Zur Theorie der abstrakten elliptischen Funktionenkörper III.

Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung.

Von *Helmut Hasse* in Göttingen.

Wie in den Teilen I und II dieser Arbeit [1]) sei K ein algebraischer Funktionenkörper einer Unbestimmten vom Geschlecht 1 über einem algebraisch-abgeschlossenen Konstantenkörper k der Charakteristik p ($= 0$ oder Primzahl). Zum Schluß werden wir k speziell als den absolut-algebraischen algebraisch-abgeschlossenen Körper der Primzahlcharakteristik p voraussetzen.

§ 1. Die Normenadditionsformel.

1. Wir beweisen die grundlegende Formel

$$(1) \qquad N(\mu+\nu) + N(\mu-\nu) = 2\,N(\mu) + 2\,N(\nu)$$

für beliebige (o. B. d. A. normierte) Meromorphismen μ, ν von K.

Für $\mu = 0$ oder $\nu = 0$ ist die Formel (1) trivialerweise richtig.

Für $\mu+\nu = 0$ oder $\mu-\nu = 0$ besagt sie

$$(1') \qquad N(2\mu) = 4\,N(\mu)\,,$$

und dies läuft nach dem Normenproduktsatz auf die spezielle Tatsache

$$(1\text{a}) \qquad N(2) = 4$$

zurück.

Als Grad von $K/K\mu$ ist $N(\mu)$ gleich dem Grad in K des $\mathfrak{o}$ enthaltenen Primdivisors $\mathfrak{o}\mu = N_\mu\mathfrak{o}$ von $K\mu$. Wir werden den Beweis der Gradrelation (1) dadurch erbringen, daß wir die Divisorenäquivalenzen

$$(2) \qquad \frac{\mathfrak{o}(\mu+\nu)\cdot\mathfrak{o}(\mu-\nu)}{(\mathfrak{o}\mu)^2\cdot(\mathfrak{o}\nu)^2} \sim 1 \quad \text{für } \mu,\ \nu,\ \mu+\nu,\ \mu-\nu \neq 0\,,$$

$$(2') \qquad \frac{\mathfrak{o}(2\mu)}{(\mathfrak{o}\mu)^4} \sim 1 \quad \text{für } \mu \neq 0$$

feststellen, deren letztere durch Anwendung des Meromorphismus μ auf die spezielle

---

[1]) H. Hasse, Zur Theorie der abstrakten elliptischen Funktionenkörper I, Die Struktur der Gruppe der Divisorenklassen endlicher Ordnung; II, Automorphismen und Meromorphismen, das Additionstheorem; Journ. f. Math. **175** (1936); im folgenden zitiert als H I, H II.

Divisorenäquivalenz

$$\text{(2a)} \qquad \frac{\mathfrak{o}2}{\mathfrak{o}^4} \sim 1$$

zurückläuft. Diese Feststellungen werden wir durch den Nachweis der Divisorengleichungen

$$\text{(3)} \qquad \frac{\mathfrak{o}(\mu+\nu)\cdot\mathfrak{o}(\mu-\nu)}{(\mathfrak{o}\mu)^2\cdot(\mathfrak{o}\nu)^2} \cong x\mu - x\nu \text{ für } \mu, \nu, \mu+\nu, \mu-\nu \neq 0,$$

$$\text{(3')} \qquad \frac{\mathfrak{o}(2\mu)}{(\mathfrak{o}\mu)^4} \cong d(x\mu) \text{ für } \mu \neq 0$$

erbringen, deren letztere wieder durch Anwendung von μ auf die spezielle Divisorengleichung

$$\text{(3a)} \qquad \frac{\mathfrak{o}2}{\mathfrak{o}^4} \cong dx$$

zurückläuft.

Wir werden allerdings (3) hier nur unter einer gewissen einschränkenden Voraussetzung über die Inseparabilitätsexponenten $J(\mu)$, $J(\nu)$, $J(\mu+\nu)$, $J(\mu-\nu)$ beweisen, die für den Rückschluß auf die allgemeine Gültigkeit von (1) ausreicht. Für die hier beabsichtigte Anwendung kommt es allein auf die Gradrelation (1) an. Es dürfte aber nicht schwer sein, mit den im Beweis dargelegten Methoden auch die allgemeine Gültigkeit von (3) zu beweisen.

Beim Beweis von (3) und (3a) erfordert der Fall $p = 2$ besondere Betrachtungen. Um die Linienführung des Beweises klar hervortreten zu lassen, werden wir an den Stellen, wo für $p = 2$ eine solche Sonderbetrachtung erforderlich ist, zunächst $p \neq 2$ voraussetzen und dann am Schluß die für $p = 2$ nötigen Ergänzungen nachholen.

2. Wir stellen einige in H II bewiesene oder leicht aus den dortigen Ausführungen zu gewinnende Tatsachen voran, die wir beim Beweis dauernd vor Augen haben müssen.

a) *Der Inseparabilitätsexponent* $J(\mu)$.

Es ist

$$J(\mu) = 1 \rightleftarrows c_\mu \neq 0,$$

wo c_μ der Faktor ist, den das ganze Differential du bei Anwendung von μ bekommt:

$$(du)\mu = c_\mu\, du.$$

Insbesondere für ganzrationale n ist nach dem Additionstheorem für du

$$(du)n = n\, du, \quad \text{d. h.} \quad c_n = n.$$

Daraus folgt

$$J(n) = 1 \rightleftarrows n \not\equiv 0 \text{ mod. } p.$$

Es gilt die Additionsregel

$$J(\mu+\nu) \geqq \operatorname{Min}(J(\mu), J(\nu)).$$

Denn es ist $K\mu \leqq K^{J(\mu)}$, $K\nu \leqq K^{J(\nu)}$, und daher

$$K(\mu+\nu) \leqq K\mu \cdot K\nu \leqq K^{\operatorname{Min}(J(\mu), J(\nu))}.$$

Hiernach und mit Hinblick auf die Produktregel $J(\mu\nu) = J(\mu)\,J(\nu)$ liefert $J(\mu)$ (durch seinen reziproken Wert) eine nichtarchimedische Bewertung des Ringes M der normierten

Meromorphismen. Dabei gilt bekanntlich als formale Folge der genannten Additionsregel die schärfere Regel

$$J(\mu + \nu) = \mathrm{Min}\,(J(\mu), J(\nu)), \quad \text{wenn} \quad J(\mu) \neq J(\nu)\,.$$

Für den in M enthaltenen Teilring Γ der ganzrationalen Meromorphismen n liefert $J(n)$ nach der obigen Feststellung die identische Bewertung, wenn $p = 0$, und eine Potenz der p-adischen Bewertung mit einem festen positiven ganzzahligen Exponenten s:

$$J(n) = p^{sf}, \quad \text{für} \quad n = p^f n_0, \quad n_0 \not\equiv 0 \bmod. p\,,$$

wenn $p \neq 0$. Auf die Bestimmung dieses Exponenten s kommen wir später zurück.

b) *Primdivisoren und normierte Primelemente.*

Es ist

$$\mathfrak{p} \,|\, \mathfrak{q}\mu \rightleftarrows \mu\mathfrak{p} = \mathfrak{q}\,.$$

Wenn $\mathfrak{p} \,|\, \mathfrak{q}\mu$, so geht $\mathfrak{p}$ in $\mathfrak{q}\mu$ genau zum Exponenten $J(\mu)$ auf; $\mathfrak{p}_0 = \mathfrak{p}^{J(\mu)}$ ist der $\mathfrak{p}$ enthaltende Primdivisor des zu K absolut-isomorphen maximal-separablen Zwischenkörpers $K_0 = K^{J(\mu)}$ von $K/K\mu$.

Ein Primelement π zu $\mathfrak{p}$ heiße *normiert*, wenn der in π verfügbare konstante Faktor $\neq 0$ so festgelegt ist, daß

$$\frac{d\pi}{du} \equiv 1 \bmod. \mathfrak{p}, \quad \text{d. h.} \quad \frac{d\pi}{du}\,\mathfrak{p} = 1$$

ist. Man beachte, daß diese Normierung, anders als die Normierung der Erzeugenden x, y oder der Meromorphismen μ, nicht auf einen festen Primdivisor $\mathfrak{o}$ bezogen ist, sondern nur auf ein festes ganzes Differential du.

Sei nun $\mathfrak{p} \,|\, \mathfrak{q}\mu$, also $\mu\mathfrak{p} = \mathfrak{q}$, und seien π, $\varkappa$ normierte Primelemente zu $\mathfrak{p}$, $\mathfrak{q}$. Ist zunächst $J(\mu) = 1$, so ist auch $\varkappa\mu$ ein Primelement zu $\mathfrak{p}$, und es entsteht die Frage nach dem zur Normierung von $\varkappa\mu$ führenden Faktor, d. h. nach dem Zusammenhang zwischen $\varkappa\mu$ und π. Sie wird beantwortet durch die Regel

$$\frac{\varkappa\mu}{\pi} \equiv c_\mu \bmod. \mathfrak{p}\,.$$

Man hat nämlich

$$\frac{d(\varkappa\mu)}{du} = c_\mu \frac{(d\varkappa)\mu}{(du)\mu} = c_\mu \frac{d\varkappa}{du}\mu,$$

also

$$\frac{d(\varkappa\mu)}{du}\,\mathfrak{p} = c_\mu \frac{d\varkappa}{du}\,\mu\mathfrak{p} = c_\mu \frac{d\varkappa}{du}\,\mathfrak{q} = c_\mu\,.$$

Für beliebige Inseparabilitätsexponenten $J(\mu)$ ergibt sich ein ganz entsprechender Sachverhalt, wenn man $\mathfrak{p}$, $\mathfrak{q}$, π, $\varkappa$, du, c_μ durch die entsprechenden Bildungen

$$\mathfrak{p}_0 = \mathfrak{p}^{J(\mu)}, \quad \mathfrak{q}_0 = \mathfrak{q}^{J(\mu)}, \quad \pi_0 = \pi^{J(\mu)}, \quad \varkappa_0 = \varkappa^{J(\mu)}, \quad du_0, \quad c_\mu^{(0)}$$

in $K_0 = K^{J(\mu)}$ ersetzt.

c) *Primdivisoren und konstante Reste von x.*

Bei der eindeutigen Charakterisierung der Primdivisoren $\mathfrak{p} \neq \mathfrak{o}$ durch die konstanten Reste a, b eines normierten Erzeugendenpaares x, y auf Grund der Relation

$$(x\mathfrak{p}, y\mathfrak{p}) = (a, b)$$

entsprechen einem gegebenen Rest a von x immer gerade zwei bzgl. $k(x)$ konjugierte (verschiedene oder auch gleiche) Primdivisoren, denn man hat $x - a \cong \frac{\mathfrak{p}\mathfrak{p}'}{\mathfrak{o}^2}$. In der Gruppe D_0 ist $\mathfrak{p}' = -\mathfrak{p}$; einem gegebenen Rest a von x entsprechen also immer zwei in D_0 entgegengesetzte Primdivisoren $\pm\mathfrak{p}$.

3. *Beweis von* (3a) (*für* $p \neq 2$). Bekanntlich ist

$$dx \cong \frac{\mathfrak{d}_x}{\mathfrak{o}^4},$$

wo $\mathfrak{d}_x$ der Differentendivisor von $K/k(x)$ ist. (3a) läuft also auf

$$\mathfrak{d}_x = \mathfrak{o}2$$

hinaus.

a) $\mathfrak{d}_x$ und $\mathfrak{o}2$ sind jedenfalls aus genau denselben Primdivisoren zusammengesetzt. Denn es ist

$$\mathfrak{p} \mid \mathfrak{d}_x \rightleftarrows \mathfrak{p} = -\mathfrak{p} \rightleftarrows 2\mathfrak{p} = \mathfrak{o} \rightleftarrows \mathfrak{p} \mid \mathfrak{o}2.$$

b) Ist $p \neq 2$, so ist einerseits jedes $\mathfrak{p} \mid \mathfrak{d}_x$ genau zur ersten Potenz in $\mathfrak{d}_x$ enthalten, weil dann $\mathfrak{p}$ die Verzweigungsordnung $2 \not\equiv 0 \bmod p$ hat, und andererseits jedes $\mathfrak{p} \mid \mathfrak{o}2$ genau zur ersten Potenz in $\mathfrak{o}2$ enthalten, weil dann $J(2) = 1$ ist.

Damit ist (3a) für $p \neq 2$ bewiesen.

4. *Beweis von* (3) (*unter der Voraussetzung* (J)). Wir legen die Voraussetzung

(J) $$J(\mu+\nu) = J(\mu-\nu) = \mathrm{Min}\,(J(\mu), J(\nu)) \quad = J(\mu) \text{ (o. B. d. A.)}$$

zugrunde. Um den Beweis möglichst klar hervortreten zu lassen, führen wir ihn zunächst sogar nur unter der Voraussetzung

(J_1) $$J(\mu+\nu) = J(\mu-\nu) = 1 \quad = J(\mu) \text{ (o. B. d. A.)},$$

und geben nachher kurz an, welche Modifikation für den Beweis unter der allgemeinen Voraussetzung (J) erforderlich ist.

Zur Abkürzung sei der in (3) auftretende Quotient

$$\frac{\mathfrak{o}(\mu+\nu)\cdot\mathfrak{o}(\mu-\nu)}{(\mathfrak{o}\mu)^2\cdot(\mathfrak{o}\nu)^2} = \mathfrak{Q}_{\mu,\nu}$$

gesetzt.

I. *Gleichheit der reduzierten Nenner von* $x\mu - x\nu$ *und* $\mathfrak{Q}_{\mu,\nu}$.

a) Da x den genauen Nenner $\mathfrak{o}^2$ hat, haben $x\mu$, $x\nu$ die genauen Nenner $(\mathfrak{o}\mu)^2$, $(\mathfrak{o}\nu)^2$. Daher kann $x\mu - x\nu$ jedenfalls als gebrochener Divisor mit dem Nennner $(\mathfrak{o}\mu)^2\cdot(\mathfrak{o}\nu)^2$ und ganzem Zähler geschrieben werden. Dabei können sich höchstens solche Primdivisoren $\mathfrak{p}$ ganz oder teilweise gegen den Zähler wegheben, für die zugleich $\mathfrak{p} \mid \mathfrak{o}\mu$ und $\mathfrak{p} \mid \mathfrak{o}\nu$, also $\mu\mathfrak{p} = \mathfrak{o}$ und $\nu\mathfrak{p} = \mathfrak{o}$ gilt. Auch in dem Divisorenbruch $\mathfrak{Q}_{\mu,\nu}$ können sich nur diese Primdivisoren $\mathfrak{p}$ *gegen den Zähler ganz* oder teilweise wegheben; denn [2]) soll etwa zugleich $\mathfrak{p} \mid \mathfrak{o}\mu$ und $\mathfrak{p} \mid \mathfrak{o}(\mu+\nu)$ sein, also $\mu\mathfrak{p} = \mathfrak{o}$ und $(\mu+\nu)\mathfrak{p} = \mathfrak{o}$, so folgt nach dem Additionstheorem auch $\nu\mathfrak{p} = \mathfrak{o}$, also $\mathfrak{p} \mid \mathfrak{o}\nu$.

b) Um die Gleichheit der reduzierten Nenner von $x\mu - x\nu$ und $\mathfrak{Q}_{\mu,\nu}$ zu beweisen, bleibt demnach festzustellen, daß die $\mathfrak{p}$ mit zugleich

---

[2]) Schlüsse dieser Art werden wir im folgenden durchweg stillschweigend vollziehen.

$$\mathfrak{p} \mid \mathfrak{o}\mu, \ \mathfrak{p} \mid \mathfrak{o}\nu, \ \text{also} \ \mu\mathfrak{p} = \nu\mathfrak{p} = \mathfrak{o}$$

dieselben Beiträge zu $x\mu - x\nu$ und $\mathfrak{Q}_{\mu,\nu}$ liefern.

Ist nun zunächst $J(\nu) \neq 1$, so liefert ein solches $\mathfrak{p}$ zu $x\mu - x\nu$ den Beitrag $\mathfrak{p}^{-2J(\nu)}$ und auch zu $\mathfrak{Q}_{\mu,\nu}$ den Beitrag

$$\frac{\mathfrak{p} \cdot \mathfrak{p}}{\mathfrak{p}^2 \cdot \mathfrak{p}^{2J(\nu)}} = \mathfrak{p}^{-2J(\nu)} .$$

Ist aber auch $J(\nu) = 1$, so sei

$$x = \frac{a}{\omega^2} + \cdots \quad (a \neq 0)$$

die $\mathfrak{o}$-adische Entwicklung von x nach einem normierten Primelement ω zu $\mathfrak{o}$. Nach dem zuvor Bemerkten ergibt sich daraus die $\mathfrak{p}$-adische Entwicklung von $x\mu - x\nu$ nach einem normierten Primelement π zu einem $\mathfrak{p}$ der genannten Art wie folgt:

$$x\mu = \frac{a}{(\omega\mu)^2} + \cdots = \frac{1}{c_\mu^2}\frac{a}{\pi^2} + \cdots .$$

$$x\nu = \frac{a}{(\omega\nu)^2} + \cdots = \frac{1}{c_\nu^2}\frac{a}{\pi^2} + \cdots .$$

$$\begin{aligned} x\mu - x\nu &= -\frac{c_\mu^2 - c_\nu^2}{c_\mu^2\, c_\nu^2}\frac{a}{\pi^2} + \cdots . \\ &= -\frac{(c_\mu + c_\nu)\,(c_\mu - c_\nu)}{c_\mu^2\, c_\nu^2}\frac{a}{\pi^2} + \cdots . \\ &= -\frac{c_{\mu+\nu}\; c_{\mu-\nu}}{c_\mu^2 c_\nu^2}\frac{a}{\pi^2} + \cdots , \end{aligned}$$

letzteres nach dem Additionstheorem für du. Wegen der Voraussetzung (J_1) und $J(\nu) = 1$ sind $c_\mu, c_\nu, c_{\mu+\nu}, c_{\mu-\nu} \neq 0$. Daher liefert $\mathfrak{p}$ zu $x\mu - x\nu$ den Beitrag $\mathfrak{p}^{-2}$. Zu $\mathfrak{Q}_{\mu,\nu}$ liefert $\mathfrak{p}$ ebenfalls den Beitrag $\mathfrak{p}^{-2}$.

II. *Gleichheit der reduzierten Zähler von $x\mu - x\nu$ und $\mathfrak{Q}_{\mu,\nu}$.*

Auf Grund des bereits Bewiesenen brauchen wir nur noch solche Primdivisoren $\mathfrak{p}$ zu betrachten, für die zugleich

$$\mathfrak{p} \nmid \mathfrak{o}\mu, \ \mathfrak{p} \nmid \mathfrak{o}\nu, \quad \text{also} \quad \mu\mathfrak{p} \neq \mathfrak{o}, \ \nu\mathfrak{p} \neq \mathfrak{o}$$

ist.

a) Die reduzierten Zähler von $x\mu - x\nu$ und $\mathfrak{Q}_{\mu,\nu}$ sind jedenfalls aus genau denselben Primdivisoren zusammengesetzt. Denn es ist für die nur noch zu betrachtenden $\mathfrak{p}$

$$(x\mu - x\nu)\,\mathfrak{p} = \mathfrak{o} \rightleftarrows x\mu\mathfrak{p} = x\nu\mathfrak{p} \rightleftarrows \mu\mathfrak{p} = \pm\, \nu\mathfrak{p} \rightleftarrows (\mu \pm \nu)\,\mathfrak{p} = \mathfrak{o} \rightleftarrows \mathfrak{p} \mid \mathfrak{o}(\mu \pm \nu) .$$

b) Um die Gleichheit der reduzierten Zähler von $x\mu - x\nu$ und $\mathfrak{Q}_{\mu,\nu}$ zu beweisen, bleibt demnach noch festzustellen, daß die $\mathfrak{p}$ mit zugleich

$$\mathfrak{p} \nmid \mathfrak{o}\mu, \ \mathfrak{p} \nmid \mathfrak{o}\nu, \ \mathfrak{p} \mid \mathfrak{o}(\mu + \nu) \ \text{oder} \ \mathfrak{p} \mid \mathfrak{o}(\mu - \nu)$$

dieselben Beiträge zu $x\mu - x\nu$ und $\mathfrak{Q}_{\mu,\nu}$ liefern. Wegen der Symmetrie in $\pm\,\nu$ genügt es, etwa

$$\mathfrak{p} \mid \mathfrak{o}(\mu - \nu), \ \text{also} \ \mu\mathfrak{p} = \nu\mathfrak{p}$$

anzunehmen. Sei $\mu\mathfrak{p} = \nu\mathfrak{p} = \mathfrak{q}$ gesetzt; es ist $\mathfrak{q} \neq \mathfrak{o}$.

Ist dann zunächst

$$\mathfrak{p} \nmid \mathfrak{o}(\mu + \nu), \ \text{also} \ \mu\mathfrak{p} \neq -\, \nu\mathfrak{p}, \ \text{d. h.} \ \mathfrak{q} \neq -\,\mathfrak{q} ,$$

so lautet die $\mathfrak{q}$-adische Entwicklung von x nach einem normierten Primelement $\varkappa$ zu $\mathfrak{q}$:

$$x = a + a'\varkappa + \cdots \qquad (a' \neq 0),$$

also analog wie vorher die $\mathfrak{p}$-adische Entwicklung von $x\mu - x\nu$ nach einem normierten Primelement π zu $\mathfrak{p}$:

$$\begin{aligned} x\mu - x\nu &= (c_\mu - c_\nu)\, a'\pi + \cdots \\ &= c_{\mu-\nu}\, a'\pi + \cdots. \end{aligned}$$

Wegen $c_{\mu-\nu} \neq 0$ liefert daher $\mathfrak{p}$ zu $x\mu - x\nu$ den Beitrag $\mathfrak{p}^1$. Zu $\mathfrak{Q}_{\mu,\nu}$ liefert $\mathfrak{p}$ ebenfalls den Beitrag $\frac{1 \cdot \mathfrak{p}}{1 \cdot 1} = \mathfrak{p}^1$.

Ist aber auch

$$\mathfrak{p} \,|\, \mathfrak{d}(\mu + \nu), \text{ also } \mu\mathfrak{p} = -\nu\mathfrak{p}, \text{ d. h. } \mathfrak{q} = -\mathfrak{q},$$

so hat man entsprechend

$$\begin{aligned} x &= a + a''\varkappa^2 + \cdots \qquad (a'' \neq 0) \\ x\mu - x\nu &= (c_\mu^2 - c_\nu^2)\, a''\pi^2 + \cdots \\ &= (c_\mu + c_\nu)(c_\mu - c_\nu)\, a''\pi^2 + \cdots \\ &= c_{\mu+\nu}\, c_{\mu-\nu}\, a''\pi^2 + \cdots. \end{aligned}$$

Da auch $c_{\mu+\nu} \neq 0$, liefert daher $\mathfrak{p}$ zu $x\mu - x\nu$ den Beitrag $\mathfrak{p}^2$. Zu $\mathfrak{Q}_{\mu,\nu}$ liefert $\mathfrak{p}$ den Beitrag $\frac{\mathfrak{p} \cdot \mathfrak{p}}{1 \cdot 1} = \mathfrak{p}^2$.

Damit ist (3) unter der Voraussetzung (J_1) bewiesen. Der Beweis unter der allgemeinen Voraussetzung (J) kommt ganz entsprechend zustande, indem man die Nachweise für das Übereinstimmen der Beiträge durchweg im Körper $K_0 = K^{J(\mu)}$ statt K führt. In der Tat übertragen sich dabei die wesentlichen Punkte, nämlich die Regel über den Zusammenhang der normierten Primelemente und das Additionstheorem für du als Additionstheorem der in K_0 zugeordneten Faktoren $c_\mu^{(0)}$. Diese Bemerkungen mögen hier genügen; ein näheres Eingehen auf den Beweis dürfen wir uns ersparen.

5. *Allgemeiner Beweis von* (1) (für $p \neq 2$). Ist die Voraussetzung (J) nicht erfüllt, gilt also o. B. d. A.

$$J(\mu - \nu) > \operatorname{Min}(J(\mu), J(\nu)),$$

so ist wegen der schärferen Additionsregel genauer

$$J(\mu - \nu) > J(\mu) = J(\nu)$$

und ferner jedenfalls

$$J(\mu + \nu) \geqq \operatorname{Min}(J(\mu - \nu), J(2)\, J(\nu)),$$

mit Gleichheitszeichen, wenn $J(\mu - \nu) \neq J(2)\, J(\nu)$ ist.

Für $p \neq 2$ ist nun $J(2) = 1$, also gilt das Gleichheitszeichen, und daraus folgt

$$J(\mu + \nu) < J(\mu - \nu).$$

Dann ist aber (nach der schärferen Additionsregel) die Voraussetzung (J) für $\mu + \nu$, $\mu - \nu$ statt μ, ν erfüllt. Nach dem bereits Bewiesenen gilt dann also

$$\frac{\mathfrak{d}(2\mu) \cdot \mathfrak{d}(2\nu)}{(\mathfrak{d}(\mu + \nu))^2 \cdot (\mathfrak{d}(\mu - \nu))^2} \sim 1.$$

Durch Kombination mit (2′) folgt daraus weiter

$$\left(\frac{(\mathfrak{o}\mu)^2 \cdot (\mathfrak{o}\nu)^2}{\mathfrak{o}(\mu+\nu) \cdot \mathfrak{o}(\mu-\nu)}\right)^2 \sim 1\,,$$

also $(2)^2$, und somit (1).

6. Ergänzungen für $p = 2$ sind an zwei Stellen dieses Beweises erforderlich, nämlich einmal im Beweis von (3a) und dann in dem zuletzt ausgeführten Rückschluß auf (1), wenn (J) nicht erfüllt ist.

Zur Vorbereitung dieser Ergänzungen aber auch für spätere Zwecke gehen wir näher auf die *ganzrationalzahligen Meromorphismen* n ein. Die Formel (1) ist für sie auf Grund eines induktiven Schlußverfahrens gleichwertig mit der expliziten Formel

$$N(n) = n^2\,. \tag{4}$$

Wir leiten nun, zunächst unabhängig von dem vorstehenden Beweis, aus dem Ergebnis von H I Aussagen in Richtung auf diese Formel her. Dabei genügt es nach dem Normenproduktsatz, die Fälle $n \not\equiv 0$ mod. p und $n = p^f$ zu betrachten (wobei in letzterem Falle durchweg stillschweigend $p \neq 0$ vorausgesetzt wird). Es ist

$$N(n) = J(n)\, N_0(n)\,.$$

Für den Inseparabilitätsexponenten $J(n)$ haben wir oben bereits

$$J(n) = 1 \qquad \text{für} \quad n \not\equiv 0 \text{ mod. } p,$$
$$J(p^f) = p^{sf} \qquad \text{für} \quad n = p^f$$

festgestellt, mit einem gewissen festen positiven ganzzahligen Exponenten s. Die reduzierte Norm $N_0(n)$ ist die Anzahl der verschiedenen $\mathfrak{p}$ mit $n\mathfrak{p} = \mathfrak{o}$; nach H I ist also

$$N_0(n) = n^2 \text{ für } n \not\equiv 0 \text{ mod. } p,$$
$$N_0(p^f) = \begin{Bmatrix} p^f & \text{für } A \neq 0 \\ 1 & \text{für } A = 0 \end{Bmatrix}.$$

Hieraus ergibt sich

a) für $n \not\equiv 0$ mod. p ein direkter Beweis der Gültigkeit von (4),

b) für $n = p^f$ die Gleichwertigkeit von (4) mit der Aussage

$$J(p^f) = \begin{Bmatrix} p^f & \text{für } A \neq 0 \\ p^{2f} & \text{für } A = 0 \end{Bmatrix}, \tag{5}$$

d. h. mit der Exponentenbestimmung

$$s = 1 \text{ für } A \neq 0, \qquad s = 2 \text{ für } A = 0\,.$$

Für $p \neq 2$ haben wir (1) bereits in voller Allgemeinheit bewiesen und sind also damit auch im Besitz der Tatsachen (4) und (5).

Für $p = 2$ schließen wir folgendermaßen:

Für $\mu = 2$, $\nu = 1$ ist die Voraussetzung (J) (sogar (J_1)) erfüllt. Daher hat man

$$N(3) + N(1) = 2N(2) + 2N(1)\,.$$

Hier wissen wir $N(1) = 1$, sowie auf Grund von a) oben auch $N(3) = 9$. Daraus folgt $N(2) = 4$. Nach b) oben ergibt das

$$J(2) = \begin{Bmatrix} 2 & \text{für } A \neq 0 \\ 2^2 & \text{für } A = 0 \end{Bmatrix},$$

und damit dann auch die allgemeine Gültigkeit von (5) und somit (4).

7. *Ergänzung für $p = 2$ zum Beweis von* (3a). Für $p = 2$ hat auf Grund der (in H I gegebenen) Definition von A die $\mathfrak{o}$-adische Entwicklung von x die Form

$$x = a\left(\frac{1}{\omega^2} - \frac{A}{\omega} + \cdots\right) \qquad (a \neq 0).$$

Hiernach ist $A = 0$ gleichbedeutend damit, daß dx ganz für $\mathfrak{o}$ und somit $dx \cong 1$, $\mathfrak{d}_x = \mathfrak{o}^4$ ist. Damit ergibt sich als Ersatz der für $p = 2$ ungültigen Schlußkette b) des obigen Beweises von (3a) — der Teil a) gilt ja auch für $p = 2$ —:

$$\mathfrak{o}2 = \mathfrak{o}^4 \rightleftarrows J(2) = 2^2 \rightleftarrows A = 0 \rightleftarrows dx \cong 1 \rightleftarrows \mathfrak{d}_x = \mathfrak{o}^4,$$

sowie

$$\mathfrak{o}2 = \mathfrak{o}^2\mathfrak{z}^2 \rightleftarrows J(2) = 2 \rightleftarrows A \neq 0 \rightleftarrows dx \cong \frac{\mathfrak{o}^2\mathfrak{z}^2}{\mathfrak{o}^4} \rightleftarrows \mathfrak{d}_x = \mathfrak{o}^2\mathfrak{z}^2.$$

Daß im letzteren Falle $\mathfrak{d}_x$ nicht gleich $\mathfrak{o}\mathfrak{z}^3$ oder $\mathfrak{o}^3\mathfrak{z}$ ist, folgt aus der an anderer Stelle [3]) bewiesenen allgemeinen Formel für den Differentendivisor eines zyklischen algebraischen Funktionenkörpers vom Grade p, oder auch einfach aus dem Dedekindschen Differentensatz.

8. *Ergänzung für $p = 2$ zum Rückschluß auf* (1), *wenn* (J) *nicht erfüllt ist.* Nachdem die Gültigkeit von (2′) auch für $p = 2$ feststeht, versagt der obige Rückschluß auf (1), wenn (J) nicht erfüllt ist, bei $p = 2$ nur dann, wenn

$$J(\mu) = J(\nu) < J(\mu + \nu) = J(\mu - \nu) < J(2)\,J(\mu) = J(2)\,J(\nu)$$

ist. Für $A \neq 0$, also $J(2) = 2$ ist das unmöglich; für $A = 0$, also $J(2) = 2^2$ besagt es

$$J(\mu + \nu) = J(\mu - \nu) = 2J(\mu) = 2J(\nu).$$

Jedenfalls ist dann (J) erfüllt, wenn das System

$$\mu, \quad \nu; \quad \mu + \nu, \quad \mu - \nu$$

durch eins der folgenden drei Systeme ersetzt wird

$$\begin{array}{lcccc} \text{(a)} & \mu + \nu, & \mu; & 2\mu + \nu, & \nu \\ \text{(b)} & \mu - \nu, & \mu; & 2\mu - \nu, & -\nu \\ \text{(c)} & 2\mu, & \nu; & 2\mu + \nu, & 2\mu - \nu. \end{array}$$

Kombiniert man die diesen Systemen entsprechenden Divisorenäquivalenzen (2) nach dem Schema $\frac{\text{(a)}\,\text{(b)}}{\text{(c)}}$ und wendet wieder (2′) an, so ergibt sich ersichtlich wieder $(2)^2$, und somit (1).

Damit ist (1) allgemein bewiesen.

§ 2. Die Struktur des Meromorphismenrings.

1. Wir leiten zunächst einige formale Folgen aus dem folgenden Tatbestand her: M ist eine additive abelsche Gruppe, und in M liegt eine Zahlfunktion $N(\mu)$ mit der Funktionalgleichung

$$N(\mu + \nu) + N(\mu - \nu) = 2N(\mu) + 2N(\nu)$$

vor.

---

[3]) H. Hasse, Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper, Journ. f. Math. **172** (1934), 42.

Zunächst ergibt sich, den drei Spezialfällen $\nu = 0$, $\mu = 0$, $\mu \pm \nu = 0$ entsprechend, speziell:

$$N(0) = 0,$$
$$N(-\nu) = N(\nu),$$
$$N(2\mu) = 4N(\mu).$$

Wir führen nun das Symbol

$$(\mu, \nu) = \frac{N(\mu + \nu) - N(\mu) - N(\nu)}{2}$$

ein. Dafür ergeben sich, der Kommutativität und Assoziativität von M und der Funktionalgleichung von $N(\mu)$ entsprechend, ohne weiteres die folgenden drei Regeln:

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

(2) $$(\mu, \nu + \varrho) + (\nu, \varrho) = (\mu + \nu, \varrho) + \cancel{(\nu, \varrho)}, (\mu, \nu)$$

(3) $$(\mu, -\nu) = -(\mu, \nu).$$

Aus diesen Regeln ergibt sich weiter die Regel:

(4) $$(\mu, \nu + \varrho) = (\mu, \nu) + (\mu, \varrho).$$

Wird nämlich

$$(\mu, \nu, \varrho) = (\mu, \nu + \varrho) - (\mu, \nu) - (\mu, \varrho)$$

gesetzt, so ist nach (1), (2)

$$(\mu, \nu, \varrho) = (\varrho, \mu, \nu).$$

(μ, ν, ϱ) ist also symmetrisch in μ, ν, ϱ. Einerseits ist nun nach (3)

$$(\mu, -\nu, -\varrho) = -(\mu, \nu, \varrho).$$

Andrerseits ist nach (3), (1)

$$(-\mu, \nu, \varrho) = -(\mu, \nu, \varrho),$$

und wegen der festgestellten Symmetrie gilt Entsprechendes auch für ν und ϱ; daher hat man auch

$$(\mu, -\nu, -\varrho) = -(\mu, \nu, -\varrho) = +(\mu, \nu, \varrho).$$

Zusammengenommen ergibt sich hieraus $(\mu, \nu, \varrho) = 0$, d. h. die Regel (4).

Nach (1), (3), (4) hat das Symbol (μ, ν) die formalen Eigenschaften eines inneren Produkts. Insbesondere ist definitionsgemäß

$$(\mu, \mu) = \frac{N(2\mu) - 2N(\mu)}{2} = N(\mu).$$

Die Funktion $N(\mu)$ ist also das zu diesem inneren Produkt gehörige Quadrat. Vermöge der Rechenregeln (1), (4) des inneren Produkts ergibt sich dann die Formel:

(5) $$\begin{aligned} N(m\mu + n\nu) &= (m\mu + n\nu, m\mu + n\nu) = (m\mu, m\mu) + 2(m\mu, n\nu) + (n\nu, n\nu) \\ &= m^2(\mu, \mu) + 2mn(\mu, \nu) + n^2(\nu, \nu) \\ &= m^2 N(\mu) + mn(N(\mu + \nu) - N(\mu) - N(\nu)) + n^2 N(\nu) \end{aligned}$$

für beliebige ganzrationale m, n. [4])

[4]) Diese Herleitung der für das Folgende wichtigen Formel (5) verdanke ich einem Hinweis von Herrn Teichmüller. Herr Teichmüller war in der Theorie der allgemeinen linearen metrischen Räume auf die an die Spitze gestellte Funktionalgleichung geführt worden, nämlich als notwendige und hinreichende Bedingung dafür, daß in einem solchen Raum das Längenquadrat als Quadrat im Sinne eines inneren Produkts darstellbar ist. Siehe dazu übrigens P. Jordan-J. v. Neumann, On inner products in linear metric spaces, Ann. of Math. 36 (1935), 721.

2. Wir nehmen jetzt hinzu, daß M ein Ring mit Einselement ist, und daß die Funktion $N(\mu)$ zudem die Eigenschaften hat:

$$N(\mu) \text{ ist ganzrational, } N(\mu) = 0 \rightleftarrows \mu = 0,$$
$$N(\mu\nu) = N(\mu)\, N(\nu).$$

Dann ergibt sich zunächst ohne weiteres:

$$N(1) = 1,$$
$$N(m) = m^2 \text{ (nach (5))},$$
M hat keine echten Nullteiler,
M hat die Charakteristik 0.

Wir beweisen ferner die grundlegende Tatsache:

Jedes Element μ aus M ist Nullstelle eines quadratischen Polynoms

$$Q(z) = z^2 - lz + m$$

mit ganzrationalen l, m, nämlich

$$l = 2(\mu, 1) = N(\mu + 1) - N(\mu) - 1,$$
$$m = (\mu, \mu) = N(\mu).$$

Zum Beweis definieren wir $\bar{\mu}$ zu μ durch

$$\mu + \bar{\mu} = 2(\mu, 1) = l;$$

Dies $\bar{\mu}$ ist mit μ vertauschbar. Die Behauptung kommt dann auf den Nachweis von

$$\mu\bar{\mu} = m$$

hinaus, und dies wiederum auf den Nachweis von

$$N(\mu\bar{\mu} - m) = 0.$$

Nun gilt allgemein

$$(\mu\xi, \mu\eta) = \frac{N(\mu(\xi + \eta)) - N(\mu\xi) - N(\mu\eta)}{2} = N(\mu)\frac{N(\xi + \eta) - N(\xi) - N(\eta)}{2} = N(\mu)\,(\xi, \eta).$$

Ersetzt man hierin μ durch $m\mu + n\nu$ mit ganzrationalen m, n, so entstehen nach (1), (4) und (5) links und rechts quadratische Formen in m, n; der Vergleich der Koeffizienten von mn ergibt die Formel

$$(\mu\xi, \nu\eta) + (\nu\xi, \mu\eta) = 2(\mu, \nu)\,(\xi, \eta).$$

Daraus folgt insbesondere für $\nu = 1$ die Regel

$$(6) \qquad (\mu\xi, \eta) = l(\xi, \eta) - (\xi, \mu\eta) = (\xi, (l - \mu)\eta) = (\xi, \bar{\mu}\eta).$$

Nun ist nach (5)

$$N(\mu\bar{\mu} - m) = N(\mu\bar{\mu}) - 2m(\mu\bar{\mu}, 1) + m^2,$$

und hier ist einerseits

$$N(\mu\bar{\mu}) = N(\mu)\, N(\bar{\mu}) = m^2,$$

weil nach (5) auch

$$N(\bar{\mu}) = N(l - \mu) = l^2 - 2l(\mu, 1) + N(\mu) = l^2 - l^2 + m = m$$

ist, andrerseits nach (6)

$$(\mu\bar{\mu}, 1) = (\bar{\mu}, \bar{\mu}) = N(\bar{\mu}) = m,$$

zusammengenommen also in der Tat

$$N(\mu\bar{\mu} - m) = m^2 - 2m^2 + m^2 = 0.\,^{5})$$

Wir nehmen schließlich hinzu, daß durchweg $N(\mu) \geqq 0$ ist. Dann ergibt sich überdies die Tatsache:

Die Diskriminante des Polynoms $Q(z)$ ist $\leqq 0$, also

$$l^2 \leqq 4m\,.$$

Dies folgt entweder, indem man zum Ausdruck bringt, daß die quadratische Form rechts in (5) durchweg $\geqq 0$ ist, oder aus dem Ausdruck

$$(\mu - \bar{\mu})^2 = -(\mu - \bar{\mu})(\bar{\mu} - \mu) = -(\mu - \bar{\mu})\,\overline{(\mu - \bar{\mu})} = -N(\mu - \bar{\mu})$$

für die Diskriminante von $Q(z)$.

3. Für den vollen Ring M existiert (abstrakt, ohne Deutung als Meromorphismen von k) der durch Erweiterung des Teilrings Γ zum Quotientenkörper P entstehende Quotientenring Σ. Da Σ nullteilerfrei ist, ist jedes Teilsystem endlichen Ranges über P eine Divisionsalgebra über P. Nach dem Bewiesenen sind ferner sämtliche nicht zu P gehörigen Elemente aus Σ imaginär-quadratisch über P. Aus dem bekannten Satz über die einzigen Divisionsalgebren vom Grade 2 über Σ ergibt sich also, daß für P nur folgende Möglichkeiten bestehen:

I. Σ *ist der rationale Zahlkörper* P.

II. Σ *ist ein imaginär-quadratischer Zahlkörper über* P, *also* $\Sigma = \mathsf{P}(\delta)$ *mit* $\delta^2 = d < 0$ *in* P.

III. Σ *ist eine imaginär-quadratische Divisionsalgebra über* P, *also* $\Sigma = \mathsf{P}(\delta, \delta')$ *mit* $\delta^2 = d < 0$, $\delta'^2 = d' < 0$ *in* P *und* $\delta\delta' = -\delta'\delta$.

M *selbst ist dann ein Integritätsbereich in* Σ, *der nur aus ganzalgebraischen Elementen besteht und den ganzrationalen Integritätsbereich* Γ *enthält, also eine Ordnung in* Σ.

§ 3. Der Fall eines absolut-algebraischen Konstantenkörpers von Primzahlcharakteristik p.

Sei von jetzt an k der absolut-algebraische algebraisch-abgeschlossene Körper der Primzahlcharakteristik p.

1. Ist $K = k(x, y)$ mit $f(x, y) = 0$ eine normierte Erzeugung von K, so liegen die Koeffizienten von $f(x, y)$ sämtlich in einem endlichen Körper k_0. Ist also $q = p^f$ die Elementzahl von k_0, so liefert die Abbildung

$$(x\pi, y\pi) = (x^q, y^q)$$

einen normierten Meromorphismus π von K.

Wegen $K\pi = K^q$ ist

$$N(\pi) = q,\ J(\pi) = q,\ c_\pi = 0\,.$$

Die quadratische Gleichung für π hat daher die Form

$$Q(\pi) = \pi^2 - l\pi + q = 0\,, \qquad l^2 \leqq 4q.$$

[5]) Den Grundgedanken dieses Beweises, der meine ursprüngliche Anwendung des Ostrowskischen Satzes über archimedisch-bewertete Körper ersetzt, verdanke ich Herrn Behrbohm; siehe dessen Note im Anschluß an meine vorläufige Mitteilung in den Göttinger Nachrichten 1935. Die dortige Beweisführung wurde durch Herrn Teichmüller noch etwas durchsichtiger gestaltet, durch Einführung der obigen Regel (6). — Siehe außerdem die Referate von E. Witt in Zbl. **13** (1936), 197—198.

Auch das durch

$$\pi + \bar{\pi} = l$$

definierte konjugierte $\bar{\pi}$ zu π ist ein normierter Meromorphismus von K, da l ein solcher ist. Um $\bar{\pi}$ explizit darzustellen, beachten wir die Relation

$$\bar{\pi}\pi = q,$$

auf Grund deren

$$K > K\pi = K^q > Kq$$

ist; wir wissen dies ja auch schon auf Grund der allgemeinen Tatsache $J(q) = q$ oder q^2. Nach der Definition des Meromorphismenprodukts entsteht dann $\bar{\pi}$ so: Man nehme die durch

$$(x\pi, y\pi) = (x^q, y^q) \to (xq, yq)$$

gelieferte isomorphe Abbildung von $K\pi = K^q$ auf Kq und leite aus ihr durch rückwärtige Anwendung von π eine isomorphe Abbildung $\bar{\pi}$ von K auf einen Teilkörper $K\bar{\pi}$ her; das ergibt

$$(x\bar{\pi}, y\bar{\pi}) = \left((xq)^{q^{-1}}, (yq)^{q^{-1}}\right),$$

insbesondere $K\bar{\pi} = (Kq)^{q^{-1}}$. Der Produktrelation

$$\pi\bar{\pi} = q$$

in der anderen Reihenfolge entspricht ebenso die Körperkette

$$K > K\bar{\pi} = (Kq)^{q^{-1}} > Kq\,.$$

Aus dem früheren allgemeinen Ergebnis

$$J(q) = \begin{Bmatrix} q & \text{für } A \neq 0 \\ q^2 & \text{für } A = 0 \end{Bmatrix}$$

folgt wegen $J(\pi) = q$, daß

$$J(\bar{\pi}) = \begin{Bmatrix} 1 & \text{für } A \neq 0 \\ q & \text{für } A = 0 \end{Bmatrix}$$

und entsprechend

$$c_{\bar{\pi}} \begin{Bmatrix} \neq 0 & \text{für } A \neq 0 \\ = 0 & \text{für } A = 0 \end{Bmatrix}$$

ist.

2. Es ist von Interesse, das Auftreten der Grenzfälle

a) $\bar{\pi} = \pi$, d. h. $l^2 = 4q$, $l = \pm 2\sqrt{q}$, $\pi = \pm\sqrt{q}$, $\pi^2 = q$

b) $\bar{\pi} = -\pi$, d. h. $l^2 = 0, l = 0, \pi^2 = -q$

näher zu verfolgen; im Falle a) muß natürlich das f in $q = p^f$ gerade sein.

In beiden Fällen ist wegen $l \equiv 0$ mod. p

$$c_{\bar{\pi}} = c_l - c_\pi = 0\,.$$

Daraus folgt

$$J(\bar{\pi}) \neq 1, \text{ also } J(\bar{\pi}) = q, \text{ und daher } A = 0.$$

Sei umgekehrt $A = 0$. Dann ist $J(q) = q^2$, also $Kq = K^{q^2}$.

Da auch $K\pi^2 = K^{q^2}$ ist, folgt

$$\pi^2 = q\zeta\,,$$

wo ζ ein normierter Automorphismus von K ist. Als Einheit in $\mathsf{P}(\pi)$ ist ζ notwendig eine 2-te, 4-te oder 6-te Einheitswurzel. Wäre aber $\zeta \neq \pm 1$, so wäre π von höherem als zweiten Grade über P. Es folgt also sogar

$$\pi^2 = \pm q\,,$$

d. h. das Vorliegen eines der obigen beiden Grenzfälle a) oder b).

Wir haben damit bewiesen:

Die Grenzfälle a) *oder* b) *treten dann und nur dann auf, wenn* $A = 0$ *ist. Für* $A \neq 0$ *ist* $0 < l^2 < 4q$.

3. Vom Grenzfall a) abgesehen ist der Körper $\mathsf{P}(\pi) > \mathsf{P}$, also ein echter imaginär-quadratischer Zahlkörper. Wir können dann zeigen, daß das volle System $\Sigma = \mathsf{P}(\pi)$ ist. Da nämlich π ersichtlich mit allen normierten Meromorphismen μ vertauschbar ist, ist für jeden solchen das System $\mathsf{P}(\pi, \mu)$ kommutativ; wegen des Grades ist also $\mathsf{P}(\pi, \mu) = \mathsf{P}(\mu)$.

Damit ist bewiesen:

Ist k absolut-algebraisch und $\bar{\pi} \neq \pi$, so ist der Meromorphismenring M *eine Ordnung eines imaginär-quadratischen Zahlkörpers, und zwar eines solchen, in dem p in zwei (verschiedene oder gleiche) Primideale zerfällt.*

Insbesondere ist dann die in H II, § 1 untersuchte Automorphismengruppe $\mathfrak{A}_0$ im allgemeinen zyklisch von der Ordnung 2, erzeugt durch die Spiegelung $\sigma_0 = -1$; nur wenn speziell M die Hauptordnung zur Diskriminante -4 oder -3 ist, ist $\mathfrak{A}_0$ umfassender, nämlich zyklisch von der Ordnung 4 oder 6, erzeugt durch eine 4-te oder 6-te Einheitswurzel ζ in M.

Hiernach bleibt die Frage nach der Struktur des Meromorphismenringes M nur in dem Falle offen, daß bei jeder möglichen Wahl der normierten Erzeugung $K = k(x, y)$ mit $f(x, y) = 0$ und darauf gegründeten Definition von π (mit kleinstmöglichem q) der Grenzfall a) vorliegt, d. h. $\bar{\pi} = \pi$ und somit $\mathsf{P}(\pi) = \mathsf{P}$ ist. Es wäre interessant, allgemein zu entscheiden, von welchem der drei Typen I, II, III der Meromorphismenring M in diesem Falle ist. Das Beispiel $p = 3$, $q = 3^2$, $y^2 = x^3 - 2x - 1$ lehrt jedenfalls, daß der Typus III wirklich vorkommt.

§ 4. Die Riemannsche Vermutung.

1. Der Körper $K_0 = k_0(x, y)$ ist ein algebraischer Funktionenkörper vom Geschlecht 1 über k als Konstantenkörper; denn die Grundgleichung $f(x, y) = 0$ hat Koeffizienten in k_0 und bleibt in der algebraisch-abgeschlossenen Hülle k von k_0 irreduzibel. Die Zetafunktion von K_0 reduziert sich nach Wegdivision der Zetafunktion zum Geschlecht 0 über k_0 auf die Funktion

$$L(s) = 1 - \frac{(q + 1 - N_1)}{q^s} + \frac{q}{q^{2s}}\,,$$

wo N_1 die Anzahl der Primdivisoren ersten Grades von K_0 bezeichnet [6]). Wir setzen $z = q^s$ und

[6]) Siehe dazu H. Hasse, Über die Kongruenzzetafunktionen, Sitz. Ber. Berlin 1934.

$$q^{2s} L(s) = P(z) = z^2 - (q + 1 - N_1) z + q\,.$$

Nach der allgemeinen Theorie der Zetafunktion ist

$$h = L(0) = P(1) = N_1$$

die Klassenzahl (Anzahl der Divisorenklassen nullten Grades) von K_0. Daß hier (für Geschlecht 1) speziell $h = N_1$ ist, sieht man auch direkt daraus, daß nach dem Riemann-Rochschen Satz die h Divisorenklassen nullten Grades von K_0 eindeutig durch die Quotienten $\frac{\mathfrak{p}}{\mathfrak{o}}$ aller N_1 Primdivisoren ersten Grades durch den festen Nennerprimdivisor $\mathfrak{o}$ von x, y repräsentiert sind.

2. Die Nullstellen von $L(s)$ in s entsprechen vermöge $z = q^s$ den beiden Nullstellen des quadratischen Polynoms $P(z)$ in z, und die *Riemannsche Vermutung* für $L(s)$ besagt, daß die beiden Nullstellen von $P(z)$ den absoluten Betrag $q^{\frac{1}{2}}$ haben, d. h. daß sie konjugiert-komplex (im Grenzfall reell und gleich) sind, oder also auch daß

$$(q + 1 - N_1)^2 \leqq 4q$$

ist.

Wir werden dies dadurch beweisen, daß wir die Identität von $P(z)$ mit dem durch π annullierten quadratischen Polynom

$$Q(z) = z^2 - lz + q$$

beweisen, für das wir ja die entsprechende Aussage über die Nullstellen $\pi, \bar{\pi}$ oder also die Ungleichung

$$l^2 \leqq 4q$$

wissen. Explizit läuft dieser Identitätsnachweis auf die Feststellung der Übereinstimmung

$$l = q + 1 - N_1$$

der beiden allein noch in Betracht zu ziehenden Koeffizienten von z hinaus. Der tiefere Grund für diese Übereinstimmung kommt aber besser heraus, wenn wir den Schluß so einkleiden: Es genügt, das Übereinstimmen von $P(z)$ und $Q(z)$ für irgendeinen Wert $z \neq 0, \infty$ festzustellen. Wir nehmen $z = 1$ (also $s = 0$).

Einerseits ist, wie schon gesagt

$$P(1) = h\,.$$

Andererseits ist

$$Q(z) = (\pi - z)(\bar{\pi} - z),$$

also

$$Q(1) = N(\pi - 1)\,.$$

Der Beweis der Riemannschen Vermutung läuft also auf die Feststellung

$$N(\pi - 1) = h$$

hinaus.

3. Der Beweis dieser Tatsache kann auf Grund unserer Theorie sehr einfach und durchsichtig erbracht werden.

Einerseits ist

$$c_{\pi-1} = c_\pi - 1 = 0 - 1 \neq 0,$$

also

$$J(\pi - 1) = 1\,,$$

und daher

$$N(\pi - 1) = N_0(\pi - 1)$$

die Anzahl der Lösungen der Gleichung

$$(\pi - 1)\,\mathfrak{p} = \mathfrak{o}$$

in der Gruppe D_0.

Andererseits ist $h = N_1$ die Anzahl derjenigen Primdivisoren $\mathfrak{p}$ von K, die bereits Primdivisoren ersten Grades von K_0 sind. Dies ist für den Bezugsprimdivisor $\mathfrak{o}$ nach der Konstruktion von K_0 der Fall. Für ein $\mathfrak{p} \neq \mathfrak{o}$ mit

$$(x\mathfrak{p},\, y\mathfrak{p}) = (a, b)$$

bedeutet es, daß die Elemente a, b aus k bereits in k_0 liegen, oder also

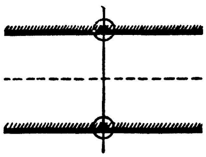
$$(a^q,\, b^q) = (a, b)$$

erfüllen. Diese Bedingung ist aber auf Grund der Definition des Meromorphismus π und nach früher entwickelten Regeln der Reihe nach gleichbedeutend mit

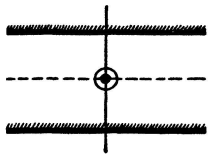
$$\begin{aligned} ((x\mathfrak{p})^q,\, (y\mathfrak{p})^q) &= (x\mathfrak{p},\, y\mathfrak{p})\,, \\ ((x\pi)\,\mathfrak{p},\, (y\pi)\,\mathfrak{p}) &= (x\mathfrak{p},\, y\mathfrak{p})\,, \\ (x(\pi\mathfrak{p}),\, y(\pi\mathfrak{p})) &= (x\mathfrak{p},\, y\mathfrak{p})\,, \\ \pi\mathfrak{p} &= \mathfrak{p}\,, \\ (\pi - 1)\,\mathfrak{p} &= \mathfrak{o}\,. \end{aligned}$$

Daher ist auch h gleich der Anzahl der Lösungen dieser Gleichung in der Gruppe D_0.

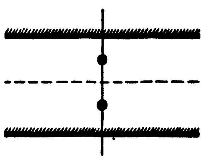
4. Die damit bewiesene Riemannsche Vermutung besagt, daß die beiden konjugierten Meromorphismen π, $\bar{\pi}$ formal als die Nullstellen von $L(s)$ (in $z = q^s$) angesehen



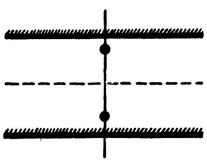
Grenzfall a) mit $\bar{\pi} = \pi = +\sqrt{q}$.



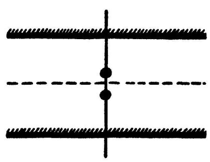
Grenzfall a) mit $\bar{\pi} = \pi = -\sqrt{q}$.



Grenzfall b), $\bar{\pi} = -\pi$.



Allgemeiner Fall
mit $2\sqrt{q} > \pi + \bar{\pi} > 0$.



Allgemeiner Fall
mit $-2\sqrt{q} < \pi + \bar{\pi} < 0$.

werden können. Da die Relation $P(\pi) = 0$ mit dem Bestehen der Identität

$$P(\pi)\mathfrak{p} = \pi^2\mathfrak{p} - (q + 1 - N_1)\pi\mathfrak{p} + q\mathfrak{p} = \mathfrak{o}$$

in der Divisorenklassengruppe D_0 von K gleichbedeutend ist, kann die Riemannsche Vermutung auch in der folgenden merkwürdigen Form ausgesprochen werden:

Ersetzt man in dem $L(s)$ zugrundeliegenden Polynom $P(z)$ die Variable $z = q^s$ durch den Operator π, so entsteht ein Nulloperator $P(\pi)$ der Divisorenklassengruppe D_0 von K.

5. Insbesondere entsprechen den in § 3 hervorgehobenen Grenzfällen a), b) die aus den ersten drei der vorstehenden Figuren ersichtlichen speziellen Lagen der Nullstellen von $L(s)$ im Periodenstreifen $0 \leqq \mathfrak{I}(s) < \frac{2\pi i}{\log q}$ der s-Ebene auf der Geraden $\mathfrak{R}(s) = \frac{1}{2}$, während die vierte und fünfte Figur die Lage im allgemeinen Fall veranschaulichen. Dabei deutet ● eine einfache Nullstelle, ⊙ eine zweifache Nullstelle an.

Wir sind damit am Ziel unserer Untersuchung angelangt.

Göttingen, den 22. November 1935.