equiv (x_2 - (x_1'(\tau) + \chi(p)\,x_1''(\tau))^p)\,(x_2^p - x_1(\tau)) \bmod p.$$

Die linke Seite von (19) erzeugt das Ideal $\mathfrak{T}_p$ in K_1K_2, wenn $x_1(\tau)$ alle Funktionen aus K_1 durchläuft. Hiernach zerfällt $\mathfrak{T}_p$ bei Reduktion mod p in ein Produkt aus zwei teilerfremden Primfaktoren $\mathfrak{T}_p^{(1)}$ und $\mathfrak{T}_p^{(2)}$, erzeugt durch alle $x_2 - (x_1' + \chi(p)x_1'')^p$ bzw. $x_2^p - x_1$. Nach der eingangs gemachten Feststellung über die Summe zweier Multiplikatoren ist also $\tau_p(p)$ die Summe der zu $\mathfrak{T}_p^{(1)}$ und $\mathfrak{T}_p^{(2)}$ gehörigen Multiplikatoren; ersichtlich sind diese die bereits in der Einleitung beschriebenen. Damit ist (7) bewiesen.

3. Der Anschluß an die RIEMANNsche Vermutung

Falls $g = 1$ ist, wurde bekanntlich von H. HASSE gezeigt: die Eigenwerte $\pi_i(p)$ von $\pi(p)$ sind die Nullstellen des Polynoms

$$f(z) = z^{2g}\,L_{K(p)}\left(\frac{1}{z}\right),$$

wo $L_{K(p)}$ durch (12) definiert ist, und ihr absoluter Betrag hat den Wert (8). Für beliebiges g bewies dasselbe A. WEIL [11, S. 70—72]. Allerdings bleibt zunächst für $g > 1$ noch offen, ob ein h-facher Eigenwert von $\pi(p)$ auch h-fache Nullstelle von $f(z)$ ist.

Aus (7) und (9) sowie $\eta^2 = 1$ (bzw. $\eta(p)^2 = 1$) einerseits, (8) andererseits folgt, daß die Eigenwerte von $\tau_p(p)$ absolut $\leqq 2\sqrt{p}$ sind. Wegen der Isomorphie der Abbildungen $T_p \to \tau_p \to \tau_p(p)$ sind die Eigenwerte $\tau_i(p)$ von T_p ebenso groß. Wie bereits oben festgestellt wurde, sind die $\tau_i(p)$ identisch mit den p-ten Entwicklungskoeffizienten der Spitzenformen $t_i(\tau)$ in (16). Die in (3) auftretende Spitzenform $S_F(\tau)$ ist eine Linearkombination der $t_i(\tau)$, somit folgt (6a) aus (8). Zum Beweise von (6) sei $n = p_1^{a_1} p_2^{a_2} \ldots$ ein Potenzprodukt aus zulässigen Primzahlen. Für die Entwicklungskoeffizienten der Funktionen (16) gelten dann die Formeln [5]:

$$\tau_i(n) = \tau_i(p_1^{a_1})\,\tau_i(p_2^{a_2}) \ldots, \quad \tau_i(p^{a+1}) = \tau_i(p^a)\,\tau_i(p) - \chi(p)\,p\,\tau_i(p^{a-1}).$$

Nach (8) und (10) ist dann also

$$|\,\tau_i(p^a)\,| \leqq f_a\, p^{\frac{a}{2}},$$

wo f_a die a-te Zahl der FIBONACCIschen Folge $f_0 = 1, f_1 = 1, f_2 = 2, \ldots$ ist. Demnach hat man

$$|\,\tau_i(n)\,| \leqq f_{a_1} f_{a_2} \ldots (p_1^{a_1} p_2^{a_2} \ldots)^{\frac{1}{2}} \leqq f_{a_1+a_2+\ldots}\, n^{\frac{1}{2}}.$$

Die Folge f_a wächst langsamer als $e^{\varepsilon a}$ mit beliebigem $\varepsilon > 0$, also gilt von einem gewissen n ab: $|\,\tau_i(n)\,| \leqq n^{\frac{1}{2}+\varepsilon}$, und das ergibt (6).

Zum Beweise der letzten Behauptung (13) bzw.

$$L_{K(p)}(p^{-s}) = |\,1_g - T_p\,p^{-s} + 1_g\,p^{1-2s}\,| \tag{20}$$

unter Voraussetzung von (7a) stützen wir uns auf die folgenden Sätze von A. WEIL [12, S. 128 (Corr. 3), S. 136—138]: Es sei l eine beliebige zu p teilerfremde Primzahl und $\mathfrak{C}_l$ (bzw. $\mathfrak{C}_l(p)$) die Gruppe der Klassen 0-ten Grades von $\overline{K}$ (bzw. $\overline{K(p)}$), deren Exponent eine Potenz von l ist. $\mathfrak{C}_l(\mathfrak{C}_l(p))$ ist isomorph mit dem direkten Produkt von $2g$ Gruppen, deren jede mit der Additionsgruppe der l-adischen Zahlen mod 1 isomorph ist. Die Elemente $\mu(\mu(p))$ von $\mathfrak{M}(\mathfrak{M}(p))$ erfahren in $\mathfrak{C}_l(\mathfrak{C}_l(p))$ eine treue Darstellung durch $2g$-reihige ganzzahlige l-adische Matrizen $M_l(\mu)$ $(M_l(\mu(p)))$. (Eigentlich müßte auch noch M_l das Symbol p tragen oder nicht; Mißverständnisse sind aber nicht möglich, wenn die Argumente μ und $\mu(p)$ von M_l unterschieden werden.) Das charakteristische Polynom von $M_l(\pi(p))$ hat aber sogar ganze rationale Koeffizienten und ist gerade der Zähler der Zetafunktion von $K(p)$:

$$L_{K(p)}(p^{-s}) = |\,M_l(1 - \pi(p)\,p^{-s})\,|\,. \tag{21}$$

Da der Antiautomorphismus * offenbar ohne Einfluß auf die Determinante von M_l ist, folgt hieraus und aus (7a)

$$\begin{aligned} L^2_{K(p)}(p^{-s}) &= |\,M_l((1 - \pi(p)\,p^{-s})(1 - \pi(p)^*\,p^{-s}))\,| = \\ &= |\,M_l(1 - \tau_p(p)\,p^{-s} + p^{1-2s})\,|\,. \end{aligned} \tag{21a}$$

Wir wollen nun

$$|M_l(1-\tau_p(p)\,p^{-s}+p^{1-2s})| = |M_l(1-\tau_p\,p^{-s}+p^{1-2s})| \tag{22}$$

beweisen und müssen dazu die Determinanten der Darstellungen in $\mathfrak{C}_l$ und $\mathfrak{C}_l(p)$ des durch τ_p bzw. $\tau_p(p)$ erzeugten Ringes vergleichen. Der Körper $\bar{K}$ entsteht aus K durch sukzessive endlich algebraische Erweiterung $k \to k' \to k'' \to \cdots$ des Konstantenkörpers. Nimmt man in diesen Körpern eine Folge von ineinander und in p aufgehenden Primidealen $\mathfrak{p}', \mathfrak{p}'', \ldots$, und reduziert man Kk' mod $\mathfrak{p}'$ usw., so entstehen endliche Konstantenerweiterungen $K(p)\,k'(\mathfrak{p}')$ usw. von $K(p)$, welche in ihrer Gesamtheit $\overline{K(p)}$ ausschöpfen. Jede Klasse C aus $\mathfrak{C}_l$ gehört bereits einem der Körper Kk' usw. an und geht bei Reduktion dieses Körpers mod $\mathfrak{p}'$ in eine Klasse $C(p)$ von $K(p)\,k'(\mathfrak{p}')$ über [3, S. 648]. Es liegt ersichtlich ein Homomorphismus von $\mathfrak{C}_l$ in $\mathfrak{C}_l(p)$ vor. Wir behaupten, daß unter der Voraussetzung $l > \mathrm{Max}\,(g+1, 2(g-1))$, $p > 2g$ jede Klasse $C \neq 1$ aus $\mathfrak{C}_l$ auf eine Klasse $C(p) \neq 1$ aus $\mathfrak{C}_l(p)$ abgebildet wird (was ohne die Voraussetzung $C^{l^n} = 1$ gewiß nicht allgemein zutrifft), verschieben den Beweis aber auf den Schluß. Hiernach geht nun eine Basis von $\mathfrak{C}_l$ in eine Basis von $\mathfrak{C}_l(p)$ über. Ferner überträgt sich die Wirkung von τ_p auf $\mathfrak{C}_l$ in isomorpher Weise auf $\mathfrak{C}_l(p)$. Daher sind bei geeigneter Basiswahl die Matrizen $M_l(\tau_p)$ und $M_l(\tau_p(p))$ identisch, und (22) ist bewiesen.

Die Determinante $M_l(\mu)$ für einen Multiplikator μ von $\bar{K}$ ist andererseits gleich der Anzahl der Klassen C 0-ten Grades von K, welche die Gleichung $C^\mu = 1$ befriedigen (es wird jetzt nicht mehr $C \in \mathfrak{C}_l$ gefordert!) [12, S. 43 prop. 9) und S. 136 (th. 36)]. Nach dem ABELschen Theorem und dem JACOBIschen Umkehrsatz ist diese Anzahl gleich der Determinante der Darstellung von μ im ($2g$-dimensionalen) Raum der Werte der ABELschen Integrale 1. Gattung mod. den Perioden, oder auch gleich dem Quadrat der Darstellung von μ im (g-dimensionalen) Raum der Differentiale 1. Gattung. Aus (21a) und (22) folgt nun (20).

Zum Schluß bleibt noch der folgende Hilfssatz zu beweisen: Der durch Reduktion von K mod p entstehende Körper $K(p)$ habe das gleiche Geschlecht g wie K. Es sei $p > 2g$ und l eine natürliche Zahl $> \mathrm{Max}\,(g+1, 2(g-1))$. Das Bild $C(p)$ in $K(p)$ einer Divisorenklasse C von $\bar{K}$ vom Exponenten l ist nicht die Einheitsklasse. — Aus [7, 8] geht hervor, daß bis auf endlich viele Ausnahmen zu einem Primdivisor $\mathfrak{o}(p)$ von $\overline{K(p)}$ vom Grade 1 kein Element existiert, dessen Nenner $\mathfrak{o}(p)^h$ mit $1 \leqq h \leqq g$ ist, sofern man $p > 2g$ voraussetzt; die Ausnahmen sind die WEIERSTRASSpunkte von $\overline{K(p)}$. Es sei $\mathfrak{o}$ ein Primdivisor 1. Grades von $\bar{K}$, der bei der Abbildung $\bar{K} \to \overline{K(p)}$ (d. h. $Kk' \to K(p)\,k'(\mathfrak{p}')$ für endliche Konstantenerweiterungen k') nicht in einen WEIERSTRASSpunkt von $\overline{K(p)}$ übergeht. In C gibt es einen Repräsentanten

$$\mathfrak{y} = \frac{\mathfrak{p}_1 \cdots \mathfrak{p}_h}{\mathfrak{o}^h}, \quad 1 \leqq h \leqq g, \quad \mathfrak{p}_i \neq \mathfrak{o}, \tag{23}$$

dabei sind die $\mathfrak{p}_i$ gewisse Primdivisoren 1. Grades. Sie gehören ebenso wie $\mathfrak{o}$ bereits einer endlichen Konstantenerweiterung Kk' an. Es sei $1, y_1, \ldots, y_m$ mit $m = l\,h - g$ eine Basis der ganzen Multipla von $\mathfrak{o}^{-hl}$. (Die Dimension der Klasse $\{\mathfrak{o}^{hl}\}$ ergibt sich nach dem RIEMANN-ROCHschen Satz aus der Voraussetzung $l > 2(g-1)$.) Voraussetzungsgemäß ist $\mathfrak{y}^l \cong y$ ein Hauptdivisor, er läßt sich in der Gestalt

$$y = a_0 + \sum_{i=1}^{m} a_i\, y_i \tag{24}$$

mit $a_i \in k'$ schreiben. Wir bilden nun die Ableitungen $y^{(\lambda)} = \frac{d^\lambda y}{dt^\lambda}$ nach einer an allen Stellen $\mathfrak{p}_i$ ortsuniformisierenden $\mathfrak{p}'$-ganzen Funktion t, und zwar in dem von H. HASSE und F. K. SCHMIDT [6] angegebenen Sinne, so daß später die entstehenden Gleichungen auch als Kongruenzen verstanden und verwertet werden dürfen. Aus (23), (24) ergibt sich das folgende Gleichungssystem für die konstanten Reste $y_{ik}^{(\lambda)}$ von $y_i^{(\lambda)}$ mod $\mathfrak{p}_k$:

$$\sum_{i=1}^{m} a_i\,(y_{ik} - y_{i1}) = 0, \quad \sum_{i=1}^{m} a_i\, y_{ik}^{(\lambda)} = 0 \quad (k = 1, \ldots, h,\ \lambda = 1, \ldots, l-1). \tag{25}$$

Die Matrix dieses Gleichungssystems

$$\begin{pmatrix} y_{12} - y_{11} & \cdots & y_{1h} - y_{11} & y_{11}^{(1)} & \cdots & y_{11}^{(l-1)} & y_{12}^{(1)} & \cdots & y_{1h}^{(l-1)} \\ \cdot & & \cdot & \cdot & & \cdot & \cdot & & \cdot \\ \cdot & & \cdot & \cdot & & \cdot & \cdot & & \cdot \\ \cdot & & \cdot & \cdot & & \cdot & \cdot & & \cdot \\ y_{m2} - y_{m1} & \cdots & y_{mh} - y_{m1} & y_{m1}^{(1)} & \cdots & y_{m1}^{(l-1)} & y_{m2}^{(1)} & \cdots & y_{mh}^{(l-1)} \end{pmatrix} \tag{26}$$

hat m Zeilen und $m + g - 1$ Spalten, es ist also nichttrivial lösbar, falls ihr Rang $\leqq m - 1$ ist. Der Rang von (26) ist nicht $< m - 1$, denn sonst könnte man durch eine lineare Substitution auf die y_i erreichen, daß die beiden ersten Zeilen verschwinden. Dann wären die Funktionen $y_1 - y_{11}$ und $y_2 - y_{21}$ im Zähler durch $(\mathfrak{p}_1 \ldots \mathfrak{p}_h)^l$ teilbar, und man könnte aus ihnen eine nicht verschwindende Funktion linear kombinieren, deren Nenner höchstens $\mathfrak{o}^{hl-1}$ ist. Das ist ein Widerspruch.

Da (26) den Rang $m-1$ hat, kann man durch geeignete lineare Transformation der y_i mit Koeffizienten in k' erreichen, daß die $y_{ik} - y_{i1}$, $y_{ik}^{(\lambda)}$ ganz sind, und daß ihre Reste $(y_{ik} - y_{i1})(p)$, $y_{ik}^{(\lambda)}(p)$ mod einem Primteiler $\mathfrak{p}'$ von p in k' eine Matrix (26) vom Rang $m - 1$ ergeben. Es gibt weiterhin ein nichttriviales Lösungssystem $a_i(p)$ von (25) mit dieser Matrix in dem Restklassenkörper $k'(\mathfrak{p}')$. Die ersten der Gleichungen (25) haben zur Folge, daß es in k' Größen $a_0(p)$, $y_{ik}(p)$ mit $y_{ik}(p) - y_{i1}(p) = (y_{ik} - y_{i1})(p)$, $a_0(p) + \Sigma\, a_i(p)\, y_{ik}(p) = 0$ $(k = 1, \ldots, h)$ gibt. Wir definieren nun in $K(p)\,k'(\mathfrak{p}')$ Divisoren

$$\mathfrak{p}_k(p) = \text{gr. gem. Teiler des Zählers aller } (y_i^{(\lambda)}(p) - y_{ik}^{(\lambda)}(p)) \qquad (i = 1, \ldots, m;\ \lambda = 0, \ldots, l-1).$$

Sie sind teilerfremd, denn hätten $\mathfrak{p}_k(p)$, $\mathfrak{p}_{k'}(p)$ einen gemeinsamen Teiler $\neq 1$, so wäre im Restklassenkörper $k'(\mathfrak{p}')$ $y_{ik} - y_{i1} = y_{ik'} - y_{i1}$, $y_{ik}^{(\lambda)} = y_{ik'}^{(\lambda)}$. In (26) wären also l Spaltenpaare einander gleich, und dann wäre der Rang höchstens $m + g - l < m - 1$, im Widerspruch zu unserer Annahme. Wegen der Vertauschbarkeit der doppelten Restbildung mod $\mathfrak{p}_k$ und mod $\mathfrak{p}'$ [3, S. 650] sind die $\mathfrak{p}_k(p)$ durch die Bilder der $\mathfrak{p}_k$ in $\overline{K(p)}$ teilbar; wir werden gleich sehen, daß sie mit ihnen sogar identisch sind. Jedenfalls sind alle so definierten $\mathfrak{p}_k(p) \neq 1$. Das Element $y(p) = a_0(p) + \Sigma a_i(p) y_i(p)$ ist durch $(\mathfrak{p}_1(p) \dots \mathfrak{p}_h(p))^l$ teilbar, sein Nenner ist höchstens $\mathfrak{o}(p)^{hl}$. Folglich sind die $\mathfrak{p}_k(p)$ Primdivisoren 1. Grades und die Bilder der $\mathfrak{p}_k$. Schließlich ist das Bild $\mathfrak{y}(p) = \frac{\mathfrak{p}_1(p) \cdots \mathfrak{p}_h(p)}{\mathfrak{o}(p)^h}$ von $\mathfrak{y}$ kein Hauptdivisor, da $\mathfrak{o}(p)$ nach Voraussetzung kein WEIERSTRASSpunkt ist.

Literaturverzeichnis

[1] M. DEURING, Arithmetische Theorie der Korrspondenzen algebraischer Funktionenkörper I. J. reine angew. Math. **177**, 161—191 (1937).

[2] M. DEURING, dasselbe II, ebenda **183**, 25—36 (1940).

[3] M. DEURING, Reduktion algebraischer Funktionenkörper nach Primdivisoren des Konstantenkörpers. Math. Z. **47**, 643—654 (1941).

[4] M. DEURING, Die Zetafunktion einer algebraischen Kurve vom Geschlechte eins. Nachr. Akad. Wiss. Göttingen, Math.-Phys. Kl. IIa, 1953, S. 85—94.

[5] E. HECKE, Über Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Produktentwicklung I, II. Math. Ann. **114**, 1—28, 316—351 (1937).

[6] H. HASSE und F. K. SCHMIDT, Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten. J. reine angew. Math. **177**, 215—237 (1937).

[7] F. K. SCHMIDT, Die Wronskische Determinante in beliebigen differenzierbaren Funktionenkörpern. Math. Z. **45**, 62—74 (1939).

[8] F. K. SCHMIDT, Zur arithmetischen Theorie der algebraischen Funktionenkörper. Math. Z. **45**, 75—96 (1939).

[9] H. WEBER, Elliptische Funktionen und algebraische Zahlen. Braunschweig 1891.

[10] A. WEIL, Jacobi Sums as "Größencharaktere". Trans. Amer. Math. Soc. **73**, 487—495 (1952).

[11] A. WEIL, Sur les courbes algébriques et les variétés qui s'en déduisent. Actual. Sci. Industr. **1041**, Paris 1948.

[12] A. WEIL, Variétés abéliennes et courbes algébriques. Actual. Sci. Industr. **1064**, Paris 1948.

Eingegangen am 21. 11. 1953