Analytische Zahlentheorie in Körpern der Charakteristik p.

Von

Friedrich Karl Schmidt in Erlangen.

Einleitung.

Die Dedekindsche Theorie der höheren Kongruenzen ist bekanntlich von Herrn E. Artin in zwei Arbeiten weiter fortgeführt worden[1]). Herr Artin adjungiert eine Quadratwurzel zum Körper $k(z)$ aller rationalen Funktionen in z mit Koeffizienten modulo einer Primzahl p_0 und entwickelt die Zahlentheorie aller in z ganzen Elemente des entstehenden Erweiterungskörpers. Auf diese Weise ergibt sich eine Idealtheorie, eine Theorie der Einheiten und eine analytische Theorie, deren Ergebnisse weitgehend mit den bekannten Verhältnissen bei den ganzen algebraischen Zahlen übereinstimmen. Hinsichtlich der verwendeten Methoden besteht jedoch ein bemerkenswerter Unterschied. Die Sätze über Ideale und Einheiten können allerdings durch Schlüsse gewonnen werden, die den üblichen nachgebildet sind, und sie gelten daher auch dann noch, wenn man an Stelle der quadratischen eine beliebige endliche Erweiterung von $k(z)$ zugrunde legt[2]). Dagegen stößt die Übertragung der gebräuchlichen analytischen Methoden zunächst auf Schwierigkeit, so daß Herr Artin die grundlegenden Sätze über die Zetafunktion in seinem quadratischen Fall durch spezielle Rechnungen herleiten mußte, die bei höheren Erweiterungen undurchführbar sind.

Die vorliegende Arbeit steckt sich daher das Ziel, die analytische Theorie für eine beliebige endliche Erweiterung K von $k(z)$ mit einfachen allgemeinen Hilfsmitteln zu begründen. Bei der Durchführung dieser Aufgabe sind zwei Gesichtspunkte wesentlich.

---

[1]) E. Artin, Quadratische Körper im Gebiet der höheren Kongruenzen I. u. II., Math. Zeitschr. **19** (1924), S. 153—206 u. S. 207—246.

[2]) Vgl. P. Sengenhorst, Körper von der Charakteristik p, Math. Zeitschr. **24** (1925), S. 1—39. Zitiert mit *S.* — F. K. Schmidt, Allgemeine Körper im Gebiet der höheren Kongruenzen, Diss. Freiburg i. B. 1925. Zitiert mit *D.*

Einmal nehmen wir gegenüber dem Körper K die Stellung ein, die in der Theorie der algebraischen Funktionen üblich ist[3]). Wir betrachten also K ganz unabhängig von seiner Entstehung und billigen keinem Element von K eine ausgezeichnete Rolle zu. Es wird daher auch keiner der unendlich vielen Integritätsbereiche von K bevorzugt, vielmehr rücken überall die körperinvarianten Begriffe in den Vordergrund. So tritt an Stelle des Ideals der Divisor, an Stelle der Idealklassengruppe die Divisorenklassengruppe. Insbesondere ersetzen wir die von Herrn Artin eingeführte Zetafunktion, die sich auf die Primideale eines Integritätsbereichs stützt, durch eine neue körperinvariante Funktion, deren Definition in analoger Weise die Primdivisoren von K benutzt und die zur Zetafunktion des Herrn Artin in einer leicht angebbaren Beziehung steht.

Der Vorteil dieser Auffassung zeigt sich darin, daß nun die Hauptsätze der analytischen Theorie eine einfache und einheitliche Gestalt annehmen und einheitlich begründet werden können, während Herr Artin bei Formulierung und Beweis seiner Sätze verschiedene Fallunterscheidungen machen mußte. Als wichtigstes Beweismittel erscheint dabei ein Satz, der die Übertragung des bekannten Riemann-Rocheschen Satzes der algebraischen Funktionentheorie darstellt und den wir deshalb kurz als Riemann-Rocheschen Satz bezeichnen.

Die zweite Bemerkung, die wir im folgenden auswerten, besteht darin, daß die Theorie des Körpers K im wesentlichen ungeändert bleibt, wenn man den Koeffizientenkörper k durch eine endliche Erweiterung $\bar{k}$ ersetzt. Hiervon machen wir Gebrauch, indem wir uns zunächst durch geeignete Erweiterung von k Vereinfachungen schaffen und dann auf den ursprünglichen Körper zurückschließen. Auf diese Weise lassen sich leicht die Schwierigkeiten umgehen, die gegenüber der algebraischen Funktionentheorie daraus entstehen, daß k nicht algebraisch abgeschlossen ist. Der grundlegende Nachweis, daß K Divisoren jeder Ordnung enthält, beruht vornehmlich auf dieser Überlegung.

Die Darstellung der Arbeit gliedert sich dem Gedankengange gemäß in zwei Teile. Im ersten Teil wird die Theorie der Divisoren von K bis zum Riemann-Rocheschen Satz entwickelt. Die dabei benutzten Methoden schließen sich denen der algebraischen Funktionentheorie an, so daß es genügt, kurz die Abweichungen in den Definitionen und in der Beweisführung anzugeben. Nur der Nachweis der Invarianz des Geschlechts er-

[3]) Vgl. R. Dedekind u. H. Weber, Theorie der algebraischen Funktionen einer Veränderlichen, Journal f. d. r. u. a. Math. **92** (1882), S. 181—290. Im folgenden mit *D.-W.* zitiert. — K. Hensel u. G. Landsberg, Theorie der algebraischen Funktionen einer Variablen und ihre Anwendung auf algebraische Kurven und Abelsche Integrale. Leipzig 1902. Zitiert mit *H.-L.*

fordert in § 5 weitergehende Überlegungen, da das übliche Differentiationsverfahren in Körpern von Primzahlcharakteristik[4]) nicht zum Ziele führt. Ein wenig ausführlicher muß ferner auch auf die Herleitung des Riemann-Rocheschen Satzes eingegangen werden; denn weder das bei *D.-W.* noch das bei *H.-L.* in der algebraischen Funktionentheorie eingeschlagene Verfahren läßt sich unmittelbar übertragen[5]).

Der zweite Teil bringt die Wendung zu Sätzen, die in der Zahlentheorie ihr Analogon haben; doch sind seine Methoden von denen der Zahlentheorie durchaus verschieden. Er beginnt mit der Behandlung der unendlichen Divisorenklassengruppe. Aus dem Riemann-Rocheschen Satz wird gefolgert, daß nur endlich viele Divisorenklassen der Ordnung 0 existieren und daß fast alle[6]) Untergruppen der Divisorenklassengruppe endlichen Index haben. Mit Hilfe des Riemann-Rocheschen Satzes läßt sich dann weiter die neu eingeführte Zetafunktion summieren und die so gewonnene Formel ermöglicht einmal die Residuenbestimmung, während andererseits abermalige Anwendung des Riemann-Rocheschen Satzes zur Funktionalgleichung führt. Zum Schluß werden die gewonnenen Ergebnisse für die von Herrn Artin betrachtete Zetafunktion nutzbar gemacht, wobei sich gelegentlich der Untersuchung des Zusammenhangs zwischen Divisoren- und Idealklassengruppe als Nebenresultat die Endlichkeit der Idealklassenzahl ergibt, die also bei unseren Überlegungen vorher nirgends vorkam[7]).

Die bekannten, häufig gebrauchten Tatsachen der Körper- und Idealtheorie sowie die einfachsten algebraischen Eigenschaften des Körpers K werden in zwei kurzen Paragraphen der eigentlichen Theorie vorangestellt, damit wir uns später ohne Weitläufigkeit darauf berufen können.

---

[4]) Zu den benutzten Begriffen und Sätzen der allgemeinen Körpertheorie vgl. E. Steinitz, Algebraische Theorie der Körper, Journ. f. d. r. u. a. Math. **137** (1910), S. 167—309.

[5]) *D.-W.* machen wesentlich davon Gebrauch, daß der in der algebraischen Funktionentheorie auftretende Koeffizientenkörper unendlich viele Elemente enthält; bei *H.-L.* wird dagegen die im allgemeinen nach gebrochenen Potenzen fortschreitende Potenzreihenentwicklung zum Ausgangspunkt genommen, die in Körpern der Charakteristik p_0 selbst bei algebraisch abgeschlossenem Koeffizientenkörper ihre Gültigkeit verliert, sobald das definierende Polynom über dem Körper aller nach ganzen Potenzen fortschreitenden Potenzreihen einen irreduziblen Faktor erster Art [4]) mit durch p_0 teilbarem Grad abspaltet. — Die in § 6 gegebene Beweisanordnung vereinigt Ansätze von *D.-W.* und *H.-L.*

[6]) D. h. alle mit nur endlich vielen Ausnahmen.

[7]) Auch der Fundamentalsatz aus der Theorie der Einheiten wird unserer ganzen Auffassung gemäß selbstverständlich nirgends benötigt. Er kann jedoch ebenso wie die Endlichkeit der Idealklassenzahl aus der Tatsache gefolgert werden, daß die Zahl aller Divisorenklassen der Ordnung 0 endlich ist. Hiervon gilt aber auch die Umkehrung, d. h. diese letzte Tatsache läßt sich auch mit Hilfe des Einheitensatzes und der Endlichkeit der Idealklassenzahl beweisen.

§ 1.

Zusammenstellung bekannter Tatsachen aus der Körper- und Idealtheorie.

1. Ist der Körper $\mathfrak{L}$ endliche Erweiterung des Unterkörpers $\mathfrak{K}$, $m=(\mathfrak{L}:\mathfrak{K})$ der Grad von $\mathfrak{L}$ bezüglich $\mathfrak{K}$ und $\beta_1, \ldots, \beta_m$ eine Basis von $\mathfrak{L}$ bezüglich $\mathfrak{K}$, so ordnet man einem Element α aus $\mathfrak{L}$ mit Hilfe der m Gleichungen

$$\alpha\beta_i = c_{i1}\beta_1 + \ldots + c_{im}\beta_m$$

die Matrix

$$C = \begin{pmatrix} c_{11} & \cdots & c_{1m} \\ \cdot & \cdots & \cdot \\ c_{m1} & \cdots & c_{mm} \end{pmatrix}$$

zu, deren Elemente c_{ij} aus $\mathfrak{K}$ stammen. Die charakteristische Funktion

$$F(x) = x^m + b_1 x^{m-1} + \ldots + b_m = |x\mathfrak{E} - C|$$

dieser Matrix ist von der besonderen Wahl der Basis $\beta_1, \ldots, \beta_m$ ganz unabhängig, also durch α, $\mathfrak{L}$ und $\mathfrak{K}$ eindeutig bestimmt und heißt die charakteristische Funktion des Elementes α aus $\mathfrak{L}$ bezüglich $\mathfrak{K}$. Die charakteristische Funktion $F(x)$ von α ist gleich einer Potenz des bezüglich $\mathfrak{K}$ irreduziblen Polynoms

$$P(x) = x^n + a_1 x^{n-1} + \ldots + a_n,$$

dessen Nullstelle α ist. Mit Hilfe der charakteristischen Funktion definiert man in bekannter Weise Norm $N(\alpha)$ und Spur $S(\alpha)$ des Elementes α von $\mathfrak{L}$ bezüglich $\mathfrak{K}$, und zwar setzt man

$$N(\alpha) = (-1)^m b_m = \begin{vmatrix} c_{11} & \cdots & c_{1m} \\ \cdot & \cdots & \cdot \\ c_{m1} & \cdots & c_{mm} \end{vmatrix}, \quad S(\alpha) = -b_1 = c_{11} + \ldots + c_{mm}.$$

Ist endlich $\gamma_1, \ldots, \gamma_m$ irgendein System von m Elementen aus $\mathfrak{L}$, so erklärt man die Diskriminante $\Delta(\gamma_1, \ldots, \gamma_m)$ dieses Elementesystems aus $\mathfrak{L}$ bezüglich $\mathfrak{K}$ durch die Gleichungen

$$\Delta(\gamma_1, \ldots, \gamma_m) = \begin{vmatrix} S(\gamma_1\gamma_1) & \ldots & S(\gamma_1\gamma_m) \\ \cdot & \cdots & \cdot \\ S(\gamma_m\gamma_1) & \ldots & S(\gamma_m\gamma_m) \end{vmatrix}.$$

Ist $\mathfrak{L}$ von zweiter Art bezüglich $\mathfrak{K}$, so ist die Diskriminante jedes Systems von m Elementen aus $\mathfrak{L}$ bezüglich $\mathfrak{K}$ gleich 0. Ist dagegen $\mathfrak{L}$ von erster Art bezüglich $\mathfrak{K}$, so ist $\Delta(\gamma_1, \ldots, \gamma_m)$ dann und nur dann von 0 verschieden, wenn $\gamma_1, \ldots, \gamma_m$ eine Basis von $\mathfrak{L}$ bezüglich $\mathfrak{K}$ bilden.

2. Unter einem Ring verstehen wir in dieser Arbeit stets einen kommutativen Ring $\mathfrak{R}$ ohne Nullteiler und mit Einselement der Multiplikation (also einen Integritätsbereich). Wir sagen, es sei $\mathfrak{R}$ ein Ring des Körpers $\mathfrak{K}$, falls alle Elemente von $\mathfrak{R}$ aus $\mathfrak{K}$ stammen und der Quotientenkörper von $\mathfrak{R}$ gleich $\mathfrak{K}$ ist, $\mathfrak{K} = Q(\mathfrak{R})$.

Für die Ideale eines Ringes $\mathfrak{R}$ verwenden wir die üblichen Definitionen[8]). Den Durchschnitt $\mathfrak{c}$ aller Ideale, die ein gegebenes System Σ von Elementen aus $\mathfrak{R}$ enthalten, bezeichnen wir als das aus Σ in $\mathfrak{R}$ abgeleitete Ideal. Ist $\mathfrak{S}$ ein Ring, der $\mathfrak{R}$ umfaßt, $\mathfrak{a}_{\mathfrak{R}}$ bzw. $\mathfrak{a}_{\mathfrak{S}}$ ein Ideal aus $\mathfrak{R}$ bzw. $\mathfrak{S}$, so nennen wir das aus $\mathfrak{a}_{\mathfrak{R}}$ in $\mathfrak{S}$ abgeleitete Ideal $\mathfrak{S} \cdot \mathfrak{a}_{\mathfrak{R}}$ das Erweiterungsideal von $\mathfrak{a}_{\mathfrak{R}}$ bezüglich $\mathfrak{S}$, das Ideal $\mathfrak{a}_{\mathfrak{S}} \cap \mathfrak{R}$ von $\mathfrak{R}$ das Verengungsideal von $\mathfrak{a}_{\mathfrak{S}}$ bezüglich $\mathfrak{R}$. Jedes Element γ aus $\mathfrak{S}$, das einer Gleichung $\gamma^s + c_1 \gamma^{s-1} + \ldots + c_s = 0$ mit Koeffizienten aus $\mathfrak{R}$ genügt, heißt ganz abhängig von $\mathfrak{R}$. Ist jedes von $\mathfrak{R}$ ganz abhängige Element aus $\mathfrak{S}$ bereits in $\mathfrak{R}$ enthalten, so sagt man, $\mathfrak{R}$ sei ganz abgeschlossen in $\mathfrak{S}$.

Im folgenden haben wir es ausschließlich mit sogenannten Multiplikationsringen zu tun, d. h. mit Ringen, in denen jedes Ideal als Potenzprodukt endlich vieler Primideale darstellbar ist. Die Idealtheorie dieser Ringe stimmt also mit der der ganzen algebraischen Zahlen eines endlichen Zahlkörpers überein und wir heben nur kurz einige häufig gebrauchte, allgemein gültige Tatsachen hervor.

3. Ein Multiplikationsring $\mathfrak{R}$ ist stets ganz abgeschlossen in seinem Quotientenkörper. Ist $\mathfrak{a}$ ein Ideal aus $\mathfrak{R}$, so verstehen wir unter $\mathfrak{R}_{\mathfrak{a}}$ den Ring aller Quotienten zweier Elemente aus $\mathfrak{R}$, bei denen das Nennerelement zu $\mathfrak{a}$ prim ist[9]). Der Ring $\mathfrak{R}_{\mathfrak{a}}$ ist ein Hauptidealring (also gewiß auch Multiplikationsring) und es stimmen die Ideale von $\mathfrak{R}_{\mathfrak{a}}$ mit den Erweiterungsidealen $\mathfrak{R}_{\mathfrak{a}} \cdot \mathfrak{c}$ derjenigen Ideale $\mathfrak{c}$ von $\mathfrak{R}$ überein, deren Primidealteiler sämtlich in $\mathfrak{a}$ aufgehen. Ist $\mathfrak{c}$ ein derartiges Ideal aus $\mathfrak{R}$, so gilt die reziproke Gleichung $\mathfrak{R}_{\mathfrak{a}} \cdot \mathfrak{c} \cap \mathfrak{R} = \mathfrak{c}$ und die Restklassenringe $\mathfrak{R}/\mathfrak{c}$ bzw. $\mathfrak{R}_{\mathfrak{a}}/\mathfrak{R}_{\mathfrak{a}} \cdot \mathfrak{c}$, die aus $\mathfrak{R}$ bzw. $\mathfrak{R}_{\mathfrak{a}}$ bei Zugrundelegung der Kongruenz nach $\mathfrak{c}$ bzw. $\mathfrak{R}_{\mathfrak{a}} \cdot \mathfrak{c}$ als Gleichheit hervorgehen, sind isomorph. Aus dem Gesagten ergibt sich: Ist $\mathfrak{a} = \mathfrak{p}$ ein Primideal von $\mathfrak{R}$, so gestattet jedes Element α von $\mathfrak{R}_{\mathfrak{p}}$ eine Darstellung $\alpha = \varepsilon \pi^{\nu}$, wo ε eine Einheit von $\mathfrak{R}_{\mathfrak{p}}$ und π eine Basis des Primideals $\mathfrak{R}_{\mathfrak{p}} \cdot \mathfrak{p}$ ist; der Ring $\mathfrak{R}_{\mathfrak{p}}$ ist also maximaler Integritätsbereich, d. h. es gibt keinen Zwischenring zwischen ihm und seinem Quotientenkörper.

---

[8]) Zu den Grundbegriffen der Ring- und Idealtheorie vgl. E. Noether, Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern. Math. Annalen **96** (1926), S. 26—61.

[9]) Zur Theorie der Quotientenringe vgl. H. Grell, Zur Theorie der Ordnungen in algebraischen Zahl- und Funktionenkörpern, Math. Annalen **97** (1926), S. 524—558, § 2.

4. Es sei der Multiplikationsring $\mathfrak{S}$ Oberring des Multiplikationsringes $\mathfrak{R}$ und $\mathfrak{S}$ endlicher $\mathfrak{R}$-Modul. Dann ist auch jedes Ideal $\mathfrak{c}$ aus $\mathfrak{S}$ endlicher $\mathfrak{R}$-Modul; es ist ferner der Quotientenkörper $\mathfrak{L} = Q(\mathfrak{S})$ von $\mathfrak{S}$ endlich bezüglich des Quotientenkörpers $\mathfrak{k} = Q(\mathfrak{R})$ und die charakteristische Funktion eines Elementes α aus $\mathfrak{L}$ bezüglich $\mathfrak{k}$ besitzt dann und nur dann Koeffizienten aus $\mathfrak{R}$, wenn α zu $\mathfrak{S}$ gehört. $\mathfrak{S}$ besteht also aus allen von $\mathfrak{R}$ ganz abhängigen Elementen des Körpers $\mathfrak{L}$. Ist $\mathfrak{a}$ ein Ideal aus $\mathfrak{R}$, so ist auch $\mathfrak{S}_{\mathfrak{S}\cdot\mathfrak{a}}$ endliche $\mathfrak{R}_{\mathfrak{a}}$-Ordnung. Unter dem Grad f eines Primideals $\mathfrak{P}$ aus $\mathfrak{S}$ verstehen wir den Grad des Restklassenkörpers $\mathfrak{S}/\mathfrak{P}$ bezüglich des Unterkörpers $\mathfrak{R}/\mathfrak{R}\cap\mathfrak{P}$. Gilt für das Primideal $\mathfrak{p}$ von $\mathfrak{R}$ in $\mathfrak{S}$ die Zerlegung $\mathfrak{S}\cdot\mathfrak{p} = \mathfrak{P}_1^{e_1}\cdot\ldots\cdot\mathfrak{P}_s^{e_s}$, wo $\mathfrak{P}_i$ den Grad f_i bezüglich $\mathfrak{R}$ hat und $m = (\mathfrak{L}:\mathfrak{k})$ ist, so ist $m = e_1 f_1 + \ldots + e_s f_s$.

5. Um die Norm[10]) eines Ideals $\mathfrak{A}$ von $\mathfrak{S}$ zu erklären, nehme man zunächst an, daß der Unterring $\mathfrak{R}$ Hauptidealring ist. Dann besitzt jedes Ideal aus $\mathfrak{S}$, also auch $\mathfrak{S}$, eine Modulbasis bezüglich $\mathfrak{R}$, die aus $m = (\mathfrak{L}:\mathfrak{k})$ in bezug auf $\mathfrak{k}$ linear unabhängigen Elementen besteht. Ist $\alpha_1, \ldots, \alpha_m$ bzw. $\sigma_1, \ldots, \sigma_m$ eine solche Basis für das Ideal $\mathfrak{A}$ bzw. für $\mathfrak{S}$ und sind

$$\alpha_i = c_{i1}\sigma_1 + \ldots + c_{im}\sigma_m$$

die m Gleichungen, die $\alpha_1, \ldots, \alpha_m$ durch $\sigma_1, \ldots, \sigma_m$ ausdrücken, so heißt das aus der Determinante der c_{ik} in $\mathfrak{R}$ abgeleitete Ideal die Norm von $\mathfrak{A}$ bezüglich $\mathfrak{R}$. Die Definition der Norm in dem allgemeinen Falle, wo $\mathfrak{R}$ Multiplikationsring ist, wird mit Hilfe der Quotientenringe auf die des Hauptidealrings zurückgeführt. Ist $\mathfrak{b} = \mathfrak{A}\cap\mathfrak{R}$ das Verengungsideal von $\mathfrak{A}$ bezüglich $\mathfrak{R}$, so ist die Norm von $\mathfrak{S}_{\mathfrak{S}\cdot\mathfrak{b}}\cdot\mathfrak{A}$ bezüglich des Hauptidealringes $\mathfrak{R}_{\mathfrak{b}}$ als Ideal von $\mathfrak{R}_{\mathfrak{b}}$ erklärt. Das Verengungsideal dieses Ideals bezüglich $\mathfrak{R}$ ist die Norm von $\mathfrak{A}$ bezüglich $\mathfrak{R}$. Die Norm eines Primideals $\mathfrak{P}$ von $\mathfrak{S}$ ist gleich der f-ten Potenz des durch $\mathfrak{P}$ teilbaren Primideals $\mathfrak{p} = \mathfrak{P}\cap\mathfrak{R}$ von $\mathfrak{R}$, wenn f der Grad von $\mathfrak{P}$ bezüglich $\mathfrak{R}$ ist; es ist ferner die Norm eines Produktes von Idealen gleich dem Produkt der Normen.

6. Im folgenden setzen wir voraus, daß $\mathfrak{L}$ ein Körper algebraischer Funktionen in einer Unbestimmten mit vollkommenem Koeffizientenkörper ist. Ist $(\mathfrak{L}:\mathfrak{k}) = m$ und durchlaufen $\sigma_1, \ldots, \sigma_m$ alle Systeme bezüglich $\mathfrak{k}$ linear unabhängiger Elemente aus $\mathfrak{S}$, so heißt das aus den zugehörigen Diskriminanten $\Delta(\sigma_1, \ldots, \sigma_m)$ in $\mathfrak{R}$ abgeleitete Ideal das Diskriminantenideal[11]) von $\mathfrak{S}$ bezüglich $\mathfrak{R}$. Das Diskriminantenideal ist von 0 verschieden,

---

[10]) Zur Theorie der Norm vgl. H. Grell, Zur Theorie der Ordnungen in algebraischen Zahl- und Funktionenkörpern, Math. Annalen **97** (1926), S. 524—558, § 4.

[11]) Zur Theorie der Diskriminante vgl. E. Noether, Der Diskriminantensatz für die Ordnungen eines algebraischen Zahl- oder Funktionenkörpers, Journ. f. d. r. u. a. Math. **157**, S. 82—104.

wenn $\mathfrak{L}$ von erster Art bezüglich $\mathfrak{K}$ ist und ist in diesem Falle durch alle und nur die Primideale $\mathfrak{p}$ von $\mathfrak{R}$ teilbar, deren Erweiterungsideal $\mathfrak{S} \cdot \mathfrak{p}$ in $\mathfrak{S}$ durch das Quadrat eines Primideals teilbar ist. Ist $\mathfrak{R}$ insbesondere Hauptidealring, so bezeichnet man die bis auf eine Einheit bestimmte Basis des Diskriminantenideals als Diskriminante von $\mathfrak{S}$ bezüglich $\mathfrak{R}$.

7. Unter einem gebrochenen Ideal von $\mathfrak{S}$ versteht man eine Menge von Elementen des Quotientenkörpers $\mathfrak{L} = Q(\mathfrak{S})$, die einen endlichen $\mathfrak{S}$-Modul bildet; die Ideale, welche nur Elemente aus $\mathfrak{S}$ enthalten, werden zur Unterscheidung ganze Ideale genannt.

Wir nehmen nun an, daß der Quotientenkörper $\mathfrak{L} = Q(\mathfrak{S})$ von erster Art in bezug auf $\mathfrak{K} = Q(\mathfrak{R})$ sei. Ist dann $\mathfrak{A}$ ein beliebiges Ideal von $\mathfrak{S}$, so bildet die Menge $\mathfrak{A}^*$ aller Elemente α^* aus $\mathfrak{L}$, für die $S(\alpha^* \alpha)$ bei beliebigem α aus $\mathfrak{A}$ stets in $\mathfrak{R}$ liegt, ein gebrochenes Ideal, daß zu $\mathfrak{A}$ bezüglich $\mathfrak{R}$ komplementäre Ideal. Es ist $\mathfrak{A}^* = \frac{1}{\mathfrak{A} \cdot \mathfrak{D}}$, wo $\mathfrak{D}$ ein ganzes, von $\mathfrak{A}$ unabhängiges Ideal aus $\mathfrak{S}$ ist. $\mathfrak{D}$ heißt die Differente[12]) von $\mathfrak{S}$ bezüglich $\mathfrak{R}$ und es ist die Norm von $\mathfrak{D}$ bezüglich $\mathfrak{R}$ gleich der Diskriminante von $\mathfrak{S}$ bezüglich $\mathfrak{R}$.

Ist $\mathfrak{R}$ Hauptidealring und $\alpha_1, \ldots, \alpha_m$ eine linear unabhängige Basis von $\mathfrak{A}$ bezüglich $\mathfrak{R}$, so ist eine Basis $\alpha_1^*, \ldots, \alpha_m^*$ von $\mathfrak{A}^*$ definiert durch die Gleichungen

$$\alpha_i = a_{i1} \alpha_1^* + \ldots + a_{im} \alpha_m^*,$$

wo $a_{ij} = S(\alpha_i \alpha_j)$ ist.

Zwischen Diskriminanten- bzw. Differentenideal ($\mathfrak{d}$ bzw. $\mathfrak{D}$) von $\mathfrak{S}$ bezüglich $\mathfrak{R}$ und den entsprechenden Idealen der Quotientenringe besteht folgender Zusammenhang. Ist $\mathfrak{a}$ ein Ideal aus $\mathfrak{R}$, so ist das Diskriminanten- bzw. Differentenideal von $\mathfrak{S}_{\mathfrak{S} \cdot \mathfrak{a}}$ bezüglich $\mathfrak{R}_{\mathfrak{a}}$ gleich $\mathfrak{S}_{\mathfrak{S} \cdot \mathfrak{a}} \cdot \mathfrak{D}$ bzw. $\mathfrak{R}_{\mathfrak{a}} \cdot \mathfrak{d}$. Das Diskriminanten- bzw. Differentenideal von $\mathfrak{S}_{\mathfrak{S} \cdot \mathfrak{p}}$ bezüglich $\mathfrak{R}_{\mathfrak{p}}$ ist also nur für endlich viele Primideale $\mathfrak{p}$ von $\mathfrak{R}$ vom Einheitsideal verschieden, nämlich für alle und nur die Primideale $\mathfrak{p}$, die im Diskriminantenideal $\mathfrak{d}$ von $\mathfrak{S}$ bezüglich $\mathfrak{R}$ aufgehen.

§ 2.

Der Grundkörper.

1. Den nachstehenden Untersuchungen liegt ein Körper K mit folgenden Eigenschaften zugrunde. Der größte in K enthaltene, absolut algebraische Körper k ist von Primzahlcharakteristik p_0 und K kann aus k durch Adjunktion eines transzendenten Elements z nebst nachfolgender endlich algebraischer Erweiterung erzeugt werden.

---

[12]) Zur Definition der Differente vgl. E. Hecke, Vorlesungen über die Theorie der algebraischen Zahlen, Leipzig 1923, § 36 und 38.

Über die Zahl der Elemente von k wird zunächst nichts vorausgesetzt; ist sie endlich, so ist sie gleich einer Potenz von p_0 und wird durch p wiedergegeben.

Offenbar kann K aufgefaßt werden als Körper algebraischer Funktionen in einer Unbestimmten z mit k als Koeffizientenbereich. Von diesem Standpunkt aus werden wir K betrachten, wobei uns die Analogie mit der Theorie der algebraischen Funktionen einer Veränderlichen und beliebigen Zahlenkoeffizienten zum Leitstern dient.

2. Sind z und ϑ zwei nicht zu k gehörige Elemente aus K, so gibt es stets ein irreduzibles Polynom[13]) $P(x, y)$ in zwei Unbestimmten x und y mit Koeffizienten aus k, das für $x = z$, $y = \vartheta$ zu Null wird, $P(z, \vartheta) = 0$. Da die p_0-te Wurzel aus einem Element von k stets wieder in k enthalten ist[14]), kann $P(x, y)$ wegen der vorausgesetzten Irreduzibilität nicht gleichzeitig Polynom in x^{p_0} und y^{p_0} sein, d. h. es ist eines der beiden Elemente z und ϑ von erster Art in bezug auf den Körper, der aus k durch Adjunktion des andern entsteht.

3. Der Körper K ist endlich in bezug auf jeden Unterkörper K^*, der k und mindesten ein nicht zu k gehöriges Element enthält. Ist z ein derartiges Element und bedeutet $\mathfrak{J}$ den Ring aller Elemente aus K, die von dem Polynombereich $k[z]$ ganz abhängen (kurz: aller in z ganzen Elemente aus K), so ist $\mathfrak{J}$ stets endlicher $k[z]$-Modul[15]). $\mathfrak{J}$ ist Multiplikationsring[16]); ist $\tilde{\mathfrak{p}}$ ein Primideal aus $\mathfrak{J}$, K^* ein beliebiger Unterkörper von K, welcher k umfaßt, so heißt der Grad des Restklassenkörpers $\mathfrak{J}/\tilde{\mathfrak{p}}$ bezüglich $\mathfrak{J} \cap K^*/\tilde{\mathfrak{p}} \cap K^*$ der Grad von $\tilde{\mathfrak{p}}$ bezüglich K^*. Zwischen dem Grad von $\tilde{\mathfrak{p}}$ bezüglich k und der Norm $N(\tilde{\mathfrak{p}})$ von $\tilde{\mathfrak{p}}$ bezüglich $k[z]$ besteht folgender Zusammenhang. Ist q ein Basiselement von $N(\tilde{\mathfrak{p}})$ in $k[z]$, q also Polynom in z, so ist der Grad dieses Polynoms in z gerade gleich dem Grad von $\tilde{\mathfrak{p}}$ bezüglich k.

4. Bedeutet $\overline{K}$ eine Erweiterung von K, die aus K durch Adjunktion eines endlichen oder unendlichen Systems absolut algebraischer Elemente entsteht, und ist $\bar{k}$ der Koeffizientenkörper von $\overline{K}$, so kann der Ring $\overline{\mathfrak{J}}$ aller in z ganzen Elemente von $\overline{K}$ aus $\mathfrak{J}$ durch Ringadjunktion von $\bar{k}$ erzeugt werden, $\overline{\mathfrak{J}} = \mathfrak{J}[\bar{k}]$[17]). Ist $\tilde{\mathfrak{a}}$ ein Ideal von $\mathfrak{J}$, so besteht also das

---

[13]) Das beweist man genau wie in der algebraischen Funktionentheorie, vgl. *D.-W.*, § 13.

[14]) Vgl. loc. cit. [4]).

[15]) Vgl. *D.*, Kap. II.

[16]) Vgl. *D.*, Kap. III, § 1.

[17]) Das schließt man so: Ist $\overline{K}$ endlich in bezug auf K, $(\overline{K}:K) = n$ und $\eta_1, \ldots, \eta_n$ ein System bezüglich k linear unabhängiger Elemente aus $\bar{k}$, so ist jedes Element $\bar{\gamma}$ aus $\overline{\mathfrak{J}}$ sicher in der Form $\bar{\gamma} = x_1\eta_1 + \ldots + x_n\eta_n$ darstellbar, wo die x_i aus K stammen.

(Fortsetzung der Fußnote [17]) auf nächster Seite.)

Erweiterungsideal $\overline{\mathfrak{J}} \cdot \mathfrak{a}$ aus allen verschiedenen Elementen der Gestalt $\alpha_1 \eta_1 + \ldots + \alpha_n \eta_n$, wo $\eta_1, \ldots, \eta_n$ alle endlichen Systeme bezüglich k linear unabhängiger Elemente aus $\bar{k}$ und die α_i sämtliche Elemente aus $\tilde{\mathfrak{a}}$ durchlaufen. Daraus folgt mühelos, daß die Differente von $\overline{\mathfrak{J}}$ bezüglich $\bar{k}[z]$ das Erweiterungsideal der Differente von $\mathfrak{J}$ bezüglich $k[z]$ ist. Für ein Primideal $\tilde{\mathfrak{p}}$ aus $\mathfrak{J}$ läßt sich ferner die Zerlegung des Erweiterungsideals $\overline{\mathfrak{J}} \cdot \tilde{\mathfrak{p}}$ vollständig übersehen. Ist nämlich f der Grad von $\tilde{\mathfrak{p}}$ bezüglich k und m der größte positive Teiler von f der Art, daß in $\bar{k}$ ein Unterkörper des Grades m bezüglich k enthalten ist, so zerfällt $\overline{\mathfrak{J}} \cdot \tilde{\mathfrak{p}}$ in $\overline{\mathfrak{J}}$ in ein Produkt von m verschiedenen Primidealen des Grades $\frac{f}{m}$ bezüglich $\bar{k}$[18]). Ist also $\tilde{\mathfrak{a}}_{\overline{\mathfrak{J}}}$ ein Ideal aus $\mathfrak{J}$, $\tilde{\mathfrak{p}}_{\overline{\mathfrak{J}}}$ ein Primideal aus $\overline{\mathfrak{J}}$, so geht $\tilde{\mathfrak{p}}_{\overline{\mathfrak{J}}}$ in dem Erweiterungsideal $\overline{\mathfrak{J}} \cdot \mathfrak{a}_{\mathfrak{J}}$ mit der gleichen Potenz auf, wie das Verengungsideal $\tilde{\mathfrak{p}}_{\mathfrak{J}} = \mathfrak{J} \cap \tilde{\mathfrak{p}}_{\overline{\mathfrak{J}}}$ in $\tilde{\mathfrak{a}}_{\mathfrak{J}}$.

I. Teil.

Theorie der Divisoren von K.

§ 3.

Die Stellen des Körpers K.

1. Die Grundlage einer arithmetischen Theorie des Körpers K, welche keinem Element von K eine ausgezeichnete Stellung einräumt, ist der Begriff des Divisors von K. Er beruht seinerseits auf der Definition der „Stellen" von K, die wir daher zunächst einführen.

Leitend ist dabei das Vorbild der algebraischen Funktionen einer Veränderlichen mit beliebigen komplexen Zahlkoeffizienten. Dort bildet die Gesamtheit der an einer Stelle endlichen Funktionen einen den Koeffizientenkörper umfassenden Integritätsbereich, der zwei wesentliche Eigenschaften besitzt. Einmal stellt die Menge der an der betreffenden Stelle verschwin-

---

In bekannter Weise ergibt sich hieraus eine Darstellung $\bar{\gamma} = \frac{\gamma_1 \eta_1 + \ldots + \gamma_n \eta_n}{\Delta_K(\eta_1, \ldots, \eta_n)}$, wo γ_i Elemente von $\mathfrak{J}$ und $\Delta_K(\eta_1, \ldots, \eta_n)$ die Diskriminante bezüglich K von $\eta_1, \ldots, \eta_n$, also $\Delta_K(\eta_1, \ldots, \eta_n)$ Element aus k ist. Wenn $\overline{K}$ endlich bezüglich K ist, ist also $\overline{\mathfrak{J}} = \mathfrak{J}[\bar{k}]$. Den Fall, daß $\overline{K}$ bezüglich K unendlich ist, führt man auf den vorigen zurück durch die Bemerkung, daß auch dann jedes Element aus $\overline{\mathfrak{J}}$ einer endlichen Erweiterung von K angehört und somit nach dem obigen in $\mathfrak{J}[\bar{k}]$ enthalten ist.

[18]) Ist $\overline{K} = K(\eta)$, wo η absolut algebraisch ist, so findet man die Zerfällung von $\overline{\mathfrak{J}} \cdot \tilde{\mathfrak{p}}$ aus der Zerlegung mod $\tilde{\mathfrak{p}}$ des bezüglich k irreduziblen Polynoms, dessen Nullstelle η ist. Daraus folgt die Behauptung des Textes zunächst für endliche Erweiterungan $\overline{K}$ von K. Für unendliche Erweiterungen ergibt sie sich dann mit Hilfe der Bemerkung, daß in einem Oberkörper $\overline{K}$ mit zu f teilerfremdem Grad nach vorstehendem keine Zerfällung des Primideals erfolgen kann.

denden Funktionen ein Ideal dieses Integritätsbereiches dar, wobei man die an der fraglichen Stelle verschwindenden Funktionen rein arithmetisch einfach als Nichteinheiten des zugehörigen Integritätsbereiches charakterisieren kann. Andererseits ist eine Funktion ξ, die einer Gleichung

$$\xi^m + a_1 \xi^{m-1} + \ldots + a_m = 0$$

genügt, bei der die Koeffizienten a_i an der betrachteten Stelle endlich sind, stets selbst endlich, d. h. der Integritätsbereich der an der Stelle endlichen Funktionen ist ganz abgeschlossen.

Das veranlaßt uns, die nachstehende Definition auszusprechen.

Definition. Unter einer Stelle des Körpers K verstehen wir einen von K verschiedenen Ring $\mathfrak{P}$ des Körpers K mit folgenden Eigenschaften:

1. Die Menge der Nichteinheiten von $\mathfrak{P}$ bildet ein Ideal $\mathfrak{p}$ von $\mathfrak{P}$.
2. $\mathfrak{P}$ ist ganz abgeschlossen in K.

Als einfache Folge aus dieser Definition ergibt sich, daß das Ideal $\mathfrak{p}$ der Nichteinheiten von $\mathfrak{P}$ ein Primideal ist, da das Produkt zweier Nichteinheiten stets wieder eine Nichteinheit ist. $\mathfrak{p}$ heißt das zu $\mathfrak{P}$ gehörige Primideal.

Die Existenz unendlich vieler Stellen des Körpers K wird durch nachfolgenden einfachen Satz sichergestellt, der zugleich die Beziehung zwischen den Stellen $\mathfrak{P}$ von K und den Primidealen $\tilde{\mathfrak{p}}$ des Ringes $\mathfrak{J}$ aller in z ganzen Elemente aus K angibt.

Satz 1. *Ist $\tilde{\mathfrak{p}}$ ein Primideal aus $\mathfrak{J}$, so ist $\mathfrak{J}_{\tilde{\mathfrak{p}}}$ eine Stelle $\mathfrak{P}$ von K.*

Umgekehrt: Ist z ein nicht zu k gehöriges Element der Stelle $\mathfrak{P}$, $\mathfrak{J}$ der Integritätsbereich aller in z ganzen Elemente aus K und $\tilde{\mathfrak{p}} = \mathfrak{J} \cap \mathfrak{p}$ das Verengungsideal des zu $\mathfrak{P}$ gehörigen Primideals $\mathfrak{p}$, so ist $\tilde{\mathfrak{p}}$ Primideal und $\mathfrak{J}_{\tilde{\mathfrak{p}}} = \mathfrak{P}$.

Der erste Teil dieses Satzes geht unmittelbar aus § 1, 3 hervor. Vom zweiten Teil leuchtet die Behauptung, $\tilde{\mathfrak{p}}$ sei Primideal, ohne weiteres ein, und es ist klar, daß $\mathfrak{J}_{\tilde{\mathfrak{p}}}$ ganz in $\mathfrak{P}$ enthalten ist. Daraus folgt aber sofort $\mathfrak{J}_{\tilde{\mathfrak{p}}} = \mathfrak{P}$, weil $\mathfrak{J}_{\tilde{\mathfrak{p}}}$ maximaler Integritätsbereich ist.

Die in Satz 1 enthaltene Gleichung $\mathfrak{J}_{\tilde{\mathfrak{p}}} = \mathfrak{P}$ führt weiter zu dem Ergebnis

Satz 2. *Eine Stelle $\mathfrak{P}$ von K ist stets Hauptidealring, und es ist jedes Element von K eindeutig in der Form $\alpha = \varepsilon \pi^e$ darstellbar, wo π eine Basis des zu $\mathfrak{P}$ gehörigen Primideals $\mathfrak{p}$, ε eine Einheit von $\mathfrak{P}$ und e eine positive oder negative ganze Zahl darstellt.*

Die Menge aller ganzen und gebrochenen Ideale von $\mathfrak{P}$ wird also durch die Menge aller positiven und negativen Potenzen $\mathfrak{p}^e$ des zugehörigen Primideals $\mathfrak{p}$ erschöpft.

Da ein Element α dann und nur dann zu $\mathfrak{P}$ gehört, wenn in der Darstellung $\alpha = \varepsilon \pi^e$ der Exponent $e \geqq 0$ ist, so folgt, daß stets entweder α oder $\frac{1}{\alpha}$ in $\mathfrak{P}$ liegt, und zwar ist $\frac{1}{\alpha}$ notwendig Element von $\mathfrak{p}$, wenn α nicht in $\mathfrak{P}$ enthalten ist. Diese Tatsache ermöglicht es, mit Hilfe von Satz 1 einen vollständigen Überblick über alle Stellen von K zu gewinnen.

Satz 3. *Bedeutet $\mathfrak{J}$ bzw. $\mathfrak{J}'$ den Ring aller in z bzw. $\frac{1}{z}$ ganzen Elemente aus K, so erhält man alle Stellen von K und jede nur einmal, wenn man die sämtlichen Quotientenringe $\mathfrak{J}_{\tilde{\mathfrak{p}}}$ bzw. $\mathfrak{J}'_{\tilde{\mathfrak{p}}'}$ betrachtet, wo $\tilde{\mathfrak{p}}$ alle Primideale aus $\mathfrak{J}$, $\tilde{\mathfrak{p}}'$ alle in $\frac{1}{z}$ aufgehenden Primideale aus $\mathfrak{J}'$ durchläuft.*

2. Ist $\mathfrak{P}$ eine Stelle von K, $\mathfrak{p}$ das zugehörige Primideal, K^* ein Unterkörper von K, der mindestens ein nicht zu k gehöriges Element enthält, so ist $K^* \cap \mathfrak{P}$ eine Stelle $\mathfrak{P}^*$ von K^* und $K^* \cap \mathfrak{p}$ das zugehörige Primideal $\mathfrak{p}^*$. $\mathfrak{P}^*$ bzw. $\mathfrak{p}^*$ heißt die Verengung von $\mathfrak{P}$ bzw. $\mathfrak{p}$ bezüglich K^*. Die Gesamtheit der Stellen $\mathfrak{P}$ von K, deren Verengung gleich $\mathfrak{P}^*$ ist, nennen wir untereinander konjugiert bezüglich K^*.

3. Unter Benützung der in Satz 2 angegebenen Darstellung jedes Elements aus K läßt sich ohne Schwierigkeit der Begriff der Ordnung eines Elements an der Stelle $\mathfrak{P}$ erklären. Diese Definition der Ordnung wird dabei so einzurichten sein, daß die aus der Theorie der algebraischen Funktionen bekannten Sätze über die Ordnung von Funktionen im wesentlichen in unserem Fall erhalten bleiben. Um dies zu erreichen, erklären wir: Ist $\mathfrak{P}\alpha = \mathfrak{p}^e$ und f der Grad von $\mathfrak{p}$ bezüglich k, so schreiben wir α die Ordnung ef für die Stelle $\mathfrak{P}$ zu. Es ist dann offenbar die Ordnung eines Produktes gleich der Summe der Ordnungen der einzelnen Faktoren.

§ 4.

Divisoren.

1. Ein Element z aus K erzeugt nur in endlich vielen Stellen $\mathfrak{P}$ ein vom Einheitsideal verschiedenes Ideal $\mathfrak{P} \cdot z$, nämlich in allen und nur den Stellen $\mathfrak{P} = \mathfrak{J}_{\tilde{\mathfrak{p}}}$ bzw. $\mathfrak{P} = \mathfrak{J}'_{\tilde{\mathfrak{p}}'}$, bei denen $\tilde{\mathfrak{p}}$ bzw. $\tilde{\mathfrak{p}}'$ ein in z bzw. $\frac{1}{z}$ aufgehendes Primideal des Ringes $\mathfrak{J}$ bzw. $\mathfrak{J}'$ aller in z bzw. $\frac{1}{z}$ ganzen Elemente bedeutet. Seien $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$ diese Stellen und $\mathfrak{P}_i \cdot z = \mathfrak{p}_i^{e_i}$ die Darstellung von $\mathfrak{P}_i \cdot z$ als Potenz des zu $\mathfrak{P}_i$ gehörigen Primideals $\mathfrak{p}_i$, wo also $e_i \gtrless 0$ ist, so läßt sich offenbar das arithmetische Verhalten von z in allen Stellen von K dadurch beschreiben, daß man z den eindeutig bestimmten, rein formalen Ausdruck $\mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \ldots \mathfrak{p}_s^{e_s}$, den sogenannten Divisor von z, zuordnet.

2. Allgemein verstehen wir unter einem Divisor $\mathfrak{c}$ von K einen beliebigen, rein formalen Ausdruck $\mathfrak{c} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\dots\mathfrak{p}_s^{e_s}$, wo $\mathfrak{p}_i$ Primideal einer Stelle $\mathfrak{P}_i$ von K und e_i eine positive oder negative ganze Zahl oder Null ist. Für Divisoren übernehmen wir die aus der algebraischen Funktionentheorie bekannten Definitionen, an die wir kurz erinnern[19]).

Der Divisor $\mathfrak{c} = \mathfrak{p}$, wo $\mathfrak{p}$ Primideal einer Stelle $\mathfrak{P}$ von K ist, heißt Primdivisor von K. Zu jeder Stelle gehört somit ein bestimmter Primdivisor und umgekehrt; sind die Stellen $\mathfrak{P}_1, \dots, \mathfrak{P}_m$ konjugiert bezüglich K^*, so sollen auch die zugehörigen Primdivisoren $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ bezüglich K^* konjugiert genannt werden. Für einen Primdivisor $\mathfrak{p}$ erklären wir den Exponenten e, mit dem $\mathfrak{p}$ in dem Divisor $\mathfrak{c} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\dots\mathfrak{p}_s^{e_s}$ auftritt, durch die Festsetzung: $e = e_i$, wenn $\mathfrak{p} = \mathfrak{p}_i$ und $i = 1, 2, \dots, s$, $e = 0$, wenn $\mathfrak{p}$ von allen $\mathfrak{p}_i$ verschieden. Wir sagen, $\mathfrak{p}$ trete in $\mathfrak{c}$ wirklich auf, wenn der Exponent $e \neq 0$ ist.

Die kommutative Multiplikationsgruppe, die durch sämtliche Primdivisoren von K als freie Erzeugende definiert ist, enthält alle und nur die Divisoren von K; sie soll daher die Gruppe der Divisoren von K genannt werden. Das in dieser Gruppe eindeutig bestimmte Produkt der Divisoren $\mathfrak{c}_1$ und $\mathfrak{c}_2$ werde durch $\mathfrak{c}_1\mathfrak{c}_2$, der Quotient durch $\frac{\mathfrak{c}_1}{\mathfrak{c}_2}$ wiedergegeben. Ein Divisor, in dem jeder Primdivisor mit dem Exponenten 0 auftritt, soll als Einheitsdivisor $\mathfrak{e}$ bezeichnet werden.

Der Divisor $\mathfrak{c}$ heißt ganz, wenn jeder Primdivisor in $\mathfrak{c}$ mit nicht negativem Exponent auftritt; $\mathfrak{c}$ ist ganz in bezug auf den Divisor $\mathfrak{c}'$, wenn jeder in $\mathfrak{c}'$ wirklich auftretende Primdivisor in $\mathfrak{c}$ mit nicht negativem Exponenten vorkommt. Offenbar ist jeder Divisor $\mathfrak{c}$ Quotient zweier ganzer Divisoren, $\frac{\mathfrak{c}_1}{\mathfrak{c}_2}$; dabei sind $\mathfrak{c}_1$ und $\mathfrak{c}_2$ eindeutig bestimmt, wenn man fordert, daß kein Primdivisor gleichzeitig in $\mathfrak{c}_1$ und $\mathfrak{c}_2$ wirklich auftritt. In diesem Fall wird $\mathfrak{c}_1$ bzw. $\mathfrak{c}_2$ der Zähler- bzw. Nennerdivisor von $\mathfrak{c}$ genannt oder, falls $\mathfrak{c}$ der Divisor eines Elements z ist, kurz der Zähler- bzw. Nennerdivisor von z.

Wir sagen: Der Divisor $\mathfrak{c}'$ ist teilbar durch den Divisor $\mathfrak{c}''$, wenn $\frac{\mathfrak{c}'}{\mathfrak{c}''}$ ganz in bezug auf $\mathfrak{c}''$ ist; $\mathfrak{c}'$ ist Multiplum von $\mathfrak{c}''$, wenn $\frac{\mathfrak{c}'}{\mathfrak{c}''}$ ganz ist. Ein Element z ist durch den Divisor $\mathfrak{c}$ teilbar bzw. Multiplum von $\mathfrak{c}$, wenn der Divisor von z durch $\mathfrak{c}$ teilbar bzw. Multiplum von $\mathfrak{c}$ ist. Ist $z_1 - z_2$ durch $\mathfrak{c}$ teilbar, so schreibt man auch $z_1 \equiv z_2 \bmod \mathfrak{c}$.

---

[19]) Vgl. etwa K. Hensel, Arithmetische Theorie der algebraischen Funktionen, Enzykl. d. math. Wiss. 2, 3. Teil, 1. Hälfte, S. 533—650, Nr. 3 und 10.

3. Im Divisor eines Elements α aus K tritt dann und nur dann jeder Primdivisor mit dem Exponenten 0 auf, wenn α absolut algebraisch ist, d. h. zu k gehört. Ein Element aus K ist daher durch seinen Divisor bis auf einen Faktor aus k eindeutig bestimmt. Der Ring $\mathfrak{Z}$ aller in z ganzen Elemente stimmt überein mit der Menge derjenigen Elemente aus K, deren Nennerdivisoren nur solche Primdivisoren wirklich enthalten, welche auch im Nennerdivisor von z vorkommen.

Ist $\mathfrak{R}$ ein Multiplikationsring des Körpers K, $\tilde{\mathfrak{c}}$ ein ganzes oder gebrochenes Ideal aus $\mathfrak{R}$ und $\tilde{\mathfrak{c}} = \tilde{\mathfrak{p}}_1^{e_1} \cdot \tilde{\mathfrak{p}}_2^{e_2} \cdot \ldots \cdot \tilde{\mathfrak{p}}_s^{e_s}$ die Primidealdarstellung von $\tilde{\mathfrak{c}}$, so bezeichnen wir den Divisor $\mathfrak{c} = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \ldots \mathfrak{p}_s^{e_s}$, wo $\mathfrak{p}_i = \mathfrak{R}_{\tilde{\mathfrak{p}}_i} \cdot \tilde{\mathfrak{p}}_i$ ist, als zu $\tilde{\mathfrak{c}}$ gehörigen Divisor. Umgekehrt gehört zu jedem Divisor $\mathfrak{c} = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_s^{e_s}$ ein ganzes oder gebrochenes Ideal $\tilde{\mathfrak{c}}$ des Multiplikationsrings $\mathfrak{R}$, sobald $\mathfrak{R}$ in allen Stellen $\mathfrak{P}_i$ enthalten ist, welche zu den in $\mathfrak{c}$ wirklich auftretenden Primdivisoren gehören. Dabei ist $\tilde{\mathfrak{c}} = \tilde{\mathfrak{p}}_1^{e_1} \ldots \tilde{\mathfrak{p}}_s^{e_s}$ und $\tilde{\mathfrak{p}}_i = \mathfrak{p}_i \cap \mathfrak{R}$.

4. Um Ordnung und Norm eines Divisors zu erklären, führen wir diese Begriffe zunächst für Primdivisoren ein.

Besitzt das Ideal $\mathfrak{p}$ der Stelle $\mathfrak{P}$ von K den Grad f bezüglich k, so schreiben wir $\mathfrak{p}$ die Ordnung f zu und definieren allgemein die Ordnung des Divisors $\mathfrak{c} = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \ldots \mathfrak{p}_s^{e_s}$ durch die ganze Zahl $e_1 f_1 + \ldots + e_s f_s$. Der Divisor eines Elements besitzt stets die Ordnung 0. Dies ist für die Elemente aus k (nach dem in der vorigen Nummer Festgestellten) trivial und ergibt sich für ein nicht zu k gehöriges Element z, indem man im Ring $\mathfrak{Z}$ bzw. $\mathfrak{Z}'$ der in z bzw. $\frac{1}{z}$ ganzen Elemente die Primidealzerlegung des aus z bzw. $\frac{1}{z}$ abgeleiteten Ideals betrachtet[20]). Im Körper $k(z)$ gibt es zu jedem vorgegebenen Divisor der Ordnung 0 dieses Körpers ein Element, dessen Divisor mit dem vorgegebenen übereinstimmt.

Ist f^* der Grad des Primideals $\mathfrak{p}$ von $\mathfrak{P}$ bezüglich K^* und $\mathfrak{p}^*$ das Primideal der Verengung $\mathfrak{P}^*$ von $\mathfrak{P}$ bezüglich K^*, so verstehen wir unter der Norm des Primdivisors $\mathfrak{p}$ bezüglich K^* den Divisor $\mathfrak{p}^{*f^*}$ von K^*. Als Norm des Divisors $\mathfrak{c} = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \ldots \mathfrak{p}_s^{e_s}$ bezüglich K^* definieren wir den Divisor $\mathfrak{c}^* = \mathfrak{p}_1^{*e_1 f_1^*} \mathfrak{p}_2^{*e_2 f_2^*} \ldots \mathfrak{p}_s^{*e_s f_s^*}$ von K^*, falls $\mathfrak{p}_i^{*f_i^*}$ die Norm von $\mathfrak{p}_i$ bezüglich K^* ist. Man erkennt: Ist der Multiplikationsring $\mathfrak{R}$ aus K endlich in bezug auf den Multiplikationsring $\mathfrak{R}^*$ aus K^*, so ist die Norm des zum Ideal $\tilde{\mathfrak{c}}$ von $\mathfrak{R}$ gehörigen Divisors $\mathfrak{c}$ von K gleich dem Divisor von K^*, der zur Norm von $\mathfrak{c}$ bezüglich $\mathfrak{R}^*$ gehört.

5. Mit Hilfe der Beziehung zwischen Idealen und Divisoren kann endlich der Begriff des Diskriminanten- bzw. Differentendivisors von K bezüglich K^* eingeführt werden.

---

[20]) Vgl. § 1, 4.

$\mathfrak{P}^*$ sei eine Stelle von K^*, $\mathfrak{Q}$ der Ring aller $\mathfrak{P}^*$-ganzen Elemente aus K. Der zum Diskriminanten- bzw. Differentenideal von $\mathfrak{Q}$ bezüglich $\mathfrak{P}^*$ gehörige Divisor von K^* bzw. K heißt der Diskriminanten- bzw. Differentendivisor von K bezüglich $\mathfrak{P}^*$, in Zeichen: $\mathfrak{d}^*_{K\mathfrak{P}^*}$ bzw. $\mathfrak{d}_{K\mathfrak{P}^*}$. Aus § 1, 7 und § 3 Satz 3 schließt man, daß $\mathfrak{d}^*_{K\mathfrak{P}^*}$ bzw. $\mathfrak{d}_{K\mathfrak{P}^*}$ nur für endlich viele Stellen $\mathfrak{P}^*$ von K^* vom Einheitsdivisor verschieden ist. Das Produkt der Diskriminanten- bzw. Differentendivisoren von K in bezug auf sämtliche Stellen $\mathfrak{P}^*$ von K^* ist daher ein bestimmter Divisor, der Diskriminantendivisor $\mathfrak{d}^*_{KK^*}$ bzw. Differentendivisor $\mathfrak{d}_{KK^*}$ von K bezüglich K^*. Man hat $\mathfrak{d}^*_{KK^*} = N(\mathfrak{d}_{KK^*})$, da für jedes $\mathfrak{P}^*$ $\mathfrak{d}^*_{K\mathfrak{P}^*} = N(\mathfrak{d}_{K\mathfrak{P}^*})$ ist. Ist $\mathfrak{c}$ ein beliebiger Divisor von K, so heißt $\frac{1}{\mathfrak{c}\,\mathfrak{d}_{KK^*}}$ der zu $\mathfrak{c}$ bezüglich K^* komplementäre Divisor.

Die Ordnung des Divisors $\mathfrak{d}_{KK^*}$ heißt die Verzweigungszahl von K bezüglich K^*. Die Verzweigungszahl w_z von K bezüglich $k(z)$ läßt sich nach dem in §§ 1, 2, 3 Angegebenen auch folgendermaßen bestimmen. Ist $\mathfrak{J}$ bzw. $\mathfrak{J}'$ der Ring aller in z bzw. in $\frac{1}{z}$ ganzen Elemente aus K, so ist w_z gleich dem Grad der Diskriminante von $\mathfrak{J}$ bezüglich $k(z)$ vermehrt um den Exponenten der höchsten Potenz von $\frac{1}{z}$ der in der Diskriminante von $\mathfrak{J}'$ bezüglich $k\left[\frac{1}{z}\right]$ aufgeht.

6. Die Divisoren der Elemente von K bilden eine Untergruppe $\mathfrak{H}$ der Gruppe $\mathfrak{D}$ aller Divisoren von K. Die Quotientengruppe $\mathfrak{D}/\mathfrak{H}$ heißt die Divisorenklassengruppe, jede Restklasse von $\mathfrak{D}$ nach $\mathfrak{H}$ eine Divisorenklasse, $\mathfrak{H}$ insbesondere die Hauptklasse. Da die Divisoren von $\mathfrak{H}$ alle die Ordnung 0 haben, besitzen die Divisoren einer Divisorenklasse sämtlich die gleiche Ordnung und man kann daher von der Ordnung einer Divisorenklasse reden.

§ 5.

Differentialquotienten. Geschlecht.

1. Sind α und β irgend zwei nicht zu k gehörige Elemente aus K und etwa α von erster Art bezüglich $k(\beta)$, (vgl. § 2, 2), ist ferner α Nullstelle des in $k[x, \beta]$ irreduziblen Polynoms $F(x, \beta)$, wobei dann $F_1'(x, \beta) \neq 0$ ist, so definiert man den Differentialquotienten $\frac{d\alpha}{d\beta}$ durch die Gleichung

$$\frac{d\alpha}{d\beta} = -\frac{F_2'(\alpha, \beta)}{F_1'(\alpha, \beta)}.$$ [1]

Diese Definition von $\frac{d\alpha}{d\beta}$ ist offenbar von der Wahl des in $k[x, \beta]$ irreduziblen Polynoms $F(x, \beta)$ unabhängig. Sie ist aber auch gegenüber

[1] $F_1(x, \beta) = F_x(x, y)\big|_{y=\beta}$
$F_2(x, \beta) = F_y(x, y)\big|_{x=\beta}$.

Erweiterungen des Körpers K invariant, d. h. ersetzt man K durch einen Oberkörper $\bar{K}$, so bleibt $\frac{d\alpha}{d\beta}$ ungeändert. Ist nämlich $\bar{k}$ der größte in $\bar{K}$ enthaltene absolut algebraische Körper, so ist das in $k[x, \beta]$ irreduzible Polynom $F(x, \beta)$ auch in $\bar{k}[x, \beta]$ irreduzibel, weil $k(\alpha, \beta) \cap \bar{k} = k$ und $\bar{k}$ Normalkörper über k ist.

Für die soeben definierten Differentialquotienten gelten ferner die Regeln der Differentiation von Summe, Produkt und Quotient, sowie die Kettenregel, d. h. sind α und β von erster Art bezüglich $k(\gamma)$, so ist

$$\frac{d(\alpha+\beta)}{d\gamma} = \frac{d\alpha}{d\gamma} + \frac{d\beta}{d\gamma}, \quad \frac{d(\alpha\beta)}{d\gamma} = \frac{d\alpha}{d\gamma}\beta + \frac{d\beta}{d\gamma}\alpha, \quad \frac{d\frac{\alpha}{\beta}}{d\gamma} = \frac{\frac{d\alpha}{d\gamma}\beta - \frac{d\beta}{d\gamma}\alpha}{\beta^2}$$

und wenn auch α von erster Art bezüglich $k(\beta)$

$$\frac{d\alpha}{d\gamma} = \frac{d\alpha}{d\beta}\frac{d\beta}{d\gamma}.$$

Diese Regeln beweist man im Falle eines algebraisch abgeschlossenen Koeffizientenkörpers, $k = k_a$, in üblicher Weise. Sie gelten daher sicher für die Differentialquotienten von $\bar{K} =$ Hülle (K, k_a) und somit auch für die Differentialquotienten von K, weil diese bei Körpererweiterungen ungeändert bleiben.

2. Satz 4. *Sind α und β zwei nicht zu k gehörige Elemente aus K der Art, daß K in bezug auf $k(\alpha)$ und $k(\beta)$ von erster Art ist, $\mathfrak{a}$ bzw. $\mathfrak{b}$ die Nennerdivisoren von α bzw. β und $\mathfrak{d}_\alpha$ bzw. $\mathfrak{d}_\beta$ die Differentendivisoren von K bezüglich $k(\alpha)$ bzw. $k(\beta)$, so ist der Divisor von $\frac{d\alpha}{d\beta}$ gleich $\frac{\mathfrak{d}_\alpha \mathfrak{b}^2}{\mathfrak{d}_\beta \mathfrak{a}^2}$.*

Die übliche Herleitung dieses Satzes versagt bei Körpern von Primzahlcharakteristik, bei denen weitergehende Tatsachen aus der Theorie der Differente herangezogen werden müssen.

Sei $\mathfrak{p}$ ein beliebiger Primdivisor von K, $\mathfrak{P}$ die zu $\mathfrak{p}$ gehörige Stelle. Wir haben zu zeigen, daß $\frac{d\alpha}{d\beta}$ durch dieselbe Potenz von $\mathfrak{p}$ teilbar ist wie $\frac{\mathfrak{d}_\alpha \mathfrak{b}^2}{\mathfrak{d}_\beta \mathfrak{a}^2}$. Da nach der Kettenregel $\frac{d\alpha}{d\beta} = -\alpha^2 \frac{d\frac{1}{\alpha}}{d\beta} = -\frac{1}{\beta^2}\frac{d\alpha}{d\frac{1}{\beta}} = \frac{\alpha^2}{\beta^2}\frac{d\frac{1}{\alpha}}{d\frac{1}{\beta}}$ und ferner $k(\alpha) = k\left(\frac{1}{\alpha}\right)$, $k(\beta) = k\left(\frac{1}{\beta}\right)$ ist, können wir uns auf den Fall beschränken, daß $\mathfrak{p}$ im Nennerdivisor von α und β nicht auftritt. Es bleibt dann zu beweisen: Das aus $\frac{d\alpha}{d\beta}$ in $\mathfrak{P}$ abgeleitete Ideal gestattet die Darstellung $\mathfrak{P} \cdot \frac{d\alpha}{d\beta} = \mathfrak{p}^{d_\alpha - d_\beta}$, wo d_α bzw. d_β der Exponent ist, mit dem der Primdivisor $\mathfrak{p}$ in $\mathfrak{d}_\alpha$ bzw. $\mathfrak{d}_\beta$ vorkommt.

Dabei dürfen wir weiter voraussetzen, daß $k = k_a$ algebraisch abgeschlossen ist; denn ein Primdivisor von $\overline{K} = \text{Hülle}\,(K, k_a)$, dessen Verengungsdivisor bezüglich K gleich $\mathfrak{p}$ ist, teilt $\frac{d\alpha}{d\beta}$ in derselben Potenz wie $\mathfrak{p}$ und tritt ferner in den Differentendivisoren von $\overline{K}$ bezüglich $k(\alpha)$ bzw. $k(\beta)$ ebenfalls mit dem Exponenten d_α bzw. d_β auf [21]). Im Falle eines algebraisch abgeschlossenen Koeffizientenkörpers k sind aber α und β nach $\mathfrak{p}$ je einem Element a bzw. b aus k kongruent und wegen $\frac{d\alpha}{d\beta} = \frac{d(\alpha-a)}{d(\beta-b)}$ können wir α und β von vornherein so gewählt denken, daß sie beide durch $\mathfrak{p}$ teilbar sind.

Unter diesen Voraussetzungen berechnen wir $\frac{d\alpha}{d\beta}$ mit Hilfe eines passend gewählten Elements γ nach der Kettenregel: $\frac{d\alpha}{d\beta} = \frac{d\alpha}{d\gamma}\frac{d\gamma}{d\beta}$, wo $\frac{d\alpha}{d\gamma} = -\frac{F_2'(\alpha,\gamma)}{F_1'(\alpha,\gamma)}$, $\frac{d\gamma}{d\beta} = -\frac{G_1'(\beta,\gamma)}{G_2'(\beta,\gamma)}$ und $F(\alpha, x)$ bzw. $G(\beta, x)$ das in $k[\alpha, x]$ bzw. $k[\beta, x]$ irreduzible Polynom bedeutet, dessen Nullstelle γ ist. Es ist dann also $\frac{d\alpha}{d\beta} = \frac{F_2'(\alpha,\gamma)}{G_2'(\beta,\gamma)}\frac{G_1'(\beta,\gamma)}{F_1'(\alpha,\gamma)}$, und wenn wir γ so wählen, daß $\mathfrak{P}\cdot F_2'(\alpha,\gamma) = \mathfrak{p}^{d_\alpha}$, $\mathfrak{P}\cdot G_2'(\beta,\gamma) = \mathfrak{p}^{d_\beta}$ und $\mathfrak{P}\cdot\frac{G_1'(\beta,\gamma)}{F_1'(\alpha,\gamma)} = \mathfrak{P}$ ist, so ist alles bewiesen.

Um dies zu erreichen, bestimme man γ so, daß folgende drei Bedingungen erfüllt sind.

1. Sind $\mathfrak{p} = \mathfrak{p}_0, \mathfrak{p}_1, \ldots, \mathfrak{p}_m$ alle zu $\mathfrak{p}$ bezüglich $k(\alpha)$ oder bezüglich $k(\beta)$ konjugierten Primdivisoren und bedeuten $0 = e_0, e_1, \ldots, e_m$ lauter untereinander verschiedene Elemente aus k, so sei $\gamma - e_i$ durch $\mathfrak{p}_i$, aber nicht durch $\mathfrak{p}_i^2$ teilbar

2. Ist $\mathfrak{p}'$ ein im Nennerdivisor von α oder β wirklich auftretender Primdivisor, so sei γ nach $\mathfrak{p}'$ einem beliebigen Element $e' \neq 0$ aus k kongruent.

3. Ist $\mathfrak{p}''$ ein im Zählerdivisor von α oder β wirklich auftretender, von $\mathfrak{p}$ verschiedener Primdivisor, so sei γ nach $\mathfrak{p}''$ einem Element $e'' \neq 0$ von k kongruent.

Versteht man dann unter $\mathfrak{P}_\alpha$ die Stelle $\mathfrak{P} \cap k(\alpha)$ von $k(\alpha)$ und unter $\mathfrak{O}_\alpha$ den Durchschnitt aller zu $\mathfrak{P}$ bezüglich $k(\alpha)$ konjugierten Stellen, so besteht $\mathfrak{O}_\alpha$ aus allen $\mathfrak{P}_\alpha$-ganzen Elementen von K. Aus 1. schließt man, daß γ in $\mathfrak{O}_\alpha$ liegt, weiter in bekannter Weise [22]), daß $K = k(\alpha, \gamma)$ und das aus der Diskriminante von γ in $\mathfrak{P}_\alpha$ abgeleitete Ideal gleich dem Diskriminantenideal von $\mathfrak{O}_\alpha$ bezüglich $\mathfrak{P}_\alpha$ ist. Es ist daher $\mathfrak{P}\cdot F_2'(\alpha,\gamma) = \mathfrak{p}^{d_\alpha}$. Entsprechend findet man $K = k(\beta, \gamma)$ und $\mathfrak{P}\cdot G_2'(\beta,\gamma) = \mathfrak{p}^{d_\beta}$.

---

[21]) Das folgt unmittelbar aus § 2, 4 in Verbindung mit § 3 Satz 3.

[22]) Vgl. *D.-W.*, S. 224 und 225.

Setzt man andererseits $\mathfrak{P}_\gamma = \mathfrak{P} \cap k(\gamma)$ und $\mathfrak{O}_\gamma$ gleich dem Ring aller $\mathfrak{P}_\gamma$ ganzen Elemente aus K, so sind α und β gemäß 2. beide in $\mathfrak{O}_\gamma$ enthalten. Nach 3. ist ferner das Primideal $\tilde{\mathfrak{p}} = \mathfrak{p} \cap \mathfrak{O}_\gamma$ gleich dem aus γ und α bzw. aus γ und β abgeleiteten Ideal, woraus in Verbindung mit $K = k(\alpha, \gamma) = k(\beta, \gamma)$ nach bekannten Sätzen folgt[23]), daß $\tilde{\mathfrak{p}}$ in $F_1'(\alpha, \gamma)$ nnd $G_1'(\beta, \gamma)$ mit der gleichen Potenz aufgeht wie in der Differente von $\mathfrak{O}_\gamma$ nach $\mathfrak{P}_\gamma$. Es ist daher $\frac{G_1'(\beta, \gamma)}{F_1'(\alpha, \gamma)}$ durch $\tilde{\mathfrak{p}}$ nicht teilbar, d. h. $\mathfrak{P} \cdot \frac{G_1'(\beta, \gamma)}{F_1'(\alpha, \gamma)} = \mathfrak{P}$.

3. Durch Satz 4 wird man veranlaßt, ebenso wie in der algebraischen Funktionentheorie, das Geschlecht g von K als wichtige Invariante einzuführen.

Definition. *Ist z ein nicht zu k gehöriges Element aus K und K von erster Art über $k(z)$, $m_z = (K : k(z))$, w_z die Verzweigungszahl von K bezüglich $k(z)$, so wird die Zahl $g = \frac{w_z}{2} - m_z + 1$ das Geschlecht von K genannt.*

Die Invarianz des Geschlechts, d. h. die Gleichung $\frac{w_\alpha}{2} - m_\alpha + 1 = \frac{w_\beta}{2} - m_\beta + 1$ für zwei Elemente α und β schließt man unmittelbar aus Satz 4.

§ 6.

Modul der Multipla eines Divisors. Riemann-Rochscher Satz.

1. Ist $\mathfrak{c}$ ein beliebiger Divisor von K, so bildet die Menge aller Elemente aus K, die Multipla von $\mathfrak{c}$ sind, einen k-Modul, den Modul $\mathfrak{m}(\mathfrak{c})$ der Multipla von $\mathfrak{c}$. In diesem Paragraphen soll gezeigt werden, daß der Modul $\mathfrak{m}(\mathfrak{c})$ eine endliche Basis in bezug auf k besitzt und daß die Länge der Basis (Elementezahl) durch eine einfache Formel gegeben wird (Riemann-Rochescher Satz).

Um den Modul $\mathfrak{m}(\mathfrak{c})$ zu bestimmen, bezeichnen wir mit z ein nicht zu k gehöriges Element aus K, dessen Nennerdivisor keinen der in $\mathfrak{c}$ wirklich auftretenden Primdivisoren wirklich enthält. Der Ring $\mathfrak{J}$ aller in z ganzen Elemente ist dann Unterring jeder Stelle $\mathfrak{P}_i$, die zu einem in $\mathfrak{c}$ wirklich auftretenden Primdivisor gehört, und das zu $\mathfrak{c}$ gehörige Ideal $\tilde{\mathfrak{c}}$ aus $\mathfrak{J}$ umfaßt den Modul $\mathfrak{m}(\mathfrak{c})$. Es liegt daher nahe, eine Basis von $\mathfrak{m}(\mathfrak{c})$ bezüglich k aus einer Basis von $\tilde{\mathfrak{c}}$ bezüglich $k[z]$ herzuleiten. Haupthilfsmittel bei dieser Untersuchung bildet der Begriff des Exponenten eines

[23]) Vgl. Dedekind, Über die Diskriminanten endlicher Körper, Abh. d. Ges. d. Wiss. z. Göttingen 29 (1882), S. 42.

Elements α aus K in bezug auf $\frac{1}{z}$ und der sich darauf gründende Begriff einer Normalbasis von $\mathfrak{c}$, die beide in den drei nächsten Nummern behandelt werden.

2. Für den Rest dieses Paragraphen bedeutet z ein Element, so daß K über $k(z)$ von erster Art algebraisch ist, $\mathfrak{J}$ den Ring aller in z ganzen Elemente aus K, $\mathfrak{c}$ ein Ideal aus $\mathfrak{J}$ und $\mathfrak{Q}$ den Durchschnitt derjenigen Stellen $\mathfrak{P}_i$, die zu den im Nennerdivisor von z wirklich auftretenden Primdivisoren gehören. Setzt man $\mathfrak{Q} \cap k(z) = \mathfrak{P}^*$, so besteht die Stelle $\mathfrak{P}^*$ von $k(z)$ aus allen Quotienten je zweier Elemente aus $k\left[\frac{1}{z}\right]$, bei denen der Nenner durch $\frac{1}{z}$ nicht teilbar ist, und $\mathfrak{Q}$ ist der Ring aller $\mathfrak{P}^*$ ganzen Elemente aus K.

Da $\frac{1}{z}$ in jeder der Stellen $\mathfrak{P}_i$ eine positive Ordnung hat, gibt es zu jedem Element α aus K sicherlich ganze (eventuell negative) Zahlen e, so daß $z^e\alpha$ in $\mathfrak{Q}$ liegt. Die größte positive oder negative ganze Zahl e dieser Art heißt der Exponent von α in $\frac{1}{z}$. Im folgenden ist stets der Exponent in $\frac{1}{z}$ gemeint, wenn kurz vom Exponent eines Elements die Rede ist.

Alle und nur die Elemente aus $\mathfrak{Q}$ besitzen einen nichtnegativen Exponenten. Sind $e_\alpha \leqq e_\beta$ die Exponenten der Elemente α, β, so ist der Exponent von $\alpha\beta$ mindestens gleich $e_\alpha + e_\beta$, der Exponent von $\alpha + \beta$ mindestens gleich e_α, und zwar ist der Exponent von $\alpha + \beta$ genau gleich e_α, wenn $e_\alpha < e_\beta$ ist. Der Exponent e_c eines Elements c aus $k(z)$ ist gleich der Ordnung von c in $\mathfrak{P}^*$, d. h. ist $c = \frac{c_1}{c_2}$, wo c_1 und c_2 aus $k[z]$ stammen, so ist e_c der Differenz der Gradzahlen von c_1 und c_2 entgegengesetzt gleich, und es hat $c\alpha$ den Exponent $e_c + e_\alpha$, wenn α den Exponent e_α hat.

Wir setzen $(K : k(z)) = m$, so daß also das Ideal $\mathfrak{c}$ eine Modulbasis von m unabhängigen Elementen in bezug auf den Hauptidealring $k[z]$ besitzt.

Definition. Die Basis $\gamma_1, \ldots, \gamma_m$ von $\mathfrak{c}$ bezüglich $k[z]$ heißt Normalbasis von $\mathfrak{c}$ bezüglich $k[z]$, wenn die Exponenten e_i der Elemente γ_i möglichst groß sind, d. h. wenn für jede Basis $\gamma_1', \ldots, \gamma_m'$ von $\mathfrak{c}$ bezüglich $k[z]$ bei geeigneter Numerierung die Exponenten e_i' von γ_i' den Ungleichungen $e_i' \leqq e_i$ genügen.

Aus der Definition folgt unmittelbar, daß die Exponenten zweier Normalbasen von $\mathfrak{c}$ bei geeigneter Numerierung übereinstimmen.

3. Satz 5. *Seien $\gamma_1, \ldots, \gamma_m$ m Elemente aus $\mathfrak{c}$, die den folgenden Bedingungen genügen.*

1. *γ_1 besitzt unter allen Elementen von $\mathfrak{c}$ einen möglichst großen Exponenten.*

2. *γ_{i+1} besitzt für $i = 1, \ldots, m-1$ unter allen nicht von $\gamma_1, \ldots, \gamma_i$ bezüglich $k(z)$ abhängenden Elementen aus $\mathfrak{c}$ einen möglichst großen Exponenten e_i.*

Dann bilden $\gamma_1, \ldots, \gamma_m$ eine Normalbasis von $\mathfrak{c}$ bezüglich $k[z]$.

Zum Beweis genügt es zu zeigen, daß $\gamma_1, \ldots, \gamma_m$ eine Basis von $\mathfrak{c}$ bezüglich $k[z]$ bilden.

Wäre dies nicht der Fall, so enthielte $\mathfrak{c}$ ein Element $\frac{c_1\gamma_1 + \ldots + c_m\gamma_m}{c}$, wo die c_i und c Elemente aus $k[z]$ und nicht jedes c_i durch c teilbar ist. Sei etwa c_l das letzte nicht durch c teilbare c_i und $c_1', c_2', \ldots, c_l'$ die reduzierten Reste von $c_1, \ldots, c_l$ nach c, so ist auch $\gamma' = \frac{c_1'\gamma_1 + \ldots + c_l'\gamma_l}{c}$ in $\mathfrak{c}$ enthalten, und da der Grad von c_i' im Falle $c_i' \neq 0$ in z niedriger als der Grad von c in z, also der Exponent von $\frac{c_i'}{c}$ größer als 0 ist, so hat γ' einen größeren Exponenten als γ_l entgegen der Wahl von γ_l.

Satz 6. *Ein Ideal $\mathfrak{c}$ aus $\mathfrak{Z}$ besitzt stets eine Normalbasis in bezug auf $k[z]$. Die Elemente einer Normalbasis genügen bei geeigneter Numerierung den Bedingungen 1 und 2 des vorigen Satzes.*

Durch Multiplikation mit einem geeigneten Element c aus $k[z]$ kann das Ideal $\mathfrak{c}$ stets in ein ganzes Ideal $c \cdot \mathfrak{c}$ überführt werden. Da der Exponent eines Elementes aus $\mathfrak{Z}$ höchstens gleich 0 ist, so lassen sich aus dem ganzen Ideal sicher m Elemente $\gamma_1', \ldots, \gamma_m'$ auswählen, die den Bedingungen 1 und 2 des vorigen Satzes genügen. $\frac{\gamma_1'}{c}, \ldots, \frac{\gamma_m'}{c}$ sind dann m die Bedingungen 1 und 2 erfüllende Elemente aus $\mathfrak{c}$ und bilden daher eine Normalbasis $\mathfrak{c}$ bezüglich $k[z]$.

Da die Exponenten der Elemente zweier Normalbasen bei passender Numerierung übereinstimmen, so folgt aus der Existenz einer den Bedingungen von Satz 5 genügender Normalbasis sofort, daß jede Normalbasis diesen Bedingungen genügt.

Satz 7. *Ist $\gamma_1, \ldots, \gamma_m$ eine Normalbasis von $\mathfrak{c}$ bezüglich $k[z]$, so ist der Exponent von $\gamma = c_1\gamma_1 + \ldots + c_m\gamma_m$, wo die c_i aus $k[z]$ stammen, gleich dem Minimum e der Exponenten der einzelnen Summanden $c_i\gamma_i$.*

Die Numerierung der Elemente $\gamma_1, \ldots, \gamma_m$ sei so gewählt, daß die γ_i den Bedingungen 1 und 2 des Satzes 5 genügen. Das Element $c_1\gamma_1 + c_2\gamma_2 + \ldots + c_m\gamma_m$ kann aufgefaßt werden als Summe von Elementen der Gestalt $a_{k_i} z^{k_i}\gamma_i$, wobei die a_{k_i} aus k stammen. $a_{s_1} z^{s_1}\gamma_{i_1}, \ldots, a_{s_t} z^{s_t}\gamma_{i_t}$ seien diejenigen unter diesen Elementen, deren Exponent gleich e ist, so

daß $e = e_{i_1} - s_1 = e_{i_2} - s_2 = \ldots = e_{i_t} - s_t$ ist, falls $e_{i_1}, \ldots, e_{i_t}$ die Exponenten von $\gamma_{i_1}, \ldots, \gamma_{i_t}$ bedeuten. Wegen $e_{i_1} \geqq e_{i_2} \geqq \ldots \geqq e_{i_t}$ ist mithin $s_1 \geqq s_2 \geqq \ldots \geqq s_t$. Der Exponent von γ kann nur dann größer als e sein, wenn der Exponent von $a_{s_1} z^{s_1} \gamma_{i_1} + \ldots + a_{s_t} z^{s_t} \gamma_{i_t}$ größer als e, d. h. der Exponent des zu $\mathfrak{c}$ gehörigen Elements $a_{s_1} z^{s_1 - s_t} \gamma_{i_1} + \ldots + a_{s_t} \gamma_{i_t}$ größer als $e + s_{i_t} = e_{i_t}$ ist. Das widerspricht der Wahl von γ_{i_t}.

Mit Hilfe von Satz 7 werden wir in **5.** ohne weiteres eine endliche Basis für den Modul $\mathfrak{m}(\mathfrak{c})$ der Multipla des Divisors $\mathfrak{c}$ gewinnen. Zur Ableitung des Riemann-Rocheschen Satzes brauchen wir jedoch noch einige weitere Tatsachen über Normalbasen, die in der folgenden Nummer entwickelt werden.

4. Satz 8. *Sind $e_1, \ldots, e_m$ die Exponenten einer Normalbasis $\gamma_1, \ldots, \gamma_m$ von $\tilde{\mathfrak{c}}$ bezüglich $k[z]$, und bedeutet $n_{\mathfrak{c}}$ die Ordnung des zu $\tilde{\mathfrak{c}}$ gehörigen Divisors, w_z die Verzweigungszahl von K bezüglich $k[z]$, so ist*

$$-2(e_1 + e_2 + \ldots + e_m) = 2n_{\mathfrak{c}} + w_z.$$

Da e_i der Exponent von γ_i ist, so ist $z^{e_i}\gamma_i$ Element von $\mathfrak{Q}$ und besitzt den Exponenten 0. Daraus folgt sofort, daß $z^{e_1}\gamma_1, \ldots, z^{e_m}\gamma_m$ eine Basis von $\mathfrak{Q}$ bezüglich $\mathfrak{P}^* = \mathfrak{Q} \cap k(z)$ bilden. Wäre dies nämlich nicht der Fall, so müßte ein Element $\frac{a_1 z^{e_1}\gamma_1 + \ldots + a_m z^{e_m}\gamma_m}{\frac{1}{z}}$ mit Koeffizienten a_i aus k zu $\mathfrak{Q}$ gehören, d. h. $a_1 z^{e_1}\gamma_1 + \ldots + a_m z^{e_m}\gamma_m$ hätte einen Exponenten, der größer als 0 ist, im Widerspruch zu Satz 7.

Bedeutet $\Delta(z^{e_1}\gamma_1, \ldots, z^{e_m}\gamma_m)$ die in bezug auf $k(z)$ genommene Diskriminante von $z^{e_1}\gamma_1, \ldots, z^{e_m}\gamma_m$, so ist also $\mathfrak{P}^* \cdot \Delta(z^{e_1}\gamma_1, \ldots, z^{e_m}\gamma_m)$ die Diskriminante von $\mathfrak{Q}$ bezüglich $\mathfrak{P}^*$. Nun ist aber

$$\Delta(z^{e_1}\gamma_1, \ldots, z^{e_m}\gamma_m) = z^{2(e_1 + \ldots + e_m)} \Delta(\gamma_1, \ldots, \gamma_m),$$

d. h. ist d der Grad von $\Delta(\gamma_1, \ldots, \gamma_m)$ in z, so ist der Exponent von $\Delta(z^{e_1}\gamma_1, \ldots, z^{e_m}\gamma_m)$ oder, was dasselbe ist, die Ordnung von $\Delta(z^{e_1}\gamma_1, \ldots, z^{e_m}\gamma_m)$ an der Stelle $\mathfrak{P}^*$ von $k(z)$ gegeben durch $d' = -2(e_1 + \ldots + e_m) - d$.

Andererseits ist $d = 2n_{\mathfrak{c}} + w_z'$, wo w_z' gleich der Ordnung des zur Differente von $\mathfrak{Z}$ bezüglich $k[z]$ gehörigen Divisors ist. Im Hinblick auf die Gleichung $w_z' + d' = w_z$ folgt somit in der Tat

$$-2(e_1 + \ldots + e_m) = d + d' = 2n_{\mathfrak{c}} + w_z' + d' = 2n_{\mathfrak{c}} + w_z.$$

Ist $\frac{1}{z}$ nicht durch das Quadrat eines Primdivisors teilbar, d. h. ist $d' = 0$ und somit der Grad von $\Delta(\gamma_1, \ldots, \gamma_m)$ gleich $2n_{\mathfrak{c}} + w_z$, so ist also nach dem vorstehenden der Grad von $\Delta(\gamma_1, \ldots, \gamma_m)$ gleich $-2(e_1 + \ldots + e_m)$

und man hat den zweiten Teil nachstehenden Satzes, dessen erster Teil sich hernach unmittelbar aus der Definition der Normalbasis ergibt.

Satz 9. *Ist* $\frac{1}{z}$ *nicht durch das Quadrat eines Primdivisors teilbar, so ist die Basis* $\gamma_1, \ldots, \gamma_m$ *von* $\mathfrak{c}$ *mit den Exponenten* $e_1, \ldots, e_m$ *dann und nur dann Normalbasis, wenn der Grad von* $D(\gamma_1, \ldots, \gamma_m)$ *in* z *gleich* $-2(e_1 + e_2 + \ldots + e_m)$ *ist.*

Um den ersten Teil dieses Satzes zu bestätigen, nehmen wir an, für die Basis $\gamma_1, \ldots, \gamma_m$ von $\mathfrak{c}$ mit den Exponenten $e_1, \ldots, e_m$ sei der Grad von $D(\gamma_1, \ldots, \gamma_m)$ gleich $-2(e_1 + \ldots + e_m)$. Ist $\gamma_1', \ldots, \gamma_m'$ mit den Exponenten $e_1', \ldots, e_m'$ eine Normalbasis von $\mathfrak{c}$ bezüglich $k[z]$, so ist nach Definition bei geeigneter Numerierung $e_i \leqq e_i'$, andererseits nach dem bereits bewiesenen Teil des Satzes der Grad von $D(\gamma_1', \ldots, \gamma_m')$ gleich $e_1' + e_2' + \ldots + e_m'$. Da nun die Gradzahlen von $D(\gamma_1', \ldots, \gamma_m')$ und $D(\gamma_1, \ldots, \gamma_m)$ gleich sind, so folgt $e_1' + e_2' + \ldots + e_m' = e_1 + e_2 + \ldots + e_m$ und daher notwendig $e_i' = e_i$, d. h. $\gamma_1, \ldots, \gamma_m$ bilden ebenfalls eine Normalbasis.

Satz 10. *Ist* $\frac{1}{z}$ *nicht durch das Quadrat eines Primdivisors teilbar, und besitzt die Normalbasis* $\gamma_1, \ldots, \gamma_m$ *von* $\mathfrak{c}$ *bezüglich* $k[z]$ *den Exponenten* $e_1, \ldots, e_m$, *so besitzt jede Normalbasis des zu* $\mathfrak{c}$ *bezüglich* $k[z]$ *komplementären Ideals* $\mathfrak{c}'$ *das Exponentensystem* $-e_1, \ldots, -e_m$.

Bezeichnet S die bezüglich $k(z)$ genommene Spur und wird $S(\gamma_i \gamma_k) = c_{ik}$ gesetzt, so ist eine Basis $\gamma_1', \ldots, \gamma_m'$ von $\mathfrak{c}$ definiert durch die Gleichungen

$$\gamma_i = \sum_{k=1}^{m} c_{ik} \gamma_k' \qquad (i = 1, \ldots, m).$$

Schreibt man kurz $D = \Delta(\gamma_1, \ldots, \gamma_m)$ für die Determinante des Koeffizientensystems c_{ik}, D_{ik} für die zum Element c_{ik} gehörige Adjunkte, so ist

$$\gamma_k' = \sum_{i=1}^{m} \frac{D_{ik} \gamma_i}{D}.$$

Hier besitzt D nach Satz 9 den Exponenten $2(e_1 + \ldots + e_m)$ und aus $S(z^e \gamma_i \gamma_k) = z^e S(\gamma_i \gamma_k) = z^e c_{ik}$ folgt, daß der Exponent von c_{ik} mindestens gleich $e_i + e_k$ ist, weil $z^{e_i + e_k} \gamma_i \gamma_k$ und damit auch $S(z^{e_i + e_k} \gamma_i \gamma_k)$ in $\mathfrak{D}$ liegt. $D_{ik} \gamma_i$ hat daher mindestens den Exponenten

$$e_k + 2(e_1 + \ldots + e_{k-1} + e_{k+1} + \ldots + e_m),$$

d. h. für den Exponenten e_k' von γ_k' gilt $e_k' \geqq -e_k$.

Aus $e_k' \geqq -e_k$ folgt, daß der Exponent von $\Delta(\gamma_1', \ldots, \gamma_m')$ sicher $\geqq -2(e_1 + \ldots + e_m)$ ist und hier gilt das $>$-Zeichen, sobald ein $e_k' > -e_k$

ist. Da andererseits $\Delta(\gamma_1', \ldots, \gamma_m') = \frac{1}{\Delta(\gamma_1, \ldots, \gamma_m)}$ und der Exponent von $\Delta(\gamma_1, \ldots, \gamma_m)$ gleich $2(e_1 + \ldots + e_m)$, also derjenige von $\Delta(\gamma_1', \ldots, \gamma_m')$ gleich $-2(e_1 + \ldots + e_m)$ ist, so muß $e_k' = -e_k$ sein. Daß $\gamma_1', \ldots, \gamma_m'$ Normalbasen von $\tilde{\mathfrak{c}}'$ bezüglich $k[z]$ sind, schließt man nun in Hinblick auf Satz 9 aus der Tatsache, daß der Grad von $\Delta(\gamma_1', \ldots, \gamma_m')$ gleich $2(e_1 + \ldots + e_m) = -2(e_1' + \ldots + e_m')$ ist.

5. Aus Satz 7 ergibt sich, daß der Modul $\mathfrak{m}(\mathfrak{c})$ aller Multipla des Divisors $\mathfrak{c}$ stets eine endliche Basis hat, und zwar zeigen wir:

Satz 11. *Besitzen die Elemente einer Normalbasis $\gamma_1, \ldots, \gamma_m$ von $\tilde{\mathfrak{c}}$ bezüglich $k[z]$ die Exponenten $e_1 \geqq e_2 \geqq \ldots \geqq e_m$ und ist e_r der letzte nicht negative unter diesen Exponenten, so hat der k-Modul aller Multipla des zu $\tilde{\mathfrak{c}}$ gehörigen Divisors $\mathfrak{c}$ eine linear unabhängige Basis von $(e_1 + 1) + (e_2 + 1) + \ldots + (e_r + 1)$ Elementen bezüglich k.*

Alle und nur die Elemente

$$\gamma = c_1\gamma_1 + c_2\gamma_2 + \ldots + c_m\gamma_m \qquad (c_i \text{ aus } k[z]),$$

deren Exponent nicht negativ ist, sind Multipla von $\mathfrak{c}$. Nach Satz 7 ist der Exponent von γ gleich dem Minimum der Exponenten der einzelnen Summanden. γ hat daher dann und nur dann nichtnegativen Exponenten, wenn $c_{r+1} = \ldots = c_m = 0$ und c_i für $i = 1, \ldots, r$ höchstens vom Grad e_i in z ist, d. h. die $(e_1 + 1) + \ldots + (e_r + 1)$ Elemente

$$\gamma_i, z\gamma_i, \ldots, z^{e_i}\gamma_i \qquad (i = 1, \ldots, r)$$

bilden eine Basis des Moduls aller Multipla von $\mathfrak{c}$ bezüglich k.

Satz 12. *Gehören die Divisoren $\mathfrak{c}_1$ und $\mathfrak{c}_2$ derselben Klasse an, so besitzen die Moduln $\mathfrak{m}(\mathfrak{c}_1)$ bzw. $\mathfrak{m}(\mathfrak{c}_2)$ der Multipla von $\mathfrak{c}_1$ bzw. $\mathfrak{c}_2$ denselben Rang.*

Ist s_1 bzw. s_2 der Rang von $\mathfrak{m}(\mathfrak{c}_1)$ bzw. $\mathfrak{m}(\mathfrak{c}_2)$ und η ein Element, dessen Divisor gleich $\frac{\mathfrak{c}_2}{\mathfrak{c}_1}$ ist, so geht aus s_1 linear unabhängigen Elementen $\eta_1, \ldots, \eta_{s_1}$ von $\mathfrak{m}(\mathfrak{c}_1)$ durch Multiplikation mit η ein System $\eta\eta_1, \ldots, \eta\eta_{s_1}$ von s_1 linear unabhängigen Elementen des Moduls $\mathfrak{m}(\mathfrak{c}_2)$ hervor, d. h. es ist $s_2 \geqq s_1$, und da ebenso $s_1 \geqq s_2$ folgt, ist $s_1 = s_2$.

Ist $\mathfrak{c}$ ein Divisor der Klasse $\mathfrak{C}$, so besitzt der Divisor eines Elementes α, das Multiplum des Divisors $\frac{\mathfrak{e}}{\mathfrak{c}}$ ist, die Gestalt $\frac{\mathfrak{c}'}{\mathfrak{c}}$, wo $\mathfrak{c}'$ ein ganzer Divisor der Klasse $\mathfrak{C}$ ist. Umgekehrt gibt es zu jedem ganzen Divisor $\mathfrak{c}'$ von $\mathfrak{C}$ stets ein Element α aus $\mathfrak{m}\left(\frac{\mathfrak{e}}{\mathfrak{c}}\right)$, dessen Divisor gerade durch $\frac{\mathfrak{c}'}{\mathfrak{c}}$ gegeben ist. Mit Hilfe der Elemente von $\mathfrak{m}\left(\frac{\mathfrak{e}}{\mathfrak{c}}\right) = (\eta_1, \ldots, \eta_r)$

lassen sich daher gerade alle ganzen Divisoren der Klasse $\mathfrak{C}$ gewinnen. Der durch die Klasse $\mathfrak{C}$ eindeutig bestimmte Rang r des Moduls $\mathfrak{m}\left(\frac{\mathfrak{e}}{\mathfrak{c}}\right)$ bezüglich k heißt die Dimension von $\mathfrak{C}$.

Ist die Elementezahl p des Körpers k endlich, so kann man auf Grund der vorstehenden Überlegungen die Zahl aller ganzen Divisoren der Klasse $\mathfrak{C}$ angeben. Der Modul $\mathfrak{m}\left(\frac{\mathfrak{e}}{\mathfrak{c}}\right)$ enthält dann nämlich $p^r - 1$ von Null verschiedene Elemente; mit α besitzen ferner die Elemente $a \cdot \alpha$ und nur sie den gleichen Divisor, falls $a \neq 0$ in k liegt. Den Elementen von $\mathfrak{m}\left(\frac{\mathfrak{e}}{\mathfrak{c}}\right)$ entsprechen daher $\frac{p^r-1}{p-1}$ verschiedene Divisoren, d. h. $\mathfrak{C}$ umfaßt $\frac{p^r-1}{p-1}$ ganze Divisoren.

Satz 13. *Ist p die Zahl der Elemente von k, r die Dimension der Divisorenklasse $\mathfrak{C}$, so enthält $\mathfrak{C}$ genau $\frac{p^r-1}{p-1}$ ganze Divisoren.*

6. Ist n_z der Nennerdivisor des Elementes z, $\mathfrak{d}_z$ der Differentendivisor von K bezüglich $k(z)$, so heißt die durch den Divisor $\frac{\mathfrak{d}_z}{n_z^2}$ bestimmte Divisorenklasse die Differentialklasse $\mathfrak{W}$ von K. Zu einer beliebigen Divisorenklasse $\mathfrak{C}$ definiert man die Klasse $\frac{\mathfrak{W}}{\mathfrak{C}}$ als Ergänzungsklasse. Versteht man noch unter $\{\mathfrak{C}\}$ die Dimension der Klasse $\mathfrak{C}$, so gilt folgender wichtige Satz, der sich nunmehr ganz ebenso wie bei *H.-L.* beweisen läßt[24]).

Satz 14 (Riemann-Rochescher Satz). *Ist $\mathfrak{C}$ eine Divisorenklasse der Ordnung q, so ist*

$$\{\mathfrak{C}\} = \left\{\frac{\mathfrak{W}}{\mathfrak{C}}\right\} + q - g + 1.$$

Aus diesem Satz ergibt sich ohne weiteres als Folgerung

$$\{\mathfrak{C}\} - \frac{q}{2} = \{\mathfrak{C}'\} - \frac{q'}{2},$$

wo $\mathfrak{C}'$ die Ergänzungsklasse von $\mathfrak{C}$ und q' die Ordnung dieser Ergänzungsklasse bedeutet.

Da die Ordnung der Differentialklasse $\mathfrak{W}$ gleich $2g - 2$ ist und eine Klasse der Ordnung $q' \leqq 0$ stets notwendig die Dimension 0 besitzt, so ist die Dimension $\{\mathfrak{C}\}$ einer Divisorenklasse $\mathfrak{C}$ mit positiver Ordnung $q \geqq 2g - 2$ nach dem Riemann-Rocheschen Satz gleich $q - g + 1 > 0$, d. h. falls $0 < q \geqq 2g - 2$ ist, gibt es sicher ganze Divisoren in der Klasse $\mathfrak{C}$.

[24]) *H.-L.*, S. 301–304.

II. Teil.

Theorie der Zetafunktion.

§ 7.

Die Divisorenklassengruppe.

Aus dem Riemann-Rocheschen Satz ergibt sich unter der Voraussetzung der Endlichkeit von k eine wichtige Folgerung für die Gruppe $\mathfrak{D}$ aller Divisoren von K. Ihrer Herleitung stellen wir den folgenden fast selbstverständlichen Satz voran.

Satz 15. *Jeder Divisor* $\mathfrak{c}$ *von* K *läßt sich darstellen in der Form* $\mathfrak{c} = \mathfrak{c}_0 \mathfrak{c}_1^s$, *wo* $\mathfrak{c}_1$ *ein fester Divisor von möglichst kleiner, positiver Ordnung* d *und* $\mathfrak{c}_0$ *ein Divisor der Ordnung* 0 *ist. Mit anderen Worten: Die Faktorgruppe von* $\mathfrak{D}$ *nach der Untergruppe* $\mathfrak{D}_0$ *aller Divisoren der Ordnung* 0 *ist eine der Additionsgruppe der ganzen Zahlen isomorphe zyklische Gruppe.*

Da die Ordnungen der Divisoren von K stets ganze Zahlen sind, gibt es einen Divisor $\mathfrak{c}_1$ von möglichst kleiner positiver Ordnung d. Die Ordnung n jedes Divisors $\mathfrak{c}$ ist dann notwendig Vielfaches von d, $n = ds$, d. h. $\frac{\mathfrak{c}}{\mathfrak{c}_1^s} = \mathfrak{c}_0$ ist ein Divisor der Ordnung 0.

Die Gruppe $\mathfrak{D}$ besteht also stets aus unendlich vielen Klassen. Dagegen gilt

Satz 16. *Ist* k *ein endlicher Körper, so umfaßt die Gruppe* $\mathfrak{D}_0$ *aller Divisoren der Ordnung* 0 *nur endlich viele Klassen, und jede Untergruppe* $\mathfrak{D}'$ *von* $\mathfrak{D}$, *die die Hauptklasse und mindestens einen Divisor mit von* 0 *verschiedener Ordnung enthält, ist von endlichem Index unter* $\mathfrak{D}$.

Im Hinblick auf Satz 15 genügt es, den ersten Teil der Behauptung zu beweisen. Wir bemerken zunächst:

Ist n eine feste natürliche Zahl, so gibt es nur endlich viele ganze Divisoren der Ordnung n und daher auch nur endlich viele Divisoren der Ordnung 0, die durch Division zweier ganzer Divisoren der Ordnung n entstehen.

Um dies einzusehen, bezeichne man mit z ein nicht zu k gehöriges Element; jeder ganze Divisor der Ordnung n ist dann Teiler eines Elements $c' = \left(\frac{1}{z}\right)^l c$, wo c Element aus $k[z]$, $0 \leqq l \leqq n$, und der Grad von c in z höchstens gleich $n - l$ ist. Solche Elemente c' gibt es aber im Falle eines endlichen Koeffizientenkörpers k nur endlich viele, und jedes ist nur durch endlich viele ganze Divisoren der Ordnung n teilbar, so daß die Zahl der ganzen Divisoren der Ordnung n in der Tat endlich ist.

Es existieren also sicher nur endlich viele Divisorenklassen, deren Divisoren die Ordnung 0 besitzen, wenn man zeigen kann: Jeder Divisor $\mathfrak{c}_0$ der Ordnung 0 ist einem Divisor äquivalent, welcher durch Division zweier Divisoren der Ordnung n entsteht, wo n geeignet, jedoch fest gewählt ist.

Zu diesem Zwecke werde $n = m\overline{n} \geqq 2g-2$ angenommen, wo $m = (K : k(z))$ und $\overline{n}$ ganz ist. Der Zählerdivisor eines beliebigen Polynoms c aus $k[z]$ vom Grad $\overline{n}$ in z ist dann ein Divisor $\mathfrak{c}_n$ der Ordnung n. Der Divisor $\mathfrak{c}_0\mathfrak{c}_n$ hat ebenfalls die Ordnung n, und da $n \geqq 2g-2$ ist, existiert nach dem Riemann-Rocheschen Satz ein Element $\alpha \neq 0$, das Multiplum von $\frac{\mathfrak{e}}{\mathfrak{c}_0\mathfrak{c}_n}$ ist, dessen Divisor also die Gestalt $\frac{\mathfrak{c}_n'}{\mathfrak{c}_0\mathfrak{c}_n}$ besitzt, wo $\mathfrak{c}_n'$ ein ganzer Divisor der Ordnung n ist. $\mathfrak{c}_0$ ist somit in der Tat dem Quotient $\frac{\mathfrak{c}_n'}{\mathfrak{c}_n}$ zweier Divisoren der Ordnung n äquivalent.

Im folgenden nehmen wir immer an, daß k ein endlicher Körper ist. Die Zahl der Divisorenklassen der Ordnung 0 soll dann mit h bezeichnet werden.

Aus Satz 15 geht hervor, daß die Ordnungen der Divisoren von K übereinstimmen mit sämtlichen Vielfachen der Zahl d, wenn d die Ordnung eines Divisors möglichst kleiner positiver Ordnung ist. Ist n ein beliebiges Vielfaches von d, $\mathfrak{c}_n$ ein Divisor der Ordnung n, so sind alle Divisoren der Ordnung n in der Restklasse $\mathfrak{D}_0\mathfrak{c}_n$ von $\mathfrak{D}$ nach $\mathfrak{D}_0$ enthalten. Bedeuten daher $\mathfrak{C}_0^{(1)}, \ldots, \mathfrak{C}_0^{(h)}$ die h Klassen der Ordnung 0, so sind $\mathfrak{C}_0^{(1)}\mathfrak{c}_n, \ldots, \mathfrak{C}_0^{(h)}\mathfrak{c}_n$ sämtlich Klassen der Ordnung n, d. h.

Satz 17. *Ist n ein Vielfaches der Ordnung d eines Divisors von möglichst kleiner positiver Ordnung, so gibt es genau h Divisorenklassen der Ordnung n.*

Unter einer Divisorengruppe $\mathfrak{D}'$ wollen wir eine Untergruppe von $\mathfrak{D}$ verstehen, die die Hauptklasse enthält. Aus Satz 16 fließt dann

Satz 18. *Jede Divisorengruppe $\mathfrak{D}'$ mit alleiniger Ausnahme der endlich vielen in $\mathfrak{D}_0$ enthaltenen Divisorengruppen ist von endlichem Index unter der Gruppe $\mathfrak{D}$ aller Divisoren von K.*

Bemerkung. Die Ordnung d eines Divisors möglichst niedriger positiver Ordnung wird sich im folgenden Paragraphen gleich 1 herausstellen.

§ 8.

Die Zetafunktion.

1. Von nun an setzen wir stets voraus, daß der Körper k aller absolut algebraischen Elemente von K nur endlich viele, und zwar genau p Elemente enthält. Ist $\mathfrak{c}$ ein ganzer Divisor, f die Ordnung von $\mathfrak{c}$, so setzen wir $|\mathfrak{c}| = p^f$.

In Analogie mit der Theorie der algebraischen Zahlen führen wir die Z-Funktion des Körpers K ein und verstehen darunter die Funktion $Z(s)$ der komplexen Veränderlichen s, die folgendermaßen definiert ist:

$$(1) \qquad Z(s) = \prod_{\mathfrak{p}} \frac{1}{1 - |\mathfrak{p}|^{-s}}.$$

Dabei ist das Produkt rechter Hand über alle Primdivisoren $\mathfrak{p}$ von K zu erstrecken.

Die Funktion $Z(s)$ hängt gemäß ihrer Definition von der Natur des Körpers K allein ab und unterscheidet sich dadurch von der Z-Funktion, die Herr E. Artin in seinem Spezialfall betrachtet. Der Zusammenhang zwischen der durch (1) definierten Funktion $Z(s)$ und der von Herrn Artin untersuchten Z-Funktion wird in § 10 hergestellt.

Aus der Definitionsgleichung (1) ergibt sich in bekannter Weise, daß die Funktion $Z(s)$ in der Halbebene $\Re(s) > 1$ regulär ist und in demselben Gebiet durch die Reihe

$$(2) \qquad Z(s) = \sum_{\mathfrak{c}} \frac{1}{|\mathfrak{c}|^s}$$

dargestellt wird, wo die Summe rechter Hand über alle ganzen Divisoren $\mathfrak{c}$ aus K auszudehnen ist.

2. Nächstes Ziel ist, das Verhalten von $Z(s)$ auf und jenseits der Geraden $\Re(s) = 1$ festzustellen. Hierzu braucht man wieder den Riemann-Rocheschen Satz, mit dessen Hilfe man zu folgendem Satz gelangt:

Satz 19. *Die Funktion $Z(s)$ ist periodisch mit der Periode $\frac{2\pi i}{\log p}$ und in der ganzen s-Ebene regulär mit Ausnahme der Stellen $0 + \frac{2l\pi i}{\log p}$ bzw. $1 + \frac{2l\pi i}{\log p}$, an denen sie jeweils einen Pol erster Ordnung mit dem Residuum $-\frac{h}{(p-1)\log p}$ bzw. $\frac{hp^{1-g}}{(p-1)\log p}$ besitzt.*

Der Beweis dieses Satzes wird in zwei Schritten geführt.

a) Indem man sich auf die Summendarstellung (2) von $Z(s)$ stützt, erhält man auf Grund des Riemann-Rocheschen Satzes nachstehende, nur in den Logarithmen abweichende Vorstufe zu Satz 19:

Ist d die Ordnung eines Divisors von möglichst kleiner positiver Ordnung und wird $p' = p^d$ gesetzt, so ist $Z(s)$ periodisch mit der Periode $\frac{2\pi i}{\log p'}$ und in der ganzen s-Ebene regulär mit Ausnahme der Stellen $0 + \frac{2l\pi i}{\log p'}$ bzw. $1 + \frac{2l\pi i}{\log p'}$, an denen sie jeweils einen Pol erster Ordnung mit dem Residuum $-\frac{h}{(p-1)\log p'}$ bzw. $\frac{hp^{1-g}}{(p-1)\log p'}$ besitzt.

Sind $\mathfrak{C}_q^{(1)}, \ldots, \mathfrak{C}_q^{(h)}$ die h Klassen der Ordnung dq, wo q eine beliebige ganze Zahl ist (vgl. § 7, Satz 17), und bedeutet $\{\mathfrak{C}_q^{(i)}\}$ die Dimension der Klasse $\mathfrak{C}_q^{(i)}$, so ist die Zahl der ganzen Divisoren der Klasse $\mathfrak{C}_q^{(i)}$ nach Satz 13 gleich

$$\frac{p^{\{\mathfrak{C}_q^{(i)}\}}-1}{p-1},$$

und daher nach (2)

$$Z(s)=\frac{1}{p-1}\sum_{q=1}^{\infty}\sum_{i=1}^{h}\frac{p^{\{\mathfrak{C}_q^{(i)}\}}-1}{p^{dqs}}=\frac{1}{p-1}\sum_{q=1}^{\infty}\sum_{i=1}^{h}\frac{p^{\{\mathfrak{C}_q^{(i)}\}}}{p'^{qs}}-\frac{h}{p-1}\sum_{q=1}^{\infty}\frac{1}{p'^{qs}}$$

$$=\frac{1}{p-1}\sum_{q=1}^{\infty}\sum_{i=1}^{h}\frac{p^{\{\mathfrak{C}_q^{(i)}\}}}{p'^{qs}}+\frac{h}{p-1}\frac{1}{1-p'^{s}}.$$

Bedeute q_0 die kleinste ganze Zahl der Art, daß $q_0 d \geqq 2g-2$, so ist für $q \geqq q_0$ nach dem Riemann-Rocheschen Satz

$$\{\mathfrak{C}_q^{(i)}\}=dq-g+1,$$

und man hat somit

$$Z(s)=\frac{1}{p-1}\sum_{q=1}^{q_0-1}\sum_{i=1}^{h}\frac{p^{\{\mathfrak{C}_q^{(i)}\}}}{p'^{qs}}+\frac{hp^{1-g}}{p-1}\sum_{q=q_0}^{\infty}\frac{p'^{q}}{p'^{qs}}+\frac{h}{p-1}\cdot\frac{1}{1-p'^{s}},$$

d. h.

$$(3)\qquad Z(s)=\frac{1}{p-1}\sum_{q=1}^{q_0-1}\sum_{i=1}^{h}\frac{p^{\{\mathfrak{C}_q^{(i)}\}}}{p'^{qs}}+\frac{hp^{1-g}}{p-1}\cdot\frac{p'^{q_0(1-s)}}{1-p'^{1-s}}+\frac{h}{p-1}\cdot\frac{1}{1-p'^{s}}.$$

Aus (3) ergeben sich ohne weiteres alle angegebenen Behauptungen über $Z(s)$.

b) Mit a) ist Satz 19 vollständig bewiesen, wenn $d=1$ nachgewiesen ist; denn dann ist $p'=p^d=p$. Nun ist d offenbar gleich dem größten gemeinschaftlichen Teiler der Ordnungen aller Primdivisoren von K. Hieran knüpfen wir an und beweisen unter Benutzung der Produktdarstellung (1) von $Z(s)$:

Der größte gemeinschaftliche Teiler d der Ordnungen aller Primdivisoren von K ist 1.

Ist η ein Element vom Grade d bezüglich k, $\overline{K}=K(\eta)$, so entsprechen jeder Primstelle $\mathfrak{p}$ von K genau d bezüglich K konjugierte Primstellen $\bar{\mathfrak{p}}_i$ von $\overline{K}$, weil die Ordnung f von $\mathfrak{p}$ durch d teilbar ist, und es hat jeder der d Primdivisoren $\bar{\mathfrak{p}}_i$ von $\overline{K}$ die Ordnung $\frac{f}{d}$ [25]), so daß aus $|\mathfrak{p}|=p^f$ und $|\bar{\mathfrak{p}}_i|=p^{d\frac{f}{d}}$ gerade $|\mathfrak{p}|=|\bar{\mathfrak{p}}_i|$ folgt.

[25]) Vgl. § 2, 4.

Für die Z-Funktion des Körpers $\overline{K}$ ergibt sich daher

$$Z_{\overline{K}}(s) = \prod_{\bar{\mathfrak{p}}} \frac{1}{1 - |\bar{\mathfrak{p}}|^{-s}} = \left(\prod_{\mathfrak{p}} \frac{1}{1 - |\mathfrak{p}|^{-s}} \right)^d = (Z_K(s))^d. \tag{4}$$

Dabei ist das erste Produkt über alle Primdivisoren $\bar{\mathfrak{p}}$ von $\overline{K}$, das zweite über alle Primdivisoren $\mathfrak{p}$ von K erstreckt. Da $Z_{\overline{K}}(s)$ und $Z_K(s)$ nach a) beide für $s = 0$ einen Pol erster Ordnung haben, muß notwendig $d = 1$ sein.

Aus der Tatsache, daß die Ordnung d eines Divisors von möglichst kleiner positiver Ordnung gleich 1 ist, folgt in Verbindung mit § 7; **3** und § 6; **5**, **6** der

Satz 20. *Ist $q \geqq 2g - 2$ eine beliebige, positive ganze Zahl, so existieren stets genau $h \frac{p^{q-g+1} - 1}{p - 1}$ ganze Divisoren der Ordnung q.*

3. Ähnlich wie man in der Zahlentheorie die Zetafunktion der einzelnen Idealklassen betrachtet, ist es auch hier für manche Anwendungen zweckmäßig, eine Verallgemeinerung der Funktion $Z(s)$ einzuführen.

Ist $\mathfrak{D}'$ eine Divisorengruppe (vgl. § 7; **3**) von endlichem Index j unter $\mathfrak{D}$ und sind $\mathfrak{D}_1' = \mathfrak{D}', \mathfrak{D}_2', \ldots, \mathfrak{D}_j'$ die Restklassen von $\mathfrak{D}$ nach $\mathfrak{D}'$, so definieren wir die Funktion

$$Z(s; \mathfrak{D}_i') = \sum_{\mathfrak{c} \text{ aus } D_i'} \frac{1}{\|\mathfrak{c}\|^s},$$

wo die Summe über alle ganzen Divisoren $\mathfrak{c}$ der Restklasse $\mathfrak{D}_i'$ erstreckt ist. Aus dem in 2a) zur Summation von $Z(s)$ eingeschlagenen Verfahren ergibt sich, wenn $\mathfrak{D}'$ einen Divisor der Ordnung 1 enthält, mühelos:

Satz 21. *$Z(s; \mathfrak{D}_i')$ ist periodisch mit der Periode $\frac{2\pi i}{\log p}$ und in der ganzen Ebene regulär mit Ausnahme der Stellen $0 + \frac{2l\pi i}{\log p}$ bzw. $1 + \frac{2l\pi i}{\log p}$, an denen sie jeweils einen Pol erster Ordnung mit dem Residuum $-\frac{h}{j(p-1)\log p}$ bzw. $\frac{h p^{1-g}}{j(p-1)\log p}$ besitzt.*

§ 9.

Die Funktionalgleichung der Zetafunktion.

Satz 22. *Die Funktion $Z(s)$ genügt der Funktionalgleichung*

$$Z(1-s) = p^{(g-1)(2s-1)} Z(s),$$

die sich mit Hilfe der Funktion $\Xi(s) = p^{s(g-1)} Z(\frac{1}{2} + s)$ auch auf die Form $\Xi(-s) = \Xi(s)$ bringen läßt.

Die beiden angegebenen Formen der Funktionalgleichung gehen ineinander über, wenn man in der ersten s durch $\frac{1}{2} + s$ ersetzt. Es genügt daher, die Funktionalgleichung in der zweiten Gestalt zu beweisen.

Zu diesem Zwecke gehen wir von der Gleichung (3) aus. Da $d=1$ ist, ist $p'=p$, und die kleinste ganze Zahl q_0, für die $q_0 d \geqq 2g-2$ ist, ist $q_0=1$ bzw. $q_0=2g-2$ im Falle $2g-2>1$. Man hat also

$$Z(s)=\frac{1}{p-1}\sum_{q=1}^{q_0-1}\sum_{i=1}^{h}\frac{p^{\{\mathfrak{C}_q^{(i)}\}}}{p^{qs}}+\frac{h\,p^{-(g-1)}}{p-1}\,\frac{p^{(2g-2)(1-s)}}{1-p^{1-s}}+\frac{h}{p-1}\,\frac{1}{1-p^{s}},$$

wo die erste Summe rechts im Falle $2g-2\leqq 1$ fortfällt, und daher

$$Z\left(\frac{1}{2}+s\right)=\frac{1}{p-1}\sum_{q=1}^{q_0-1}\sum_{i=1}^{h}\frac{p^{\{\mathfrak{C}_q^{(i)}\}}}{p^{\frac{q}{2}+qs}}+\frac{h}{p-1}\left(\frac{p^{-2s(g-1)}}{1-p^{\frac{1}{2}-s}}+\frac{1}{1-p^{\frac{1}{2}+s}}\right),$$

d. h.

$$\begin{aligned}\Xi(s)&=p^{s(g-1)}\frac{1}{p-1}\sum_{q=1}^{q_0-1}\sum_{i=1}^{h}\frac{p^{\{\mathfrak{C}_q^{(i)}\}}}{p^{\frac{q}{2}+qs}}+\frac{h}{p-1}\left(\frac{p^{-s(g-1)}}{1-p^{\frac{1}{2}-s}}+\frac{p^{s(g-1)}}{1-p^{\frac{1}{2}+s}}\right)\\&=S_1(s)+S_2(s).\end{aligned}$$

Hier genügt $S_2(s)=\frac{h}{h-1}\left(\frac{p^{-s(g-1)}}{1-p^{\frac{1}{2}-s}}+\frac{p^{s(g-1)}}{1-p^{\frac{1}{2}+s}}\right)$ offenbar der Funktionalgleichung

$$S_2(-s)=S_2(s),$$

und wir haben nur noch zu zeigen, daß auch

$$S_1(-s)=S_1(s)$$

ist.

Nun ist

$$(p-1)\,S_1(s)=p^{s(g-1)}\sum_{q=1}^{2g-3}\sum_{i=1}^{h}\frac{p^{\{\mathfrak{C}_q^{(i)}\}}}{p^{\frac{q}{2}+qs}}=\sum_{q=1}^{2g-3}\sum_{i=1}^{h}\frac{p^{\{\mathfrak{C}_q^{(i)}\}-\frac{q}{2}}}{p^{s(q-g+1)}}.$$

Bezeichnet man mit $\mathfrak{C}_q'$ die Ergänzungsklasse von $\mathfrak{C}_q$, so daß also $\mathfrak{C}_q'$ die Ordnung $q'=2g-2-q$ hat, so durchläuft $\mathfrak{C}_q'$ zugleich mit $\mathfrak{C}_q$ alle Klassen, deren Ordnung kleiner als $2g-2$ ist, d. h. es ist

$$(p-1)\,S_1(s)=\sum_{q=1}^{2g-3}\sum_{i=1}^{h}\frac{p^{\{\mathfrak{C}_q'^{(i)}\}-\frac{q'}{2}}}{p^{s(q'-g+1)}}=\sum_{q=1}^{2g-3}\sum_{i=1}^{h}\frac{p^{\{\mathfrak{C}_q'^{(i)}\}-\frac{q'}{2}}}{p^{-s(q-g+1)}}.$$

Daraus folgt

$$(p-1)\,S_1(s)=\frac{1}{2}\sum_{q=1}^{2g-3}\sum_{i=1}^{h}\left(\frac{p^{\{\mathfrak{C}_q^{(i)}\}-\frac{q}{2}}}{p^{s(q-g+1)}}+\frac{p^{\{\mathfrak{C}_q'^{(i)}\}-\frac{q'}{2}}}{p^{-s(q-g+1)}}\right),$$

und da nach dem Riemann-Rocheschen Satz

$$\{\mathfrak{C}_q\}-\frac{q}{2}=\{\mathfrak{C}_q'\}-\frac{q'}{2}$$

ist, gilt in der Tat

$$S_1(-s)=S_1(s).$$

§ 10.

Anwendungen.

1. Es soll zum Schluß noch der Zusamenhang zwischen den vorstehenden Ergebnissen und den von Herrn E. Artin in seinem Spezialfall hergeleiteten Resultaten hergestellt werden.

Sei z ein nicht zu k gehöriges Element, $\mathfrak{Z}$ der Ring aller in z ganzen Elemente, $\tilde{\mathfrak{p}}$ ein Primideal von $\mathfrak{Z}$. Herr Artin untersucht dann die Funktion

$$Z_{\mathfrak{Z}}(s) = \prod_{\tilde{\mathfrak{p}}} \frac{1}{1-|\tilde{\mathfrak{p}}|^{-s}},$$

wo das Produkt über alle Primideale $\tilde{\mathfrak{p}}$ von $\mathfrak{Z}$ erstreckt wird und $|\tilde{\mathfrak{p}}|$ gleich der Zahl der Restklassen von $\mathfrak{Z}$ modulo $\tilde{\mathfrak{p}}$ ist. Ist $\mathfrak{p}$ der zu dem Primideal $\tilde{\mathfrak{p}}$ gehörige Primdivisor, so ist offenbar $|\mathfrak{p}| = |\tilde{\mathfrak{p}}|$. Zwischen der Funktion $Z_{\mathfrak{Z}}(s)$ und der von uns betrachteten Funktion $Z(s)$ besteht daher die Gleichung

$$Z(s) = \prod_{\mathfrak{u}} \frac{1}{1-|\mathfrak{u}|^{-s}} Z_{\mathfrak{Z}}(s), \tag{4}$$

wo das Produkt über die endlich vielen verschiedenen in $\frac{1}{z}$ aufgehenden Primdivisoren $\mathfrak{u}$ zu nehmen ist. Das Produkt

$$\prod_{\mathfrak{u}} \frac{1}{1-|\mathfrak{u}|^{-s}}$$

ist periodisch mit der Periode $\frac{2\pi i}{\log p}$ und in der ganzen Ebene regulär mit Ausnahme der Stellen $s = 0 + \frac{2l\pi i}{\log p}$, an denen es einen Pol hat, dessen Ordnung gleich der Zahl der verschiedenen in $\frac{1}{z}$ aufgehenden Primdivisoren $\mathfrak{u}$ ist.

Daraus folgt sofort:

Satz 23. *Die Funktion $Z_{\mathfrak{Z}}(s)$ ist periodisch mit der Periode $\frac{2\pi i}{\log p}$ und in der ganzen Ebene regulär mit Ausnahme der Stellen $s = 1 + \frac{2l\pi i}{\log p}$, an denen sie einen Pol erster Ordnung besitzt. $Z_{\mathfrak{Z}}(0)$ ist dann und nur dann von 0 verschieden, wenn der Nennerdivisor von z gleich der Potenz eines Primdivisors $\mathfrak{u}$ ist, und zwar ist in diesem Falle $Z_{\mathfrak{Z}}(0) = -\frac{u_z \cdot h}{p-1}$, wo u_z die Ordnung von $\mathfrak{u}$ bedeutet.*

Auch das Residuum der Funktion $Z_{\mathfrak{Z}}(s)$ an den Polstellen läßt sich mit Hilfe von (4) leicht auf das bekannte Residuum von $Z(s)$ an der Stelle 1 zurückführen. Es treten dann in der Residuenformel für $Z_{\mathfrak{Z}}(s)$ das Geschlecht g und die Zahl h der Divisorenklassen 0-ter Ordnung auf,

während sich das Residuum im Spezialfall des Herrn Artin wesentlich mit Hilfe der Diskriminante von $\mathfrak{J}$ bezüglich $k[z]$, dem Regulator und der Idealklassenzahl von $\mathfrak{J}$ ausdrücken ließ.

Nun ist $g = \frac{w_z}{2} - m_z + 1$, falls K über $k(z)$ von erster Art, m_z der Grad von K bezüglich $k(z)$ und w_z die Verzweigungszahl von K bezüglich $k(z)$ ist. Dabei ist die Beziehung von w_z zur Diskriminante bekannt (vgl. § 4, 5). Um auch die Zahl h der Divisorenklassen 0-ter Ordnung mit der Zahl der Idealklassen von $\mathfrak{J}$ in Verbindung zu setzen, haben wir kurz das Verhältnis von Divisorenklassen und Idealklassen zu untersuchen.

2. Die Gesamtheit aller ganzen und gebrochenen Ideale von $\mathfrak{J}$ bildet bei der Multiplikation eine Gruppe, die Gruppe $\mathfrak{A}$ aller Ideale von $\mathfrak{J}$. Die Restklassen von $\mathfrak{A}$ nach der Untergruppe $\mathfrak{B}$ aller Hauptideale heißen die Idealklassen von $\mathfrak{J}$.

Bezeichne $\mathfrak{U}$ die Gruppe aller Divisoren, in denen nur die in $\frac{1}{z}$ aufgehenden Primdivisoren $\mathfrak{u}$ wirklich auftreten. Ist $\mathfrak{c}$ der zum Ideal $\tilde{\mathfrak{c}}$ aus $\mathfrak{J}$ gehörige Divisor und wird dem Ideal $\tilde{\mathfrak{c}}$ die Menge der Divisoren $\mathfrak{U}\mathfrak{c}$ zugeordnet, so erhält man einen Homomorphismus zwischen $\mathfrak{A}$ und der Gruppe $\mathfrak{D}/\mathfrak{U}$. Bei diesem Homomorphismus entspricht der Untergruppe $\mathfrak{B}$ von $\mathfrak{A}$ die Untergruppe $\mathfrak{H}\mathfrak{U}$ von $\mathfrak{D}$, und es sind die Faktorgruppen $\mathfrak{A}/\mathfrak{B}$ bzw. $\mathfrak{D}/\mathfrak{H}\mathfrak{U}$ isomorph, $\mathfrak{A}/\mathfrak{B} \simeq \mathfrak{D}/\mathfrak{H}\mathfrak{U}$. Da $\mathfrak{H}\mathfrak{U}$ die Hauptklasse und mindestens einen Divisor mit von 0 verschiedener Ordnung umfaßt, ist $(\mathfrak{D}:\mathfrak{H}\mathfrak{U}) = (\mathfrak{A}:\mathfrak{B})$ endlich.

Satz 24. *Die Ideale von $\mathfrak{J}$ verteilen sich auf endlich viele Idealklassen. Die Zahl der Idealklassen von $\mathfrak{J}$ wird mit h_z bezeichnet.*

Um h_z durch h auszudrücken, dienen uns folgende einfache Gleichungen:

$$h_z = (\mathfrak{D}:\mathfrak{H}\mathfrak{U}) = (\mathfrak{D}:\mathfrak{D}_0\mathfrak{U})(\mathfrak{D}_0\mathfrak{U}:\mathfrak{H}\mathfrak{U}),$$
$$(\mathfrak{D}_0\mathfrak{U}:\mathfrak{H}\mathfrak{U}) = (\mathfrak{D}_0:\mathfrak{D}_0 \cap \mathfrak{H}\mathfrak{U}) = \frac{(\mathfrak{D}_0:\mathfrak{H})}{(\mathfrak{D}_0 \cap \mathfrak{H}\mathfrak{U}:\mathfrak{H})}.$$

Bedeutet $\mathfrak{U}_0$ die Untergruppe aller Divisoren der Ordnung 0 aus $\mathfrak{U}$, so ist $\mathfrak{D}_0 \cap \mathfrak{H}\mathfrak{U} = \mathfrak{H}\mathfrak{U}_0$ und $(\mathfrak{D}_0 \cap \mathfrak{H}\mathfrak{U}:\mathfrak{H}) = (\mathfrak{H}\mathfrak{U}_0:\mathfrak{H}) = (\mathfrak{U}_0:\mathfrak{H} \cap \mathfrak{U}_0)$. Man hat also schließlich

$$h_z = (\mathfrak{D}:\mathfrak{D}_0\mathfrak{U})\frac{(\mathfrak{D}_0:\mathfrak{H})}{(\mathfrak{U}_0:\mathfrak{H} \cap \mathfrak{U}_0)} = h\frac{(\mathfrak{D}:\mathfrak{D}_0\mathfrak{U})}{(\mathfrak{U}_0:\mathfrak{H} \cap \mathfrak{U}_0)}.$$

Hier ist $(\mathfrak{D}:\mathfrak{D}_0\mathfrak{U})$ nach Satz 15 gleich der Ordnung des Divisors kleinster positiver Ordnung aus $\mathfrak{D}_0\mathfrak{U}$ und damit aus $\mathfrak{U}$, also $(\mathfrak{D}:\mathfrak{D}_0\mathfrak{U})$ gleich dem größten gemeinschaftlichen Teiler u_z der Ordnungen der in $\frac{1}{z}$ aufgehenden Primdivisoren $\mathfrak{u}$. Andererseits ist ein Element ε, dessen Divisor nur Primdivisoren $\mathfrak{u}$ wirklich enthält, stets Einheit von $\mathfrak{J}$, da mit ε auch $\frac{1}{\varepsilon}$ in $\mathfrak{J}$

enthalten ist[26]). $\mathfrak{H} \cap \mathfrak{U}_0$ besteht daher aus den Divisoren der Einheiten von $\mathfrak{Z}$, und der Index $(\mathfrak{U}_0 : \mathfrak{H} \cap \mathfrak{U}_0)$ soll infolgedessen der Regulator r_z von $\mathfrak{Z}$ heißen.

Zusammenfassend ergibt sich also

Satz 25. *Es ist* $h = \frac{h_z r_z}{u_z}$, *wo* u_z *der größte gemeinschaftliche Teiler der Ordnungen der in* $\frac{1}{z}$ *aufgehenden Primstellen und* r_z *der Regulator von* $\mathfrak{Z}$ *ist.*

3. Nunmehr läßt sich das Residuum der Funktion $Z_{\mathfrak{Z}}(s)$ an der Stelle $s = 1$ in der Tat mit Hilfe von Diskriminante, Idealklassenzahl und Regulator ausdrücken. Wie aus (4) hervorgeht, hängt das Residuum von der Zahl und der Ordnung der in $\frac{1}{z}$ aufgehenden Primdivisoren ab. Wir nehmen daher an, daß $\mathfrak{u}_1^{e_1} \mathfrak{u}_2^{e_2} \dots \mathfrak{u}_s^{e_s}$ der Nennerdivisor von z und f_i die Ordnung von $\mathfrak{u}_i$ sei, so daß $e_1 f_1 + \dots + e_s f_s = m_z = (K : k(z))$ ist. Es sei ferner K über $k(z)$ von erster Art. Dann ist

$$\frac{h p^{1-g}}{(p-1)\log p} = \left(\frac{1}{1-p^{-f_1}}\right)^{e_1} \dots \left(\frac{1}{1-p^{-f_s}}\right)^{e_s} \lim_{s \to 1} (s-1) Z_{\mathfrak{Z}}(s),$$

also

$$\lim_{s \to 1} (s-1) Z_{\mathfrak{Z}}(s) = \frac{h_z r_z}{p^{\frac{w_z}{2}} u_z} \frac{(p^{f_1}-1)^{e_1} \dots (p^{f_s}-1)^{e_s}}{(p-1)\log p}.$$

Spezialisiert man auf $m_z = 2$ und bedenkt, daß dann für den Zählerdivisor von $\frac{1}{z}$ genau drei Möglichkeiten bestehen, so erhält man die von Herrn Artin durch Rechnung einzeln abgeleiteten Formeln.

---

[26]) Vgl. § 4, 3.

(Eingegangen am 30. April 1929.)